دریچه

ویژگی‌های هوش مصنوعی اپل برای توسعه‌دهندگان ارایه شد

در هفته جاری اپل نسخه بتا iOA18.1 را همراه برخی از آپدیت‌های اپل اینتلیجنس در اپ‌های فون، نوتس، فتوز، میل، رایتینگ و سیری ارایه کرد که توجهات زیادی را به خود جلب کرده است. به گزارش مهر به نقل از تک رادار، به نظر می‌رسد هوش مصنوعی اپل همه توجهات را به خود جلب کند. حتی در این مرحله اولیه کاملا واضح است که هوش مصنوعی اپل می‌تواند شیوه استفاده بهینه از آیفون را متحول کند اما باید توجه داشت این نسخه بتا برای همه قابل دسترسی نیست.

نام این آپدیت نیز نشان‌دهنده آن است که فقط برای توسعه‌دهندگان نرم افزار و جهت آشنایی آنها با نسخه آپدیت شده پلتفرم و قابلیت‌های هوش مصنوعی جدید اپل ارایه شده است. این قابلیت برای مصرف‌کنندگان نیست و البته تکمیل نیز نشده است. در این نسخه بتا قابلیت‌هایی مثل ادغام ChatGPT در آیفون و امکان استفاده از سیری برای کلید زدن اقدامات در اپلیکیشن‌های شخص ثالث در بتاهای آینده در اختیار توسعه‌دهندگان قرار می‌گیرد. توسعه‌دهندگان می‌توانند از طریق دکمه جدید Apple Intelligence و سیری در تنظیمات دستگاه به این قابلیت‌ها دسترسی یابند. همچنین اپل اعلام کرده پذیرش یک‌باره تعداد زیادی از کاربران بار بیش از حدی را بر سرور اعمال می‌کند، لیست انتظاری را برای توسعه‌دهندگان در نظر گرفته است. همانطور که قبلا اعلام شد، ویژگی‌هایی مذکور فقط روی آیفون ۱۵ و آیفون ۱۵ پرومکس قابل استفاده است.

آپدیت جذاب سیری

آپدیت سیری از بقیه به روزرسانی‌ها جذاب‌تر است. سیری ظاهر و انیمیشن تازه‌ای دارد اما جذاب‌ترین بخش آن تغییر لحن سخن گفتن سیری به شکل محاوره‌ای است وبه نسبت گذشته کمتر رباتیک به نظر می‌رسد. همچنین کاربر می‌تواند بین صحبت‌های سیری به بحث خود ادامه داده و از او سوال جدیدی بپرسید که حس واقعی‌تر از مکالمه را القا می‌کند.با این وجود سیری همچنان در پاسخ به سوالاتی با جزییات بالا به مشکل می‌خورد و همچنان از اجرای یک سری دستورهای ساده ناتوان است.

قابلیت‌های نگارشی جدید با هوش مصنوعی اپل

ابزارهای نگارشی (Writing Tools) شامل چندین ویژگی اپل اینتلیجنس برای کمک به نوشتن است. این قابلیت چیزی شبیه به Chat Assist در گلگسی اس ۲۴ اولترا است. اما هوش مصنوعی اپل گزینه‌هایی مثل لحن دوستانه، حرفه‌ای و غیره در اختیار کاربر قرار می‌دهد.

با انتخاب هر گزینه، اپل متن انتخاب شده را براساس لحن انتخابی شما بازنویسی می‌کند. شما همچنین می‌توانید از هوش مصنوعی بخواهید تا چکیده، لیست، جدول یا نکات کلیدی از ایمیل یا یک صفحه وب در اختیار شما بگذارد.

هوش مصنوعی در میل

نخستین موردی که در این زمینه جلب‌توجه می‌کند، پیام‌های اولویت‌داری است که در بالای این باکس نمایش داده می‌شود.هوش مصنوعی اپل با انتخاب هر ایمیل، گزینه‌ای برای خلاصه‌سازی در اختیار شما می‌گذارد و متن پیام دریافتی را به شکل فشرده برای کاربر بیان می‌کند. همچنین کاربر در اپ Notes، می‌تواند فایل صوتی را ضبط و به متن تبدیل کنید وهوش مصنوعی خلاصه‌ای در اختیار وی قرار می‌دهد. این قابلیت برای ضبط، نگارش و خلاصه‌سازی ارایه‌های طولانی و حتی کلاس درس کاربرد دارد. در اپلیکیشن فتوز، گزینه‌ای در اختیار کاربر قرار می‌گیرد که براساس تصاویر ثبت شده در آیفون یک ویدیو از خاطرات ایجاد می‌کند. کاربر می‌تواند توصیفی از آنچه می‌خواهد در اختیار اپل اینتلیجنس بگذارید تا نتیجه بهتری حاصل شود. علاوه بر آنچه گفته شد اپل از دو مدل متفاوت برای رایانش داخلی و ابری استفاده می‌کند.

مدل داخلی که با سخت افزار دستگاه اجرا می‌شود AFM-on-device نام دارد و شامل ۳ میلیارد پارامتر است.با این وجود اپل می‌گوید این مدل را برای بازدهی بهتر و پاسخ سریع در داخل دستگاه بهینه‌سازی کرده است. اما برای کارهای پیچیده‌تری که از طریق ابر پردازش می‌شوند، اپل از یک مدل بزرگ مستقر در سرور به نام AFM-server استفاده می‌کند. با اینکه اندازه و تعداد پارامترهای این مدل فاش نشده است، اما این مدل به گونه‌ای طراحی شده که با استفاده از زیرساخت ابری اپل و سیستمی به نام Private Cloude Compute فعالیت کند تا از داده‌های کاربران محافظت شود. این شرکت همچنین بر توسعه مسوولانه هوش مصنوعی و محافظت از حریم خصوصی در این مسیر تاکید کرده است. با اینکه تا عرضه نهایی Apple Intelligence در ماه اکتبر زمان زیادی باقی مانده است اما موفقیت این استراتژی بیش از آنکه به توانمندی‌های فنی آن بستگی داشته باشد، به مهارت اپل و ادغام کارآمد آنها در اکوسیستم این شرکت بستگی دارد.

بهره‌گیری از فناوری‌های پیشرفته، کارایی و شفافیت سیستم‌های دولتی را بهبود می‌بخشد

بروز و ظهور دولت هوشمند برای تحول در ارایه خدمات به شهروندان

دولت هوشمند به عنوان یکی از روندهای اصلی در حکمرانی مدرن، ظرفیت بالقوه‌ای برای ایجاد تحول در نحوه ارایه خدمات عمومی و تعامل با شهروندان دارد. این مدل حکمرانی می‌تواند با بهره‌گیری از فناوری‌های پیشرفته، کارایی و شفافیت سیستم‌های دولتی را بهبود بخشد و مشارکت فعال شهروندان را در فرآیندهای تصمیم‌گیری افزایش دهد. با این حال، دستیابی به یک دولت هوشمند موفق، نیازمند تلاش‌های گسترده و هماهنگ در چندین جبهه است.در دهه‌های اخیر، ظهور فناوری‌های نوین و تحول دیجیتال منجر به ایجاد مفهومی جدید در عرصه حکمرانی شده است که از آن به عنوان «دولت هوشمند» یاد می‌شود. دولت هوشمند به معنای استفاده از فناوری‌های اطلاعاتی و ارتباطی برای بهبود خدمات دولتی، افزایش شفافیت و مشارکت شهروندان در فرآیندهای تصمیم‌گیری است همچنین مجموعه‌ای از فرآیندها و ساختارهایی است که با استفاده از فناوری‌های پیشرفته مانند اینترنت اشیا، هوش مصنوعی، کلان داده‌ها و بلاک‌چین، تلاش می‌کند تا خدمات دولتی را کارآمدتر، شفاف‌تر و پاسخگوتر کند.مهر نوشت دولت هوشمند فراتر از دولت الکترونیک است و شامل ادغام فناوری‌ها برای ایجاد سیستمی یکپارچه و هوشمند است که قادر به تحلیل داده‌ها و اتخاذ تصمیمات هوشمندانه باشد.

مزایای دولت هوشمند

یکی از مزایای اصلی دولت هوشمند، بهبود کارایی در ارایه خدمات عمومی است. با استفاده از فناوری‌های پیشرفته، دولت‌ها می‌توانند فرآیندهای پیچیده و زمان‌بر را به صورت خودکار انجام دهند. برای مثال، در یک دولت هوشمند، درخواست‌های شهروندان برای خدماتی مانند صدور مجوزها یا پرداخت مالیات‌ها می‌تواند به صورت آنلاین و بدون نیاز به مراجعه حضوری انجام شود. این امر منجر به کاهش هزینه‌ها و افزایش سرعت در ارایه خدمات می‌شود. در نتیجه، شهروندان می‌توانند از خدمات بهتری بهره‌مند شوند و دولت‌ها نیز می‌توانند منابع خود را به‌طور موثرتری مدیریت کنند. از دیگر مزایای دولت هوشمند، افزایش شفافیت و کاهش فساد است. با استفاده از سیستم‌های شفافیت‌ساز مانند بلاک‌چین، امکان پیگیری و نظارت بر تمامی تراکنش‌ها و تصمیمات دولتی فراهم می‌شود. این امر موجب کاهش فساد و افزایش اعتماد عمومی به دولت می‌شود. برای مثال، در یک سیستم بلاک‌چین، تمامی تراکنش‌ها به صورت غیرقابل تغییر ثبت می‌شوند و هرگونه تغییر یا دستکاری در آنها به وضوح قابل مشاهده است. این شفافیت باعث می‌شود تا افراد نتوانند به راحتی در فرآیندهای دولتی دخالت کرده و فساد کنند.

مشارکت شهروندان در تصمیم‌گیری

یکی دیگر از ویژگی‌های برجسته دولت هوشمند، ایجاد پلتفرم‌های دیجیتال برای مشارکت شهروندان در فرآیندهای تصمیم‌گیری است. این پلتفرم‌ها به شهروندان امکان می‌دهند تا نظرات و پیشنهادات خود را به صورت آنلاین مطرح کنند و در تصمیمات عمومی مشارکت فعال داشته باشند. به عنوان مثال، در برخی کشورها، شهروندان می‌توانند از طریق اپلیکیشن‌های موبایل یا وب‌سایت‌های دولتی در نظرسنجی‌ها و مشورت‌های عمومی شرکت کنند. این نوع مشارکت فعال می‌تواند منجر به اتخاذ تصمیماتی شود که بهتر با نیازها و خواسته‌های جامعه هماهنگ باشند.

چالش‌های دولت هوشمند

با وجود تمامی مزایای دولت هوشمند، اجرای آن با چالش‌هایی نیز همراه است که باید به‌طور جدی مورد توجه قرار گیرند. یکی از چالش‌های اصلی دولت هوشمند، حفظ امنیت داده‌ها و سیستم‌ها در برابر تهدیدات سایبری است. با افزایش استفاده از فناوری‌های دیجیتال، خطر حملات سایبری نیز افزایش می‌یابد. این حملات می‌توانند منجر به نقض حریم خصوصی و اطلاعات حساس شوند. برای مثال، یک حمله سایبری موفق می‌تواند باعث دسترسی غیرمجاز به داده‌های شخصی شهروندان یا اطلاعات حیاتی دولتی شود. بنابراین، دولت‌ها باید به‌طور مداوم از تکنولوژی‌های امنیتی پیشرفته استفاده کنند و کارکنان خود را در زمینه امنیت سایبری آموزش دهند.

عدم دسترسی برخی اقشار جامعه به اینترنت

نابرابری در دسترسی به فناوری‌های دیجیتال یکی دیگر از چالش‌های دولت هوشمند است. عدم دسترسی برخی اقشار جامعه به اینترنت و دستگاه‌های دیجیتال می‌تواند منجر به نابرابری در بهره‌مندی از خدمات دولتی شود. به عنوان مثال، در مناطق روستایی یا کم‌درآمد، ممکن است دسترسی به اینترنت پرسرعت و دستگاه‌های هوشمند محدود باشد. این نابرابری می‌تواند باعث شود تا افراد نتوانند به خدمات دولتی آنلاین دسترسی پیدا کنند و از مزایای دولت هوشمند بهره‌مند شوند. دولت‌ها باید برنامه‌هایی برای ارتقای دسترسی به فناوری‌های دیجیتال در این مناطق اجرا کنند. اجرای دولت هوشمند نیازمند تغییرات اساسی در فرهنگ سازمانی و نحوه عملکرد کارکنان دولتی است. این امر ممکن است با مقاومت‌هایی از سوی کارکنان و نهادهای سنتی مواجه شود. به عنوان مثال، کارکنانی که به روش‌های سنتی کار عادت کرده‌اند، ممکن است در برابر تغییرات مقاومت کنند و از استفاده از فناوری‌های جدید خودداری کنند. بنابراین، برنامه‌های آموزشی و تغییر مدیریت باید به گونه‌ای طراحی شوند که کارکنان را به استفاده از فناوری‌های نوین ترغیب کنند و مقاومت‌های احتمالی را کاهش دهند.

کشورهای موفق در دولت هوشمند

یکی از نمونه‌های موفق دولت هوشمند، استونی است. این کشور با اجرای پروژه‌هایی مانند «e-Residency» و «X-Road»، توانسته است خدمات دولتی را به صورت کامل دیجیتال کند و امکان دسترسی شهروندان به خدمات را بهبود بخشد. در پروژه «e-Residency»، افراد از سراسر جهان می‌توانند به صورت آنلاین اقامت الکترونیکی استونی را دریافت کنند و از خدمات دولتی این کشور بهره‌مند شوند. این برنامه نه تنها خدمات دولتی را بهبود بخشیده بلکه فرصت‌های جدیدی برای کسب و کارها ایجاد کرده است. سنگاپور نیز یکی دیگر از نمونه‌های موفق دولت هوشمند است. این کشور با ایجاد پلتفرم‌های دیجیتال برای مدیریت ترافیک، بهداشت، و آموزش، توانسته است کارایی خدمات عمومی را به‌طور چشمگیری افزایش دهد. برای مثال، در حوزه مدیریت ترافیک، سنگاپور از سیستم‌های هوشمند برای کنترل ترافیک و کاهش تراکم استفاده می‌کند. این سیستم‌ها با تحلیل داده‌های ترافیکی به صورت زنده، تصمیمات بهینه‌تری برای مدیریت ترافیک اتخاذ می‌کنند. کره جنوبی با استفاده از فناوری‌های نوین مانند هوش مصنوعی و داده‌های بزرگ، توانسته است خدمات دولتی را بهبود بخشد و به یکی از پیشروترین کشورهای جهان در زمینه دولت هوشمند تبدیل شود. این کشور با استفاده از کلان داده‌ها و هوش مصنوعی در حوزه‌هایی مانند بهداشت، امنیت عمومی، و حمل و نقل، توانسته است بخش خدمات دولتی را متحول ساخته و به شهروندان خدمات بهتری ارایه دهد.

راهکارهای پیاده‌سازی دولت هوشمند

برای اجرای موفق دولت هوشمند، نیاز به تدوین استراتژی‌های بلندمدت و جامع است که تمامی جنبه‌های فنی، قانونی، و اجتماعی را در بر گیرد. این استراتژی‌ها باید با توجه به نیازها و اولویت‌های ملی تدوین شوند. برای مثال، یک استراتژی جامع دولت هوشمند باید شامل برنامه‌هایی برای توسعه زیرساخت‌های دیجیتال، آموزش نیروی کار، و ایجاد قوانین و مقررات مناسب برای حمایت از اجرای فناوری‌های نوین باشد. سرمایه‌گذاری در زیرساخت‌های دیجیتال مانند شبکه‌های پهن‌باند، دیتاسنترها، و پلتفرم‌های دیجیتال یکی از الزامات اصلی دولت هوشمند است. این زیرساخت‌ها باید قابلیت پشتیبانی از حجم بالای داده‌ها و ارتباطات را داشته باشند. برای مثال، شبکه‌های پهن‌باند با سرعت بالا می‌توانند ارتباطات سریع و قابل اعتمادی را بین دستگاه‌ها و سیستم‌های مختلف فراهم کنند و دیتاسنترها می‌توانند ظرفیت لازم برای ذخیره و پردازش داده‌های بزرگ را فراهم کنند. یکی از عوامل کلیدی در اجرای موفق دولت هوشمند، آموزش و توانمندسازی نیروی کار دولتی است. برنامه‌های آموزشی باید به کارکنان دولتی کمک کنند تا با فناوری‌های نوین آشنا شوند و بتوانند از آنها به صورت کارآمد استفاده کنند. به عنوان مثال، برنامه‌های آموزشی می‌توانند شامل دوره‌های آموزشی در زمینه امنیت سایبری، تحلیل داده‌ها و استفاده از هوش مصنوعی باشند. مشارکت بخش خصوصی در اجرای دولت هوشمند می‌تواند به توسعه و بهره‌برداری از فناوری‌های پیشرفته کمک کند. همکاری با شرکت‌های فناوری، استارتاپ‌ها، و مراکز تحقیقاتی می‌تواند منجر به نوآوری و بهبود خدمات دولتی شود. برای مثال، دولت‌ها می‌توانند با ایجاد برنامه‌های شراکت عمومی-خصوصی، فرصت‌های جدیدی برای همکاری با شرکت‌های فناوری فراهم کنند و از تخصص و نوآوری آنها بهره‌مند شوند.

ضرورت ایجاد دولت هوشمند

ابتدا باید به توسعه زیرساخت‌های دیجیتال توجه ویژه‌ای شود. شبکه‌های پهن‌باند پرسرعت، دیتاسنترهای قدرتمند و سیستم‌های امن برای مدیریت داده‌ها، ستون فقرات یک دولت هوشمند هستند. بدون زیرساخت‌های قوی، اجرای فناوری‌های پیشرفته ممکن نخواهد بود و خدمات دولتی نمی‌توانند بهبود یابند. علاوه بر زیرساخت‌ها، آموزش و توانمندسازی نیروی کار دولتی نیز از اهمیت ویژه‌ای برخوردار است. کارکنان دولتی باید مهارت‌های لازم برای استفاده از فناوری‌های نوین را کسب کنند و با فرآیندهای دیجیتال آشنا شوند. برنامه‌های آموزشی مستمر و کارآمد می‌توانند این اطمینان را ایجاد کنند که نیروی کار دولتی قادر به بهره‌برداری کامل از امکانات دولت هوشمند باشد. مساله امنیت سایبری یکی دیگر از چالش‌های حیاتی است که باید به دقت مدیریت شود. حفظ امنیت داده‌ها و سیستم‌ها در برابر تهدیدات سایبری امری ضروری است. دولت‌ها باید به‌طور مستمر از تکنولوژی‌های امنیتی پیشرفته استفاده کنند و پروتکل‌های امنیتی قوی را برای حفاظت از اطلاعات حساس و حریم خصوصی شهروندان پیاده‌سازی کنند. علاوه بر این، توجه به نابرابری دیجیتال نیز از اهمیت بالایی برخوردار است. دولت‌ها باید برنامه‌های جامعی برای ارتقای دسترسی به فناوری‌های دیجیتال در مناطق محروم و کم‌درآمد اجرا کنند. این برنامه‌ها می‌توانند شامل فراهم کردن دسترسی به اینترنت پرسرعت و تأمین دستگاه‌های دیجیتال برای اقشار مختلف جامعه باشند. تنها در این صورت است که همه افراد می‌توانند به صورت برابر از خدمات دولت هوشمند بهره‌مند شوند. مشارکت بخش خصوصی نیز نقش کلیدی در توسعه دولت هوشمند ایفا می‌کند. همکاری با شرکت‌های فناوری، استارتاپ‌ها و مراکز تحقیقاتی می‌تواند نوآوری و بهبود مستمر خدمات دولتی را به همراه داشته باشد. برنامه‌های شراکت عمومی-خصوصی می‌توانند فرصت‌های جدیدی برای توسعه فناوری‌ها و بهبود خدمات عمومی ایجاد کنند. در نهایت، تدوین استراتژی‌های جامع و بلندمدت برای هدایت فرآیند پیاده‌سازی دولت هوشمند ضروری است. این استراتژی‌ها باید تمامی جنبه‌های فنی، قانونی و اجتماعی را در بر گیرند و با توجه به نیازها و اولویت‌های ملی تنظیم شوند. تنها با یک برنامه‌ریزی دقیق و هماهنگ می‌توان به اهداف دولت هوشمند دست یافت و از مزایای آن بهره‌مند شد. دولت هوشمند می‌تواند آینده‌ای روشن‌تر و کارآمدتر را برای حکمرانی به ارمغان آورد. با بهره‌گیری از فناوری‌های نوین، دولت‌ها می‌توانند خدمات بهتری به شهروندان ارایه دهند، شفافیت و پاسخگویی خود را افزایش دهند و مشارکت فعال‌تر شهروندان را در فرآیندهای تصمیم‌گیری جلب کنند. این رویکرد نه تنها به بهبود کیفیت زندگی افراد کمک می‌کند، بلکه می‌تواند منجر به توسعه اقتصادی و اجتماعی پایدارتری نیز شود.

نگاهی به ارتقای حوزه امنیت سایبری در سایه حمایت‌های دولت سیزدهم

امنیت سایبری مساله مهمی است که به حفاظت دارایی‌های اطلاعاتی سازمان‌ها کمک می‌کند؛ اطلاعاتی که اگر دیگران به آنها دست پیدا کنند، به سازمان یا افراد آسیب می‌رسد؛ بر این اساس به این موضوع طی سه سال گذشته و در دولت سیزدهم توجه ویژه شده و اقدامات گوناگونی برای ارتقای این حوزه مانند راه‌اندازی سامانه بومی مقابله با حملات DDoS و کشف آسیب‌پذیری‌های سامانه‌های دستگاه‌های غیرزیرساختی انجام شده است. به گزارش ایسنا، طی سال‌های گذشته و همزمان با گسترش تعداد کاربران، افزایش حجم داده‌ها و نیاز به برقراری امنیت در فضای مجازی، بیش از گذشته مفاهیمی مانند هک، امنیت و دیوارهای امنیتی مطرح شده است. یکی از این اصطلاحات، مفهومی به نام امنیت سایبری است که نقطه مقابلی برای هک و حملات مخرب در فضای دیجیتال محسوب می‌شود. در توضیح این مفهوم باید گفت امنیت سایبری به معنای محافظت از سیستم‌های متصل به اینترنت شامل سخت‌افزار، نرم‌افزار و داده‌ها در برابر تهدیدات دیجیتال است و این روش هم توسط افراد و هم توسط سازمان‌ها برای جلوگیری از نفوذ غیرمجاز به پایگاه‌های داده و سایر سیستم‌های دیجیتال مورد استفاده قرار می‌گیرد. حملات هکرها یکی از مهم‌ترین تهدیداتی است که معمولاً برای نفوذ، اصلاح، پاک کردن، تخریب یا باج‌گیری سیستم‌ها و داده‌های محرمانه کاربر یا سازمان طراحی شده‌اند. یکی از روش‌هایی که برای کنترل و خنثی کردن حملات هکرها می‌تواند استفاده شود، به کارگیری رویکردهای تدافعی در امنیت سایبری است. کارشناسان معتقدند امنیت سایبری یک مساله مهم است؛ امروزه اطلاعات پزشکی، دولتی، شغلی و سوابق مالی همه افراد نگهداری می‌شود و حملات سایبری ممکن است منجر به سرقت اطلاعات، حذف اطلاعات، کلاهبرداری و لطمه خوردن به اعتبار افراد و سازمان شوند. زمانی که زیرساخت‌های مهم یک کشور مورد حمله سایبری قرار می‌گیرد، به این معناست که نوعی جدید از جنگ در حوزه سایبری شکل گرفته و در این میان مدیران و مسوولان سازمان‌ها باید از حداقل اطلاعات امنیت سایبری برخوردار باشند. استفاده از مولفه‌های قدیمی و آسیب‌پذیر، بسیاری از سیستم‌های دفاعی سامانه‌های کاربران را سست کرده، به‌نحوی که تبدیل به پنجره‌ای برای نفوذ هکرها و بروز حملات سایبری طی سال‌های اخیر شده است. به تایید کارشناسان و مسوولان حوزه ارتباطات و فناوری اطلاعات، حجم حملات سایبری طی یک سال گذشته افزایش داشته و عمده هدف این حملات کور، مختل کردن و از کار انداختن روند خدمت‌رسانی بوده است. طی سال‌های گذشته تمرکز بر امنیت سایبری نه به اندازه کافی و شاید کمتر از مقداری که باید باشد، در این حوزه بوده است و اشکال هم آنجاست که امنیت در حوزه فناوری اطلاعات بیشتر با فرآیندها و روش‌ها پیاده می‌شود نه با تجهیزات. در این راستا اقداماتی در سه سال گذشته برای ارتقای این حوزه انجام شده است و عیسی زارع‌پور-وزیر ارتباطات و فناوری اطلاعات-اخیرا در گزارشی از مهم‌ترین اقدامات انجام شده در زمینه امنیت سایبری در یک شبکه اجتماعی داخلی اظهار کرد: از اقدامات راهبردی این دوره تلاش برای توسعه بومی زیرساخت‌های لازم برای تامین امنیت سایبری بود. در این راستا ضمن حمایت مادی و معنوی از شرکت‌های دانش بنیان این حوزه، بازارسازی داخلی و خارجی برای محصولاتشان نیز صورت گرفت. سامانه بومی مقابله با حملات DDoS حاصل این نگاه و مسیر بود. وی افزود: کشف آسیب‌پذیری‌های سامانه‌های دستگاه‌های غیرزیرساختی کشور یکی از وظایف سازمان فناوری اطلاعات، است. در این دوره با افزایش ظرفیت‌ها، از طریق ۳۷ مراکز آپا، ۲۰ شرکت همکار و برگزاری ۲۲۵ «مسابقه کشف آسیب‌پذیری»، بیش از ۲۵۰۰ آسیب‌پذیری کشف و در تعامل با دستگاه مربوطه حل شد. زارع‌پور با بیان اینکه یکی از دلایل هک‌شدن سامانه‌ها به‌ویژه ابزارهای متن‌باز، عدم وصله‌زنی به‌موقع (patch management) است، توضیح داد: برای حل این مشکل، همکارانم ابزاری برای شناسایی و وصله‌زنی خودکار آسیب‌پذیریهای شناخته شده طراحی کرده‌اند و تاکنون ۲۵۰ هزار مورد وصله‌زنی برای سامانه‌های دولتی انجام شده است. راه‌اندازی مرکز ارایه خدمات امنیتی مدیریت شده (MSSP) برای ارایه خدمات امن‌سازی زیرساخت‌ها، مقابله برخط با بیش از ۴۰۰ حمله سایبری پیچیده، رسیدگی به بیش از ۲۹۰۰ رخداد امنیتی و برگزاری ۱۲۱ دوره آموزشی از جمله خدمات امنیت سایبری ارایه شده به دستگاه‌های غیرزیرساختی دولتی در این دوره است. همچنین طراحی و پیاده‌سازی سامانه مرکز تحلیل و اشتراک‌گذاری داده‌های امنیتی (ISAC)، راه‌اندازی شبکه تله بدافزار (Honey Pot) با ۲۸ گره شناسایی بدافزار در دستگاه‌های دولتی و ایجاد ۶ آزمایشگاه تخصصی ارزیابی امنیتی از دیگر اقدامات زیرساختی این دوره برای ارتقای امنیت سایبری دستگاه‌های دولتی بود. کمبود اعتبارات برای ارتقای امنیت سایبری موردی است که به گفته وزیر ارتباطات، همواره به عنوان یکی از دلایل هنگام بروز حوادث سایبری ذکر می‌شود. برای حلِ ریشه‌ای این مساله، با پیگیری این وزارتخانه در قوانین بودجه دو سال اخیر همه دستگاه‌های دولتی مکلف به صرف یک درصد از اعتباراتشان برای امن‌سازی زیرساخت‌های خود شده‌اند. کارشناسان بر این باور هستند که در دنیا هر روز تکنولوژی‌های جدیدی وارد می‌شود و حفظ امنیت دارایی‌های اطلاعاتی بسیار مهم است و تحول دیجیتال بدون حفظ امنیت آن بی‌معنی است، به همین دلیل نیروی انسانی در حوزه امنیت که هر روز صنعت بزرگ‌تری می‌شود، بزرگ‌ترین چالش این حوزه است.

دنیای فناری

رونمایی مقررات امریکا برای ممنوعیت صادرات تجهیزات تراشه خارجی به چین

دولت بایدن قصد دارد ماه آینده، مقررات جدیدی را رونمایی کند که اختیارات امریکا برای توقف صادرات تجهیزات تولید تراشه به چین را به بعضی از کشورهای خارجی، گسترش می‌دهد. به گزارش ایسنا، منابع آگاه به رویترز گفتند که صادرات از متحدانی که تجهیزات تراشه‌سازی مهمی را صادر می‌کنند شامل ژاپن، هلند و کره جنوبی، شامل این ممنوعیت نمی‌شود و در نتیجه، تاثیر این مقررات را محدود می‌کند. بر همین اساس، شرکت‌های بزرگ تولیدکننده تجهیزات تراشه‌سازی مانند ASML و توکیو الکترون، شامل این ممنوعیت‌ها نخواهند شد.

ارزش سهام این دو شرکت، در پی انتشار این خبر، افزایش یافت. یکی از این منابع آگاه گفت: این مقررات، دامنه مقررات محصولات مستقیم خارجی را گسترش داده و دریافت صادرات از بسیاری از کشورها را برای ده‌ها کارخانه چینی سازنده تراشه‌های پیشرفته ممنوع می‌کند. کشورهایی که شامل مقررات جدید می‌شوند، سرزمین‌های اشغالی فلسطین، تایوان، سنگاپور و مالزی هستند. امریکا با هدف جلوگیری از پیشرفت چین در عرصه ابررایانش و هوش مصنوعی، در سال‌های ۲۰۲۲ و ۲۰۲۳، کنترل‌های صادراتی را برای ارسال تراشه‌ها و تجهیزات تراشه‌سازی به چین، اعمال کرد. مقررات جدید که در مرحله پیش‌نویس هستند، نشان می‌دهد واشنگتن به دنبال حفظ فشار بر صنعت نیمه‌رسانای چین بدون ناراحت کردن هم‌پیمانانش است. بر اساس گزارش رویترز، تحت مقررات محصول مستقیم خارجی، اگر محصولی با استفاده از فناوری امریکایی ساخته شده باشد که شامل محصولات ساخته شده در یک کشور خارجی، دولت امریکا این اختیار را دارد که مانع فروش آن شود.

متا برای ساکت کردن تگزاس ۱.۴ میلیارد دلار می‌دهد

شرکت متا، توافق کرد ۱.۴ میلیارد دلار به تگزاس پرداخت کند تا شکایت این ایالت درباره استفاده غیرقانونی این شرکت از فناوری تشخیص چهره برای جمع‌آوری داده‌های بیومتریک میلیون‌ها تگزاسی را حل و فصل کند. به گزارش ایسنا، وکلای تگزاس اعلام کردند شرایط این توافق که روز سه شنبه اعلام شد، به منزله بزرگ‌ترین توافق از سوی یک ایالت امریکاست. این شکایت که در سال ۲۰۲۲ تنظیم شد، نخستین پرونده بزرگ بود که تحت قانون حریم خصوصی بیومتریک ۲۰۰۹ تگزاس، به دادگاه برده شد. نقض این قانون، حداکثر ۲۵ هزار دلار جریمه به ازای هر مورد تخلف دارد. تگزاس، فیس‌بوک را متهم کرده بود اطلاعات بیومتریک را میلیاردها بار، از تصاویر و ویدئوهایی که کاربران، تحت ویژگی پیشنهادهای برچسب (Tag Suggestions)، به این پلتفرم شبکه اجتماعی بارگزاری کرده‌اند، جمع‌آوری کرده است. سخنگوی شرکت متا اعلام کرد این شرکت از حل این مساله، خوشنود است و به دنبال بررسی فرصت‌های آینده برای عمیق کردن سرمایه‌گذاری تجاری در تگزاس است که شامل ساخت دیتاسنترها خواهد بود. این شرکت همچنان منکر ارتکاب خلاف شد. کن پاکستون، دادستان کل تگزاس در بیانیه‌ای گفت: این توافق به منزله تعهد این ایالت برای ایستادن در مقابل بزرگ‌ترین شرکت‌های فناوری و مسوول شناختن آنها برای نقض حقوق حریم خصوصی مردم تگزاس است. تگزاس و متا اعلام کردند در ماه مه و چند هفته قبل از آغاز جلسه دادگاه در این ایالت، به توافق رسیدند. شرکت متا همچنین در سال ۲۰۲۰، توافق کرده بود ۶۵۰ میلیون دلار برای حل و فصل شکایت گروهی نقض حریم خصوصی بیومتریک تحت قانون حریم خصوصی ایلینویز، پرداخت کند. بر اساس گزارش رویترز، گوگل هم سرگرم مبارزه با شکایتی در تگزاس است که این شرکت را به نقض قانون بیومتریک این ایالت متهم کرده است.

ادامه از صفحه اول

بازار در بیم و امید اخبار مثبت و منفی

هرچند برخی افراد و جریانات تلاش می‌کنند وزن اخبار نگران کننده را سنگین‌تر کرده و اقدام به پمپاژ ناامیدی می‌کنند اما خبر خوب این است که اعتماد بازار بر اساس عملکرد دولت قابل ترمیم است و عمدتا قدرت روندهای مثبت بورس قابل تکرار است و در صورت وجود اعتماد توان همراه شدن قشر بزرگ‌تری از سرمایه‌گذاران را دارد خصوصا اینکه رکود بزرگی در اقتصاد کشور وجود دارد و سرمایه به دنبال بازاری مطمئن برای رسوب میان‌مدت و بلندمدت است. نکته‌ای که فعلا می‌توان بیان کرد آن است که در حال حاضر ارتباط بازار سرمایه و فعالان آن کاملا قطع شده است. هیچ خبر و مصوبه‌ای هم نتوانسته فعلا بازار را به حرکت درآورد. اما نشانه‌ها به مرور پدیدار خواهند شد. در یادداشت‌های بعدی دلیل یک چنین مکانیسمی را بیان خواهم کرد.