آزمایشگاه جنگی اسرائیل

ارتش اسرائیل چگونه با همکاری غول‌های فناوری پیشران جنگ‌های مدرن شده است

فاطمه موسوی کریمی

اعتراض کارکنان گوگل به همکاری با اسرائیل

استفاده از شبکه‌های اجتماعی، لایک کردن پست‌های دلخواه، دیدن ویدئوی دوستان و آشنایان یا گشتن دنبال محتوای خاص کار هرروزه بسیاری از ماست. جست‌وجو در گوگل و سر زدن به یوتیوب هم که دیگر گروه سنی خاصی نمی‌شناسد و از ملزومات زندگی در این دوران است. حال اگر بدانیم تک‌تک این لایک‌ها و جست‌وجوها، محتوایی که می‌بینیم، چه آن‌هایی که روی آن‌ها مکث می‌کنیم و چه آن‌هایی که سریع اسکرول می‌کنیم، همه و همه برای ساخت پروفایلی از ما از سوی گوگل و متا و دیگر غول‌های فناوری به اشتراک گذاشته می‌شود چه می‌کنیم؟ برای انسان این دوران اسم هم اختراع شده، نتیزن یا شهروند اینترنت نامی است که احتمالاً برازنده بسیاری از ماها است. مایی که تمام اطلاعات مورد نیاز را از اینترنت می‌گیریم، در شبکه‌های اجتماعی عضو هستیم و از بسیاری از اپلیکیشن‌ها برای راحت‌تر بودن کارمان استفاده می‌کنیم. موتور جست‌وجوی گوگل، اینستاگرام، فیسبوک، یوتیوب و بسیاری از این اپ‌ها رایگان هستند، تا به حال از خود پرسیده‌اید چرا و چطور این خدمات رایگان به دست ما می‌رسد؟ جوابش ساده و ترسناک است، «ما» آن پولی هستیم که هزینه می‌کنیم؛ اطلاعات ما، علایق ما، حریم خصوصی ما. حتماً دیده‌اید وقتی اپی را دانلود می‌کنید یا می‌خواهید از خدمات رایگان وب‌سایتی استفاده کنید یا نسخه جدیدی از آندروید یا آی‌او‌اس را در گوشی خود نصب کنید یا «terms and conditions» مواجه می‌شوید که باید حتماً آن را قبول کنید وگرنه از خدمات و یا به‌روزرسانی خبری نیست. وقتی روی آن کلیک می‌کنید تا آن را بخوانید یا چند صفحه مطلب مواجه می‌شوید که با فونت بسیار ریز نوشته شده، فهمیدنش سخت است و برای شما هم گنگ به نظر می‌رسد پس عطایش را به لقایش می‌بخشید و با آن موافقت می‌کنید. این متن طولانی که عمداً سخت و گنگ نوشته شده کلید همان جاسوسی غول‌های فناوری از من و شماست. ما با زدن تیک مقابل آن‌ها به این اپ‌ها اجازه می‌دهیم اطلاعات شخصی، ترجیحات وعلایق ما را به «دلالان داده» بفروشند.

دلالان داده؛ تاجران سایه

دلالان داده شرکت‌ها یا افرادی هستند که اطلاعات شخصی افراد را از منابع مختلف جمع‌آوری، تجمیع و به فروش می‌رسانند. این اطلاعات اغلب شامل جزئیات حساس مانند نام، آدرس، شماره تلفن، ایمیل، سن، جنسیت، وضعیت تأهل، درآمد، علایق سیاسی و حتی عادات خرید است. در دنیای امروز شبکه‌های اجتماعی و اینترنت منبع اصلی این داده‌ها هستند. دلالان این اطلاعات را به شرکت‌های تبلیغاتی، دولت‌ها و حتی مجرمان سایبری می‌فروشند. یکی از کاربردهای اصلی این داده‌ها فروش برای تبلیغات هدفمند است. حتماً متوجه شده‌اید که گاهی صبح در گوگل قیمت لپ‌تاپ را سرچ کرده‌اید و دو ساعت بعد موقع چرخیدن در اینستاگرام با انبوه ویدئوهایی مواجه شده‌اید که در مورد کارایی و قیمت لپ‌تاپ‌های مختلف توضیح می‌دهند. یکی دیگر از کاربردهای اطلاعات ما برای دلالان داده ساختن پروفایل است. گاهی کار آن‌ها اینقدر دقیق است که حتی فیسبوک نیز این اطلاعات را از آن‌ها می‌خرد. ولی ساختن پروفایل دقیقاً به چه معناست؟

پروفایل‌سازی؛ نقشهٔ نامرئی از زندگی ما

در قدم اول دلال داده اطلاعات مختلف را از منابع عمومی و تجاری (خرید آنلاین و فعالیت‌های اجتماعی) جمع‌آوری می‌کند. مثلاً اگر کاربر در فیسبوک پستی را لایک کند یا در گوگل جست‌وجویی انجام دهد متادیتای آن (مانند زمان و مکان) جمع‌آوری می‌شود. آن‌ها حتی گاهی برای افرادی که در اینترنت حسابی ندارند هم از طریق اطلاعات دوستان و بستگان «پروفایل سایه» می‌سازند. در قدم دوم این داده‌ها را ترکیب می‌کنند تا به «دسته‌بندی‌هایی مانند «علاقه‌مند به سیاست چپ» و یا «خریدار آنلاین لباس» یا «مرد متأهل دارای فرزند» برسند و در قدم بعدی این اطلاعات را به پلتفرم‌ها می‌فروشند تا آن‌ها بتوانند تبلیغات مناسب بر اساس علایق و محل زندگی کاربر را به او نمایش دهند. حال، دولتی را تصور کنید که خریدار و یا دارنده این اطلاعات باشد، رژیمی را تصور کنید که دسترسی به پیشرفته‌ترین هوش مصنوعی‌ها دارد و می‌تواند اطلاعات شخصی میلیون‌ها کاربر را در زمانی بسیار کم پردازش کرده و پروفایل‌های پرجزئیات بسازد، مردمی را تصور کنید که نام خود را «ملت استارتاپ» گذاشته‌اند و تمام غول‌های فناوری را در سرزمین خود جمع کرده‌اند و اتاق‌هایی را تصور کنید که نظامیان بر پردازش این اطلاعات در آن‌ها نظارت دارند. به اسرائیل خوش آمدید.

سیلیکون وادی؛ نسخه نظامی سیلیکون ولی

مسئولیت اصلی جمع‌آوری، تحلیل و رمزگشایی اطلاعات الکترونیک در اسرائیل با واحد ۸۲۰۰ است. نام رسمی آن «واحد مرکزی جمع‌آوری است» اما با کد ۸۲۰۰ شناخته می‌شود و زیر نظر شاخه اطلاعات نظامی «امان» فعالیت می‌کند و فرمانده آن عموماً یک سرتیپ است. بسیاری از بازنشستگان این واحد پس از پایان خدمت به شرکت‌های بزرگ فناوری می‌پیوندند. البته کلمه بازنشسته شما را به اشتباه نیندازد و یاد مدیران ۸۰-۹۰ ساله‌ای نیفتید که در اوج ضعف قوای بدنی و فکری هم حاضر به ترک میز خدمت نیستند. اینجا صحبت از افرادی است که نهایتاً ۱۰ سال در واحد ۸۲۰۰ و سازمان‌های مشابه خدمت کرده و حالا قرار است هم جای خود را به نیروهای جوان‌تر بدهند و هم از تجربه خود در آن سازمان‌ها در قالبی نو بهره ببرند. آن قالب نو «سیلیکون وادی» نام دارد. احتمالاً نام «سیلیکون ولی» به گوشتان خورده، همان جایی در کالیفرنیا که محل تجمع تمام غول‌های فناوری و مرتبط با عصر اینترنت است. اسرائیل هم برای خود سیلیکون ولی دارد که نامش را «سیلیکون وادی» گذاشته و کپی برابر اصل همان نسخه آمریکایی را ساخته است. با این تفاوت که در اسرائیل تمام این اطلاعات به خدمت نظامیان درمی‌آید و واحد ۸۲۰۰ یکی از مهم‌ترین آن قسمت‌هاست.

غزه؛ آزمایشگاهی برای تمام فصول

غزه به عنوان «زمین صفر» انواع فناوری‌ها و هوش مصنوعی عمل می‌کند. هوش مصنوعی‌هایی مانند «گاسپل» و «لوندر» اول در غزه تست شده‌اند. از این فناوری‌ها برای مکان‌یابی اعضای حماس و چهره‌نگاری آن‌ها استفاده می‌شود. این فناوری در کنار «گوگل فوتوز» به اسرائیل اجازه می‌دهد که چهره افراد را حتی اگر فقط قسمتی از صورتشان در عکس وجود دارد شناسایی کنند و همه این‌ها به جز استفاده اسرائیل از انواع موشک‌ها و پهپادهای جنگی و شناسایی در غزه است که پس از هر درگیری در غزه تقاضای جهانی برای سلاح‌های اسرائیلی را افزایش می‌دهند زیرا آن‌ها به عنوان «تست شده در جنگ» بازاریابی می‌شوند. کتاب «آزمایشگاه فلسطین» نوشته آنتونی لونشتاین (به همراه مستندی که وی برای الجزیره انگلیسی ساخت) به خوبی توضیح می‌دهد که چگونه اشغال فلسطین به اسرائیل کمک کرده تا فناوری‌های نظارتی را توسعه داده و از تکنولوژی در خدمت نظارت و آدم‌کشی استفاده کند. بازوی اسرائیل در استفاده و توسعه از این ابزارها همان واحد ۸۲۰۰ است.

پگاسوس؛ جاسوسی در جیب

شرکت اسرائیلی NSO در سال ۲۰۱۶ بدافزاری به نام پگاسوس (در افسانه‌های یونان باستان پگاسوس اسب بالدار سفیدرنگ و نماد آزادی شناخته می‌شود) را عرضه کرد که به یکی از مخوف‌ترین ابزارهای جاسوسی دیجیتال معروف شد. نرم‌افزاری که به جای پرواز در آسمان‌ها در گوشی‌های هوشمند پرسه می‌زد و شخصی‌ترین اطلاعات افراد را جمع‌آوری می‌کرد و حتی در صورت خاموش کردن تلفن همراه هم باز می‌توانست به مکالمات گوش دهد. پگاسوس اولین بدافزاری بود که بدون کلیک کاربر می‌توانست وارد گوشی شده و به دوربین، پیام‌ها عکس‌ها و حتی موقعیت مکانی دسترسی کامل پیدا کند. دولت اسرائیل از این بدافزار علیه روزنامه‌نگاران، فعالان حقوق بشر، سیاستمداران و حتی رهبران کشورها استفاده کرده است. در سال ۲۰۲۱ سازمان عفو بین‌الملل روش‌های تشخیص پگاسوس را فاش کرد و نشان داد این شرکت اسرائیلی از آن برای هک حساب‌های واتساپ استفاده کرده است. در سال ۲۰۲۵ NSO محکوم به پرداخت ۱۷۰ میلیون دلار به واتساپ شد و این فقط یکی از ابزارهای جاسوسی دولتی اسرائیل است که لو رفته است.

نیمبوس؛ ابری که سایه انداخت

در سال ۲۰۲۱ گوگل و آمازون قراردادی به ارزش ۱٫۲ میلیارد دلار با اسرائیل امضا کردند تا در قالب پروژه نیمبوس (ابر باران‌زا) خدمات ابری، هوش مصنوعی و زیرساخت دیجیتال را به دولت و ارتش اسرائیل ارائه دهند، اما از همان ابتدای کار با انتقادات زیادی برای استفاده از این خدمات در عملیات نظامی روبه‌رو شدند. فعالان حقوق بشر و کارمندان گوگل به خاطر موضوعی که آن را «آپارتاید دیجیتال» می‌نامیدند علیه این موضوع تظاهرات کردند. یکی از کارمندان گوگل به آنتونی لوونشتاین گفته بود شرکت‌های فناوری از جنگ سود می‌برند و می‌توانند برای این خدمات میلیاردها دلار دریافت کنند، ضمن اینکه این کار برای آن‌ها عواقبی در پی ندارد و حتی باعث می‌شود به خاطر تجربیات دست اولشان دیگر کشورها هم به آن‌ها مراجعه کنند.

فرادداده؛ جزئیات کوچک، افشاگری‌های بزرگ

متادیتا داده‌هایی است که درباره داده‌های دیگر توصیف یا توضیحی ارائه می‌دهد بدون اینکه خود محتوای اصلی را شامل شود. به عبارت ساده‌تر متادیتا مانند اطلاعات جانبی است که به ساماندهی، جست‌وجو و مدیریت داده‌های اصلی کمک می‌کند. مثلاً وقتی با گوشی عکس می‌گیرید محتوای اصلی عکس (تصویر) است، اما متادیتا شامل اطلاعاتی مانند زمان گرفته شدن عکس، مکان جی‌پی‌اس، مدل دوربین، رزولوشن تصویر و حتی تنظیمات نوردهی می‌شود. این اطلاعات در فایل عکس ذخیره می‌شود اما مستقیماً نشان داده نمی‌شود مگر اینکه از ابزارهای خاصی برای استخراج آن استفاده کنید. متادیتا نقشی کلیدی در نظارت دارد، زیرا بدون محتوای اصلی الگوها را فاش می‌کند. آژانس امنیت اسرائیل برنامه‌ای برای جمع‌آوری متادیتای انبوده دارد، مثلاً متادیتای گوگل فوتوز (زمان و مکان عکس) و یا گوگل مپس (مسیرها) برای نقشه‌برداری استفاده می‌شوند و تمام این اطلاعات در ساختن پروفایل برای افراد کاربرد دارند.

بیایید مورد فرضی علی را بررسی کنیم تا بهتر متوجه موضوع شویم:

۱- جمع‌آوری اطلاعات در اکوسیستم متا

علی در ایران زندگی می‌کند، در فیسبوک پست‌هایی را لایک می‌کند که مربوط به اعتراضات اجتماعی است و یا زیر بعضی پست‌های سیاسی کامنت می‌گذارد. در اینستاگرام او استوری‌های دوستانش که محتوای ضدجنگ یا حمایت از حقوق بشر دارد را بازنشر می‌کند، همچنین موقعیت مکانی او نشان می‌دهد که در تجمعات عمومی شرکت کرده است. متا این داده‌ها را جمع‌آوری می‌کند: لایک‌ها، کامنت‌ها، دنبال‌کنندگان و حتی زمان صرف شده روی محتواهای خاص. از این داده‌ها الگوریتم می‌تواند استنباط کند که علی ممکن است دیدگاه لیبرال یا مخالف دولت داشته باشد.

۲- جمع‌آوری داده در خدمات گوگل

علی در گوگل جست‌وجوهایی مانند «اخبار جنگ غزه» و یا «تحریم اسرائیل» انجام می‌دهد و ویدئوهایی با همین موضوع در یوتیوب تماشا می‌کند و از طریق گوگل مپس، موقعیت او نشان می‌دهد که به رویدادهای فرهنگی و اجتماعی مرتبط رفته است. گوگل این داده‌ها را ثبت می‌کند: تاریخچه جست‌وجو، ویدئوهای تماشا شده و مکان‌های بازدید شده. از این داده‌ها می‌تواند استنباط کند که علی به مسائل خاورمیانه علاقه‌مند و منتقد اسرائیل است.

۳- ادغام چندپلتفرمی و ایجاد پروفایل جامع

حالا تصور کنید یک سیستم اطلاعاتی (مانند دولت یا شرکت‌های خصوصی اسرائیل) به این اطلاعات دسترسی دارند. داده‌های متا و گوگل با هم ترکیب می‌شوند، لایک‌های فیسبوک علی با جست‌وجوهای گوگلش همخوانی دارد، همچنین روابط او (دوستان فیسبوکی که محتوای مشابه به اشتراک می‌گذارند) با مکان‌های بازدید شده (از گوگل مپس) لینک می‌شود تا شبکه اجتماعی او کامل شود. درنتیجه یک پروفایل جامع نه تنها از علی بلکه از دوستان او ساخته می‌شود.

ترکیب داده‌ها در شبکه‌های اجتماعی (به همراه تگ و کامنت) با داده‌های رفتاری روابط واقعی خانوادگی و دوستی را آشکار می‌کند. هوش مصنوعی این داده‌ها را تحلیل کرده و از افراد به استنباط‌هایی می‌رسد و این استنباط‌ها منبع عمل تحلیل‌گران و تصمیم‌گیران نظامی و اطلاعاتی قرار می‌گیرد.

اوسینت OSINT؛ وقتی اطلاعات عمومی به سلاح تبدیل می‌شود

در سال‌های ۲۰۱۴ تا ۲۰۱۸ سازمان‌های اطلاعاتی سیا و ام‌آی ۶ از طریق OSINT (جمع‌آوری و تحلیل اطلاعات از منابعی که به طور عمومی در دسترس همه قرار دارند) برای نظارت بر داعش استفاده کردند. داعش از طریق شبکه‌های اجتماعی برای پروپاگاندا، استخدام عضو و هماهنگی عملیات استفاده می‌کرد. گزارش‌ها نشان می‌دهند تحلیل متادیتا از پست‌های عمومی این گروه و هوادارانش به ساخت پروفایل‌های دقیق افراد و گروه‌ها کمک کرد و منجر به عملیات علیه آن‌ها شد. این گروه‌ها توانستند از روی geotag پست‌ها (برچسب مکانی) مکان دقیق آن‌ها (مانند اردوگاه‌های سوریه و عراق) را شناسایی کنند. کاربران هوادار داعش در اپ‌هایی مانند فیسبوک وارد می‌شدند که مکان واقعی تجمعات آن‌ها را فاش می‌کرد. این به نقشه‌برداری از گروه‌های محلی کمک کرد. کامنت‌ها، لایک‌ها و به اشتراک‌گذاری ویدئوها نشان‌دهنده وابستگی بود. مثلاً اگر کاربری ویدئوهای داعش را به اشتراک می‌گذاشت الگوریتم osint، روابط او با دیگر اعضا را استنباط می‌کرد. با ترکیب این متادیتا، سازمان‌ها پروفایل افراد (مانند استخدام‌کنندگان داعش) و گروه‌ها را ساختند. مثلاً از geotag برای استنباط مسیر مهاجرت اعضا استفاده کردند و توانستند با همین روش در سال ۲۰۱۵ یکی از اعضای داعش در اروپا را رهگیری کنند.

مورد ترسناک ادوارد اسنودن

ادوارد اسنودن، کارمند سازمان امنیت ملی آمریکا، همان جوانی که در سال ۲۰۱۳ با افشای اسناد محرمانه سازمان متبوعش جهان را تکان داد حالا یکی از مهم‌ترین صداهای هشداردهنده در دنیای دیجیتال است. وی یک روز تصمیم گرفت همه چیز را فاش کند و بگوید دولت آمریکا چگونه از شرکت‌های فناوری برای جاسوسی از شهروندان خود استفاده می‌کند و البته به گفته خودش «کاری که آمریکا با شهروندانش می‌کند در مقایسه با کاری که با مردم جهان می‌کند بسیار مهربانانه است.» افشاگری او نشان داد غول‌هایی مانند گوگل و متا نه تنها داده‌های ما را جمع‌آوری می‌کنند بلکه آن را با دولت‌ها به اشتراک می‌گذارند تا پروفایل‌های دقیق از زندگی ما بسازند. وی در سال ۲۰۱۵ و در گفت‌وگو با بی‌بی‌سی توضیح داد که سازمان امنیت ملی می‌تواند با یک پیامک رمزنگاری شده -که کاربر حتی نمی‌بیند- گوشی را هک کرده و به میکروفون، دوربین و پیام‌ها دسترسی پیدا کند. او هشدار داد خاموش کردن گوشی کافی نیست، زیرا موبایل‌های هوشمند می‌توانند «تظاهر به خاموش بودن» کرده و همچنان جاسوسی کنند، چرا؟ چون باتری غیرقابل تعویض اجازه می‌دهد دستگاه همچنان سیگنال بفرستد. اسنودن این را «صنعت ناامنی» می‌نامد، صنعتی که آسیب‌پذیری‌ها عمداً فروخته می‌شوند تا دولت‌ها و هکرها از آن سوء استفاده کنند.

پروفایل‌های سایه

تصور کنید شما خواهرزاده دانشمند هسته‌ای یا فرماندهی نظامی هستید. دایی شما نه تنها در شبکه‌های اجتماعی حضور ندارد بلکه اصلاً گوشی هوشمند هم ندارد، ولی شما از اینستاگرام و گوگل استفاده می‌کنید. کافی است که عکسی خانوادگی را در گوگل فوتوز یا فضای ابری مایکروسافت آپلود کنید. از این طریق آنها پی به دایره دوستان و خویشاوندان می‌برند. متادیتای عکس اطلاعات بیشتری را فاش می‌کند. اگر از گوگل مپس برای رفت و آمد استفاده کنید یا نام وی را در گوگل سرچ کنید سیستم‌های اطلاعاتی (ازجمله واحد ۸۲۰۰) این داده‌ها را ترکیب می‌کنند و ممکن است برای هک، جاسوسی، عملیات سایبری و یا تحت نظر قرار گرفتن شما، دوستان و اعضای خانواده‌تان از آن اطلاعات استفاده کنند.

داده به مثابه مهمات

طبق گزارش ۳۰ آگوست نیویورک تایمز و بر اساس مصاحبه با مقامات ایرانی و اسرائیلی این رسانه مدعی شده، فرماندهان سپاه مانند شهیدان حاجی‌زاده و سلامی گوشی هوشمند نداشتند اما محافظان و رانندگان آن‌ها این قوانین را نادیده می‌گرفتند و حتی پست‌هایی در شبکه‌های اجتماعی منتشر می‌کردند. اسرائیل با هک این دستگاه‌ها موقعیت لحظه‌ای فرماندهان را ردیابی و حملات هوایی دقیق خود را اجرا کرد. یکی دیگر از عملیات‌های تروریستی اسرائیل در جنگ دوازده روزه حمله به پناهگاه زیرزمینی جلسه شعام با حضور رئیس جمهور بود. هک گوشی محافظان، مکان را فاش کرد و اسرائیل با شش بمب ورودی‌ها را مسدود ساخت که منجر به شهادت چند تن شد. ساسان کریمی در مورد عملیات «عروسی خونین» که سردار حاجی‌زاده و ۱۹ فرمانده هوافضا در جلسه اضطراری هدف حمله قرار گرفتند به نیویورک تایمز گفت «محافظان احتیاط لازم را نکردند و این ضعف بزرگی بود.» یکی از مقامات اسرائیلی هم گفته بود «تعداد زیاد محافظان نقطه ضعفی شد که از آن استفاده کردیم.»

شمشیر دولبه

تمام آنچه در متن گفته شد می‌تواند مانند شمشیری دولبه عمل کند. آنچه به حماس کمک کرد تا در حمله هفت اکتبر بتواند تصویر دقیقی از پایگاه‌ها و پاسگاه‌های ارتش داشته باشد تصاویری بود که سربازان اسرائیلی از خود در شبکه‌های اجتماعی منتشر کرده بودند. طبق گزارش روزنامه هاآرتص در ژوئیه ۲۰۲۴، حماس اطلاعات حساس بسیاری را از طریق منابع عمومی جمع‌آوری کرده و از آن‌ها در جریان حمله خود بهره برد. طبق این گزارش آن‌ها برای بیش از ۳۰۰۰ سرباز پروفایل‌های دقیق ساخته بودند. نمونه دیگر بنیاد هند رجب است که کارش شناسایی سربازان اسرائیلی‌ای است که در نسل‌کشی شرکت کرده‌اند. آن‌ها هم عموماً از طریق اوسینت و عکس و داده‌های سربازان اسرائیلی در شبکه‌های اجتماعی توانسته‌اند تعدادی از آن‌ها را شناسایی کرده و به محض ورودشان به کشورهای سراسر جهان علیه آن‌ها به جرم ارتکاب جرائم جنگی اعلام جرم کنند. این موارد باعث شده ارتش اسرائیل قوانین سخت‌گیرانه‌ای برای انتشار اطلاعات در رسانه‌های اجتماعی وضع کند، زیرا پست‌ها به عنوان «نشت اطلاعاتی» عمل می‌کنند.

بهای پنهان خدمات رایگان

ما هر روز بی‌آنکه بدانیم، ردپاهایی از خود در دنیای دیجیتال به جا می‌گذاریم؛ یک لایک ساده، جست‌وجویی کوتاه در گوگل یا چند ثانیه مکث روی یک ویدئو. همین ردپاها برای غول‌های فناوری و دولت‌ها مانند طلاست که از دلشان پروفایلی ساخته می‌شود دقیق‌تر از آنچه ما خود از خویش می‌دانیم. داستان پگاسوس نشان داد که این داده‌ها فقط ابزار تبلیغات یا سرگرمی نیستند، بلکه می‌توانند به سلاح تبدیل شوند. در جنگ‌های مدرن، خدمات رایگان بهایی پنهان دارند؛ بهایی که با حریم خصوصی، آزادی و حتی امنیتمان پرداخته می‌شود.