اخبار

## چرا سکوهای ایرانی باید محل ساختن آینده دیجیتال ایران باشند؟

سخنگوی مرکز ملی فضای مجازی گفت: ما به سکوهایی نیاز داریم که نه فقط زنده بمانند، بلکه بتوانند رشد کنند، سرمایه جذب کنند، بازار بسازند و در نهایت بخشی از اقتصاد دیجیتال ایران را شکل بدهند. به گزارش مهر به نقل از مرکز ملی فضای مجازی، حسین دلیریان، سخنگوی مرکز ملی فضای مجازی در یادداشتی نوشت: برای فهم جامعه امروز ایران، دیگر نمی‌توان فقط به آمارهای رسمی، گزارش‌های رسانه‌ای یا پیمایش‌های سنتی تکیه کرد. بخش قابل توجهی از نبض جامعه، در فضای مجازی می‌تپد؛ جایی که مردم در آن خبر می‌گیرند، تحلیل می‌کنند، خرید و فروش می‌کنند، سرگرم می‌شوند، کسب‌وکار راه می‌اندازند و درباره مسائل مورد علاقه و نگرانی خود گفت‌وگو می‌کنند. «رادار فضای مجازی» از همین منظر اهمیت پیدا می‌کند: تلاش برای دیدن و فهمیدن آن چیزی که در سطح رفتار واقعی کاربران ایرانی در حال رخ دادن است. یکی از آخرین برش‌های این رصد، تصویری معنادار پیش روی ما می‌گذارد: در مردادماه، موضوعات مورد توجه کاربران ایرانی دو سکوی ایرانی در یک نمونه رصد شده به ۴۵ میلیارد بازدید رسیده است. در میان این موضوعات، محتواهای مربوط به «طلا»، «تنگه هرمز» و «بنزین» از جمله موضوعات داغ فضای مجازی بودند. پشت هر کدام از این موضوعات، بخشی از دغدغه، کنجکاوی، نیاز یا گفت‌وگوی جامعه ایرانی قرار دارد. کاربر ایرانی همزمان درباره اقتصاد، امنیت، سیاست خارجی، معیشت و هویت ملی خود در فضای مجازی می‌نویسد و می‌خواند. بنابراین، فضای مجازی را دیگر نمی‌توان فقط یک ابزار ارتباطی یا یک صنعت سرگرمی دید؛ این فضا اکنون بخشی از زیرساخت اجتماعی و اقتصادی کشور است.

## درخواست وزیر ارتباطات برای تعیین تکلیف فوری IPV۶

پروتکل اینترنت نسخه ۶ یا به اختصار IPv۶ جدیدترین نسخه پروتکل اینترنت است که ارتباط‌های اینترنتی بر پایه آن شکل می‌گیرد و فضای بسیار بزرگ‌تری برای اتصال دستگاه‌ها فراهم می‌کند؛ وزیر ارتباطات بر همین اساس خواستار تعیین تکلیف فوری IPV۶ شده است. به گزارش ایسنا، سید ستار هاشمی وزیر ارتباطات و فناوری اطلاعات اخیرا خواستار بررسی سریع محدودیت‌های IPV۶ شده و تاکید کرده که اگر برای این محدودیت‌ها مصوبه قانونی وجود ندارد، دلیلی برای ادامه آنها نیست.

### اما IPV۶ چیست؟

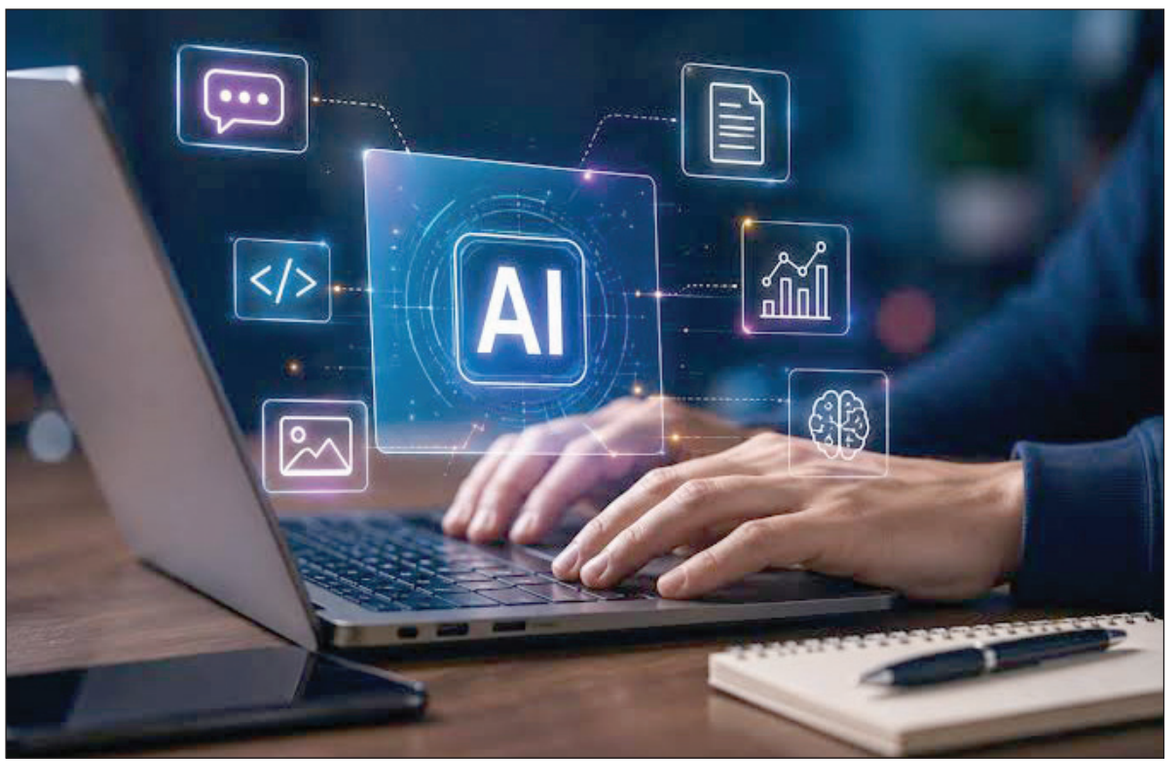
خانواده‌ای را تصور کنید که دارای جمعیت زیادی است و ناچار است در یک آپارتمان بسیار کوچک و اصطلاحا نقلی سکونت کند. آنها برای داشتن فضای کافی باید مدام دنبال یک خانه بزرگ‌تر باشند. IPV۶ حکم این خانه جادار و بزرگ را دارد. پروتکل IPV۶ نسل جدید سیستم آدرس‌دهی IP با فضای آدرس‌دهی بزرگ‌تر و قابلیت پشتیبانی از دستگاه‌های بیشتر نسبت به IPV۴ است که چالش‌های کمبود آدرس در دنیای وب را برطرف می‌کند. پروتکل IPV۶ نسل جدید سیستم آدرس‌دهی IP با فضای آدرس‌دهی بزرگ‌تر و قابلیت پشتیبانی از دستگاه‌های بیشتر نسبت به IPV۴ است که چالش‌های کمبود آدرس در دنیای وب را برطرف می‌کند. آدرس IP مجموعه‌ای از اعداد است که به دستگاه‌های مختلف در شبکه مثل رایانه، تلفن‌های هوشمند و وب‌سایت‌ها هویت منحصربه‌فردی می‌دهد تا جایی که این آدرس‌ها مثل کدپستی عمل می‌کنند و به دستگاه‌ها می‌گویند چگونه با یکدیگر ارتباط برقرار کنند. IPV۶ در حقیقت نسل جدید آدرس‌های اینترنت است. در حال حاضر هر دستگاه متصل به اینترنت به یک آدرس IP نیاز دارد. IPV۶ نسل جدید این سیستم آدرس‌دهی است که فضای بسیار بزرگ‌تری برای اتصال دستگاه‌ها فراهم می‌کند. فضای آدرس‌دهی نامحدود، سادگی و کارایی، اتصال امن و مستقیم، پیکربندی خودکار، مسیریابی سریع‌تر، امنیت بیشتر با IPSec از مهم‌ترین ویژگی‌های IPv۶ است. مشکل از IPV۴ شروع می‌شود زیرا آدرس‌های قدیمی محدود شده‌اند. تعداد آدرس‌های IPV۴ محدود است، به همین دلیل اپراتورها ناچارند گاهی تعداد زیادی کاربر را پشت یک آدرس عمومی مشترک قرار دهند. این محدودیت باعث پیچیده‌تر شدن شبکه می‌شود. اشتراک یک IP میان کاربران، مدیریت شبکه را دشوارتر می‌کند و می‌تواند بعضی از ارتباطات مستقیم، بازی‌های آنلاین و برخی سرویس‌های اینترنتی را با محدودیت روبه‌رو کند. در حال حاضر IPV۶ برای ایران اهمیت زیادی دارد زیرا اینترنت آینده دستگاه‌های بیشتری دارد. از 5G و اینترنت اشیا تا مراکز داده و خدمات دیجیتال، تعداد اتصال‌ها دایما بیشتر می‌شود. IPV۶ یکی از زیرساخت‌های لازم برای پاسخ به این رشد است و تاکید وزیر ارتباطات و فناوری اطلاعات دقیقا به همین دلیل مهم است. وزیر ارتباطات معتقد است شبکه ایران نباید در تقابل با فناوری‌های روز دنیا توسعه پیدا کند و محدودیت استفاده از IPV۶ باید هرچه سریع‌تر تعیین تکلیف شود. البته IPV۶ قرار نیست معجزه کند اما یک زیرساخت ضروری است. در حال حاضر نروژ، هلند و مالزی سه کشوری هستند که بیشترین میزان تغییر به IPv۶ را داشته و از این پروتکل استفاده می‌کنند. لازم به ذکر است که IPV۶ به تنهایی اینترنت را سریع‌تر نمی‌کند و به معنی رفع فیلترینگ نیست اما می‌تواند پیچیدگی‌های فنی شبکه را کمتر و آن را برای رشد آینده آماده‌تر کند.

### چالش‌های IPv۶ چیست؟

اگرچه از نظر فنی و امنیتی آدرس‌های آی‌پی نسخه ۶ برتری قابل توجهی نسبت به نسخه ۴ دارند، اما به دلیل هزینه‌های بالای انتقال زیرساخت استفاده از نسخه ۴ همچنان رایج‌تر است. مهاجرت کامل به IPV۶ به زمان و سرمایه‌گذاری زیادی نیاز دارد در نتیجه اغلب سازمان‌ها ترجیح می‌دهند عطای آن را به لقایش ببخشند با این وجود دیر یا زود شاهد درخشانی آینده IPV۶ خواهیم بود. یکی از تفاوت‌های کلیدی بین IPV۶ و نسخه قبلی آن، ساختار آدرس‌دهی آنهاست. IPV۶ از آدرس‌های ۱۲۸ بیتی استفاده می‌کند که فضای آدرس‌دهی بسیار بزرگ‌تری را در مقایسه با آدرس‌های ۳۲ بیتی IPV۴ ارایه می‌دهد. هر دستگاه متصل به شبکه صاحب یک آدرس IP نسخه ۶ منحصربه‌فرد می‌شود که فقط در محدوده زیرشبکه خود قابل شناسایی است. پروتکل اینترنت نسخه ۶ یا به اختصار IPV۶ جدیدترین نسخه پروتکل اینترنت (Internet Protocol) است که ارتباط‌های اینترنتی بر پایه آن شکل می‌گیرد.

## راهکاری برای عبور از بن‌بست دسترسی به دیتا در پروژه‌های هوش مصنوعی

# از مجوز داده تا پردازش امن




سال‌هاست کمبود و دسترسی دشوار به داده به عنوان یکی از اصلی‌ترین موانع توسعه هوش مصنوعی در ایران مطرح می‌شود؛ اما مساله لزوما نبود داده نیست، بلکه چگونگی استفاده از آن است. در بسیاری از پروژه‌ها، دستگاه دولتی داده را در اختیار دارد اما نگران افشا و مسوولیت حقوقی آن است و شرکت توسعه‌دهنده نیز بدون دسترسی پایدار نمی‌تواند محصولی قابل اتکا بسازد. یک راهکار عملی می‌تواند این معادله را تغییر بدهد: پردازش داده در محیط حفاظت‌شده، بدون آنکه داده خام الزاما در اختیار انسان یا شرکت مجری قرار بگیرد.

داده در ایران کم نیست؛ آنچه کم است، راهی برای استفاده از آن بدون تحویل دادن افسار گسیخته داده خام است. بسیاری از پروژه‌های هوش مصنوعی نه به‌دلیل ضعف فنی، بلکه در نقطه‌ای متوقف می‌شوند که دستگاه دولتی باید داده حساس خود را در اختیار یک شرکت قرار بدهد. راه‌حل می‌تواند تغییر همین نقطه شروع باشد: به‌جای انتقال داده، امکان پردازش کنترل‌شده آن فراهم شود؛ به‌گونه‌ای که شرکت بتواند مدل خود را بسازد و ارزیابی کند، بدون آنکه الزاما داده خام را ببیند یا در اختیار داشته باشد.

### اختیار اقدام از قبل وجود دارد

وقتی صحبت از گره داده در توسعه هوش مصنوعی می‌شود، بخش قابل توجهی از بحث‌ها به اصلاح قوانین، تعارض منافع و همکاری نکردن دستگاه‌ها اختصاص پیدا می‌کند. این مسائل مهمند، اما برای شروع یک مسیر اجرایی لزوما نیازی به انتظار برای تصویب قانون جدید یا ایجاد نهاد تازه نیست. بر اساس ماده ۷ اساسنامه سازمان فناوری اطلاعات، طراحی و اصلاح معماری فناوری اطلاعات، پیشنهاد ضوابط و استانداردها، مدیریت مخاطرات و فراهم کردن ظرفیت ممیزی فناوری‌ها و فرآیندها در حوزه فعالیت این سازمان قرار دارد. آیین‌نامه استقرار چارچوب تعامل‌پذیری نیز این نقش را مشخص‌تر کرده و سازمان را مسوول تأمین الزامات فنی و ارزیابی بلوغ فنی و انطباق‌سنجی می‌داند. از سوی دیگر، در آیین‌نامه اجرایی بند «الف» ماده ۱۰۷ برنامه هفتم توسعه، زیرساخت اجرای و آموزش مدل‌های هوش مصنوعی بخشی از ابر دولت تعریف شده و تدوین ضوابط معماری، امنیت و حفاظت از داده نیز در چارچوب وزارت ارتباطات و همکاری وزارت اطلاعات قرار گرفته است. بنابراین، بخشی از ظرفیت حقوقی لازم برای طراحی الگوهای استفاده امن از داده از پیش وجود دارد. مساله اصلی این است که این اختیار تا چه اندازه به فرآیندی تبدیل شده که یک دستگاه و یک شرکت بتوانند با اتکا به آن، یک پروژه واقعی هوش مصنوعی را اجرا کنند.

### به‌جای تحویل داده، پردازش را مجاز کنیم

راهکار می‌تواند از تغییر یک پیش‌فرض آغاز شود: برای اجرای یک پروژه هوش مصنوعی، الزاما نباید داده خام در اختیار تیم توسعه قرار بگیرد. برای مثال، شرکتی را در نظر بگیریم که قرار است مدلی برای پیش‌بینی خرابی تجهیزات صنعتی طراحی کند. این شرکت به سابقه واقعی عملکرد تجهیزات نیاز دارد، اما لزوما نیازی نیست کارکنان آن بتوانند تک‌تک داده‌های عملیاتی را مشاهده کنند. می‌توان داده را در یک محیط حفاظت‌شده نگهداری و پردازش کرد، مدل را همان‌جا آموزش داد و تنها نتایج مجاز ارزیابی یا خروجی مورد تأیید را در اختیار مجری قرار داد. در چنین معماری‌ای، «دریافت داده خام»، «اجرای پردازش»، «دریافت نتیجه» و «دریافت فایل مدل» اختیارهای متفاوتی هستند و نباید به‌صورت خودکار به یکدیگر وابسته شوند. این رویکرد که می‌توان آن را در قالب معماری «هوش مصنوعی بدون اعتماد» یا ZTAI دنبال کرد، حضور و دسترسی انسانی به داده حساس را از ضرورت‌های معماری خارج می‌کند. انسان همچنان هدف، سیاست و حدود استفاده را تعیین می‌کند و مسوولیت دارد، اما اجرای روزمره پردازش می‌تواند در محدوده مجوزهای از پیش تعریف‌شده و به‌صورت کنترل‌شده انجام شود. نتیجه می‌تواند آموزش مدل با داده واقعی بدون مشاهده داده توسط تیم توسعه، ارزیابی کیفیت مدل با داده محرمانه و ارایه صرفا نتیجه مجاز، ثبت سوابق فرآیند برای ممیزی و حتی مشارکت چند دستگاه در یک تحلیل مشترک بدون انتقال نسخه‌ای از داده خام باشد. البته چنین راهکاری مجوز قانونی جدید ایجاد نمی‌کند. قوانین مربوط به مدیریت داده و اطلاعات ملی همچنان حدود پردازش، دسترسی و مسوولیت حفاظت را تعیین می‌کنند. موضوع اصلی، اجرای همان استفاده‌ای است که مجاز شده، اما با دسترسی انسانی محدودتر و امکان ارزیابی روشن‌تر رعایت حدود مجوز.

### سازمان فناوری اطلاعات از معماری تا اجرای الگوی مرجع

نقطه اثرگذاری سازمان فناوری اطلاعات می‌تواند تبدیل این امکان فنی به «الگوی همکاری» برای دستگاه‌ها و شرکت‌ها باشد. دستگاه دارنده داده نباید برای هر پروژه مجبور شود تمام مسائل معماری، امنیت و مسوولیت را از ابتدا حل کند و شرکت نیز نباید پیش از سرمایه‌گذاری، با ابهام درباره امکان استفاده از داده مواجه باشد. راهکار پیشنهادی، تدوین مجموعه‌ای از الگوهای مرجع برای کاربست‌های مشخص است؛ الگوهایی که ابتدا در یک پروژه واقعی آزمایش شوند و سپس با اعمال ملاحظات بخشی، در دستگاه‌های دیگر قابل استفاده باشند. در هر الگو باید هدف مجاز، نوع داده، محیط پردازش، حدود خروجی، مسوولیت طرفین و معیار ارزیابی مشخص باشد. این الگوها می‌توانند در چارچوب برنامه زیست‌بوم‌های دولت هوشمند و با مشارکت یک دستگاه میزبان، شرکت مجری و دانشگاه‌ها طراحی و آزموده شوند. به این ترتیب، خروجی پروژه فقط یک محصول هوش مصنوعی نخواهد بود؛ بلکه معماری آزموده‌شده و روش مشخصی برای استفاده از داده نیز تولید می‌شود. در این تقسیم کار، سازمان فناوری اطلاعات می‌تواند مسوولیت تخصصی خود در معماری و ایجاد مسیر پردازش حفاظت‌شده را دنبال کند. سازمان ملی هوش مصنوعی نیز در چارچوب ساختار جدید راهبری، می‌تواند اولویت‌های مشترک را پیگیری و موانع میان دستگاه‌ها را دنبال کند. معاونت علمی و ستاد هوش مصنوعی نیز ظرفیت ارتباط با شرکت‌ها و دانشگاه‌ها و حمایت از اجرای آزمایشی پروژه‌ها را در اختیار دارند. حتی فراخوان‌های موجود برای پروژه‌های هوش مصنوعی در حوزه‌هایی مانند پولی و بانکی و حمل‌ونقل می‌توانند محل مناسبی برای اجرای چنین الگوهایی باشند؛ به‌ویژه پروژه‌هایی که مساله مشخص، مجری و بهره‌بردار دارند اما دسترسی به داده حساس مانع اجرای آنها شده است. در نهایت، موفقیت این مسیر باید با شاخص‌های قابل اندازه‌گیری سنجیده شود: مدت زمان رسیدن از درخواست تا پردازش مجاز، هزینه همکاری، کیفیت خروجی و میزان کاهش نیاز به دسترسی انسانی به داده. اگر یک پروژه واقعی بتواند نشان دهد که داده حساس می‌تواند بدون تحویل گسترده و غیرضروری، برای حل یک مساله واقعی به کار گرفته شود، همان پروژه می‌تواند الگوی دستگاه‌های بعدی باشد. مساله داده در ایران شاید با یک قانون یا نهاد جدید حل نشود؛ اما می‌توان از ظرفیت‌های موجود برای تبدیل «اجازه دسترسی» به «امکان پردازش» استفاده کرد. گره اصلی، اکنون بیش از آنکه نبود اختیار باشد، نبود یک الگوی اجرایی آزموده‌شده است.

# «بیمه سایبری» به چه کار کسب‌وکارها می‌آید؟

حملات هکرها یکی از تهدیداتی است که با انگیزه‌های مختلف مالی، سیاسی، جاسوسی، خرابکاری و حتی تفریح با هدف نفوذ، تخریب یا باج‌گیری از سیستم‌ها و داده‌های محرمانه کاربران صورت می‌گیرد. در دنیای امروز فروشگاه‌های آنلاین، پلتفرم‌های تجارت الکترونیک و موسسات مالی و بانکی به دلیل هزینه‌های سنگین حملات سایبری بیش از پیش در معرض خطرند و پوشش بیمه سایبری برای آنها یک ضرورت مدیریت ریسک به شمار می‌رود. به گزارش ایسنا، امنیت سایبری یا (Cybersecurity) مجموعه‌ای از ابزارها، روش‌ها و فناوری‌هایی است که از سیستم‌ها، شبکه‌ها و داده‌های شما در برابر حملات دیجیتال، سرقت یا آسیب محافظت می‌کند؛ مثل زمان‌هایی که برای در خانه‌تان قفل محکمی نصب می‌کنید یا وقتی که از یک گوشی هوشمند استفاده می‌کنید یا کسب و کاری دارید که داده‌های مشتریان را مدیریت می‌کند. در ساده‌ترین تعریف امنیت سایبری به معنای ایجاد یک حصار دیجیتال پیرامون دارایی‌های اطلاعاتی شماست تا از دسترسی و نفوذ بیگانگان و تخریب آگاهانه یا ناآگاهانه داده‌ها در امان بماند. در تعریف آکادمیک، امنیت سایبری به معنای تمرین محافظت از سیستم‌ها، شبکه‌ها و برنامه‌ها در برابر حملات دیجیتال است. این حملات با اهدافی همچون دسترسی، تغییر یا نابودی اطلاعات حساس، باج‌گیری یا اخاذی از کاربران یا اختلال در فرایندهای عادی کسب‌وکار صورت می‌گیرد. حفاظت از محتوا و اطلاعات موجود و بهبود عملکرد سیستم‌های دیجیتالی از جمله اهداف اصلی امنیت سایبری به شمار می‌رود تا به بهترین شکل ممکن از خسارت‌های احتمالی، سوءاستفاده‌های ناشی از نفوذهای غیرمجاز، جرایم سایبری و سرقت اطلاعات جلوگیری شود. تهدیدات سایبری ممکن است در قالب هک کردن، نفوذ، برنامه‌های ضد آنتی‌ویروس، برنامه‌های مخرب و سایر اشکال حملات الکترونیکی باشد از این رو امنیت سایبری از ابزارها، تکنیک‌ها و استراتژی‌های متنوعی استفاده می‌کند تا شناسایی، پیشگیری، تشخیص و پاسخگویی به تهدیدات سایبری را ممکن سازد.

### تاریخچه امنیت سایبری

تاریخچه امنیت سایبری به اواخر دهه ۱۹۶۰ بازمی‌گردد. زمانی که استفاده از رایانه‌ها و شبکه‌ها در سازمان‌های دولتی و دانشگاهی آغاز شد. در دهه ۱۹۷۰ و ۱۹۸۰ با افزایش استفاده از اینترنت و شبکه‌های رایانه‌ای نیاز به امنیت سایبری بیشتر شد و مفاهیمی مانند رمزنگاری و فایروال‌ها توسعه یافتند. در دهه ۱۹۹۰ و ۲۰۰۰ با رشد چشمگیر تجارت الکترونیک و فناوری‌های وب، تهدیدات سایبری پیچیده‌تر شدند و امنیت سایبری به یک حوزه تخصصی با ابزارها و روش‌های پیشرفته‌تری مانند سیستم‌های تشخیص نفوذ و امنیت شبکه تبدیل شد. امروزه امنیت سایبری به یک ضرورت حیاتی برای حفاظت از اطلاعات در برابر تهدیدات پیشرفته و حملات سایبری تبدیل شده است.

### انواع امنیت سایبری

در حال حاضر امنیت سایبری حوزه‌های مختلفی را شامل می‌شود که هر کدام بخشی از دنیای دیجیتال را ایمن می‌کند. امنیت شبکه، امنیت ابری، امنیت نقطه پایانی، امنیت اینترنت اشیا، امنیت موبایل، امنیت برنامه‌ها، امنیت عملیاتی از جمله انواع امنیت سایبری به شمار می‌رود. در امنیت موبایل هدف حفاظت از گوشی‌ها و تبلت‌هایی است که به داده‌های سازمانی دسترسی دارند. در امنیت اینترنت اشیا، هدف شناسایی و ایمن‌سازی دستگاه‌های متصل به اینترنت است یا در امنیت شبکه حفاظت از زیرساخت شبکه و جلوگیری از دسترسی غیرمجاز از اهداف اصلی است. در راستای امنیت سایبری، بحث بیمه سایبری از اهمیت بسزایی برخوردار است. در دنیای امروز که تمامی کسب‌وکارها به نوعی با فضای دیجیتال و داده‌های الکترونیکی سر و کار دارند، بیمه سایبری نقش یک «سپر دفاعی» را در برابر خسارات مالی ناشی از حوادث دنیای مجازی بازی می‌کند.

### چرا به بیمه سایبری نیاز داریم؟

حقیقت آن است که در اقتصادی که بخش بزرگی از فعالیت‌ها به داده و زیرساخت دیجیتال وابسته است، مساله تنها جلوگیری از حملات سایبری نیست زیرا سازمان‌ها باید برای هزینه و پیامدهای روزی که ناگزیر گرفتار حمله می‌شوند آماده باشند. یک حمله سایبری ممکن است در عرض چند ساعت رخ بدهد اما تبعات اقتصادی آن می‌تواند ماه‌ها و سال‌ها ادامه داشته باشد. حملات سایبری از نوع باج‌افزارها، فیشینگ و هک کردن سیستم‌ها می‌توانند هزینه‌های سنگینی به دنبال داشته باشند. خسارات ناشی از توقف کسب و کار و درآمد از دست رفته، هزینه‌های بازگرداندن سیستم‌ها و بازیابی اطلاعات، آسیب به اعتبار و شهرت برند و هزینه‌های اطلاع‌رسانی به مشتریان در صورت لو رفتن اطلاعات آنها از جمله هزینه‌هایی است که حمله‌های سایبری ممکن است به بار بیاورند. کشور ما از نظر ساختار اداری، اقتصادی و زیرساختی کشوری بسیار گسترده است. وزارتخانه‌ها، بانک‌ها و موسسات مالی، سازمان‌های دولتی، نهادهای عمومی، شرکت‌های بزرگ صنعتی، اپراتورها، مراکز درمانی، دانشگاه‌ها، شهرداری‌ها، شرکت‌های خدماتی و هزاران کسب‌وکار خصوصی، هر کدام دارای سامانه‌ها و دارایی‌های اطلاعاتی خاص خود هستند. از سوی دیگر بخش قابل توجهی از زیرساخت‌های حیاتی کشور مثل برق و آب، انرژی، ارتباطات، نظام بانکی و سلامت به شبکه‌ها و سامانه‌های دیجیتال وابسته هستند. در چنین شرایطی تصور اینکه «امنیت سایبری کشور» توسط یک نهاد واحد مدیریت شود، عملا امکان‌پذیر نیست. هر دستگاه هم مسوولیت تخصصی خود را دارد و هم باید الزامات عمومی امنیت سایبری را رعایت کند. مثلا امنیت سایبری یک بانک تنها یک مساله فناوری اطلاعات نیست بلکه به استمرار خدمات مالی، حفاظت از اطلاعات مشتریان و اعتماد عمومی مربوط می‌شود و حمله به یک زیرساخت انرژی می‌تواند از یک رخداد فنی فراتر رفته و به مساله‌ای در سطح تداوم خدمات عمومی و امنیت ملی تبدیل شود. بیتا کیامهر، مدیرکل توسعه صنعت افتا سازمان فناوری اطلاعات چندی قبل در نشست تخصصی «شبکه‌های تاب‌آور، نقش بیمه در پایداری شبکه و زیرساخت» بیمه امنیت سایبری را یکی از دغدغه‌های مهمی عنوان کرد که در بخش حاکمیتی مورد توجه قرار گرفته است. او معتقد است از آنجا که موضوع بیمه سایبری، اطلاعات هستند و دارایی نامشهود به حساب می‌آیند برای بخش بیمه کشورمان که همیشه با دارایی‌های فیزیکی مثل ملک و خودرو مواجه بوده کمی ناآشناست. به گفته کیامهر، برآورد ارزش ملک و خودرو برای بیمه‌ها ملموس است ولی ارزش‌گذاری دارایی‌های ناملموس موضوع جدیدی برای بیمه‌هاست. امین ترابی -فعال حوزه امنیت سایبری و زیرساخت نیز در پنل «تحلیل حملات زنجیره‌ای به زیرساخت پرداخت» در جریان نمایشگاه الکامپ ۱۴۰۵ با اشاره به نقش ابزارهای مکمل مالی و مشارکت بخش خصوصی در ارتقای امنیت گفت: آن بخش از ریسک باقی‌مانده که پس از اقدامات امنیتی همچنان می‌تواند برای سازمان‌ها مساله ساز شود، باید از طریق صنعت بیمه مدیریت و منتقل شود. به گفته وی تنها راهکار موثر، اعتماد به توان بدنه شرکت‌های خصوصی و فعالان امنیت سایبری کشور و واگذاری بخشی از وظایف اجرایی و نظارتی به آنهاست. این فعال حوزه امنیت سایبری معتقد است که طرح اپراتور امنیت می‌تواند مسوولیت قانونی امنیت سازمان‌ها را تنفیذ کرده و امکان امن‌سازی و نظارت بر زیرساخت‌ها را فراهم کند. به گفته ترابی، بیش از ۹۰ درصد از حملات سایبری ناشی از نقاط ضعفی است که دانش پیشگیری از آنها در کشور و شرکت‌های تخصصی وجود دارد و در صورت استقرار اپراتورهای امنیت و بهره‌گیری از بیمه مسوولیت سایبری، می‌توان ریسک‌های باقی‌مانده را جبران کرده و خسارات مالی ناشی از حوادث را به حداقل رساند.

### اما چه کسانی به بیمه سایبری نیاز دارند؟

امروزه هر کسب‌وکاری که داده‌های دیجیتال مثل ایمیل مشتریان، اطلاعات کارت بانکی یا اسرار تجاری را نگهداری می‌کند، فروشگاه‌های آنلاین و پلتفرم‌های تجارت الکترونیک، شرکت‌های فناوری و نرم‌افزاری، موسسات مالی و بانکی، مراکز درمانی و بیمارستان‌ها به دلیل حساسیت بالای پرونده‌های پزشکی و هر شرکتی که دارای وب‌سایت یا شبکه داخلی متصل به اینترنت است در معرض ریسک و خطر است. هرچه کسب‌وکارها بیشتر به فناوری و داده وابسته می‌شوند، هزینه احتمال دیجیتال نیز به همان نسبت بالاتر می‌رود. در چنین شرایطی، توان یک سازمان برای پرداخت هزینه‌های یک حادثه و ادامه فعالیت به اندازه توان آن برای جلوگیری از حادثه اهمیت پیدا می‌کند. البته این نکته را نباید از نظر دور داشت که بیمه سایبری جایگزین امنیت نیست و داشتن بیمه به این معنا نیست که نیازی به فایروال، آنتی‌ویروس یا آموزش کارکنان وجود ندارد. بیمه‌گرها معمولا پیش از صدور بیمه‌نامه، استانداردهای امنیتی شما را بررسی می‌کنند. اکثر بیمه‌های سایبری، حوادثی که ناشی از خطاهای عمدی داخلی مثلا توسط کارمند خود شرکت یا جنگ‌های سایبری رسمی باشند را پوشش نمی‌دهند. ایجاد امنیت سایبری یک فرایند دائمی و چندلایه است؛ یعنی هیچ راه‌حل جادویی وجود ندارد که شما را ۱۰۰ درصد امن کند بلکه باید ترکیبی از روش‌های فنی، مدیریتی و آموزشی را به کار بگیرید. تدابیر فنی و روش‌های امنیت سایبری مثل دیواره آتش (Firewall) آنتی‌ویروس و ضد بدافزار، رمزگذاری، احراز هویت چندعاملی، به‌روزرسانی و تهیه نسخه پشتیبان از جمله روش‌هایی است که برای جلوگیری از هک کردن، نفوذ، برنامه‌های مخرب و دیگر حملات هکری به کار گرفته می‌شوند. به گزارش ایسنا، در حال حاضر بیمه سایبری مزایای متعددی دارد که می‌تواند به‌طور قابل توجهی به پایداری و امنیت مالی کسب‌وکارها در برابر تهدیدات دیجیتال کمک کند. بیمه سایبری اگر درست، طراحی و در کنار سایر ابزارهای مدیریت ریسک، استفاده شود می‌تواند بخشی از همین ظرفیت دوام آوردن باشد. آینده بیمه سایبری آینده مدیریت ریسک دیجیتال است؛ مسیری که در آن امنیت، تاب‌آوری و بیمه نه سه موضوع جداگانه بلکه سه بخش از یک مساله واحد خواهد بود. اینکه سازمان چگونه در جهانی که ریسک سایبری اجتناب‌ناپذیر شده است همچنان بتواند به فعالیت خود ادامه بدهد.

دنیای فناوری

## شرکت انگلیسی داده‌های مشتریانش را به هکرها داد

شرکت فناوری مالی انگلیسی «رولت» (Revolt) تایید کرد پس از دریافت درخواست‌های جعلی از سوی یک دامنه ایمیلی آژانس دولتی، داده‌های حساس مشتریانش برای یک طرف ثالث غیرمجاز فاش کرده است. به گزارش مهر به نقل از رویترز، سخنگوی این شرکت در بیانیه‌ای اعلام کرد: ما به محض ردیابی به سرعت آدرس را مسدود کردیم و به آژانس دولتی مرتبط و همچنین سازمان‌های مجری قانون، حفاظت از داده و رگولاتورهای مالی اطلاع دادیم. سیستم‌های رولت و سرمایه‌های مشتریان تحت تاثیر این رویداد قرار نگرفته‌اند. البته این سخنگو اطلاعات دیگری از جمله تعداد افرادی که تحت تاثیر این حمله قرار گرفته‌اند، را اعلام نکرد. داده‌های به خطر افتاده شامل تاریخ تولد مشتریان، آدرس پستی و آدرس ایمیل و شماره موبایل آنها در کنار کپی اسناد هویتی‌شان از جمله پاسپورت و گواهینامه رانندگی است. رولت یکی از موفق‌ترین شرکت‌های فناوری مالی اتحادیه اروپا به حساب می‌آید که هیچ شعبه فیزیکی ندارد.

## جاسوسی فناوری برای کشورهای خارجی در کره جنوبی جرم شد

قانون جاسوسی توسعه‌یافته کره جنوبی از امروز اجرایی می‌شود و دامنه جرایم جاسوسی را از اقداماتی که تنها کره شمالی را در بر می‌گرفت به همه کشورهای خارجی گسترش می‌دهد. به گزارش خبرگزاری مهر به نقل از رویترز، این اقدام در حالی اجرا می‌شود که کره سعی دارد با اتکا به آن از فناوری‌های کلیدی خود در بحبوحه تشدید رقابت در صنعت نیمه‌رساناها و دیگر صنایع راهبردی محافظت کند. مجلس ملی کره جنوبی نسخه اصلاح شده قانون کیفری را در فوریه ۲۰۲۶ میلادی و ۲۶ سال پس از انتقاد به آنکه قوانین فعلی برای مجازات خرابکاری صنعتی مرتبط با عامل‌های غیر از کره شمالی نامناسب است، اصلاح کرد. بندهای این قانون یک جرم جدید خلق می‌کنند که خرابکاری برای کشور یا سازمان خارجی را نیز دربر می‌گیرد و حداقل مجازات آن سه سال زندان است. قانون فعلی خرابکاری از سوی کشور متخاصم نیز همچنان پابرجاست. بر اساس قانون پیشین، اتهام جاسوسی عموما فقط شامل اقداماتی می‌شد که به نفع کره شمالی بود؛ در نتیجه، دادستان‌ها در بسیاری از پرونده‌های مرتبط با دولت‌ها یا شرکت‌های خارجی، ناچار بودند به قوانین دیگری درباره فناوری‌های صنعتی یا اسرار تجاری استناد کنند. سازمان ملی اطلاعات کره جنوبی از تصویب این قانون استقبال و اعلام کرد چنین اقدامی توانایی کشور در جلوگیری از نشت فناوری‌های استراتژیک مانند نیمه رساناها، نمایشگرها، باتری و هوش مصنوعی موثر است. کارشناسان حقوقی و امنیتی معتقدند این تغییرات حفره‌هایی قدیمی را می‌بندد که بیشتر اوقات سبب می‌شود موارد نشت فناوری‌های پیشرفته صنعتی با مجازات‌های سبک‌تری روبرو شوند. حامیان این قانون استدلال می‌کنند اقدام مذکور بازدارندگی در مقابل خرابکاری صنعتی را قدرتمندتر می‌کند. این تغییر پس از چند مورد پر سروصدای نشت فناوری رخ داد از جمله پرونده‌ای مربوط به سال گذشته که در آن پنج کارمند سابق سامسونگ به انتقال فناوری حساس تراشه DRAM به شرکت تراشه‌سازی چینی CXMT متهم شدند.

## مدیران هوش مصنوعی خواستار کندتر شدن پیشرفت آن شدند

ایلان ماسک و سم آلتمن از درخواست داریو آمودئی مدیر ارشد اجرایی آنتروپیک برای حضور بازبین‌های طرف ثالث در شرکت‌های پیشرو هوش مصنوعی به‌طور دایمی پشتیبانی کردند. به گزارش مهر به نقل از اسکای نیوز، داریو آمودئی مدیر ارشد اجرایی آنتروپیک مقاله‌ای با عنوان «ما باید در پیشروی مرزها شتاب زده عمل نکنیم» (We Must Pace the Frontier) را منتشر کرده که در آن از شرکت‌های فناوری می‌خواهد سرعت بهبود قابلیت‌های مدل‌های هوش مصنوعی را کندتر کنند. این مقاله در حالی منتشر می‌شود که نگرانی‌ها درباره سواستفاده از هوش مصنوعی شدت گرفته است. از سوی دیگر آنتروپیک اخیرا فاش کرده چند هکر از مدل‌های کلاود آن برای فعالیت‌هایی مانند توسعه اسلحه، عملیات‌های نظامی و نظارت و کلاهبرداری استفاده کرده‌اند. آمودئی در همین زمینه طرحی سه بخشی ارایه کرده که شرکتش نیز به آن متعهد است. او در پستی در شبکه اجتماعی ایکس نوشت: ما ارزیاب‌های طرف ثالث را با دسترسی دایمی و در سطح کارمندان برای سیستم‌هایمان فراهم می‌کنیم تا آنها بتوانند التزام‌مان به اقدامات ایمنی را تایید کنند، درباره رویدادها گزارش دهند و همسویی مدل‌ها طی آموزش را ارزیابی کنند. پس از آن ایلان ماسک مدیر ارشد اجرایی ایکس و سم آلتمن مدیر ارشد اجرایی اوپن‌ای‌آی نیز از این مقاله دفاع کردند. ماسک نیز پاسخ به پست آمودئی نوشت: داریو درست می‌گوید.

## حریم خصوصی کاربران اینستاگرام زیر ذره‌بین هوش مصنوعی متا

متا یک جنجال دیگر را پشت سر گذاشت و اعلام کرد مشکلی را برطرف کرده که در آن نرم‌افزار «متا‌ای‌آی» پرامپت‌هایی را به کاربران پیشنهاد می‌کرد که اطلاعات خصوصی کاربران را جمع‌آوری و آشکار می‌کرد. به گزارش مهر به نقل از سی‌نت، این جنجال از دوم سپتامبر آغاز شد؛ زمانی که «کیلی رابینز»، بلاگر حوزه فرزندپروری و سبک زندگی اینستاگرام، ویدیویی منتشر کرد و در آن درباره پست قبلی خود که در آن مشغول آواز خواندن همراه دخترش در صندلی عقب خودرو بود، صحبت کرد. رابینز در این ویدئو فاش کرد متا در بخش هوش مصنوعی خود، چند پرامپت نامتعارف مانند «چه کسی در صندلی کودک است؟» یا «کیلی رابینز کجا زندگی می‌کند