



با تلاش دولت سیزدهم و تصویب در مجلس جدید

«حفاظت از داده‌های شخصی کاربران» قانونمند می‌شود

گزارش

گروه فناوری/ داده‌های شخصی و حفاظت از آنها یکی از مهم‌ترین موضوعاتی است که باید در استفاده از ابزارهای الکترونیکی مورد توجه قرار گیرد و با پیشرفت‌های حوزه فناوری اطلاعات، حفاظت از این اطلاعات و داده‌ها از اهمیت بیشتری برخوردار می‌شوند. بخشی از اقدامات وزارت ارتباطات و فناوری اطلاعات به منظور حمایت از حقوق کاربران این بخش، رونمایی از لایحه صیانت و حفاظت از داده‌های شخصی به منظور حمایت از حقوق خصوصی کاربران فضای مجازی بوده است. در این راستا عیسی زارع‌پور، وزیر ارتباطات و فناوری اطلاعات چندی پیش در حاشیه نخستین جلسه هیأت دولت در سال جدید درباره آخرین وضعیت لایحه امنیت کاربران اظهار کرد: این لایحه در کمیسیون حقوقی-قضایی دولت در دست بررسی است و مراحل پایانی خود را طی می‌کند. وی افزود: قسمت‌هایی از لایحه به علت بخش‌های قضایی نیازمند تأیید قوه قضائیه بوده که در همین راستا نامه‌ای به رئیس قوه قضائیه ارسال شده است تا نظر آنها برای این بخش‌ها کسب شود.

تجدید مهلت اجرای دستورالعمل حفاظت از حریم خصوصی کاربران آنچه مسلم است اینکه دولت سیزدهم به دنبال آن است که لایحه «حفاظت از داده‌های شخصی کاربران در فضای مجازی» را برای تصویب به مجلس دوازدهم ارسال کند. این دغدغه در یادداشت پایان سال وزیر ارتباطات و فناوری اطلاعات و جمع‌بندی عملکرد این وزارتخانه ملموس بود. با توجه به اینکه در سال گذشته شاهد وقوع چندین حمله سایبری و به دنبال آن، لورفتن اطلاعات و داده‌های شخصی کاربران بودیم، یکی از بندهای عملکرد این وزارتخانه، تصویب لایحه حفاظت از داده‌های شخصی کاربران در فضای مجازی در دولت بوده است که نشان‌دهنده عزم دولت سیزدهم برای به نتیجه رساندن این لایحه در مجلس جدید است تا به این ترتیب بتوان سدی مقابل هکرها قرار داد. امروزه حجم بالایی از داده‌ها با گسترش پلتفرم‌ها، شبکه‌های اجتماعی و کسب‌وکارهای مجازی جمع‌آوری می‌شود و فعالان فضای مجازی به اطلاعات زیادی از کاربران دسترسی دارند و همین موضوع نگرانی‌های زیادی را ایجاد کرده است. از این رو قانونگذاران به دنبال تنظیم قانونی مشخص در این حوزه هستند. گفتنی است علاوه بر وزارت ارتباطات و فناوری اطلاعات، مرکز ملی فضای مجازی هم به عنوان

یکی از متولیان، دغدغه تأمین امنیت داده‌های کاربران را دارد. به تازگی سخنگوی این مرکز از تمدید مهلت اجرای دستورالعمل حفاظت از حریم خصوصی کاربران خبر داده است. حسین دلیریان با اشاره به آخرین روند اجرای دستورالعمل حفاظت از حریم خصوصی کاربران گفت: دبیر شورای عالی فضای مجازی ۲۷ دی‌ماه سال ۱۴۰۲ این دستورالعمل را به منظور کاهش مخاطرات نقض حریم خصوصی کاربران و حمایت از آنها برابر تهدیدات سایبری ابلاغ کرد و در آخرین پیگیری‌هایی که سال گذشته توسط کمیسیون عالی تنظیم مقررات فضای مجازی کشور صورت گرفت، سکوها و سامانه‌ها در حال اجرای آن هستند. وی افزود: تا قبل از سال جدید، بخش‌هایی از دستورالعمل که امکان اجرای سریع‌تر آن وجود داشت توسط کسب‌وکارهای بخش خصوصی و سامانه‌های دولتی اجرا شد و بقیه مفاد دستورالعمل نیز در مسیر اجرا قرار دارد. سخنگوی مرکز ملی فضای مجازی خاطرنشان کرد: البته پس از ابلاغ این دستورالعمل، جلسه‌های متعددی به منظور پیگیری اجرای آن در سکوها و سامانه‌ها برگزار شد و در فرایند این نظارت و پیگیری، سامانه‌ها و کسب‌وکارهای بخش خصوصی از مرکز ملی فضای مجازی خواستند فرصت اجرای این دستورالعمل به

مراجع صدور مجوز، منوط به حصول اطمینان از رعایت این مقررات است که از طریق سازگار نظارتی تدوین شده توسط مرکز ملی فضای مجازی، مورد سنجش و ارزیابی قرار خواهد گرفت.

مزایای لایحه حفاظت از داده‌های کاربران

حفاظت از داده‌های شخصی کاربران در فضای مجازی دارای اهمیت زیادی است و کاربران دوست ندارند زمانی که با شماره خود در سایتی ثبت‌نام می‌کنند، آن شماره در اختیار شرکت‌های تبلیغاتی قرار گیرد. اما تکلیف داده در این مقوله مشخص نیست چراکه قوانین فعلی ما به دلیل بازخوانی‌های متفاوت از قوانین، نمی‌تواند به شکل شفاف عمل کند.

این درحالی است که تصویب لایحه حفاظت از داده‌های کاربران، به افراد اجازه می‌دهد با کنترل بر داده‌های شخصی خود، انتخاب‌های آگاهانه درباره استفاده از آنها داشته باشند. چنین قانونی اعتماد و وفاداری را میان کاربران تقویت می‌کند و در عین حال خطر رسوایی‌های مرتبط با سوءاستفاده از داده‌ها توسط پلتفرم‌ها را نیز کاهش می‌دهد. در صورت تصویب این لایحه که بر شفافیت و پاسخگویی در شیوه‌ها پردازش آنها تأکید دارد، پلتفرم‌ها موظف می‌شوند اطلاعات واضح و قابل دسترسی درباره روش‌های جمع‌آوری داده‌ها، اهداف و نتایج‌ها که داده‌ها با آنها به اشتراک گذاشته می‌شود، ارائه دهند. علاوه بر این، آنها مسئول پایبندی به اصول حفاظت از داده‌ها و توجیه مبنای قانونی فعالیت‌های حوزه پردازش داده‌ها هستند به این ترتیب شفافیت و پاسخگویی پلتفرم‌ها تا حد زیادی افزایش می‌یابد. از سوی دیگر کاربران اطلاعات شخصی خود را به پلتفرم‌هایی خواهند سپرد که تعهد حفاظت از داده‌ها و حفظ حریم خصوصی را پذیرفته‌اند و محیطی مساعد برای تعاملات و تراکنش‌های دیجیتال ایجاد می‌کنند.

تعیین حقوق کاربران این لایحه، یک چهارچوب قانونی قوی برای حفاظت از داده‌های شخصی کاربران و طبیفی از مقررات و پادمان‌ها را با هدف تقویت حریم خصوصی کاربران و امنیت داده‌ها دربرمی‌گیرد. اجزای کلیدی چنین سازگاری شامل نیاز به رضایت صریح کاربر برای پردازش داده‌ها، محدودیت در نگهداری و استفاده از داده‌ها و تعیین حقوق کاربران همچون حق دسترسی، اصلاح و پاک کردن داده‌های شخصی می‌شود. بنابراین چهارچوب حقوقی چنین قوانینی، به زبان ساده کنترل بر حریم خصوصی داده‌ها و از آنجا که پلتفرم‌ها خارج کرده و به کاربران بازمی‌گرداند. هرچند برخی تصویب این لایحه و مقررات سختگیرانه آن از بار سنگینی بردوش کسب‌وکارها به ویژه شرکت‌های کوچک و متوسط می‌داند، ولی در درازمدت مطمئناً چنین قانونی می‌تواند زمینه‌ساز

تداوم رشد اقتصاد دیجیتال و رشد خدمات آنلاین در جامعه شود. به گفته رضا باقری اصل، معاون وزیر ارتباطات و فناوری اطلاعات، در امور مجلس، ویژگی این لایحه، نظام‌مند کردن داده‌ها، حفظ حریم خصوصی کاربران و حفاظت از داده‌ها در سکوها اینترنتی است و به نفع حمایت بیشتر از مردم و کسب‌وکارهای این حوزه تدوین و تکمیل شده است.

محمد خوانساری، معاون وزیر و رئیس سازمان فناوری اطلاعات ایران هم در این باره گفته است: اگر استارت‌آپ‌ها قصد دارند کار خود را به شکل درستی انجام دهند و رشد متوازی داشته باشند، باید از داده‌های مردم حفاظت کنند. در این راستا یکی از مواردی که در بخش حقوقی مربوط به شرکت‌های استارت‌آپی پیگیری می‌کنیم، ارسال لایحه حفاظت از داده‌های شخصی از طریق دولت به مجلس است.

لزوم ایجاد یک مرجع واحد

کارشناسان معتقدند درحالی که امروز بسیاری از نهادها می‌توانند به اطلاعات کاربران در شرکت‌ها و اپراتورها دسترسی داشته باشند اما باید یک مرجع واحد دارای صلاحیت، برای دریافت اطلاعات کاربران از شرکت‌هایی که دیتاها را در اختیار دارند، ایجاد شود. به اعتقاد این کارشناسان، به این ترتیب تشخیص منطقی یا غیرمنطقی بودن درخواست نهادها، عهده این مرجع خواهد بود و شرکت‌ها و اپراتورها دیگر دچار سردرگمی نمی‌شوند چراکه می‌دانند می‌توانند با دستور قضایی اطلاعات را در اختیار نهادهای مربوطه قرار دهند.

نظارت بر کنترل‌گرها

کارشناسان همچنین معتقدند نظارت بر کنترل‌گرها بسیار مهم است چراکه اکنون داده‌های زیادی از کاربران و حریم خصوصی آنها در اختیار شرکت‌ها و اپراتورها قرار دارد. آنها به این اطلاعات دسترسی دارند و از این‌رو باید بر این کنترل‌گرها نظارت صورت بگیرد. به اعتقاد کارشناسان، اپراتورها و شرکت‌ها دارای تعهداتی برای حفظ حریم خصوصی و اطلاعات کاربران خود هستند ولی این احتمال وجود دارد که بعضاً این تعهدات را زیر پا بگذارند، از این‌رو باید بر آنها نظارت صورت گیرد.

این کارشناسان همچنین اعتقاد دارند در هر طرح و لایحه‌ای باید خود قانون و مصادیق بیرونی آن به طور کامل دیده شود و ضمانت اجرایی داشته باشد. به نظر می‌رسد باید برای شرکت‌هایی که دیتاهای کاربران را در اختیار دارند، اصول و استانداردهایی تعریف و بر آنها نظارت شود. اعتقاد این گروه، ضمانت اجرایی آن می‌تواند مانند اتحادیه اروپا محرومیت‌های انضباطی و اجتماعی باشد. همچنین اتحادیه اروپا قانونی را وضع کرده و اجرا می‌کند مبنی بر اینکه هر شرکتی اطلاعات کاربران را در اختیار داشته باشد، هیچ شرکتی حق ندارد با آن کار کند. چنین ضمانت‌های اجرایی می‌تواند میزان حفاظت از داده‌های شخصی کاربران را افزایش دهد.

فناوری

اخبار



پرتاب کپسول زیستی به فضا در سال جدید

رئیس سازمان فضایی ایران از برنامه‌ریزی برای پرتاب کپسول زیستی با جرم و حجم بالاتر در سال جدید خبر داد. به گزارش مهر، حسن سالاریه گفت: در سال ۱۴۰۲، بعد از سال‌ها توقف، نخستین پرتاب زیست‌مداری کپسول زیستی انجام شد. جرم این کپسول زیستی حدود ۵۰۰ کیلوگرم بود که به نسبت پرتاب‌هایی که در سال‌های قبل یعنی سال‌های دهه ۸۰ و اوایل دهه ۹۰ داشتیم، تجربه کاملاً متفاوتی بود.

وی تصریح کرد: داده‌های کپسول زیستی که در سال گذشته پرتاب شد، دریافت شده و در طراحی کپسول‌های بعدی از آن استفاده می‌کنیم. نقاط ضعف و قوت این کپسول شناسایی شده، کیت‌های زیستی قرارگرفته در آن، ارزیابی و بررسی شده و برای طراحی ساخت کپسول بزرگ‌تر همه این داده‌ها مورد استفاده قرار می‌گیرد. سالاریه افزود: قرارداد جدیدی برای ارتقای این کپسول با جرم و حجم بالاتر منعقد کردیم و ان شاء‌الله دنبال این هستیم که در قدم اول با پرتاب‌های اولیبه‌قابلیت زیست در فضا را در پرتاب‌های آزمایشی بررسی‌های قابلیت حمل انسان در آن از ظرفیت موجود استفاده خواهیم کرد تا به نقطه‌ای برسیم که قابلیت حمل انسان در کپسول‌های زیستی با قابلیت اطمینان بسیار بالا ایجاد شود.

وی درخصوص پرتاب کپسول زیستی در سال ۱۴۰۳ و سال‌های آینده گفت: به دلیل اینکه به لحاظ تکنولوژیک تست خیلی از موارد قبل از پرتاب اصلی یعنی پرتاب فضانورد به فضا لازم است، بنابراین در حال برنامه‌ریزی هستیم که برای سال‌های ۱۴۰۳ و ۱۴۰۴ نیز پرتاب کپسول زیستی با جرم و حجم بیشتری داشته باشیم.

پذیرش ۵ شرکت دانش بنیان در بازار نواقرین

مدیرکل دفتر تأمین مالی و سرمایه‌گذاری معاونت علمی، فناوری و اقتصاد دانش بنیان ریاست جمهوری از افزایش ۱۰۰ هزار میلیارد ریالی (۱۰ همتی) ظرفیت صدور ضمانتنامه در زیست بوم فناوری و نوآوری کشور خبر داد و گفت: با افتتاح بازار نواقرین اکنون ۷ شرکت در این بازار پذیرش شده‌اند که از این تعداد ۵ شرکت دارای تأییدیه دانش بنیان است. به گزارش روابط عمومی معاونت علمی ریاست جمهوری، عبدالعزیز مرشدی خاطر نشان کرد: در این مسیر از صندوق حمایت مستقیم از مناطق کمتر برخوردار نیز حمایت مناسبی صورت گرفت و در راستای استفاده از ظرفیت کمک‌های فنی و اعتباری پیش‌بینی شده از محل تبصره ۱۸ قانون بودجه کل کشور با همکاری نهادهای همکار طی برنامه‌ریزی انجام شده نسبت به افزایش سرمایه صندوق‌ها اقدامات لازم صورت گرفت که مبلغ بیش از ۳۰۰ میلیارد ریال به عنوان سهم بخش دولتی به صندوق‌های منتخب اختصاص یافت.

وی ایجاد بازار اختصاصی تحت عنوان «بازار نواقرین» برای شرکت‌های دانش بنیان، خلاق، فناور و فعال در حوزه اقتصاد دیجیتال را از مهم‌ترین دستاوردهای معاونت علمی، فناوری و اقتصاد دانش بنیان ریاست جمهوری در سال ۱۴۰۲ برشمرد و اظهار کرد: بازار نواقرین، بخشی از بازار معاملاتی فرابورس است که تنها مختص شرکت‌های کوچک نیست و شرکت‌هایی که ریسک بالایی دارند یا در صنعت جدیدی فعال هستند را هم شامل می‌شود.

وزیر ارتباطات عنوان کرد

کاهش اختلال پیام‌رسان‌ها باره‌اندازی دیتاستر

وزیر ارتباطات و فناوری اطلاعات درباره علت برخی اختلال‌ها در پیام‌رسان‌ها توضیح داد و اعلام کرد در حال راه‌اندازی دیتاستر دوم این پیام‌رسان‌ها هستیم تا دیگر شاهد چنین مشکلاتی نباشیم.

به گزارش استات، عیسی زارع‌پور درباره اختلال در یکی از پیام‌رسان‌های داخلی اظهار کرد: این پیام‌رسان یک مشکل ساخت‌افزایی داشت که حل شد و تلاش بر این است که مردم این اختلال‌ها را تجربه نکنند. وی درباره تعدد اختلال‌ها در پیام‌رسان‌ها گفت: یک پیام‌رسان خارجی هم چند ساعت اختلال داشت. گاهی اختلال طبیعی است، ولی باید تلاش شود که تکرار نشود و به حداقل برسد. زیرساخت این پیام‌رسان‌ها را وزارت ارتباطات تأمین می‌کند و تلاش ما این است که روز به روز کیفیت زیرساخت‌ها تقویت شود. وی در ادامه یادآور شد: در حال راه‌اندازی دیتاستر دوم این پیام‌رسان‌ها هستیم تا دیگر شاهد چنین مشکلاتی نباشیم.

استفاده قرار می‌گیرد. اگر وب‌سایتی از پروتکل گفته شده استفاده نمی‌کند، احتمال افساس و سرقت هرگونه اطلاعات رد و بدل شده وجود خواهد داشت. البته وجود HTTPS شرط کافی برای اعتماد به یک سایت نخواهد بود؛ اما ععد استفاده از آن، نشان‌دهنده صخه‌ای ناامن است. استفاده از آیکون قفل بسته شده در کنار آدرس بار در بیشتر مرورگرها برای نشان دادن بهره‌گیری از پروتکل مورد اشاره است.

چک کردن آدرس سایت

یکی از ساده‌ترین روش‌ها برای بررسی امنیت سایت در موبایل، توجه به آدرس آن‌ها است. صفحه‌های فیشینگ به‌طور معمول سعی دارند از آدرسی مشابه یا سرویس‌های معتبر استفاده کنند و تنها یک یا چند حرف از نام آنها را در آدرس خود تغییر می‌دهند. همچنین استفاده از دامنه‌های غیرمعمول در سایت‌های جعلی بسیار شایع است؛ زیرا سازندگان آنها می‌دانند که در نهایت آدرس صفحه سددوی می‌شود، پس ترجیح می‌دهند از دامنه‌های ناشناس ارزان قیمت استفاده کنند.

این صفحه‌های پاپ‌آپ در دسرساز صفحه‌های پاپ‌آپ یکی از علاقه‌مندی‌های مجرمان اینترنتی است که می‌توانند از آنها برای مقاصد مختلف استفاده کنند. چنین صفحه‌هایی تنها محدود به نمایش تبلیغات آزاردهنده نمی‌شوند و ممکن

چگونه وب‌سایت‌های ناامن را تشخیص دهیم؟

جعلی صرف نمی‌کنند؛ در نتیجه با دقت به جزئیات می‌توان آنها را شناسایی کرد هرچند این موضوع برای همه سایت‌ها صدق نمی‌کند و برخی هم کاملاً حرفه‌ای طراحی شده‌اند. اگر از قبل بدانید که به چه مواردی باید دقت کنید، مطمئناً بررسی امنیت سایت بسیار آسان‌تر خواهد بود.

توجه به نواقص سایت

برای تشخیص وب‌سایت‌های جعلی، به دنبال نواقص باشید. برخی از سایت‌های جعلی کاملاً حرفه‌ای طراحی شده‌اند و نمی‌توان هدف شوم آنها را به راحتی حدس زد. اما بیشتر صفحه‌های مشکوک این‌گونه نیستند و نواقص متعددی در آنها یافت می‌شود. برای مثال اشتباهی‌های نگارشی یا تصاویر غیراختصاصی‌کیی شده از اینترنت بعنوان نقض‌های رایج محسوب می‌شوند. البته دقت به چنین مواردی در نگاه اول با گوشی‌های هوشمند کمی دشوارتر است؛ در نتیجه توصیه می‌شود قبل از وارد کردن هرگونه اطلاعاتی، با اسکروال به پایین و بازدید از سایر صفحه‌ها، اعتبار سایت را کمی بیشتر بسنجید.

بررسی امنیت سایت و صفحه‌های اینترنتی در موبایل برای تشخیص ناامن بودن یک وب‌سایت باید به چه مواردی توجه کرد؟ معمولاً کلاهبرداران اینترنتی به‌طور معمول زمان چندان زیادی را برای طراحی سایت‌ها و صفحه‌های

امروزه بخش عمده خرید آنلاین کاربران از طریق گوشی‌های هوشمند انجام می‌گیرد و البته مجرمان سایبری هم از این ظرفیت چشم‌پوشی نکرده‌اند و با ارائه وب‌سایت‌های جعلی، به دنبال شکار نغمه‌های خود هستند که توجه چندانی به امنیت وب‌سایت‌ها ندارند.

این هکرها با این کردن دام‌های خود مترصد فرصت می‌شوند و تنها کافی است شما یک بار وارد این سایت جعلی شوید و خرید خود را به پایان برسانید پس از دقایقی متوجه می‌شوید که همه موجودی کارت خود را از دست داده‌اید بدون اینکه هیچ کالایی دریافت کنید. هرچند تفاوت چندانی ندارد که شما از چه دستگاهی برای خرید آنلاین استفاده می‌کنید ولی سازندگان سایت‌های جعلی توجه ویژه‌ای به کاربران گوشی‌های هوشمند دارند چراکه صفحه گوشی نسبتاً کوچکتر است و احتمالاً نواقص وب‌سایت کمتر به چشم شما می‌آید. در برخی وب‌سایت‌های جعلی که از آنها با عنوان وب‌سایت‌های فیشینگ (رمزگیری یا تله‌گذاری) یاد می‌شود، احتمال سرقت رمزهای عبور می‌رود. برخی دیگر هم هویت کاربر را جعل می‌کنند.



امنیت آنلاین

برخی از سایت‌های جعلی کاملاً حرفه‌ای طراحی شده‌اند و نمی‌توان هدف شوم آنها را به راحتی حدس زد. اما بیشتر صفحه‌های مشکوک این‌گونه نیستند و نواقص متعددی در آنها یافت می‌شود