

حقوق ما

ما از عدالت سهمی داریم

سال یازدهم، شماره ۲۶ / ۲۵۹ فروردین ۱۵ / ۱۴۰۵ آوریل ۲۰۲۶

هوش مصنوعی و حقوق بشر



در این شماره می‌خوانید:

هوش مصنوعی و حقوق بشر؛ فرصت‌ها و چالش‌ها

محسن عمادی: هر حقیقتی در برابر تن انسانی است که محک می‌خورد

پویش عزیزالدین: «نظارت مبتنی بر هوش مصنوعی» فناوری واحدی نیست

روزنامه‌نگاری و هوش مصنوعی

معین خزائلی: هوش مصنوعی قلمروی خارج از حقوق نیست

ما از عدالت سهمی داریم

دو هفته نامه الکترونیکی تخصصی حقوق بشر

صاحب امتیاز و مدیر مسئول: سازمان حقوق بشر ایران / محمود امیری مقدم

سر دبیر این شماره: مریم غفوری

تحریریه: مقاله حقوقی: محمد مقیمی؛ مصاحبه‌ها: پویان مکاری

صفحه‌بندی: ماهور خوش‌قدم

تماس با مجله: mail@iranhr.net

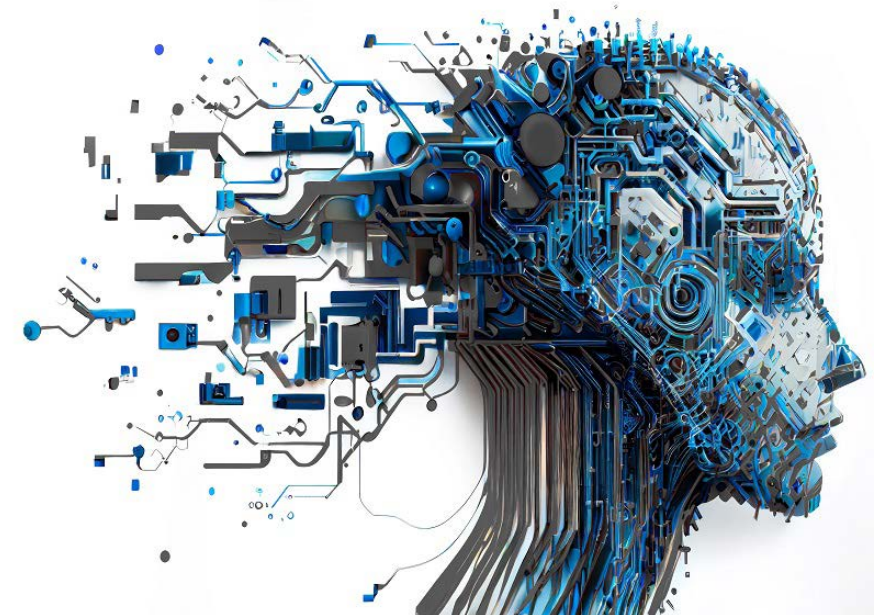
حقوق ما در ویرایش مطالب آزاد است!

یادداشت‌هایی که از روزنامه‌نگاران و اشخاص دریافت می‌شود نظر شخصی آنان است و دیدگاه مجله حقوق ما نیست.



محمد مقیمی

هوش مصنوعی و حقوق بشر؛ فرصت‌ها و چالش‌ها



هوش مصنوعی در مدتی کوتاه از موضوعی تخصصی در علوم رایانه به بخشی از زندگی روزمره انسان تبدیل شده است. موتورهای جست‌وجو، سامانه‌های ترجمه، تشخیص پزشکی، خدمات بانکی، شبکه‌های اجتماعی، آموزش، استخدام و حتی برخی تصمیم‌های اداری و قضایی، به درجات مختلف از الگوریتم‌ها و سامانه‌های هوشمند تأثیر می‌پذیرند. از این رو، هوش مصنوعی را دیگر نمی‌توان صرفاً یک فناوری فنی یا تجاری دانست؛ زیرا طراحی و کاربرد آن می‌تواند بر آزادی، برابری، حریم خصوصی، اشتغال، سلامت، آموزش و دسترسی شهروندان به خدمات عمومی اثر مستقیم بگذارد.

هوش مصنوعی به مجموعه‌ای از فناوری‌های محاسباتی گفته می‌شود که با پردازش حجم گسترده‌ای از داده‌ها، قابلیت‌هایی مانند تشخیص الگو، تحلیل، پیش‌بینی، تولید محتوا و کمک به تصمیم‌گیری را شبیه‌سازی یا تقویت می‌کنند. البته ابزارهای هوش مصنوعی به‌خودی‌خود منبع معتبر علمی محسوب نمی‌شوند. این سامانه‌ها ممکن است اطلاعات نادرست، ناقص یا فاقد منبع تولید کنند؛ بنابراین، اعتبار پاسخ‌های آنها باید با مراجعه به منابع مستقل و معتبر سنجیده شود. با این حال، استفاده مسئولانه از هوش مصنوعی می‌تواند سرعت تحلیل اطلاعات را افزایش دهد و به گسترش دانش و پیشرفت علمی کمک کند.

حقوق بشر حوزه‌ای میان‌رشته‌ای است که با حقوق، سیاست، اقتصاد، اخلاق، فناوری و علوم اجتماعی ارتباط دارد. تقریباً هر تحول اجتماعی را می‌توان از منظر تأثیر آن بر کرامت و حقوق انسان بررسی کرد؛ اما اهمیت هوش مصنوعی به دلیل عمق و گستره تأثیر آن بر جوامع انسانی دوچندان است. این فناوری می‌تواند هم وسیله‌ای برای ارتقای حقوق بشر باشد و هم، در صورت فقدان نظارت و پاسخ‌گویی، به ابزاری برای نقض گسترده و نظام‌مند حقوق انسان تبدیل شود.

فرصت‌هایی برای ارتقای حقوق بشر

یکی از مهم‌ترین ظرفیت‌های هوش مصنوعی، تسهیل دسترسی به دانش و اطلاعات است. ابزارهای ترجمه، خلاصه‌سازی و آموزش هوشمند می‌توانند موانع زبانی، جغرافیایی و اقتصادی را کاهش دهند و امکان استفاده افراد بیشتری را از منابع علمی و آموزشی فراهم کنند. این ظرفیت می‌تواند به تحقق بهتر حق آموزش و گردش آزاد اطلاعات کمک کند؛ مشروط بر آنکه دسترسی به این فناوری‌ها به گروه‌های برخوردار محدود نماند.

در حوزه سلامت نیز سامانه‌های هوشمند می‌توانند با تحلیل تصاویر و داده‌های پزشکی، به تشخیص سریع‌تر بیماری‌ها، مدیریت اطلاعات بیماران و ارائه خدمات از راه دور کمک کنند. البته تصمیم نهایی درباره درمان نباید بدون نظارت متخصصان انسانی به ماشین واگذار شود. خطای یک ابزار در این حوزه صرفاً اشتباهی فنی نیست، بلکه ممکن است سلامت یا جان انسان را به خطر اندازد.

هوش مصنوعی همچنین می‌تواند کیفیت خدمات عمومی را بهبود بخشد. دولت‌ها

قادرند از آن برای ساده‌سازی خدمات اداری، تحلیل نیازهای اجتماعی، برنامه‌ریزی شهری، توزیع بهتر منابع و تصمیم‌سازی استفاده کنند. ابزارهای تبدیل گفتار به متن، توصیف تصاویر، ترجمه خودکار و دستیارهای هوشمند نیز می‌توانند استقلال و دسترسی افراد دارای معلولیت را افزایش دهند.

در حوزه حقوق بشر، تحلیل تصاویر ماهواره‌ای، ویدئوها، اسناد و داده‌های گسترده می‌تواند به شناسایی الگوهای خشونت، مستندسازی نقض‌ها و هشدار زودهنگام درباره بحران‌های انسانی کمک کند. با این حال، همان ابزارها ممکن است در اختیار حکومت‌های اقتدارگرا برای شناسایی معترضان، کنترل شهروندان و سرکوب آزادی‌های مدنی قرار گیرند.

مخاطرات و چالش‌ها

نقض حریم خصوصی یکی از جدی‌ترین مخاطرات این فناوری است. سامانه‌های هوشمند می‌توانند حجم عظیمی از داده‌های شخصی، رفتارهای اینترنتی، اطلاعات مکانی، تصاویر و صداهای افراد را گردآوری و تحلیل کنند. ترکیب این داده‌ها امکان ترسیم تصویری دقیق از زندگی، روابط، علایق و گرایش‌های اشخاص را فراهم می‌کند؛ موضوعی که در صورت نبود محدودیت قانونی، می‌تواند به نظارت گسترده دولتی یا تجاری منجر شود.

دیپ‌فیک (محتوای صوتی یا تصویری ساختگی که با هوش مصنوعی چهره یا صدای افراد را به‌گونه‌ای واقع‌نما بازسازی می‌کند) نمونه دیگری از این مخاطرات است. چنین محتوایی می‌تواند برای جعل هویت، کلاهبرداری، تخریب اعتبار، آزار افراد یا دست‌کاری افکار عمومی استفاده شود. مرز میان واقعیت و جعل

با گسترش این فناوری دشوارتر تشخیص داده می‌شود و اعتماد عمومی به رسانه‌ها و اسناد تصویری آسیب می‌بیند.

تبعیض الگوریتمی نیز چالشی بنیادین است. سامانه‌هایی که با داده‌های تاریخی، ناقص یا نامتوازن آموزش می‌بینند، ممکن است تبعیض‌های موجود در جامعه را بازتولید یا تشدید کنند. برای مثال، اگر یک سامانه استخدامی با داده‌های سازمانی آموزش دیده باشد که در گذشته مردان بیشتری را به سمت‌های مدیریتی برگزیده است، ممکن است رزومه زنان را نامناسب‌تر ارزیابی کند. در تشخیص چهره، اعطای وام، بیمه، سلامت، پلیس و خدمات عمومی نیز یک معیار ظاهراً خنثی ممکن است در عمل علیه گروه‌های خاص یا افراد کم‌برخوردار عمل کند. بی‌طرف بودن ماشین الزاماً به معنای عادلانه بودن نتیجه نیست؛ زیرا داده‌ها، معیارها و اهداف سامانه را انسان‌ها و نهادهای انسانی تعیین می‌کنند.

هوش مصنوعی می‌تواند برخی مشاغل را حذف یا دگرگون کند و شکاف میان نیروی کار برخوردار از مهارت‌های دیجیتال و سایر افراد را افزایش دهد. استفاده گسترده از آثار نویسندگان، هنرمندان و پژوهشگران برای آموزش سامانه‌ها نیز پرسش‌های پیچیده‌ای درباره رضایت، حق مؤلف و مالکیت معنوی ایجاد کرده است. افزون بر این، توسعه مراکز داده و سامانه‌های بزرگ هوش مصنوعی با مصرف انرژی و منابع طبیعی همراه است و آثار زیست‌محیطی آن نیز باید در سیاست‌گذاری‌ها در نظر گرفته شود. توصیه‌نامه اخلاق هوش مصنوعی یونسکو بر پیوند میان کرامت انسانی، حقوق بشر، شفافیت، عدالت و پایداری زیست‌محیطی تأکید می‌کند. [۱]

ضرورت تنظیم‌گری حقوق‌بنیان

مسئله اصلی، پذیرش یا رد مطلق هوش مصنوعی نیست؛ بلکه تعیین حدود کاربرد آن، مسئولیت بازیگران و تضمین نظارت انسانی است. دولت‌ها باید سامانه‌ها را متناسب با میزان خطری که برای حقوق انسان دارند تنظیم کنند. افراد باید بدانند چه زمانی تصمیمی درباره آنان با کمک هوش مصنوعی گرفته شده، بتوانند دلایل آن را دریافت کنند و امکان اعتراض و جبران خسارت داشته باشند. تصمیم‌های حساس در زمینه‌هایی مانند درمان، استخدام، آموزش، وام، خدمات اجتماعی، بازداشت یا مجازات نباید کاملاً به ماشین واگذار شود.

پیش از استفاده از سامانه‌های پرخطر، باید ارزیابی آثار حقوق‌بشری صورت گیرد. شرکت‌ها و نهادهای دولتی نیز نباید مسئولیت تصمیم‌های زیان‌بار را پشت پیچیدگی فنی الگوریتم پنهان کنند. برخی کاربردهایی که ذاتاً با کرامت، آزادی یا برابری انسان ناسازگارند، باید ممنوع یا به‌شدت محدود شوند.

در سطح بین‌المللی، چارچوب‌های مشترک و الزام‌آور برای هدایت توسعه و کاربرد هوش مصنوعی ضروری است. در اروپا، کنوانسیون

اروپایی حقوق بشر، به‌ویژه ماده ۸ درباره احترام به زندگی خصوصی و ماده ۱۰ درباره آزادی بیان، مبنایی برای ارزیابی کاربردهای هوش مصنوعی فراهم می‌کند. [۲]

شورای اروپا نیز «کنوانسیون چارچوب درباره هوش مصنوعی، حقوق بشر، دموکراسی و حاکمیت قانون» را در سال ۲۰۲۴ تصویب کرد؛ نخستین معاهده الزام‌آور بین‌المللی در این حوزه که هدف آن سازگار ساختن چرخه کامل سامانه‌های هوش مصنوعی با حقوق بشر، دموکراسی و حاکمیت قانون است. این سند بر اصولی مانند کرامت انسانی، شفافیت،

پاسخ‌گویی، برابری، حریم خصوصی و نظارت تأکید دارد. [۳]

قانون هوش مصنوعی اتحادیه اروپا نیز با رویکردی مبتنی بر خطر، برای سامانه‌های پرخطر الزامات بیشتری پیش‌بینی کرده و برخی کاربردهای غیرقابل قبول را محدود کرده است. این تجربه نشان می‌دهد که تنظیم‌گری مؤثر باید هم از حقوق بنیادین حمایت کند و هم به‌گونه‌ای طراحی شود که مانع نوآوری‌های مفید و مسئولانه نشود. [۴]

هوش مصنوعی می‌تواند به گسترش دانش، سلامت، آموزش، دسترسی عمومی و مستندسازی نقض حقوق بشر کمک کند؛ اما بدون قانون‌گذاری عادلانه، شفافیت، نظارت انسانی و پاسخ‌گویی، ممکن است تبعیض، نابرابری، نظارت و دست‌کاری افکار عمومی را تشدید کند. آینده این فناوری را صرفاً توانایی ماشین‌ها تعیین نمی‌کند، بلکه تصمیم‌هایی تعیین خواهد کرد که انسان‌ها امروز درباره طراحی، مالکیت، کنترل و حدود استفاده از آن اتخاذ می‌کنند.

منابع و مآخذ

۱. یونسکو، «توصیه‌نامه اخلاق هوش مصنوعی»، مصوب ۲۰۲۱. پیوند رسمی
۲. دیوان اروپایی حقوق بشر، «کنوانسیون اروپایی حقوق بشر»، به‌ویژه مواد ۸ و ۱۰. پیوند رسمی
۳. شورای اروپا، «کنوانسیون چارچوب درباره هوش مصنوعی، حقوق بشر، دموکراسی و حاکمیت قانون»، ۲۰۲۴. پیوند رسمی
۴. اتحادیه اروپا، «مقرره (EU) ۱۶۸۹/۲۰۲۴؛ قانون هوش مصنوعی اتحادیه اروپا». پیوند رسمی

محسن عمادی: هر حقیقتی در برابر تن انسانی است که محک می خورد



پویان مکاری

هوش مصنوعی چگونه مفهوم عاملیت انسانی (Human Agency) را تغییر می دهد؟ آیا خطر آن وجود دارد که انسان با این نگاه به مجموعه ای از داده تقلیل پیدا کند؟

محسن عمادی: به این پرسش از جوانب مختلفی می توان نزدیک شد: چنین وضعیتی هنوز بر ما حاکم نیست. هنوز عاملیت انسانی بر روال آموزش، برنامه ریزی و به کارگیری هوش مصنوعی تعیین کننده است. نگرانی این پرسش از تخیل تصویری در آینده بر می آید، از تصور افق جهانی که توسط هوش مصنوعی احاطه می شود. این افق را شاید بتوان با شرح نسبت میان زبان و انسان راحت تر شرح داد. افق غایی هوش مصنوعی، استرداد عاملیت «انسان سخن گو» - که پیش تر زبان را به عنوان «ابزار»ی به کار می گرفت- به خود «زبان» است. مسیری که جامعه ی بشری قرن هاست در حال پیمودن آن است. جوامعی که روزی به کارگیرنده ابزار/تکنولوژی بودند، به جوامع تکنوکراتیک بدل شدند که در آن اعتبارسنجی درک انسانی توسط تکنولوژی صورت می گرفت. فی المثل تکنولوژی «آمار» برای اعتباربخشی به هر گزاره سیاسی، یا تلاش برای استفاده از زبان علوم دقیقه در علوم اجتماعی یا حتی امور متافیزیکی (مثل نمونه های مضحکی چون رویکرد ترمودینامیکی به قرآن). جوامع تکنوکراتیک در نهایت در حال تبدیل شدن به جوامع تکنوپولی اند. در این گونه از جوامع، سخن «حقیقت» به تکنولوژی مسترد می شود. در همین موقعیت است که تکنولوژی، مرجعیت تفکر را مطالبه می کند. در واقع، خود را همچون «تمامیت

ورود هوش مصنوعی به زندگی انسان تنها یک تحول فناورانه نیست، بلکه پرسش های تازه ای درباره آزادی، برابری، کرامت انسانی و حقوق بشر پیش روی ما گذاشته است. الگوریتم ها و مدل های هوش مصنوعی می توانند دسترسی به دانش و اطلاعات را گسترده تر کنند، اما هم زمان سوگیری های موجود در داده ها و ساختارهای قدرت ممکن است به بازتولید تبعیض های اجتماعی، نابرابری و حتی محدود شدن برخی حقوق و آزادی های فردی منجر شوند. از سوی دیگر، گسترش دیپ فیک و تولید انبوه واقعیت های جعلی، اعتماد عمومی و امکان دسترسی به حقیقت را تهدید می کند و سلطه فناوری های بزرگ بر زبان و اطلاعات، نگرانی هایی درباره تنوع فرهنگی و «استعمار دیجیتال» به وجود آورده است. در چنین شرایطی، مسئله فقط این نیست که هوش مصنوعی چه توانایی هایی دارد، بلکه این است که این توانایی ها در خدمت چه کسانی و چه ارزش هایی قرار می گیرند و آیا می توان از آن برای تقویت عدالت اجتماعی و حقوق بشر استفاده کرد یا نه. برای بررسی این ابعاد و نسبت میان هوش مصنوعی، عاملیت انسانی، حقیقت و حقوق بشر، با محسن عمادی، شاعر، مترجم و مهندس کامپیوتری که دکترایش را در حوزه نشانه شناسی ادبیات دیجیتال دریافت کرده، گفت و گو کردیم.

زبان» در برابر «تن انسانی» بازمی‌نماید. عاملیت انسان، و به عبارتی، حضور و نقش تن انسانی از آغاز عصر تکنوکراسی کم شده بود. ولی در افقی که با «تکنوپولی» تصویر می‌شود این عاملیت به حداقل خود می‌رسد. این‌جا می‌توان پرسید: منظورمان از زبان چیست؟ یا چه نهاده‌ای این زبان را به پیش می‌برد؟ نمی‌شود پاسخ خیلی سر راستی به این سوال‌ها داد. ولی می‌توان نقش سرمایه و قدرت را - که امروزه در دست بخش اندکی از جمعیت انسانی متمرکز است - برجسته دید. انسانی که از وجوه تئانه خود تهی می‌شود، در نهایت یک ایده، یک کلمه و شاید یک داده است، همین و بس.

سوگیری الگوریتمی (Algorithmic Bias) چگونه می‌تواند به بازتولید تبعیض‌های اجتماعی و نابرابری در دسترسی به فرصت‌ها منجر شود؟ آیا الگوریتم‌ها می‌توانند واقعاً بی‌طرف باشند؟

محسن عمدادی: سوگیری‌های الگوریتمی، از یک طرف به «سیاست» اربابان هوش مصنوعی بر می‌گردد و از طرف دیگر به «تاریخ» مکتوب. وجه تاریخی، روی آموزش اولیه مدل‌های هوش مصنوعی اثر می‌گذارد. ولی وجه سیاسی این تکنولوژی، می‌تواند این تاریخ را بازنویسی کند، آن را ادامه دهد یا حتی این تبعیض‌ها را مشخص کند. ترکیب تاریخ و سیاست است که جهت تصمیم‌گیری را معین می‌کند. فی‌المثل وقتی مدلی را با داده‌هایی آموزش می‌دهید که در آن اکثریت مجرمان سیاه‌پوستند، طبعاً وقتی آن را برای تشخیص مجرمان بالقوه در یک موقعیت بکار می‌برید، الگوریتم، سیاه‌پوستان

بیشتری را هدف قرار می‌دهد. به همین شکل، تبعیض‌های جنسیتی، دینی، نژادی و غیره بازتولید می‌شوند و حتی ممکن است تشدید شوند. نقش سیاست در این‌جا، تشخیص، اصلاح و تنظیم سوگیری‌هاست. اگر این نقش را درست انجام دهد، می‌تواند سوگیری‌های تاریخ را کنترل و حتی اصلاح کند و اگر نه، فاجعه‌ای به فجایع تاریخ خواهد افزود.

با گسترش هوش مصنوعی مولد (Generative AI) آیا خطر تضعیف تنوع زبانی و فرهنگی وجود دارد؟ آیا زبان‌های کمتر برخوردار ممکن است در عصر هوش مصنوعی با نوعی استعمار دیجیتال (Digital Colonialism) روبه‌رو شوند؟

محسن عمدادی: اصولاً هر تکنولوژی در عین حال که افق تازه‌ای پیش می‌گذارد، شرایط و افق‌های دیگری را غایب می‌کند. مثلاً، با اختراع ماشین تایپ و فونت‌ها، سرعت تولید متن بیشتر شد ولی خوش‌نویسی و خط خوش که یک روز برای هر فرد باسوادی «تشخص»‌ای ویژه ایجاد می‌کرد به محاق رفت. قبول هر شکل از استاندارد به معنی به محاق بردن و گاه نفی هر بیان غیر استاندارد است و تنوع‌های زبانی و فرهنگی معمولاً در همین دسته بیرون از استاندارد قرار می‌گیرند. استعمار دیجیتال، از دوره‌ی فراگیر شدن کامپیوترهای خانگی وجود داشت. همین‌که زبان‌های برنامه‌نویسی به خط لاتین نوشته می‌شدند و منطق حاکم بر آن‌ها بستاری از منطق ارسطویی بود، شکلی از استعمار دیجیتال بود و هست. هوش مصنوعی می‌تواند این استعمار را مشخص کند. برای چهره‌هایی مثل

احمد شاملو، نوشتن کتاب کوچه تلاشی بود برای اعتباربخشی به گونه‌ای از زبانی در زبان فارسی که در فرهنگ‌نامه‌های رسمی پیدا نمی‌شد. زبانی زبان در نسبت با همین تنوع‌های قومی، فرهنگی و زیستی ممکن است. یعنی از یک طرف، با نرمالیزه‌شدن تفکر و البته با استرداد مرجع‌گزینی تفکر و حقیقت، زبان نسبت به تنوع‌های فرهنگی بی‌اعتنا خواهد شد و از طرف دیگر مراجع جدید حقیقت، شکلی از مواجهه با اندیشگی و حق را ترویج می‌کنند که ممکن است فقط ابعاد مختصری از کلیت فرهنگ‌های دیگر را بازتاب دهند و ابعاد دیگر را به مرور به محاق بسپارند. استعماری که «طبیعی» می‌نماید و «عادی‌سازی» می‌شود.

آیا می‌توان به یک هوش مصنوعی انسان‌محور (Human-Centric AI) امیدوار بود که به جای ابزار کنترل، به گسترش حقوق بشر و عدالت اجتماعی کمک کند؟

آدمیزاد به امید زنده است. زبان، همیشه محمل فرمان امپراطوران نبوده و گاه انسان‌های دردمند از گذر تاریخ، با من و ما سخن گفته‌اند. صنعت چاپ، در آغاز پیدایش‌اش در خدمت کلیسا و قدرت‌ها بود. به مرور علیه همان کلیسا و قدرت‌ها شورید. وضعیت امروز هوش مصنوعی در خدمت نهادهای قدرتی است که برای حقوق بشر و عدالت اجتماعی پیش‌روی ارزش قایل نیستند. آن‌را، سلاحی برای تحمیل انسان و تسلط بر آن می‌خواهند. ولی همیشه حتی سلاح هم از انحصار گریخته است. ترجیح می‌دهم در جنگ نامتقارن میان انسان و صاحبان زر و زور، طرف انسان بایستم و بگویم: امیدوارم. آدمیزاد به امید زنده است.

در عصر جعل عمیق (Deepfake) و تولید واقعیت‌های جعلی، چگونه می‌توان از حقیقت، حافظه تاریخی و اعتماد عمومی دفاع کرد؟

در نهایت هر حقیقتی در برابر تن انسانی است که محک می‌خورد. «بازنمایی تن» برابر نهاد «تن» نیست. میان سه شکل محاکات که از یک پدیده می‌توان متصور شد، یعنی «اصل»، «تقلید یا کپی» و «شبیه‌سازی»، این آخری یعنی شبیه‌سازی از هر دوتای دیگر قوی‌تر است: چون هم سیالیت دارد، هم قابلیت تکثیر مکانیکی و هم اصلاح‌پذیر است. حتی می‌تواند «درد» و «لذت» را بازنمایی کند. روی همین اصل، اعتبارسنجی و کشف حقیقت کار بسیار دشواری است. دشوار از این جهت که نیازمند تعهدی عمیق است به حقیقت. در گذشته اگر شایعه می‌شد که اهالی فلان جزیره آدم‌خوارند، تنها راه

پویش عزیزالدین:

«نظارت مبتنی بر هوش مصنوعی» فناوری واحدی نیست



در سال‌های اخیر، ورود فناوری‌های نظارتی مبتنی بر هوش مصنوعی به فضای امنیتی ایران، ابعاد تازه‌ای به تدابیر کنترل اجتماعی و پایش شهروندان بخشیده است. استفاده حاکمیت از سامانه‌های تشخیص چهره، تحلیل داده‌های کلان بیومتریک و یکپارچه‌سازی داده‌های ارتباطی و مالی، مرزهای حریم خصوصی را بیش از پیش تنگ‌تر کرده است. این تغییر پارادایم نظارتی، علاوه بر افزایش وابستگی ساختاری به سخت‌افزارها و نرم‌افزارهای امنیتی کشورهای خارجی، ابزارهای سرکوب دیجیتال، عملیات روانی و گردآوری داده توسط ارتش‌های

سایبری را نیز پیچیده‌تر و کم‌هزینه‌تر کرده است؛ وضعیتی که حتی کارایی ابزارها و فناوری‌های ضدنظارت را برای حفاظت از شهروندان با چالش‌های جدی مواجه می‌سازد. در این زمینه با پویش عزیزالدین، پژوهشگر فناوری دیجیتال و کارشناس امنیت اینترنت، گفت‌وگو کردیم.

فناوری‌های نظارتی مبتنی بر هوش مصنوعی در ایران، مانند تشخیص چهره و تحلیل تصویر، تا چه اندازه عملیاتی شده‌اند و محدودیت‌های فنی آن‌ها چیست؟

پویش عزیزالدین: فناوری‌های نظارتی مبتنی بر هوش مصنوعی در ایران را نه می‌توان صرفاً پروژه‌هایی نمایشی دانست و نه شبکه‌ای یکپارچه و هم‌بند. این فناوری‌ها پیش‌تر از مسیر احراز هویت بیومتریک در سامانه‌هایی مانند ثنا، سجام و برخی خدمات بانکی وارد زندگی روزمره شده‌اند. داده‌هایی که در ظاهر برای ارائه خدمات گردآوری می‌شوند، می‌توانند با سامانه‌های انتظامی و قضایی پیوند بخورند. مقام‌های حکومتی نیز از تطبیق تصاویر تازه‌ای به تدابیر کنترل اجتماعی و پایش شهروندان برخوردارند. استفاده حاکمیت از سامانه‌های تشخیص چهره، تحلیل داده‌های کلان بیومتریک و یکپارچه‌سازی داده‌های ارتباطی و مالی، مرزهای حریم خصوصی را بیش از پیش تنگ‌تر کرده است. این تغییر پارادایم نظارتی، علاوه بر افزایش وابستگی ساختاری به سخت‌افزارها و نرم‌افزارهای امنیتی کشورهای خارجی، ابزارهای سرکوب دیجیتال، عملیات روانی و گردآوری داده توسط ارتش‌های

آنچه اکنون دیده می‌شود، بیش از آنکه سامانه‌ای کاملاً خودکار باشد، معماری نظارتی ترکیبی است که دوربین، پایگاه داده، تحلیل ماشینی، گزارش انسانی و مجازات اداری را به هم متصل می‌کند. تجهیزات موجود قابلیت‌هایی مانند برآورد سن و جنسیت، تحلیل حالت چهره و تشخیص پوشش سر را عرضه می‌کنند؛ اما اجرای کنترل اجتماعی، به‌ویژه در طرح‌هایی مانند تحمیل حجاب اجباری، همچنان به ابزارهایی مانند اپلیکیشن «ناظر»، ثبت پلاک، حضور مأموران و گزارش رانندگان شرکت‌های تاکسیرانی اینترنتی وابسته است.

محدودیت‌های فنی این زیرساخت جدی‌اند. پوشش دوربین‌ها و کیفیت تصاویر یکنواخت نیست؛ تشخیص سن، حالت چهره و احساسات دقت ثابتی ندارد؛ و کیفیت پایین داده‌های آموزشی می‌تواند نرخ خطا را افزایش دهد. اتکای مداوم به گزارش انسانی نیز نشان می‌دهد که شناسایی فراگیر و دقیق هنوز محقق نشده است. کمبود توان پردازشی، دشواری

توسعه مراکز داده مجهز به پردازنده‌های گرافیکی و بحران برق، امکان پردازش پیوسته و بلادرنگ را محدود می‌کند. با این همه، ناکامل بودن فناوری به معنای بی‌خطر بودن آن نیست: در ساختاری که تصمیم‌های اداری و امنیتی شفاف نیستند، حتی یک تطبیق اشتباه می‌تواند به بازداشت، محرومیت از خدمات یا مجازات منجر شود.

بعبارت دیگر مسئله فقط دیده‌شدن شهروندان و نظارت بر آنان و میزان پیشرفتگی فناوری بکارگرفته شده در این راه نیست، بلکه تبدیل بدن، پوشش، شخصیت و سبک زندگی شهروندان به داده‌ای قابل طبقه‌بندی و سپس پیوند زدن آن داده با تنبیه، محرومیت و خودسانسوری است.

این زیرساخت‌ها تا چه حد به فناوری‌ها و شرکت‌های خارجی وابسته‌اند و وابستگی خارجی چه تأثیری بر توان نظارتی حکومت دارد؟

پویش عزیزالدین: وابستگی زیرساخت نظارتی ایران به فناوری خارجی عمیق و ساختاری است. حکومت برای تکمیل زنجیره نظارت به دوربین‌ها، تجهیزات شبکه و سامانه‌های تحلیل تصویر شرکت‌های چینی مانند داهوا، هایک‌ویژن، تیاندی و یونیوو و نیز زیرساخت‌های قدیمی‌تر هواوی و ZTE متکی است. در لایه نرم‌افزاری نیز فناوری تشخیص چهره شرکت روسی NtechLab و خدمات شرکت Protei برای پایش ترافیک و مسدودسازی اینترنت به کار گرفته شده‌اند. قطعات و تجهیزات غربی، از دوربین‌های بوش، زیمنس و دال‌مایر تا تراشه‌های اینتل، نیز از طریق واسطه‌ها و واردات موازی وارد

را نباید صرفاً تهدیدی علیه حکومت تلقی کرد؛ نخستین کسانی که بهای افشا یا دست‌کاری این اطلاعات را می‌پردازند، شهروندانی هستند که بر نحوه جمع‌آوری و استفاده از داده‌های خود کنترل مؤثری ندارند. وابستگی خارجی، در آن واحد، توان سرکوب را افزایش می‌دهد و ناامنی کسانی را که موضوع نظارت‌اند عمیق‌تر می‌کند.

یکپارچه‌سازی داده‌های شهروندان از منابع مختلف، مانند داده‌های ارتباطی، هویتی و مالی، چه چالش‌های فنی و امنیتی ایجاد می‌کند؟

پویش عزیزالدین: ترکیب داده‌های ارتباطی، هویتی، مالی، درمانی و رفت‌وآمد می‌تواند تصویری از زندگی هر شهروند بسازد که هیچ پایگاه داده‌ای به‌تنهایی قادر به تولید آن نیست: نقشه‌ای از روابط اجتماعی، عادت‌ها، وضعیت اقتصادی، سلامت و آسیب‌پذیری‌های فرد. ایجاد چنین تصویری از نظر فنی پیچیده است. پایگاه‌های داده نهادهای مختلف براساس استانداردهای متفاوت و با درجات نابرابری از دقت، به‌روز بودن و امنیت طراحی شده‌اند. موازی‌کاری و رقابت میان نهادهای حکومتی نیز مانع شکل‌گیری معماری واحد و قابل اتکای داده می‌شود. در نتیجه، اتصال سامانه‌ها لزوماً به معنای تولید شناخت دقیق‌تر نیست و گاهی فقط حجم بیشتری از داده‌های ناسازگار را کنار هم قرار می‌دهد.

خطر اصلی، نحوه تکثیر خطا در سراسر این شبکه است. وقتی خروجی خطاپذیر یک دوربین یا داده مکانی نادقیق به اطلاعات ثبت احوال، حساب بانکی یا پرونده قضایی متصل شود، اشتباهی کوچک می‌تواند به هویتی ظاهراً قطعی و سپس تصمیمی اداری یا امنیتی تبدیل شود. داده‌های تاریخی آغشته به تبعیض نیز همان نابرابری‌های موجود را با ظاهری علمی بازتولید می‌کنند. این خطر برای زنان، اقلیت‌های قومی و مذهبی، افراد کویر، مهاجران و کسانی که به خدمات سلامت روان یا سلامت باروری نیاز دارند شدیدتر است؛ زیرا اطلاعاتی که برای دریافت خدمت ثبت شده‌اند، ممکن است در بستری دیگر به ابزار انگ‌زنی، محرومیت یا تعقیب بدل شوند. از این رو، یکپارچه‌سازی داده صرفاً مسئله‌ای مهندسی نیست؛ مرز میان ارائه خدمت عمومی و نظارت امنیتی را جابه‌جا می‌کند.

تمرکز این حجم از اطلاعات همچنین هدفی بسیار ارزشمند و نقطه شکستی واحد برای نفوذ ایجاد می‌کند. رخدادهای امنیتی در سیستم بانکی، سامانه سوخت، ثبت احوال، تپسی، اسنپ‌فود و شرکت‌های بیمه نشان داده‌اند که نشت گسترده اطلاعات در ایران خطری فرضی نیست. اتصال وزارتخانه‌ها، بانک‌ها، اپراتورها و پیمانکاران، سطح حمله را گسترش می‌دهد و امنیت کل شبکه را به ضعیف‌ترین حلقه آن وابسته می‌کند.

این آسیب‌پذیری با رواج نرم‌افزارهای کرک‌شده در نتیجه تحریم‌ها یا محدودیت‌های مالی شرکت‌ها، قطعی‌های گسترده اینترنت و اختلال در دریافت وصله‌های امنیتی و به‌روزرسانی منظم، تشدید می‌شود. همچنین مهاجرت گسترده متخصصان امنیت سایبری و کمبود نیروی ماهر نیز توان شناسایی، مهار و پاسخ‌گویی به رخدادهای امنیتی را کاهش داده است.

مهم‌تر از همه، داده در فرایند ادغام از زمینه اولیه

خود جدا می‌شود: یک پیام، تراکنش مالی یا مراجعه درمانی ممکن است معنایی امنیتی پیدا کند که هنگام ثبت آن وجود نداشته است. مسئله فقط گستره دانسته‌های حکومت نیست؛ مسئله فقدان کنترل شهروندان بر نحوه تفسیر، اصلاح و استفاده از این اطلاعات است.

هوش مصنوعی چگونه توان حکومت‌ها و بازیگران سایبری را در تولید اطلاعات نادرست، عملیات روانی و ارتش‌های سایبری تغییر داده است؟

پوبش عزیزالدین: هوش مصنوعی مولد بیش از آنکه هدف عملیات روانی را تغییر داده باشد، هزینه، سرعت، مقیاس و دقت آن را دگرگون کرده است. فعالیت‌هایی که پیش‌تر به تیم‌های بزرگی برای ترجمه، جعل هویت، نگارش پیام و اداره حساب‌های جعلی نیاز داشتند، اکنون با نیروی انسانی کمتر و به زبان و سبک متناسب با هر مخاطب انجام می‌شوند. گروه ایرانی Crimson Sandstorm از این ابزارها برای تولید ایمیل‌های فیشینگ انگلیسی استفاده کرده و Storm-۲۰۳۵ نیز مطالبی ظاهراً معتبر درباره انتخابات آمریکا، جنگ غزه و المپیک ۲۰۲۴ ساخته است. تقلید لحن کاربران واقعی نیز تشخیص حساب‌های جعلی را دشوارتر می‌کند. پیوند این قابلیت با تحلیل ردپای دیجیتال، تبلیغات عمومی را به مهندسی اجتماعی شخصی‌سازی شده تبدیل می‌کند: هر فرد می‌تواند براساس ترس‌ها، وضعیت اقتصادی، جنسیت یا آسیب‌پذیری‌های

خاص خود هدف قرار گیرد. در جنگ دوازده‌روزه ایران و اسرائیل در ژوئن ۲۰۲۵، ۷۲ درصد از محتوای نادرست بررسی‌شده در خدمت بزرگ‌نمایی قدرت نظامی ایران و ایجاد هراس بود. پیامد عمیق‌تر این فناوری، گسترش بی‌اعتمادی به امکان تشخیص حقیقت است. وقتی جعل هر تصویر و صدایی ممکن به نظر می‌رسد، صاحبان قدرت می‌توانند اسناد واقعی را نیز ساختگی بنامند؛ چنان‌که در همان جنگ، ویدئوی واقعی اصابت موشک به ساختمانی در تهران از سوی برخی کاربران جعلی تلقی شد. برای قربانیان و مستندسازان نقض حقوق بشر، این تردید فراگیر سازوکاری تازه برای بی‌اعتبارکردن شهادت و خاموش کردن شاهدان است.

در ایران، این ظرفیت تازه بر زیرساخت‌های موجود گردان‌های سایبری، رسانه‌های حکومتی، عملیات «هک و نشت» و اعترافات اجباری سوار شده است. حدود ۳۵۰۰ گردان سایبری تحت نظارت سپاه، گروه‌هایی مانند APT۴۲ و Storm-۱۳۶۴ و شبکه‌ای از رسانه‌های نیابتی برای دست‌کاری افکار عمومی و تشدید شکاف‌های سیاسی، قومی و جنسیتی به کار گرفته شده‌اند. معرفی معترضان به‌عنوان «عامل بیگانه» یا «تروریست»، پخش اعترافات گرفته‌شده تحت فشار و کارزارهای بدنام‌سازی دیجیتال، سرکوب را مشروع جلوه می‌دهد. زنان و اقلیت‌های جنسی و جنسیتی نیز غالباً با حمله به آبرو، بدن و زندگی خصوصی خود مواجه می‌شوند. این ابزارها البته در انحصار یک دولت نیستند؛ عملیات منسوب به «گنجشک

درنده» در ژوئن ۲۰۲۵ نیز با پیام‌های جعلی درباره کمبود سوخت و فروپاشی نظام بانکی، ترس را متوجه شهروندان عادی کرد. هوش مصنوعی ارتش‌های سایبری را از میان نبرده، بلکه توان هر عامل انسانی را چند برابر کرده است.

در مقابل گسترش ابزارهای نظارتی مبتنی بر هوش مصنوعی، فناوری‌های ضدنظارت چه میزان امکان حفاظت از شهروندان را فراهم می‌کنند؟

پوبش عزیزالدین: این پرسش در صورت‌بندی فعلی بیش از اندازه کلی است، زیرا «نظارت مبتنی بر هوش مصنوعی» به فناوری واحدی اشاره نمی‌کند. همان‌طور که هوش مصنوعی ممکن است در طیفی از ابزارها، از مسواک هوشمند تا ساتنریفیوژهای عظیم صنعتی، به کار رود، نظارت نیز صورت‌های بسیار متفاوتی دارد: تشخیص چهره، تحلیل تصویر، شنود ارتباطات، رهگیری مکانی، تحلیل ترافیک شبکه، شناسایی الگوهای رفتاری یا ترکیب داده‌های مالی و هویتی. بنابراین، پیش از ارزیابی فناوری ضدنظارت باید مشخص شود با کدام نوع نظارت، کدام عامل تهدید و چه سطحی از خطر روبه‌رو هستیم. هیچ ابزار واحدی نمی‌تواند در برابر همه این اشکال محافظت ایجاد کند.

باین‌حال، نمونه‌هایی از وضعیت دائمی «موش و گربه» میان نظارت و ضدنظارت وجود دارد. رمزگذاری سرتاسری در سیگنال از محتوای پیام محافظت می‌کند، اما لزوماً زمان، حجم و الگوی ارتباط را پنهان نمی‌سازد. Tor و VPN مسیر

اتصال را مبهم‌تر می‌کنند، اما در برابر دسترسی فیزیکی به تلفن، بدافزار یا نسخه پشتیبان ناامن کافی نیستند. غیرفعال‌کردن شبکه نسل دوم می‌تواند برخی حملات مبتنی بر ایستگاه‌های مخابراتی جعلی را دشوارتر کند، درحالی‌که ابزارهای تشخیص این تجهیزات خود محدودیت دارند و ممکن است احساس امنیت کاذب ایجاد کنند. روش‌های مختل‌کننده تشخیص چهره و ابزارهایی مانند Glaze و Nightshade نیز ممکن است برخی مدل‌های تحلیل تصویر را به خطا بیندازند، اما با تغییر مدل‌ها یا استفاده هم‌زمان از نشانه‌های دیگر، کارایی آن‌ها کاهش می‌یابد. هر پیشرفت دفاعی معمولاً با روشی تازه برای دورزدن آن پاسخ داده می‌شود.

ازاین‌رو، فناوری‌های ضدنظارت را باید ابزارهایی برای کاهش خطر و افزایش هزینه ردیابی دانست، نه تضمینی برای ناشناس‌ماندن. حفاظت مؤثر به ترکیبی از ابزار مناسب، شناخت تهدید، آموزش عملی و رفتار متناسب با موقعیت نیاز دارد. باین‌حال، نباید مسئولیت مقابله با زیرساخت‌های عظیم نظارتی را بر دوش افراد گذاشت یا قربانیان را به دلیل رعایت‌نکردن توصیه‌های پیچیده سرزنش کرد. ابزارها و آموزش‌ها باید با امکانات و زندگی واقعی کسانی که در معرض خطرند سازگار باشند.

دفاع فنی می‌تواند فضایی محدود برای حفاظت و مقاومت ایجاد کند، اما جایگزین محدودیت حقوقی بر اختیارات حکومت، پاسخ‌گویی نهادی و امکان دادخواهی نیست.

روزنامه‌نگاری و هوش مصنوعی



روزنامه‌نگاری تحقیقی و ساخت مستند، بیش از بسیاری از حوزه‌های رسانه‌ای با جست‌وجو، بررسی و تحلیل حجم گسترده‌ای از اسناد، داده‌ها و منابع سروکار دارند؛ فرایندی که هوش مصنوعی در سال‌های اخیر آن را متحول کرده است. از جست‌وجو و خلاصه‌سازی هزاران سند و مقایسه داده‌ها و راستی‌آزمایی گرفته تا کمک به روایتگری و تولید محتوای تصویری، ابزارهای هوش مصنوعی فرصت‌های تازه‌ای برای افزایش سرعت و عمق تحقیقات روزنامه‌نگارانه ایجاد کرده‌اند. در مقابل، گسترش دیپ‌فیک و محتوای جعلی، سوگیری منابع، امکان فریب ابزارهای هوش مصنوعی و استفاده سازمان‌یافته از آن برای تولید اطلاعات گمراه‌کننده، چالش‌های تازه و جدی برای اعتبار و استقلال روزنامه‌نگاری به وجود آورده است؛

چالش‌هایی که در فضای رسانه‌ای ایران، با توجه به فیلترینگ و محدودیت دسترسی به منابع، ابعاد پیچیده‌تری پیدا می‌کند. برای بررسی این فرصت‌ها و تهدیدها و اینکه روزنامه‌نگاران در مواجهه با این فناوری چه تغییراتی را باید در شیوه کار خود ایجاد کنند، با شهریار صیامی، روزنامه‌نگار و مستندساز، گفت‌وگو کردیم.

روزنامه‌نگاری و ساخت مستند، بیش از بسیاری از حوزه‌های رسانه‌ای با جست‌وجو، بررسی و تحلیل حجم گسترده‌ای از اسناد، داده‌ها و منابع سروکار دارند؛ فرایندی که هوش مصنوعی در سال‌های اخیر آن را متحول کرده است. از جست‌وجو و خلاصه‌سازی هزاران سند و مقایسه داده‌ها و راستی‌آزمایی گرفته تا کمک به روایتگری و تولید محتوای تصویری، ابزارهای هوش مصنوعی فرصت‌های تازه‌ای برای افزایش سرعت و عمق تحقیقات روزنامه‌نگارانه ایجاد کرده‌اند. در مقابل، گسترش دیپ‌فیک و محتوای جعلی، سوگیری منابع، امکان فریب ابزارهای هوش مصنوعی و استفاده سازمان‌یافته از آن برای تولید اطلاعات گمراه‌کننده، چالش‌های تازه و جدی برای اعتبار و استقلال روزنامه‌نگاری به وجود آورده است؛

با همه‌گیر شدن دیپ‌فیک و ابزارهای تولید انبوه محتوای جعلی، مرز میان سندیت و دستکاری بسیار باریک شده؛ مهم‌ترین چالش در تفکیک واقعیت از تولیدات AI چیست؟

شهریار صیامی: هوش مصنوعی می‌تواند خبرنگاران خبرهای روزانه و فوری را در دام منابع فیک گرفتار کند. خبرنگار می‌تواند به اشتباه از تصاویری استفاده کند که ساخته هوش مصنوعی درباره اتفاقی است که رخ داده ولی هنوز تصاویری از آن در دسترس نیست.

هوش مصنوعی در کدام بخش از فرآیند روزمره روزنامه‌نگاری تحقیقی و ساخت مستند (از تحلیل اسناد و داده‌ها

این موضوع در مورد حوادثی بیشتر دیده می‌شود صداها را ضبط کنید؟ اگر تحت پیگرد پلیس که از نظر جغرافیایی گسترده‌تر هستند و امکان یا سازمان‌های امنیتی قرار بگیرید حقوق اولیه رخ دادن اتفاق در چند نقطه وجود دارد. مانند شما بدون دسترسی به وکیل چیست؟ چطور اعتراضات خیابانی در چندین محله یا شهرهای وکیل یا مشاور خوب حقوقی پیدا کنید؟ مختلف، بلاهای طبیعی یا یک اتفاق هم زمان در موارد «فکت چک» هوش مصنوعی می‌تواند در چند کشور. بعضی از گروه‌های سیاسی و به پیدا کردن نکات مورد نظر شما بین هزاران هزاران منبع مختلف با سرعت زیاد کمک کند. حتی در مواردی حکومت‌ها از این روش برای به دام انداختن روزنامه‌نگاران استفاده می‌کنند. قابلیت مقایسه آمار توسط هوش مصنوعی طول در جنگ آمریکا و اسرائیل با ایران بارها تصاویر پژوهش را به طور چشمگیری کاهش می‌دهد هوش مصنوعی به جای تصاویر واقعی توسط و خطاهای انسانی در مقایسه اعداد و ارقام را از بعضی از خبرنگاران استفاده شد. بین می‌برد.

در گذشته بسیاری از اسناد در میان هزاران سند موجود در یک پروژه تحقیقاتی نادیده گرفته می‌شد. اسنادی که بعضی می‌توانستند کلید حل معما باشند اما هوش مصنوعی می‌تواند تمام این اسناد را در کوتاه‌ترین زمان ممکن بررسی کند. ضمن اینکه جستجوی ده‌ها کلیدواژه در اینترنت برای یک روزنامه‌نگار به دلیل زمان طولانی تقریباً غیرممکن بود، اما این امکان را هوش مصنوعی فراهم کرده است.

اگر از جنبه مثبت نگاه کنیم، ابزارهای جدید تحلیل داده یا الگوریتم‌ها چطور می‌توانند به افشای فساد، تحلیل اسناد پیچیده یا کشف الگوهایی کمک کنند که پیش‌تر از چشم روزنامه‌نگار دور می‌ماند؟ شه‌ریار صیامی: بیش از همه یک روزنامه‌نگار می‌تواند از هوش مصنوعی به عنوان یک مشاور حقوقی استفاده کند و تا حدود زیادی محافظت قانونی به‌دست آورد تا سازمان‌های امنیتی و حکومتی نتوانند بدون اطلاع خبرنگاران حقوق آن‌ها را پایمال کنند. این حتی در کشورهای آزاد و دموکرات هم کاربرد دارد چرا که شما از موارد قانونی در شغل روزنامه‌نگاری مطلع می‌شوید. مثلاً کجا می‌توانید تصویربرداری کنید؟ کدام

سازمان‌یافته تولید اطلاعات ضمن اینکه نیروهای فعال حکومتی در فضای مجازی دائماً در حال آموزش و فریب دادن **گمراه‌کننده (Desinformation)** هوش مصنوعی در مورد فکت‌ها هستند. وقتی **سنگین‌کند؟**

شه‌ریار صیامی: متأسفانه در فضای رسانه‌ای ایران هوش مصنوعی می‌تواند کاملاً برعکس عمل کند. چون در اول دسترسی به وبسایت‌های هوش مصنوعی فیلتر شده و به سختی در دسترس هستند و فقط افراد مورد تایید حکومت به هوش مصنوعی دسترسی بدون فیلتر دارند. که فعالان مدنی و سیاسی توانایی تصحیح این امواج پروپاگاندا در هوش مصنوعی را ندارند.

مصنوعی مثل تولید محتوی، انیمیشن و تصویر نیاز به پرداخت مالی آن هم به‌صورت ارزی دارد که برای خیلی از ایرانی‌ها غیرممکن است. این موارد باعث می‌شود هوش مصنوعی عملاً در خدمت دستگاه‌های حکومتی باشد و برای تولید محتوی پروپاگاندا و گاهی گمراه‌کننده استفاده شود.

روزنامه‌نگاران در ارتباط با هوش مصنوعی چه مهارت‌های فنی جدیدی را باید بیاموزند و چه اصول اخلاقی تغییرناپذیری را باید حفظ کنند؟ به‌طور کامل هنوز نمی‌توان گفت چه مهارت‌های نیاز است. اما باید به فکت‌ها بیش از گذشته شک کرد. باید بیش از گذشته چند منبع مستقل را چک کرد. باید بیش از حد به هوش مصنوعی اعتماد نکرد و پذیرفت که هوش مصنوعی هم اشتباه می‌کند، گمراه می‌شود و گاهی تحت کنترل حکومت‌ها قرار می‌گیرد. از نظر اخلاقی روزنامه‌نگاران باید از هوش مصنوعی به عنوان یک قلم شیک که محتوی آن‌ها را پربار می‌کند استفاده کنند نه وسیله تولید محتوی که جایگزین تولید محتوی ذهن و توانایی آنان شود. می‌دهد و به تولید خبرهای نادرست می‌انجامد.

در فضای رسانه‌ای ایران با چالش‌هایی مثل سانسور، فیلترینگ و ابزارهای ضعیف‌تر در زبان فارسی، هوش مصنوعی چقدر به نفع روزنامه‌نگاری مستقل عمل می‌کند و چقدر می‌تواند کفه ترازو را به نفع جریان‌های

معین خزائلی: هوش مصنوعی قلمروی خارج از حقوق نیست



گسترش روزافزون فناوری‌های مبتنی بر هوش شناسایی و تعقیب شهروندان را در مقیاسی مصنوعی و به‌کارگیری آن توسط دولت‌ها، فراهم کند که پیش از این به نیروی انسانی و در کنار تمام فرصت‌های نوآورانه، چالش‌ها و امکانات بسیار گسترده نیاز داشت.

نگرانی‌های جدیدی را در حوزه حقوق بشر، نمونه عینی این نگرانی را می‌توان در برخورد حریم خصوصی و آزادی‌های فردی به همراه با زنان بر سر حجاب اجباری مشاهده کرد. داشته است. در جوامعی که با خالاهای قانونی، گزارش‌های زیادی از گسترش استفاده عدم شفافیت الگوریتمی و محدودیت‌های جمهوری اسلامی از نوعی از هوش مصنوعی ساختاری در نظارت قضایی مستقل مواجه‌اند، در قالب دوربین‌های نظارتی، فناوری تشخیص این فناوری‌ها بالقوه می‌توانند به ابزارهایی چهره و ابزارهای الکترونیکی برای شناسایی کارآمد برای توسعه نظارت عمومی، کنترل زنان وجود دارند؛ روندی که حریم خصوصی، اجتماعی و تشدید سرکوب تبدیل شوند. برای آزادی رفت‌وآمد و اصل منع تبعیض را همزمان بررسی ابعاد حقوقی این مسئله، پیامدهای آن تحت تاثیر قرار می‌دهد.

بر حقوق شهروندی و بررسی تعهدات بین‌المللی خطر دیگر، اتصال این فناوری‌ها به ساختاری حاکمیت در مواجهه با ابزارهای نوین نظارتی، در است که پیش از این نیز سابقه گسترده‌ای در این زمینه با معین خزائلی، حقوقدان و پژوهشگر حقوق بشر، گفت‌وگو کرده‌ایم.

با ظهور هوش مصنوعی چه چالش‌هایی در زمینه حقوق بشر در ایران ایجاد شده است؟

جریان اعتراضات دی‌ماه ۱۴۰۴ قطع گسترده اینترنت نیز گزارش شد؛ بنابراین اضافه شدن ابزارهای هوش مصنوعی به چنین ساختاری می‌تواند توانایی حکومت برای شناسایی، طبقه‌بندی و کنترل مخالفان، منتقدان و شهروندان را به شکل بی‌سابقه‌ای افزایش دهد.

مهم‌ترین نگرانی حقوق بشری درباره هوش مصنوعی در ایران، نه خود این فناوری، بلکه ظرفیت آن برای گسترش نظارت حکومتی است. ترکیب دوربین‌های شهری، تشخیص چهره، تحلیل تصاویر، پردازش داده‌های کلان و رصد شبکه‌های اجتماعی می‌تواند امکان

با توجه به توسعه استفاده دولت‌ها از هوش مصنوعی، جمهوری اسلامی ایران چه تعهدات حقوق بشری در این

زمینه دارد؟

چنین رویکردی است.

هوش مصنوعی قلمروی خارج از حقوق نیست.

جمهوری اسلامی همان تعهداتی را که در جهان

فیزیکی نسبت به حقوق شهروندان دارد، هنگام

استفاده از فناوری‌های هوش مصنوعی نیز باید

رعایت کند. به ویژه میثاق بین‌المللی حقوق

مدنی و سیاسی، حقوقی مانند حریم خصوصی،

آزادی بیان، آزادی عقیده، دادرسی عادلانه،

تجمع مسالمت‌آمیز و برابری در برابر قانون را

تضمین کرده است.

بنابراین حاکمیت نمی‌تواند و نباید صرفاً با استناد

به «امنیت ملی» استفاده نامحدود از هوش

مصنوعی برای نظارت بر شهروندان را توجیه

کند. هرگونه محدودیت بر حقوق افراد باید

مبنای قانونی روشن داشته و ضروری و متناسب

با هدف مشروع مورد نظر باشد. نظارت گسترده

و بدون ظن مشخص بر میلیون‌ها شهروند با

چنین معیارهایی به دشواری قابل توجیه است.

تعهد مد نظر ما فقط خودداری از نقض مستقیم

حقوق نیست؛ بلکه حاکمیت باید از شهروندان

در برابر سوءاستفاده شرکت‌ها و اشخاص

خصوصی از فناوری نیز حمایت کند. ایجاد نظام

حفاظت از داده‌های شخصی، تعیین محدودیت

برای پردازش داده‌های حساس و بیومتریک،

ایجاد سازوکار اعتراض به تصمیمات الگوریتمی

و تضمین امکان دادخواهی از جمله الزامات

آیا قوانین و ساختارهای حقوقی موجود

در ایران برای کنترل استفاده دولت از

هوش مصنوعی کافی هستند؟

خیر. در قوانین ایران مقررات پراکنده‌ای

وجود دارد که می‌توان برای حمایت از برخی

حقوق در فضای دیجیتال به آنها استناد کرد.

برای نمونه، اصل ۲۲ قانون اساسی از حقوق

اشخاص در برابر تعرض حمایت می‌کند و اصل

۲۵ نیز تعرض به مکاتبات و ارتباطات را جز در

موارد مقرر قانونی ممنوع می‌داند. قانون جرایم

رایانه‌ای نیز در بخش‌هایی دسترسی غیرمجاز

به داده‌ها یا سامانه‌ها را جرم‌انگاری کرده است.

اما این مقررات برای مواجهه با ویژگی‌های خاص

هوش مصنوعی طراحی نشده‌اند. پرسش‌هایی

مانند اینکه پلیس یا نهادهای امنیتی تحت چه

شرایطی حق استفاده از تشخیص چهره دارند،

داده‌های بیومتریک تا چه زمانی قابل نگهداری

است، آیا شهروند حق دارد بداند موضوع یک

تصمیم الگوریتمی قرار گرفته یا خیر و چه

نهادی الگوریتم‌های دولتی را ارزیابی می‌کند،

پاسخ حقوقی جامع و روشنی ندارند.

ایران از سال ۲۰۲۴ دارای سند ملی هوش

مصنوعی شده و ساختارهایی برای توسعه این

فناوری ایجاد کرده است، اما توسعه فناوری با

تنظیم حقوقی آن یکسان نیست. مساله اساسی،

ایجاد نظامی مستقل برای حفاظت از داده‌ها،

شفافیت الگوریتمی، ارزیابی اثرات حقوق بشری

و امکان نظارت قضایی موثر بر استفاده حکومت

از هوش مصنوعی است.

خطر در ایران شدیدتر است، زیرا فناوری در

یک خلاء سیاسی و حقوقی مورد استفاده قرار

نمی‌گیرد. هنگامی که نظارت هوشمند در کنار

محدودیت اینترنت، رصد شبکه‌های اجتماعی

و برخورد قضایی با منتقدان قرار گیرد، هوش

مصنوعی می‌تواند از یک فناوری عمومی به

هوش مصنوعی می‌تواند هزینه و زمان سرکوب

را به میزان قابل توجهی کاهش دهد. در گذشته

شناسایی هزاران نفر حاضر در یک تجمع مستلزم

بررسی دستی تصاویر بود؛ اما فناوری تشخیص

چهره بالقوه می‌تواند تصاویر دوربین‌های شهری

یا شبکه‌های اجتماعی را با پایگاه‌های اطلاعاتی

تطبیق دهد و افراد را با سرعت بسیار بیشتری

شناسایی کند. تحقیقات اخیر نیز از دستیابی

ایران به فناوری‌های پیشرفته تشخیص چهره

خبر داده‌اند.

این وضعیت علاوه بر حریم خصوصی، آزادی

تجمع و آزادی بیان را نیز تهدید می‌کند. اگر

شهروند بداند حضور او در یک تجمع، انتشار

یک تصویر یا حتی قرار گرفتن در کنار افراد

خاص می‌تواند توسط سامانه‌های هوشمند

استفاده احتمالی حکومتی مانند

جمهوری اسلامی از هوش مصنوعی در

حوزه‌هایی مانند نظارت، کنترل اجتماعی

و امنیت چگونه به نقض حقوق بشر در

ایران دامن زده است؟

فعالان اجتماعی و حقوق بشر چگونه

می‌توانند میان ظرفیت‌های هوش

مصنوعی و رعایت حقوقی مانند حریم

خصوصی، آزادی بیان و منع تبعیض

تعادل برقرار کنند؟

نخست باید از این تصور فاصله گرفت که

هوش مصنوعی ذاتاً در خدمت سرکوب یا ذاتاً

در خدمت آزادی است. همین فناوری می‌تواند

برای مستندسازی نقض حقوق بشر، تحلیل

حجم بزرگی از اطلاعات، شناسایی الگوهای

سرکوب، بررسی تصاویر و اسناد و تسهیل

دسترسی شهروندان به اطلاعات و خدمات



ما از عدالت سهمی داریم
دو هفته نامه الکترونیکی تخصصی حقوق بشر
صاحب امتیاز و مدیر مسئول:
سازمان حقوق بشر ایران / محمود امیری مقدم
سر دبیر این شماره: مریم نفوری
تماس با مجله: mail@iranhr.net

حقوقی مورد استفاده قرار گیرد. و موثر برای حفاظت از داده‌های شخصی و در مقابل، فعالان حقوق بشر باید اصل «حقوق بشر از مرحله طراحی» را مطالبه کنند؛ یعنی پیش از راه‌اندازی هر سامانه دولتی، آثار آن بر حریم خصوصی، تبعیض، آزادی بیان و سایر حقوق بنیادین بررسی شود. همچنین شهروندان باید بدانند چه اطلاعاتی از او جمع‌آوری می‌شود، مشخص و قابل نظارت مجاز بدانند. با چه هدفی پردازش می‌شود، چه نهادی به آن دسترسی دارد و تا چه زمانی نگهداری خواهد شد. جامعه مدنی همچنین می‌تواند موارد سوءاستفاده از هوش مصنوعی را مستندسازی کند، درباره فناوری‌های نظارتی آموزش عمومی ارایه دهد و از شرکت‌های فناوری نیز پاسخگویی بخواهد. در این زمینه نباید تمام مسئولیت متوجه شهروند باشد؛ اصل اساسی این است که حکومت باید ضرورت و قانونی بودن نظارت را اثبات کند، نه اینکه شهروند مجبور باشد بی‌گناهی خود را در برابر یک الگوریتم ثابت کند.

برای اینکه ایران در مسیر توسعه هوش مصنوعی با استانداردهای حقوق بشری حرکت کند، چه تغییرات یا اقداماتی ضروری است؟

نخستین ضرورت، تصویب یک قانون جامع و موثر برای حفاظت از داده‌های شخصی و تنظیم هوش مصنوعی است. این قانون باید داده‌های بیومتریک مانند تصویر چهره، صدا و سایر شناسه‌های زیستی را در شمار داده‌های حساس قرار دهد و جمع‌آوری و پردازش آنها توسط حکومت را تنها در شرایط استثنایی، مشخص و قابل نظارت مجاز بداند. دوم، استفاده دولتی از سامانه‌های پرخطر باید مشمول شفافیت و نظارت مستقل باشد. استفاده از تشخیص چهره در تجمعات، امتیازدهی یا طبقه‌بندی شهروندان بر اساس رفتار سیاسی و اجتماعی و تصمیم‌گیری کاملاً خودکار در موضوعاتی که بر آزادی، اشتغال، آموزش یا سایر حقوق اساسی افراد اثر می‌گذارد، باید ممنوع یا به شدت محدود شود.

در نهایت، هیچ قانون هوش مصنوعی بدون قوه قضاییه مستقل، رسانه آزاد، جامعه مدنی فعال و امکان دادخواهی موثر نمی‌تواند از حقوق شهروندان حفاظت کند. مساله اصلی این نیست که ایران هوش مصنوعی داشته باشد یا نداشته باشد؛ مساله این است که فناوری در خدمت شهروند قرار گیرد، نه اینکه به ابزاری برای نظارت دائمی، تبعیض، خاموش کردن اعتراض و توسعه ظرفیت سرکوب تبدیل شود.