ضرر و زیان قطع اینترنت چقدر بوده است؟

دنیای اقتصاد: ستار هاشمی، وزیر ارتباطات، اعلام کرد محدودیت‌های اینترنتی در جریان جنگ تا اواسط اردیبهشت بیش از ۶۷هزار میلیارد تومان خسارت مستقیم و کاهش درآمد برای حوزه فاوا و اقتصاد دیجیتال به همراه داشته است. او این رقم را تنها بخشی از پیامدهای اقتصادی دانست و تاکید کرد هزینه‌هایی مانند از دست رفتن فرصت‌های سرمایه‌گذاری، کاهش اعتماد، مهاجرت نیروی متخصص و آسیب‌های علمی و انسانی در آن محاسبه نشده‌اند. هاشمی با اشاره به اینکه وزارت ارتباطات از نخستین روزهای جنگ خواستار محدودیت‌های مدیریت‌شده، هدفمند و کوتاه‌مدت بود، گفت طولانی شدن این وضعیت آثار آن را بر آموزش، پژوهش، خدمات عمومی و حکمرانی فضای مجازی آشکارتر کرد.

بازار دیجیتال

مرورگرها به کاربران هشدار امنیتی می‌دهند

چرا سایت‌های ایرانی باز نمی‌شوند؟

حامد ناری

اخیرا کاربران ایرانی برای دسترسی به سایت نهادهای رسمی با مشکل مواجه شده‌اند؛ از جمله سایت بانک مرکزی و سایت تنظیم مقررات و چند نمونه دیگر. موضوع پیچیده‌ای هم در میان نیست. نهادهای رسمی ایرانی برای جلب اعتماد دیجیتال و دریافت گواهی‌نامه‌های لازم مشکل دارند.

گواهی‌نامه‌هایی که بدون آنها دست‌کم حضورشان در وب با چالش روبه‌رو خواهد شد. مثلا بانک مرکزی در اطلاعیه‌ای رسمی، این اختلال را به اقدامات خصمانه دشمنان نسبت داد و اعلام کرد گواهی فنی-امنیتی برخی از پایگاه‌های وابسته به این بانک از سوی تامین‌کننده خارجی لغو شده است.

بررسی فنی دقیق‌تر نشان می‌دهد مسیر تامین این گواهی‌ها، حداقل در یک نمونه مستندشده، از صادرکنندگانی غیرغربی، از جمله یک شرکت چینی، عبور کرده است. مسیری که هرچند برای دور زدن محدودیت‌های بین‌المللی طراحی شده، خود نیز از همان آسیب‌پذیری در امان نمانده است.

سرنخ ماجرا

نقطه عزیمت ورود به سایت تنظیم مقررات برای بحث دیگری بود که از شما چه پنهان به حاشیه رفت. سرنخی که ختم به طرح این گزارش شد ماندن پشت درهای مجازی سایت سازمان تنظیم مقررات بود. سرنخی که به رشته‌ای بلندتر بدل شد.

بعد از بررسی گواهی امنیتی دامنه سازمان تنظیم مقررات (cra.ir) نتیجه آن شد که صادرکننده آن، یک شرکت چینی به نام TrustAsia بوده است. شرکتی که خود، برای معتبر شناخته‌شدن در مرورگرهای جهانی، از یک نهاد صدور گواهی لهستانی به نام Certum ضمانت گرفته است. زنجیره‌ای سه‌حلقه‌ای که در نهایت به گواهی‌ای منتهی می‌شود که اکنون باطل یا منقضی شده است.

در این شرایط نمی‌توان در مورد منقضی شدن یا چرایی باز نشدن وب‌سایت‌ها دقیق سخن گفت. برای رسیدن به این نتیجه نیاز به تایید خود سازمان خواهیم داشت. البته این تنها سایت تنظیم مقررات نیست که خود جایگاه مهمی در معماری شبکه اینترنت ایران دارد، آن هم شبکه‌ای که اعمال فیلترینگ گسترده بر آن سبب بروز میزان بالایی آلودگی در تاروپود آن شده است. بانک مرکزی نمونه دوم همین الگو به شمار می‌رود.

در بیانیه‌ای که بانک مرکزی منتشر کرد، اختلال سایت این نهاد در بستر تنش‌های امنیتی و نظامی گسترده‌تر میان ایران و غرب تفسیر شد. بعد از تحمیل جنگ در ابعاد مختلف به کشور، فعالیت‌های بین‌المللی با دشواری‌هایی بیش از پیش روبه‌رو شد. نمونه سومی هم وجود دارد؛ خبرگزاری فارس.

بر اساس گزارش‌های منتشرشده، درخواست‌های این خبرگزاری برای صدور یا تمدید گواهی امنیتی توسط تمام صادرکنندگان عمومی و بین‌المللی مورد اعتماد مرورگرها، از Let's Encrypt و DigiCert گرفته تا Sectigo و HARICA، یا رد شده یا بی‌پاسخ مانده بود. اتفاقی که ریشه در تحریم‌های یکجانبه و مستقیم دامنه این رسانه از سوی خزانه‌داری آمریکا در سال ۲۰۲۰ و افزودن آن به فهرست تحریمی SDN در سال ۲۰۲۳ داشت. در نهایت، گزارش‌ها از تاثیر مشابه این مساله بر تعدادی از بانک‌ها و سایت‌های دولتی خبر می‌دهند. سرنخ ما به احتمال زیاد ما را به عمقی فرومی کشد که موجب اعجاب خواهد شد.

پای کدام شرکت در میان است؟

برای فهم اینکه چرا یک سازمان دولتی ایرانی باید گواهی امنیتی‌اش را از یک شرکت چینی با ضمانت یک نهاد لهستانی تهیه کند، باید یک قدم به عقب برگردیم و سراغ خود مفهوم گواهی امنیتی برویم. آن قفل سبزرنگ کنار آدرس هر سایت، در واقع یک برگه تاییدیه است که می‌گوید این سایت همان چیزی است که ادعا می‌کند، و ارتباط شما با آن رمزگذاری شده است. اما این تاییدیه را خود سایت به خودش نمی‌دهد؛ باید یک نهاد ثالث و مستقل که در ادبیات فنی «مرجع صدور گواهی» یا CA خوانده می‌شود آن را صادر و امضا کند.

مشکل اینجاست که مرورگرها (کروم، فایرفاکس، سافاری) فقط به گواهی‌هایی که توسط یکی از چند ده CA از پیش تاییدشده و مورد اعتماد صادر شده باشند، بدون هشدار اعتماد می‌کنند. برای یک سازمان دولتی ایرانی، دقیقا همین جا کار گره می‌خورد: بسیاری از همین CAهای معتبر و شناخته‌شده، شرکت‌های آمریکایی یا اروپایی‌اند که به‌دلیل تحریم‌ها حاضر به خدمت‌رسانی به دامنه‌های ایرانی نیستند.

علی کیایی‌فر، کارشناس امنیت شبکه، در پاسخ به این سوال که چرا نهادهای ایرانی به مراجع صادرکننده غیرغربی مراجعه می‌کنند و اینکه آیا پای مسائل فنی یا اقتصادی در میان است یا خیر، گفت: «مساله اصلی ریسک دسترسی و تداوم سرویس است. امروزه موضوع این نیست که مثلا CA چینی از CA آمریکایی بهتر است یا برعکس. الان موضوع اصلی در این پرسش نهفته است که چه کسی حاضر است به یک سازمان ایرانی گواهی بدهد و بتواند این سرویس را به‌صورت پایدار به منقاضی ایرانی ارائه دهد.»

او در پاسخ به این پرسش که آیا مسیرهای جایگزین ریسک امنیتی یا حقوقی ایجاد می‌کند، گفت: «بله، ولی باید دو موضوع را از یکدیگر جدا کرد: یکی ریسک امنیتی و دیگری ریسک عملیاتی. اگر مرجع صدور گواهی معتبر باشد، به‌درستی عمل کند و روت آن مورد اعتماد مرورگرها باشد، صرف چینی یا لهستانی بودنش مشکل فنی ایجاد نمی‌کند و بنابراین مشکل امنیتی به همراه ندارد. اما برای یک سرویس حیاتی حاکمیتی، وابستگی به یک مرجع صدور گواهی خارجی، خود نوعی ریسک شخص ثالث محسوب می‌شود. برای نمونه، ممکن است این مرجع سرویس را قطع کند، گواهی را باطل کند، سیاست خود را تغییر دهد یا حتی خودش اعتماد مرورگرها را از دست بدهد. در آن صورت، بدون آنکه زیرساخت شما هک شده باشد، بخشی از سرویس عمومی‌تان دچار اختلال می‌شود.»

هشدارهایی که به کاربر داده می‌شود

تا اینجای کار، ماجرا در حد وحدود مهندسی شبکه باقی می‌ماند؛ زنجیره‌ای از روت‌ها و ضمانت‌ها (certificates) که شاید برای خواننده عادی، انتزاعی و دور از دسترس و اطلاعاتی بلااستفاده به نظر برسد. اما درست همین‌جاست که تکنولوژی از اتاق سرورها بیرون می‌زند و پا به زندگی روزمره شهروندان می‌گذارد. بانک مرکزی، در همان اطلاعیه‌ای که پیش‌تر از آن یاد شد، از کاربران خواسته بود تا زمان رفع مشکل، با عبور از پیام خطای نمایش‌داده‌شده در مرورگر، به خدمات موردنظر خود دسترسی پیدا کنند. توصیه‌ای که در نگاه نخست ساده و بی‌خطر جلوه می‌کند. شاید ما ایرانی‌ها خیلی به چنین هشدارهایی توجه نکنیم و اصلا متوجه تبعات آن نباشیم؛ اینکه همان هشدار ساده که از آن عبور می‌کنیم حفاظ امنیت ما در برابر خطرات است. رفتاری که از دید کیایی‌فر، خطرناک ارزیابی می‌شود.

او درباره راه‌حل‌های جایگزینی مانند گواهی‌های خود امضا می‌گوید: «اینجا باید تفکیک جدی قائل شد. برای یک شبکه داخلی سازمان که تمام کامپیوترها تحت مدیریت سرورهای همان سازمان است، مرجع صدور گواهی اختصاصی کاملا قابل استفاده است و اتفاقا راهکار استانداردی نیز به شمار می‌رود. اما برای یک وب‌سایت عمومی که میلیون‌ها کاربر ناشناس از اینترنت به آن متصل می‌شوند، گواهی خودامضا راه‌حل مناسبی نیست. چرا که مرورگر به کاربر هشدار می‌دهد و اگر مردم را عادت دهیم که این هشدار را نادیده بگیرند و ادامه دهند، عملا یکی از مهم‌ترین مکانیسم‌های امنیتی مرورگر را بی‌اثر کرده‌ایم. فرداروزی اگر یک کاربر وارد یک سایت جعلی شود، همان هشدار را می‌بیند و می‌گوید این هم مثل سایت فلان سازمان است و ادامه می‌دهد. این از منظر فرهنگ امنیتی بسیار خطرناک است و آسیب‌های امنیتی زیادی برای مردم ایجاد می‌کند.»

در این نقطه، توصیه رسمی یک نهاد حاکمیتی و هشدار یک کارشناس مستقل، بی‌آنکه با یکدیگر گفت‌وگو کرده باشند، در برابر هم می‌ایستند. یکی می‌گوید: از هشدار عبور کنید. دیگری می‌گوید: عبور از هشدار، خود بیماری است، نه درمان آن. میان این دو صدا، کاربر عادی می‌ماند و تصمیمی که باید گرفته شود.

چرایی نگاه به شرق

پرسشی که در ابتدای این گزارش پشت درهای بسته سایت سازمان تنظیم مقررات جا مانده بود، حالا با وزن بیشتری بازمی‌گردد: آیا آنچه رخ داده، تنها مجموعه‌ای از تصادف‌های هم‌زمان است، یا نشانه‌ای از یک تغییر جهت آگاهانه در معماری اعتماد دیجیتال کشور؟

کیایی‌فر حرکت نهادهای ایرانی به‌سمت صادرکنندگان غیرغربی را روندی طبیعی توصیف می‌کند و می‌گوید: «به نظرم این اتفاق تا حد زیادی روندی طبیعی و قابل پیش‌بینی است. وقتی سازمان‌های ایرانی مشاهده می‌کنند ریسک تحریم، عدم تمدید یا ابطال گواهی از سوی برخی مراجع غربی افزایش یافته، طبیعی است که به‌سراغ مراجعی بروند که روت‌های آنها در مرورگرهای معتبر شناخته‌شده است، اما در کشورهایی مانند چین یا سایر کشورهای غیرغربی قرار دارند. هدف نیز مشخص است: کاهش ریسک تحریم، مسدودسازی یا ابطال گواهی و افزایش پایداری سرویس. بنابراین اینکه در سال‌های اخیر برخی سازمان‌های ایرانی به‌سمت مراجع چینی یا غیرغربی رفته‌اند، به‌خودی خود امری غیرعادی نیست و می‌توان آن را نوعی مدیریت ریسک در برابر محدودیت‌های بین‌المللی دانست. البته ظاهرا این راهکار نیز ریسک را به صفر نرسانده است. در مورد چند سازمان ایرانی مشاهده می‌شود که با وجود مراجعه به مراجع چینی یا غیرغربی، باز هم مساله ابطال گواهی مطرح شده است. به‌هرحال ما در شرایط جنگی قرار داریم؛ دشمن از تمام توان خود استفاده می‌کند تا در اقتصاد کشور و کارکرد دستگاه‌های دولتی اختلال ایجاد کند.» آخرین جمله راه گشاست. این بیانگر تحمیل جنگ و گسترش آن به جهان دیجیتال است.

راهکاری برای کم کردن ریسک

اما اگر مدیریت ریسک از طریق مراجع صدور گواهی خارجی، خودش هم به منبع تازه‌ای از ریسک بدل شده، چرا کسی به فکر یک راه‌حل داخلی نیفتاده؟ این پرسشی است که در گفت‌وگو با هر کارشناس امنیت شبکه‌ای، دیر یا زود سر برمی‌آورد. عده‌ای از کارشناسان، در پاسخ به همین پرسش، ایده‌ای ساده و در نگاه نخست قانع‌کننده مطرح می‌کنند: چرا ایران به‌جای وام گرفتن اعتماد از بکن و ورشو، اعتماد را از دل خودش نسازد؟

پاسخ کیایی‌فر این گونه است: «اینکه ما در داخل کشور مرجع صدور گواهی روت داشته باشیم، یک موضوع است و اینکه آن روت در فهرست معتمدان مرورگرها و سیستم عامل‌های اصلی دنیا پذیرفته شده باشد، موضوعی کاملا متفاوت است. اگر روت ما به‌صورت عمومی مورد اعتماد کروم، فایرفاکس، سافاری و سیستم عامل‌ها نباشد، کاربر عادی همچنان هنگام ورود به سایت با خطای گواهی مواجه می‌شود. نصب دستی این «روت» (Root) روی سامانه‌های مردم نیز عملا امکان‌پذیر نیست، مگر آنکه یک مرورگر بومی تولید شود و مرجع صدور گواهی روت ملی به فهرست معتمدان آن افزوده شود. آنگاه می‌توان از مردم خواست برای کار با سامانه‌ها و سرویس‌های حاکمیتی از همان مرورگر بومی استفاده کنند.»

این جمله آخر، بی‌آنکه قصد چنین کاری را داشته باشد، یک بحث تازه را باز می‌کند، بحثی که البته این گزارش قصد ورود به آن را ندارد، اما نامش برای گوش ایرانی آشناست: ایده ساخت یک مرورگر ملی، در کنار شبکه‌ای ملی که سال‌هاست موضوع مناقشه است.

بازگشت به آغاز

این گزارش از جایی آغاز شد که یک سایت باز نمی‌شد. یک صفحه سفید، یک هشدار سرخ، و یک کاربر که نمی‌دانست مشکل از کجاست. حالا، در پایان همان مسیر، تصویر روشن‌تر شده، اما پاسخ نهایی همچنان در دست هیچ‌کس نیست. گزارش‌ها از دامنه‌ای وسیع‌تر خبر می‌دهند که هنوز نقشه کاملش کشیده نشده است. آیا اینها بخشی از یک مساله ساختاری در دسترسی نهادهای ایرانی به معماری اعتماد دیجیتال جهانی‌اند، یا رخدادهایی پراکنده‌اند که اتفاقا هم‌زمان دیده شده‌اند؟

پاسخ این پرسش، دست‌کم تا امروز، در اختیار نویسنده این سطور نیست. شاید هم در اختیار هیچ‌کس نباشد؛ نه در اختیار کارشناسی که هر روز با این زنجیره کار می‌کند و نه در اختیار نهادی که نامش را بر تارک این زنجیره حک کرده‌اند. آنچه می‌ماند، همان دری است که این گزارش پشت آن آغاز شد؛ دری که هنوز، برای بسیاری از کاربران ایرانی، باز نشده است.

سلنا گومز؛ کلاهبردار یا بنیان‌گذار استارت‌آپ؟

سلنا گومز قصد داشت «اولین اکوسیستم تناسب اندام ذهنی جهان» را ایجاد کند. در عوض، این استارت‌آپ به دردسر شخصی خودش تبدیل شده است. به گزارش بیزینس اینسایدر، یک دادخواست فدرال که روز پنج‌شنبه ثبت شد، شرح مفصلی از آنچه سرمایه‌گذاران می‌گویند در واندرماید (WonderMind) اشتباه رخ داده است، ارائه می‌دهد؛ از اپلیکیشنی که هرگز ساخته نشد تا مشارکت‌های بزرگ شرکتی که ادعا می‌کنند هرگز وجود نداشته‌اند.

گومز این استارت‌آپ را در سال ۲۰۲۱ به همراه مادرش، مندی تیفی و دانیلا پیرسون، شریک تجاری‌اش، راه‌اندازی کرد. این دادخواست، گومز، هم‌بنیان‌گذارانش و واندرماید را به کلاهبرداری از سرمایه‌گذاران و ادعاهای دیگر متهم می‌کند.

سرمایه‌گذاران شامل برنت ساندرز، مدیرعامل Bausch + Lomb و مدیرعامل سابق Allergan، و مارک رابرتز، کارآفرین و سرمایه‌گذار املاک و مستغلات، می‌شوند. در این شکایت آمده است: «شاکیان نزدیک به ۱,۲ میلیون دلار در Wondermind Global Inc. سرمایه‌گذاری کردند، زیرا متهمان به‌دروغ ادعا کرده بودند که این شرکت زیرساخت، رهبری و منابع لازم برای راه‌اندازی یک پلتفرم سودآور و بی‌نظیر در حوزه سلامت روان و تندرستی را دارد.»

سرمایه‌گذاران گفتند که بنیان‌گذاران واندرمایند بخش‌های کلیدی کسب‌وکار و برنامه‌های رشد شرکت را تیز به‌اشتباه ارائه داده‌اند. به‌طور خاص، اینکه گومز، بازیگر و خواننده مشهور جهانی، نقش مهمی در این شرکت به‌عنوان رئیس بازاریابی ایفا خواهد کرد؛ اینکه پیرسون با شرکت‌هایی مانند جی‌پی‌مورگان و فیدلیتی همکاری‌هایی را تضمین کرده است؛ و اینکه «طرح‌های درآمدزا» از قبل در حال انجام است. سرمایه‌گذاران به دنبال بازگشت سرمایه‌گذاری‌ها با خسارات خود و همچنین هزینه‌ها و حق‌الوکاله هستند.

در این شکایت آمده است: «این مشارکت‌ها وجود نداشتند. ابتکارات هرگز محقق نشدند. این اپلیکیشن هرگز ساخته نشد و به مدت سه سال، درحالی که شرکت بی‌سروصدا در اطراف آنها فروپاشید، هیچ‌یک از بنیان‌گذاران، مسوولان یا مدیران آن کلمه‌ای به سرمایه‌گذارانی که پولشان این فروپاشی را تامین می‌کرد، نگفتند.»

واندرمایند برخی پیشنهادها را در اختیار کاربران قرار داده است. وب‌سایت آن شامل مقالات، مصاحبه‌ها و برگه‌های کاری در مورد سلامت روان است. این استارت‌آپ همچنین یک خبرنامه ارسال می‌کند و دو پادکست تولید کرده است.

گومز، تیفی و پیرسون به درخواست‌های اظهارنظر بیزینس اینسایدر پاسخ ندادند. وکیلی که نماینده گومز است به مجله «بیبل» گفت که اتهامات علیه او «کاملا بی‌اساس» است. متیو زُرنگارت روز شنبه به این رسانه گفت: «ادعاهایی مبنی بر اینکه سلنا گومز به هر نحوی در هرگونه «کلاهبرداری» یا سایر تخلفات ادعایی دست داشته است، چه از نظر واقعی و چه از نظر قانونی، کاملا بی‌اساس است.»

نماینده پیرسون در بیانیه‌ای به «بوای‌ای تودی» گفت که او «قطعا اتهامات علیه خود را رد می‌کند و از فرصت ارائه اسناد و مدارک مالی محکم که حقایق را اثبات می‌کند، استقبال می‌کند.» در این بیانیه آمده است: «برای روشن شدن موضوع، او هرگز از وجوه سرمایه‌گذاران برای هزینه‌های شخصی استفاده نکرده است. کاملا برعکس: دانیلا پول خودش را در این تجارت سرمایه‌گذاری کرده و از شرکت حقوقی دریافت نکرده است.»

تیفی به‌طور علنی درباره دادخواست پاسخ نداده است. در این دادخواست، سرمایه‌گذاران اظهار کردند که در مورد مشکلاتی که واندرمایند را درگیر کرده بود، بی‌اطلاع بودند و از «آشفتگی مطلق مالی و عملیاتی» بی‌اطلاع بودند تا اینکه The Cut در سپتامبر ۲۰۲۵ مقاله‌ای در مورد این شرکت منتشر کرد.

این مقاله به‌تفصیل ادعاهای مربوط به مشکلات مدیریتی را که اندکی پس از راه‌اندازی این استارت‌آپ در سال ۲۰۲۱ آغاز شد، شرح داد. در آن زمان، تیفی و پیرسون به عنوان مدیرعامل مشترک فعالیت می‌کردند، درحالی که گومز به عنوان مدیر ارشد تاثیرگذار منصوب شد. کارکنان به The Cut گفتند تیفی که ریاست دفتر لس‌آنجلس شرکت را بر عهده داشت، سبک رهبری نامنظمی داشت و با پیرسون که دفتر نیویورک را رهبری می‌کرد، اختلاف‌نظر داشت. The Cut گزارش داد که پیرسون در سال ۲۰۲۳ در بحبوحه این تنش‌ها، استارت‌آپ را ترک کرد. در همین حال، کارکنان به The Cut گفتند گومز به دلیل اختلاف با تیفی از Wondermind فاصله گرفت. پیش‌تر بیزینس اینسایدر متوجه اختلافاتی بین ارقام مشترکین و ارقام تجاری شد که پیرسون علنا برای گروه رسانه‌ای Newsette و سوابق داخلی ذکر کرده بود. گفتنی است تحقیقات فوربس در دادخواست سرمایه‌گذاران ذکر شده است.

درآمد ۱۲ همتی فیلترشکن‌فروش‌ها

دنیای اقتصاد: اظهارات اخیر محمدجعفر قائم‌پناه، معاون اجرایی رئیس جمهور، درباره فیلترشکن‌ها یک پرسش قدیمی را با صورت‌بندی تازه‌ای مطرح کرده است: اگر فیلترشکن‌ها از نگاه مقامات امنیتی می‌توانند راه نفوذ و جاسوسی را هموار کنند، چرا بخش بزرگی از کاربران ایرانی برای دسترسی عادی به اینترنت به همین ابزارها وابسته شده‌اند؟ قائم‌پناه استفاده از فیلترشکن را از منظر امنیتی پرریسک دانسته، از گردش مالی ۷ تا ۱۲ هزار میلیاردتومانی این بازار سخن گفته و همزمان ابراز امیدواری کرده است دولت بتواند راهی برای رفع فیلترینگ پیدا کند.

اما برای سنجش این اظهارات، باید از سطح موضع‌گیری سیاسی فاصله گرفت و به وضعیت موجود نگاه کرد. بر اساس آخرین داده‌های ایسپا، ۷۴٫۴ درصد کاربران اینترنت ایران به‌طور مستمر از فیلترشکن استفاده می‌کنند. آمار را می‌توان طور دیگری هم بیان کرد. شما به این نیتر برخورده‌اید که از هر ۴ ایرانی ۳ نفر از فیلترشکن استفاده می‌کنند؟ این اعداد در کنار داده‌های دیگر، تصویری از بازاری را نشان می‌دهد که طی سال‌های فیلترینگ از یک ابزار حاشیه‌ای به بخشی از زیرساخت روزمره دسترسی ایرانیان تبدیل شده است. ابزار کنترل محتوا، حالا رونقی دارد که مگو و مپرس.

اقتصاد تاریک فیلترینگ

همان‌طور که ذکر شد، نتایج نظرسنجی ایسپا در بازه ۲۵ تا ۳۱ خرداد ۱۴۰۵ نشان می‌دهد ۷۴٫۴ درصد کاربران اینترنت اعلام کرده‌اند برای دسترسی به برخی خدمات و پلتفرم‌ها از فیلترشکن استفاده می‌کنند. تنها ۲۵٫۶ درصد گفته‌اند اصلا از آن بهره نمی‌برند. هرچند همین گروه نیز برآورد کرده‌اند حدود ۴۰ درصد اطرافیانشان از فیلترشکن استفاده می‌کنند. بخش عمده کاربران (۶۶٫۷ تا ۶۷٫۷ درصد) سرویس‌های رایگان را ترجیح می‌دهند. در میان کاربران پولی، میانگین هزینه ماهانه حدود ۲۶۲ هزار تومان گزارش شده است.

این رقم با برآوردهای دیگر نیز هم‌خوانی نسبی دارد. مرکز پژوهش‌های مجلس در اسفند ۱۴۰۳ رقم ۸۱ درصد را اعلام کرده بود و برخی گزارش‌های صنفی ارقام بالاتری برای گروه‌های سنی خاص ذکر کرده‌اند. در مقابل، قائم‌پناه در همان گفت‌وگو مدعی شد بر اساس نظرسنجی‌های انجام‌شده، ۶۵ تا ۷۵ درصد مردم در استان‌های مختلف با استفاده از فیلترشکن مخالف‌اند. دو مجموعه داده، بدون آنکه یکدیگر را نفی کنند، تصویری از فاصله میان رفتار و اظهارنظر ارائه می‌دهند. نسبتی که بدون اعداد هم می‌توان صحت آنها را به‌طور حسی تایید کرد. ما در زمانه‌ای زندگی می‌کنیم که فیلترشکن‌ها احتمالا در دستان همه پیدا می‌شوند. البته این می‌تواند محل یا منشأ مشکلات بسیاری باشد.

قائم‌پناه با استناد به گزارش مقامات امنیتی تاکید کرد: «استفاده از فیلترشکن‌ها راه نفوذ دشمن و استفاده از سرویس‌های جاسوسی را در ایران آسان‌تر کرده است. وقتی از فیلترشکن استفاده می‌کنیم راه برای دیگران باز می‌شود که ورود پیدا کنند و دیگر کنترل در اختیار شما نباشد.» او قطع چندروزه اینترنت را تنها برای شرایط اضطرار دانست و افزود فروش فیلترشکن بین ۷ تا ۱۲ هزار میلیارد تومان عواید دارد که به جیب وزارت ارتباطات، مخابرات یا اپراتورها نمی‌رود. در سوی دیگر میدان، علی حکیم‌جوادی، رئیس سازمان نظام صنفی رایانه‌ای کشور، در مرداد ۱۴۰۵ اعلام کرد بیش از ۶ درصد ترافیک شبکه کشور به حملات DDoS و سایر حملات سایبری مربوط می‌شود. این رقم در کنار گزارش‌های پیشین شرکت ارتباطات زیرساخت درباره دفع ده‌ها هزار حمله و حجم بالای ترافیک آلوده، بعدی فنی به بحث می‌افزاید. کارشناسان امنیت بارها به خطرات فیلترشکن‌های ناشناس اشاره کرده‌اند: امکان هدایت کاربر به صفحات جعلی، حضور بدافزار در برخی نسخه‌ها، و عبور ترافیک از سرورهای کنترل‌نشده.

داده‌های مربوط به زمان قطع و محدودیت اینترنت، رابطه میان اختلال دسترسی و افزایش تقاضا برای ابزارهای دور زدن فیلترینگ را روشن‌تر می‌کند. بر اساس داده‌های Top10VPN، تقاضا برای VPN در ایران در ۲۳ ژانویه ۲۰۲۶ به ۵۷۹ درصد بالاتر از میانگین روزانه ۲۸ روز پیش از خاموشی ۸ ژانویه رسید و پس از فروکش کردن موج اولیه نیز به‌طور میانگین حدود ۳۴۰ درصد بالاتر از سطح پیش از خاموشی باقی ماند. در ادامه، همزمان با بازگشت نسبی اینترنت در اواخر مه ۲۰۲۶، Proton VPN از افزایش ۱۷۵۰۰ درصدی ثبت‌نام کاربران ایرانی در ۲۸ مه خبر داد؛ این رقم یک روز پیش از آن ۶۰۰۰ درصد گزارش شده بود. پیش‌تر نیز در جریان محدودیت‌های ژوئن ۲۰۲۵، داده‌های Top10VPN از جهش تقاضای VPN تا حدود ۷۰۷ درصد بالاتر از سطح پایه حکایت داشت. این داده‌ها یک نکته مهم دارند: تقاضا برای فیلترشکن از تمایل کاربران به استفاده از یک اپلیکیشن خاص تبعیت نمی‌کند. هرچه دسترسی رسمی دشوارتر می‌شود، تقاضا برای مسیر جایگزین افزایش پیدا می‌کند. آنچه بازار سیاه را زنده نگه می‌دارد اشتیاق به اتصال است.

آن کسانی که فیلترشکن می‌فروشند

قائم‌پناه در ادامه گفت که امیدوار است مسوولان مربوطه منشأ فروش فیلترشکن‌ها را پیدا کنند و افزود کسانی که این ابزار را می‌فروشند «شاید منفعت شخصی‌شان است و شاید هم نفوذ دارند و نمی‌گذارند برای برداشته شدن فیلترینگ تصمیم‌گیری شود». او همزمان به مصوبه ستاد ویژه راهبری فضای مجازی اشاره کرد و گفت با شیوه فعلی فیلترینگ نمی‌توان مانع کشف حقیقت توسط مردم شد. به گفته وی، بسیاری از مسوولان کشور، از جمله در دفاتر مرتبط با رهبری و ریاست جمهوری، از پلتفرم‌هایی مانند توییتر و اینستاگرام استفاده می‌کنند. داده‌های ایسپا در بخش نگرش کاربران نیز نشان می‌دهد ۵۷٫۶ درصد با قطع اینترنت در شرایط بحرانی مخالف‌اند و ۵۱٫۸ درصد رفع فیلتر شبکه‌های اجتماعی را مهم یا خیلی مهم می‌دانند. اولویت اول کاربران برای رفع فیلتر، اینستاگرام (۴۷٫۸ درصد) اعلام شده است.