

«دیپ فیک» تیغ برنده مجرمان سایبری در آینده

میترا جلیلی خبرنگار

هوش مصنوعی (AI) یکی از فناوری های نوظهور است که این روزها با سرعتی بالا در حوزه های مختلف از بازی و سرگرمی گرفته تا آموزش، سلامت، روایات ها، امور مالی و بانکداری، کشاورزی، حمل و نقل و ترافیک و... به کار گرفته می شود. هرچند هدف فعالان حوزه هوش مصنوعی، تنها رفاه مردم جهان و سرعت بخشیدن به روند اجرای پروژه های مختلف بوده است اما قابلیت های عظیم این فناوری توجه مجرمان سایبری را نیز جلب کرده و با روش های گوناگون به دنبال سوءاستفاده از هوش مصنوعی هستند که این موضوع نگرانی هایی را رقم زده است. اما بیشترین خطرات این فناوری پرکاربرد در سال های آینده کدام هستند؟

۴ بررسی خطرات هوش مصنوعی با شاخص

پس از ارائه گزارش دانشمندان یک دانشگاه تحقیقاتی واقع در لندن با نام UCL (University College London) و هشدار آنها درباره خطرات بالقوه هوش مصنوعی در آینده، یک نشست دوازده با حضور ۳۱ متخصص حوزه هوش مصنوعی برگزار شد تا مخاطرات این فناوری در ۱۵ سال آینده مورد بحث و بررسی قرار بگیرد. هرچند ابتدا قرار بود برخی از دانشجویان و علاقه مندان به این حوزه نیز در این نشست حضور داشته باشند ولی به دلیل شیوع کرونا این موضوع عملی نشد و این نشست با جمعیتی کمتر از حد انتظار برپا شد. در مقابل، تعداد بیشتری از علاقه مندان موفق شدند بحث و گفت وگوهای این نشست را در فضای مجازی و به صورت آنلاین مشاهده کنند.

در این نشست از اقشار دانشگاهی، بخش خصوصی، پلیس، دولت و آژانس های امنیتی دولتی حضور داشتند و شرکت کنندگان بر اساس چهار شاخص، نگرانی های خود از هوش مصنوعی در آینده را دسته بندی کردند. یکی از این شاخص ها میزان زمانی است که هوش مصنوعی می تواند برای کند، بتناسیل هوش مجرمان و اینکه هوش مصنوعی چقدر می تواند انجام یک سندباکس یا مقررگذاری محیط آزمون نوعی تنظیم گری است که برای ایده های جدید بخصوص در حوزه فناوری های مالی (فین تک ها) که پیامدها و ابعاد اجرای آنها برای حاکمیت شناخته شده نیست، مورد استفاده قرار می گیرد. به عبارتی موضوع و ایده ای که از سوی یک شرکت به عنوان یک ایده نو مطرح شده و عموماً به حوزه های فناوری ارائه جدید و نوپدید زنجیره های بلوکی و رمزارزها مربوط می شود، یک تنظیم گر حاکمیتی و بخشی مانند بیمه، بورس، حوزه بانکی یک محیط آزمونی که مشتمل بر رویه ها، قواعد و ساختار نظارت است، ایجاد می کند.

در سال های گذشته نیاز به ایجاد چنین محیطی جهت بررسی و تحقیقات میدانی در این خصوص به وضوح ملموس بود و توسط بسیاری از فعالان در حوزه فناوری های نوین پیشنهاد شده بود. بعضی از آثار، عوارض و نواقص گاه برای بانیان طرح نیز ناشناخته بوده که این مصوبه برای فناوری های نوظهور فرصتی جهت پایش، رصد و تحلیل نتایج ایجاد کرده که به اصلاح، تدوین و طی مراحل پیاده سازی و حتی قانونگذاری کمک شایانی خواهد کرد.

مشکل اساسی در کسب و کارهای نوپا در حوزه فناوری بلاکچین، خلاهای قانونی است. مشکلات این حوزه اکثراً حول محور تعدد و ناآشنایی مشاوران و تصمیم سازان نسبت به فناوری های نوین است و فرصت سوزی ها بیشتر به زمانی برمی گردد که صرف ایجاد آشنایی و رفع ابهامات این افراد و فناوری ها می شود. در این شرایط ایجاد محیط آزمونی برای بررسی میدانی طرح ها و پروژه های مبتنی بر فناوری های نوظهور می تواند تسریع کننده مراحل قانونگذاری و عاملی در جهت تسریع در بررسی، تکمیل و بهرپوری از طرح ها شود. چه بسا گاهی طرح های مطرحه دارای اثرات و موانعی است که در محیط آزمون نمود یافته و بدین ترتیب فرصت بررسی جهت دفاع یا اصلاح طرح مهیا می شود.

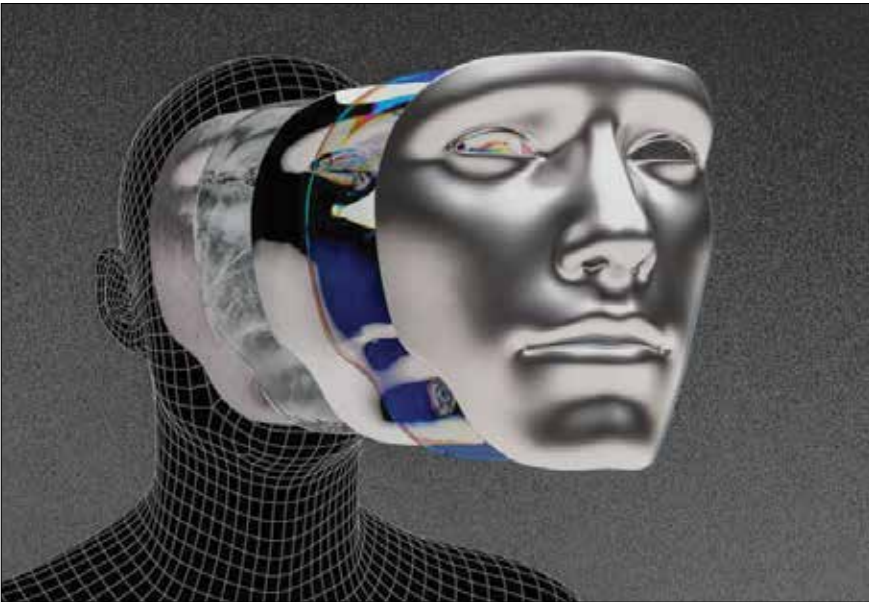
از آنجایی که هر فعالیت اقتصادی در ابتدا نیازمند دریافت مجوز فعالیت بوده و کسب مجوز اعتبار کسب و کار را در پی دارد و این امر در کسب و کارهای نوپا (بدلیل عدم شناخت عموم جامعه) از اهمیت بیشتری برخوردار است، مشکلات متعددی در همان بدو امر (تا مشخص بودن نهاد یا نهادهای متولی و صادرکننده مجوز فعالیت، فرآیند صدور مجوز، الزامات اخذ مجوز و...) نمود می یابد که عمدتاً ریشه در عدم شناخت و پذیرش حاکمیت سبب به کسب و کارهای نوین دارد. بهره گیری از حمایت های بیمه ای حق عمومی فعالان اقتصادی است که خود نیز به دلیل موارد فوق می شود. و در نهایت شاهد مشکلات دیگری مانند مالیات، مطالبات و دعاوی حقوقی و... خواهیم بود که عمدتاً ریشه در یک موضوع دارند و در بسیاری موارد سبب ناکامی کسب و کارها می شوند.

قطعاً پیاده سازی هر طرح نیازمند مقدمات و بسترهای مناسب است. مهم ترین موضوع بهره گیری از کارشناسان آگاه جهت بررسی، تأیید و پیاده سازی خواهد بود کارشناسانی که باغدغه این فعالیت ها آشنا بوده و از سر مسئولیت نسبت به بررسی اقدام کنند. محیط آزمون نیز باید متناسب با طرح بوده و امکان پیاده سازی را فراهم کند و نهایتاً دآوری و بررسی باید در عین بی طرفی و با تسلط بر موضوع صورت پذیرد.

تکنولوژی های نوظهور به شمار می رود و به نظر می رسد باید چنین نشست هایی در زمینه سایر فناوری ها نیز برپا شود تا بتوان با ابزاری قویتر به مقابله با مجرمان سایبری پرداخت.

■ خطرسازی هوش مصنوعی

نخستین موضوعی که در این نشست مورد بررسی قرار گرفت خطرات بالای هوش مصنوعی در آینده بود که در رأس آنها فناوری دیپ فیک (Deep Fake) قرار دارد. از نگاه فعالان حوزه هوش مصنوعی، دیپ فیک ها این توانایی را دارند که اخبار را نیز تحت تأثیر قرار دهند و به راحتی یک خبر جعلی را در کوتاه ترین زمان ممکن به دست مردم برسانند. با وایرال شدن یک ویدئوی دستکاری شده، به زحمت می توان برای کاربرانی که با سرعت درحال دست به دست کردن این ویدئوهای تقلبی هستند یادآور شد که موضوع چیز دیگری است و این ویدئو اصلی نیست. دیپ فیک همچنین می تواند دموکراسی را در برخی کشورها مورد حمله قرار دهد به عنوان مثال در امریکا سخنرانی دستکاری شده ناسی پلوسی رئیس مجلس نمایندگان امریکا با فناوری دیپ فیک در سال گذشته، بیش از ۲۰۵ میلیون بازدید در فیس بوک داشت و این موضوع نگرانی های زیادی را ایجاد کرد. مقابله با دیپ فیک برای



امریکا که اکنون در آستانه انتخابات ۲۰۲۰ قرار گرفته بشدت حیاتی است چراکه این فناوری می تواند به راحتی در نتیجه انتخابات تأثیر گذار باشد.

مؤسسه تحقیقاتی Future Advocacy در بریتانیا نیز در این نشست نمونه هایی از دیپ فیک ها در فضای سیاسی کشورهای مختلف را به عنوان نمونه ارائه کرد. هرچند برخی ویدئوهای دیپ فیک که به طور مشابه از هوش مصنوعی برای ایجاد فیلم های جعلی استفاده کرده بودند هیچ خطری منوجه جامعه نمی کردند اما نشان از پتانسیل دیپ فیک، برای تأثیر گذاری در دنیای سیاست و ایجاد تغییراتی ناخواسته دارند. با اینکه اکنون با کمک برخی الگوریتم ها می توان دیپ فیک های آنلاین را تشخیص داد ولی همچنان راه های بسیاری برای انتشار این ویدئوهای دستکاری شده وجود دارد که این موضوع می تواند سبب بی اعتمادی مردم به محتواهای صوتی و تصویری شود.

یکی دیگر از مواردی که در رده خطرهای بالای هوش مصنوعی قرار می گیرد، خودروهای خودران هستند. در این زمینه عنوان شد امکان دارد در آینده از این خودروهای بدون سرنشین به عنوان مکانیسمی برای حمل و انتقال مواد منفجره و اسلحه

بود که در این نشست مطرح شد.

■ سلامت، در تیررس مجرمان سایبری

شرکت کنندگان در این نشست به نگرانی های خود در زمینه خطرات میانی خود در زمینه توسعه هوش مصنوعی نیز اشاره کردند. کلاهدرداری و فروش سرویس ها و محصولات با سوءاستفاده از عنوان هوش مصنوعی و همچنین تبلیغات هدفدار، در این دسته از نگرانی های متخصصان حوزه هوش مصنوعی جای می گیرد. این نگرانی ها وقتی بیشتر می شود که پای سلامت مردم در میان باشد. سوءاستفاده از هوش مصنوعی در زمینه سلامت و کلاهدرداری هایی که در تبلیغات و... با کمک هوش مصنوعی انجام می گیرد در این دسته جای می گیرند. یکی از نمونه های آن هم تبلیغات دارو از زبان پزشکان با سوءاستفاده از فناوری هوش مصنوعی و در قالب دیپ فیک است که می تواند بسیار در دساز و نگران کننده باشد.

بخشی دیگری از این نگرانی ها سوءاستفاده از روایات های نظامی و خودروها کمک بگیرند. از دیگر موارد خطرناک استفاده از هوش مصنوعی می توان به فیشینگ های سازماندهی شده با استفاده از قابلیت فناوری هوش مصنوعی اشاره کرد که می تواند هم نشأت اطلاعاتی بسیار گسترده ای به همراه داشته باشد و هم به سیستم های بانکی ضربتی جبران ناپذیر وارد کند.

ایجاد اختلال عمدی در سیستم های هوش مصنوعی نیز یکی از بزرگترین خطرات این فناوری به شمار می رود چرا که این اختلال می تواند بسته به توان فرد یا گروه ایجادکننده این اختلال، در دسرها و خسارات جدی ایجاد کند. یکی از مواردی که بسیاری از خطررات را فناوری به آن اشاره دارند روایات های قاتل هستند. این افراد معتقدند در آینده امکان دارد افرادی که صلاحیت لازم را ندارند هوش مصنوعی به کار رفته در روایات ها را تحت کنترل خود درآورند تا این روایات ها عملاً همه خواسته هایشان را عملی کنند. لزوماً همه این خواسته ها اخلاقی نیستند و گاه می توانند در دسر زیادی برای یک جامعه ایجاد کنند. باج خواهی ها و اخاذی های گسترده نیز بخشی دیگر از نگرانی های عمده ناشی از سوءاستفاده از هوش مصنوعی در آینده می برند.

چگونه پهنای باند و مصرف اینترنت را مدیریت کنیم



خود را مشاهده کنید. ازسوی دیگر می توانید مصرف و ترافیک خود را محدود و برنامه ریزی کنید تا اینترنت شما بی دلیل و فقط برای وب گردی های بی هدف، مصرف نشود. از ویژگی های این نرم افزار می توان به تخصصی نمایش جزئیات ترافیکی برای پردازش ها و کارهای مختلف دانلود و آپلود اشاره کرد. مدیریت مصرف هر یک از کاربران، کنترل کامل ترافیک در حال مصرف اینترنت شما و همچنین متعادل کردن مصرف کاربران در شبکه های کامپیوتری از دیگر مزایای

این نرم افزار به شمار می رود. با کمک این نرم افزار همچنین می توانید برای ترافیک جهانی، محدودیت تعیین کنید و همچنین شاهد نمایش حرفه ای و اختصاصی ترافیک و وضعیت شبکه باشید.

گفتنی است این نرم افزار حالت های مختلف High, Normal, Low, Block, Ignore, Limit, Drop, Delay دارد پس در هر حالتی می توان از آن بهره گرفت. از دیگر ویژگی های این نرم افزار، قابلیت رمزگذاری تمامی تنظیمات، پشتیبانی نسخه ۶۴ آ آی پی ها و نیز پشتیبانی از نسخه های ۶۴ بیتی ویندوز است. گراف های ویژه و اختصاصی نمایش فعالیت های اینترنتی و همچنین نمایش جزئیات مصرف هر یک از کاربران به صورت داده های دریافتی و ارسالی هم از دیگر مزایای این نرم افزار است. علاقه مندان برای بارگذاری رایگان این نرم افزار می توانند به وبسایت P30world.com مراجعه کنند.

طراحی یک ماوس خاص برای گیمرها



ال ای دی RGB استفاده شده که می توانند ۷ طیف رنگی را از موس بتایانند. Zephyr اکنون روی وب سایت کیک استارتز حدود ۶ هزار و ۵۰۰ دلار سرمایه جمع آوری کرده که ۴ برابر رقم پیش بینی شده است. گیمرها می توانند یک ماوس را با بهای ۸۹ دلار به هر حجت به قیمت ۱۶۹ دلار پیش خرید کنند. اگر همه چیز به خوبی پیش برود این محصول در اکتبر راهی بازار می شود و البته بهای آن هم بیشتر از زمان پیش فروش خواهد بود.

یکی دیگر در ساخت این ماوس به کار رفته تا بر حسب نیاز بتوان آن را به حالت گیم یا کار معمولی در دفتر تبدیل کرد. گفته می شود کمپانی سازنده، مدعی است که طول عمر این ماوس ۶۸ گرمی تا ۵۰ میلیون کلیک خواهد بود که طول عمر مناسبی برای یک ماوس بر کار به حساب می آید. این ماوس نسبت به نمونه های معمولی که عمدتاً ۱۲۰ گرم هستند بسیار سبک تر است. از سوی دیگر در ساخت این ماوس خاص از چراغ های

وزیر ارتباطات و فناوری اطلاعات:

تخلف ۶۰۰ میلیارد تومانی اپراتورها احراز شده است

«میزان گرانفروشی اپراتورها به مبلغ ۶۰۰ میلیارد تومان توسط سازمان تنظیم مقررات و ارتباطات رادیویی کشور احراز شده است.» به گزارش ایرنا، محمد جواد آذری جهرمی وزیر ارتباطات و فناوری اطلاعات با بیان مطلب فوق افزود: «میزان گرانفروشی و تخلف اپراتورهای کشور از سوی سازمان تنظیم مقررات و ارتباطات رادیویی کشور به شعبه تعزیرات ارسال شده است و در این خصوص دادگاهی تشکیل شده و دادگاه با توجه به ضوابط خود احکامی را صادر خواهد کرد. عمل کردن بر خلاف مقررات و در جهت ظلم به مردم، اتفاق ناخوشایندی است که ما با قاطعیت با آن برخورد خواهیم کرد.

وزیر ارتباطات اعلام کرد: گزارش های سال مالی که از سوی شرکت های اپراتورها اعلام شده است و بر اساس آن مالیات پرداخت می کنند، حکایت از سودهای چند هزار میلیارد تومانی در سال گذشته دارد.

وی افزود: شیوع کرونا استفاده مردم از اینترنت را بالا برده است و بر اساس گزارش هایی که وجود دارد در برخی از ماه ها در آمد آنها رشد ۴۰ درصدی داشته است.

جهرمی افزود: هزینه های اپراتورها مانند اجاره مکان، مسائل فنی و نیروی انسانی ثابت است، اما درآمدشان رشد بسیار خوبی داشته است. بنابراین افزایش تعرفه آنها توجیه اقتصادی ندارد. البته برخی اپراتورها عنوان کردند برای حمایت از محتوای داخلی و رشد پیام رسان این اقدامات را انجام داده اند، اما باید گفت در تمام مدتی که تعرفه ها افزایش پیدا کرده نه تنها در مصرف پیام رسان های داخلی رشدی اتفاق نیفتاده بلکه استفاده از پیام رسان خارجی نیز با کاهش مواجه نشده است.

اواشاره کرد: سیاست محدودسازی اینترنت های بسته های اینترنت ثن می دهد عملاً مصرف ترافیک داخلی در برخی اپراتورها کاهش پیدا کرده و در واقع این سیاست بر ضد خودشان عمل کرده است.

وزیر ارتباطات افزود: بحث سوم در حوزه مقررات است که اقدام خلاف مقررات وضع شده است. وزارت ارتباطات و سازمان تنظیم مقررات برای برخورد با این تخلف، اختیاری تا حد جرمه دو میلیارد تومانی را داشت که انجام شد. پس از آن از دولت درخواست شد اختیارات بیشتری به این وزارتخانه بدهد تا بتواند با تخلفات، جدی تر برخورد کند.

اواشاره کرد: ۲۱ مرداد این مصوبه صادر شد و بر اساس آن اگر تا ۴۸ ساعت بسته ها به حالت اول برنگردد ما مجاز هستیم روزانه برای همراه اول حدود ۱۲ میلیارد تومان و برای اپراتور ایرنسل ۱۲ میلیارد تومان جرمه اعمال کنیم.

جهرمی با اشاره به اینکه مردم به دنبال این هستند تا بداندن اعمال جرمه ها چه سودی به حال آنها خواهد داشت، گفت: این جرمه ها به این دلیل است که اپراتورها با ملزم به تبعیت از مقررات کند. بحث دیگر تخلف از مقررات است. پرونده تخلف این دو اپراتور به سازمان حمایت مصرف کننده ارجاع داده شده است و روز گذشته سازمان حمایت، این تخلف را گرانفروشی، تشخیص داد.

نماینده ویژه در دولت الکترونیک:

مشکلات فنی شبکه علمی حل می شود

نماینده ویژه ریاست جمهوری در امور دولت الکترونیک از اتصال بخش اعظمی از دانشگاه های بزرگ کشور تا ۱۵ شهریور به شبکه علمی خبر داد.

به گزارش مهر، نصرالله جهانگرد در همایش ملی تبادل تجربیات دانشگاه ها در اجرای آموزش الکترونیک در بحران کووید ۱۹ به تشریح روند پیشرفت شبکه علمی و مشکلات و چالش های آن در تکمیل شبکه پرداخت و اظهار کرد: در برنامه پنجم و ششم توسعه، پروژه شبکه علمی به وزارت ارتباطات واگذار شده است. در حال حاضر تعداد کمی از دانشگاه های تهران به این شبکه متصل هستند و دانشگاه های خارج از تهران به ندرت به این شبکه متصل شده اند.

نماینده ویژه ریاست جمهوری در امور دولت الکترونیک با اشاره به اینکه در حال حاضر نه می توان گفت این پروژه اجرایی شده و نه می توان گفت اجرا نشده است، افزود: در سال های اخیر این پروژه بین سازمان های علمی دست به دست شد و در نهایت مجدد به سازمان پژوهش های علمی و صنعتی ایران و یک شرکت خصوصی محول شد. وی ادامه داد: در دوره آقای جهرمی در وزارت ارتباطات، ایشان بر تکمیل این پروژه تأکید کردند و گفتند اگر مشکلی وجود دارد، خودمان برای حل مشکل اقدام کنیم.

جهانگرد با بیان این مطلب که در همین راستا با مخابرات گفت وگوها شروع شده و امیدواریم طی روزهای آینده مشکلات فنی این پروژه حل و فصل شود، تصریح کرد: آن شالائه تا ۱۵ شهریور بخش اعظمی از دانشگاه های بزرگ به شبکه علمی وصل شوند و تجهیزات لازم برای تکمیل آن نیز فراهم خواهد شد.

نماینده ویژه ریاست جمهوری در امور دولت الکترونیک با اشاره به اینکه در اجرایی کردن پروژه شبکه علمی، بحث بهره برداری حائز اهمیت است، افزود: امیدواریم این موضوع با همکاری وزارت ارتباطات، وزارت علوم و ریاست جمهوری به سرانجام برسد.

فیس بوک ۲۲.۵ میلیون پست ممنوعه را حذف کرد



شرکت فیس بوک در سه ماهه دوم امسال ۲۲.۵ میلیون پستی که سیاست های این شرکت در خصوص نفرت پراکنی را نقض کرده بودند، حذف کرد که بیش از دو برابر پست های حذف شده در سه ماهه نخست بود.

به گزارش ایسنا، فیس بوک اعلام کرد حدود ۹۵ درصد از این پست های نفرت پراکنی را با استفاده از سیستم های نرم افزاری اتوماتیک و بدون اینکه کاربران آنها را گزارش دهند، حذف کرده است. این آمار نشان داد که چگونه فیس بوک ۱.۵ میلیارد اکانت جعلی و میلیون ها پست نفوذ کننده سیاست عدم نفرت پراکنی و تروریسم را طی مدت مذکور حذف کرده است.

بر اساس گزارش بلومبرگ، «گروه ها و صفحات» خصوصی فیس بوک که به گروه دست راستی افراطی QAnon اختصاص یافته، میلیون ها هوادار در این شبکه اجتماعی دارد. گزارش اخیر فیس بوک به این گروه اشاره ای نکرده است.

فیس بوک همچنین اعلام کرد هفت میلیون پست را برای اشتراک گذاری اطلاعات نادرست درباره ویروس کرونا حذف کرده ماهه دوم حذف کرده است.