نوروزنامه فیلتربان

بسته نوروزی فیلتربان به همراه عیدی فیلترشکن پرمیوم رایگان

زمستان بلند سرکوب دیجیتال

این بسته را با بلوتوث برای دیگران بفرستید

این بسته را با بلوتوث برای دیگران بفرستید

فهرست مطالب

تصویرسازی روی جلد با استفاده از اثر ارنستو یرنا

مقدمه

زمستان بلند سرکوب دیجیتال

بسته نوروزی ایران در خاموشی به همراه عیدی فیلترشکن پرمیوم رایگان لنترن

سالی که گذشت سالی تلخ برای ایرانیان در تمام زمینه‌ها و به خصوص حوزه حقوق دیجیتال بود. سالی که در بهار و تابستان با قطعی متمادی اینترنت همراه بود، پس از خیزش سراسری بر اثر مرگ مهسا امینی به زمستانی بلند در حوزه حقوق دیجیتال بدل شد.

مجموعه پیش رو گوشه‌ای از محتوای تولیدی گروه کارشناسان فیلتربان و وب سایت ایران در خاموشی در سال ۱۴۰۱ است که آن را می‌توان به عنوان چکیده آنچه در این سال بر حقوق دیجیتال ایران رفت، در نظر گرفت.

سالی که سرکوبگران و مخالفان جریان آزاد اطلاعات در جمهوری اسلامی ایران قطعات باقی مانده از پازل طرح موسوم به صیانت را به مرور در کنار یکدیگر قرار دادند تا در واپسین روزهای اولین سال قرن جدید شمسی، تصویری واضح از بزرگترین کابوس فعالین حقوق دیجیتال در ایران یعنی فیلترینگ غیرهمسان و برقراری اینترنت طبقاتی به دست دهند؛

سال ۱۴۰۱ با خبرهایی از افزایش صد درصدی قیمت ترافیک خارجی اینترنت آغاز شد و به بهانه اعتراضات سراسری به مسدودسازی شبکه‌های اجتماعی و خدمات محبوب ارتباطی از جمله واتساپ و اینستاگرام انجامید. زیرساخت‌های شبکه ملی اطلاعات به سرعت گسترش پیدا کرد و به موازات تصویب قوانینی برای جرم‌انگاری فروش وی‌پی‌ان در مجلس، اعطای وی‌پی‌ان های قانونی به افراد و اقشار گزینش شده آغاز شد.

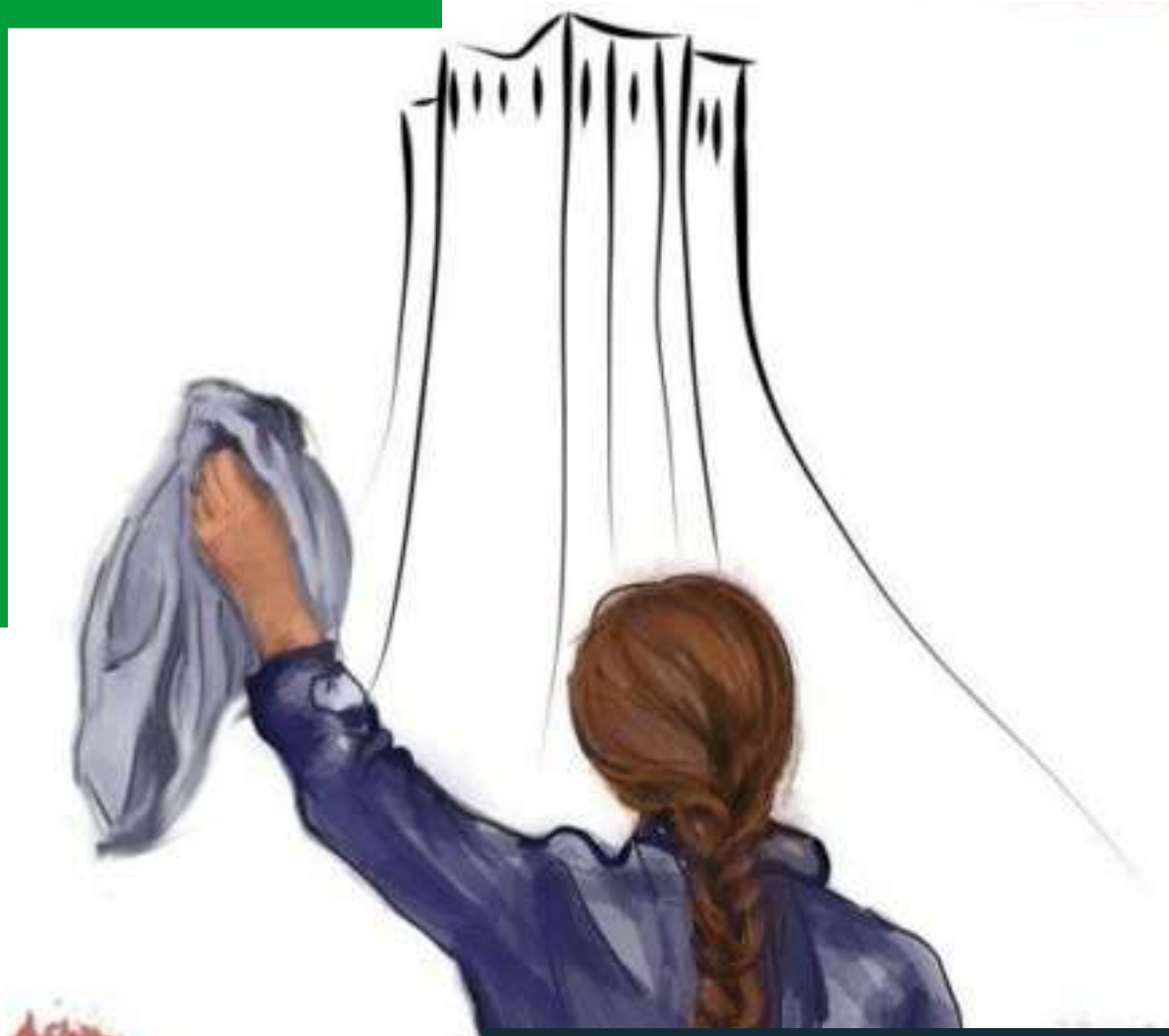
شیوه‌های نوین ردگیری معترضین و شهروندان نظیر طرح سیام و استفاده از تکنولوژی تشخیص چهره در کنار الحاق فضای مجازی به قلمروی اخلاقی جمهوری اسلامی با ارایه طرح‌هایی در مجلس نظیر طرح مجازات «بازنشردهندگان روایت غیررسمی» نیز از دیگر اخبار مهم حوزه دیجیتال در سالی که گذشت، بود.

ما در فیلتربان باور داریم که مهمترین راه برای مقابله با سرکوب سازمان یافته دیجیتال و محدودیت‌های روزافزون اینترنت، آگاهی رسانی گسترده و ایجاد حساسیت عمومی نسبت به این موضوع است.

ما یک بسته نوروزی کم‌حجم برایتان فراهم کرده‌ایم که می‌توانید آن را از طریق بلوتوث برای همدیگر بفرستید. استفاده از بلوتوث همچنین یادآور این مهم است که این ابزار قدیمی در مواقع قطع اینترنت و برای استفاده از برخی پیام‌رسان‌ها قابل استفاده است. این بسته همچنین شامل توصیه‌های فنی برای پیشگیری از شنود و دسترسی به اطلاعات شخصی شما توسط نیروهای امنیتی در زمان اعتراضات است. مقاله‌های بلندتری هم در این بسته گنجانده شده که وضعیت ایران از نظر سرکوب حقوق دیجیتال را بررسی کرده است.

در این بسته، تعداد محدودی وی‌پی‌ان لنترن (نسخه پرمیوم) قرار دارد. برای دریافت این وی‌پی‌ان‌ها می‌توانید درخواست‌تان را به بات تلگرامی @MIAAN_HELPLINE، یا شماره تلفن ۴۶۷۶۶۸۶۰۵۰۳+ در واتساپ یا سیگنال پیام بفرستید.

این وی‌پی‌ان‌ها توسط شرکت خوش‌نام لنترن و در همکاری با وب‌سایت ایران در خاموشی ارایه می‌شود.



گزارش تحقیقی

زن، زندگی، آزادی: جمع‌بندی از وضعیت حقوق دیجیتال در ایران در جریان اعتراضات

ملودی کاظمی

در این گزارش به برخی از مسایل کلیدی حقوق دیجیتال در ایران می‌پردازیم که پس از مرگ مهسا امینی در اعتراضات ماه‌های اخیر مطرح شدند.

بیش از چهار ماه از مرگ مهسا ژینا امینی می‌گذرد، زن جوان کردی که به دلیل «بدحجابی» دستگیر شد و در بازداشتگاهِ گشت ارشاد جان خود را از دست داد. مرگ تراژیک او در جهان طنین انداخت و یکی از بزرگترین موج های اعتراضی در تاریخ جمهوری اسلامی را سبب شد. جنبشی با عنوان کردی «ژن، ژیان، ئازادی» شکل گرفت که آن‌را انقلابی و فمینیستی توصیف کرده‌اند و همین جنبش توانست طبقات مختلف و اقلیت‌های گوناگون را متحد سازد.

در حالی‌که این جنبش با اوج و فرودهای خود ادامه دارد، واکنش دولت همان روال همیشگیِ خشونت بیش از اندازه و غیرقانونی علیه معترضان و توسل به سلاح‌های مرگبار است که با محدودیت بیشترِ دسترسی به اینترنت همراه است. طبق آمار خبرگزاری «هرانا»، از شروع تظاهرات تا کنون ۵۲۵ معترض کشته شده‌اند که ۷۱ نفر از آنها کودک بوده‌اند، ۱۹ هزار و ۵٤۵ نفر دستگیر شده، و ٤ تن نیز اعدام شده‌اند؛ آماری که تقریبا روزانه بالا می‌رود. تعداد کشته‌شدگان در میان اقلیت‌های کرد و بلوچ بسیار بالا بوده‌است.

بنا به گفته «کمیته دفاع از گزارشگران» (CJP)، از میان دستگیرشدگان دست‌کم ۸۸ نفر خبرنگار بوده‌اند. تعدادی از کنشگران سرشناس حقوق دیجیتال در ایران نیز در میان دستگیرشدگان هستند. چند نفر از آنها بعدا آزاد شدند اما بسیاری دیگر هنوز در بند هستند.

زن، زندگی، آزادی اثر گلنار عادلی

اینترنت و ارتباطاتِ دیجیتال نقش مهمی در انتقال اطلاعات میان داخل و خارجِ کشور بازی می‌کنند. این نقش به ویژه در زمان اعتراضات و برهه‌های حساس سیاسی اهمیت بیشتری پیدا می‌کند. این رابطه شامل ارتباط میان شهروندان در داخل کشور و رساندن اخبار به خارج از مرزها می‌شود تا از آن طریق بتوان رویدادهای جاری را مستند کرد. مثل موارد قبلی، برخورد پیش‌بینی‌پذیر دولت برای ساکت کردن معترضان شامل «حکومت نظامی دیجیتالی» یا «منع عبور و مرور دیجیتالی» بوده است؛ به معنیِ قطع اینترنت در مناطق خاص و ساعت‌های معین، پایین آوردن عمدی سرعت اینترنت و مسدود کردن پلتفرم‌های بین‌المللی. سال‌هاست که جمهوری اسلامی درصدد پیاده‌کردن طرحی است که محدودیت‌های اجتماعی و سیاسی جامعه مدنی را در پهنه فضای مجازی نیز بگستراند و همزمان کاری کند که این محدودیت‌ها موجب قطع منافع اقتصادیِ اینترنت نشود.

با هر بحران سیاسی یا اعتراضات مردمی، فرصتی فراهم می‌شود که دولت بتواند ضمن تحکیم ابزارهای موجود سانسور و فیلترینگ، تازه‌ترین فاز سیاست‌های اقتدارگرایانه دیجیتالیِ خود را به آزمون بگذارد. در اعتراضات کنونی ما شاهد سیاست تازه «منع عبور و مرور اینترنتی یا دیجیتالی» بودیم. در کنار «فیلترینگ غیرهمسان یا طبقه‌بندی شده» و رصد کردن رفتار کاربران در فضای مجازی نیز جریان داشت و روش‌های مرسوم و آشنای سانسور اینترنت نیز مثل گذشته اعمال می‌شدند.

گزارشی که می‌خوانید خلاصه‌ای از این تحولات و موقعیت حقوق دیجیتال در ایران را از شروع اعتراضات در شهریور ۱٤۰۱ به دست می‌دهد. هدف این گزارش ارایه یک تصویر چکیده از موضوعات کلیدی در چند ماه اخیر است. «فیلتربان» امیدوار است در آینده نزدیک بعضی از این موضوع‌ها را با جزییات بیشتری مورد تحقیق قرار دهد.

نقض حقوق زنان در فضای مجازی و بیرون از فضای مجازی: به‌هم‌ریختن مرزها

مرگ غم‌بار مهسا ژینا امینی در بازداشتگاه گشت ارشاد رویدادی بود که سرکوب سیستماتیک حقوق زنان و اقلیت‌های قومی را خاطرنشان کرد و شعله اعتراضاتی که تا امروز ادامه دارد را برافروخت. شعار «زن، زندگی، آزادی» معرف این جنبش و مساله حقوق زنان شاخص اصلی آن شد. سرکوب زنان در فضاهای واقعی و فیزیکی بر همگان شناخته‌شده است، اما به طور روزافزون شاهد سرکوب در فضای مجازی را هستیم. تجهیز شدن به به تکنولوژی و ابزار رصد و نظارت، محدودیت‌های تحمیل شده بر زنان در فضاهای عمومی را تشدید کرده‌است.
برخی از این محدودیت‌ها مدت‌ها قبل از اعتراضات اخیر آغاز شده بودند. «فیلتربان» و «تراز» در سال ۱۴۰۱ گزارش مشترکی با عنوان «حقوق بشر و دیجیتالی‌شدن فضاهای عمومی در ایران» منتشر کردند که نشان می‌داد چگونه پلتفرم‌های دیجیتال، مثل اپلیکیشن اشتراک دوچرخه، سیاست‌های تفکیک جنسیتی را بر کاربران تحمیل می‌کنند. این کار با منع ثبت‌نام زنان دراین اپلیکیشن و محدود کردن دوچرخه‌سواری به پارک‌های «مخصوص بانوان» صورت گرفته‌است.

پس از پایان پژوهش ما و تنها چند هفته قبل از آنکه اعتراضات مردمی آغاز شود، محمدصالح هاشمی گلپایگانی، رییس ستاد امر به معروف و نهی از منکر در گفتگویی فاش کرد که این ستاد از «تکنولوژی تشخیص چهره برای حرکات نامتعارف و ناموزون» از جمله «قصور در اجرای قوانین حجاب» استفاده می‌کند. هاشمی گلپایگانی گفت، «تصویر به دست آمده از دوربین‌های نظارتی با عکس کارت شناسایی ملی تطبیق داده می‌شود و در صورت تخلف، اقدامات قانونی از جمله جریمه و بازداشت را به دنبال خواهد داشت.»
کارت شناسایی ملی یا کارت هوشمند حامل اطلاعات بیومتریک مثل عکس چهره شهروندان است و دولت این اطلاعات را در اختیار دارد. طبق گزارش کنشگران حقوق بشر در ایران، در سال ۲۰۲۲ میلادی هزار و ۷۰۱ مورد نقض حقوق زنان ثبت شده است.
ما نمی‌دانیم استفاده از فناوری تشخیص چهره در ایران چقدر رایج است و از همین‌رو تخمین تعداد کسانی که از این طریق مورد تعقیب قانونی قرار گرفته‌اند، دشوار است. همین‌طور روشن نیست که دولت این تکنولوژی را از کجا به دست آورده است. آنچه می‌دانیم این است که یک شرکت چینی به نام «تیاندی» که تولیدکننده فناوری رصد ویدیویی است با سپاه پاسداران، نیروی انتظامی و ارتش همکاری داشته است. مشخص شده است که تعداد دیگری از شرکت‌های فناوری چینی در زمینه تکنولوژی نظارت ویدیویی ارتباط‌هایی با جمهوری اسلامی داشته‌اند.

> **سرکوب زنان در فضاهای واقعی و فیزیکی بر همگان شناخته‌شده است، اما به طور روزافزون شاهد سرکوب در فضای مجازی را هستیم.**

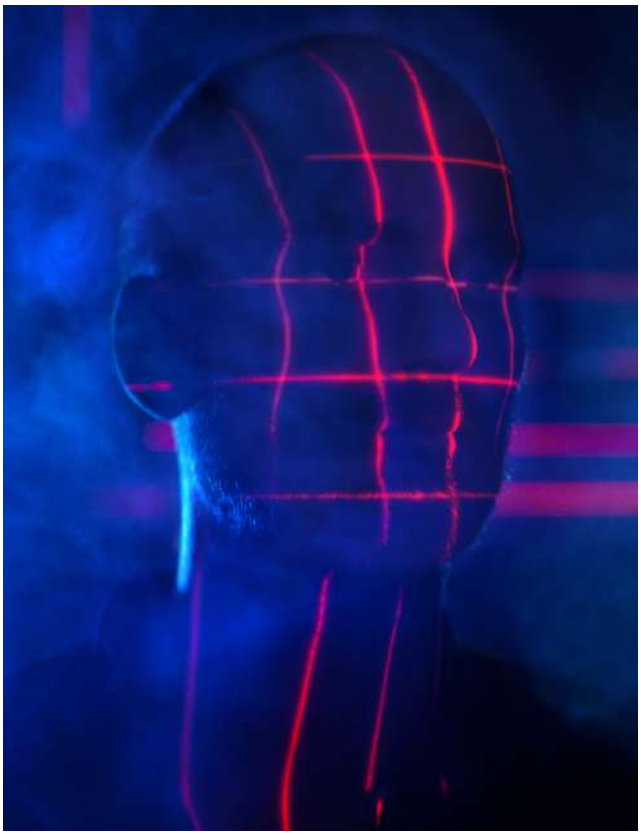
باید به یاد داشته باشیم که عیرغم استفاده بیشتر از فناوری تشخیص چهره، انواع قدیمی‌تر فناوری نیز این قابلیت را دارند که با کارکردهای جدیدی مثل رصد شهروندان به خدمت گرفته شوند.
در طرح «ناظر» که توسط نیروهای انتظامی پیاده شد،پلیس با استفاده از دوربین‌های ترافیک شهری بانوانی که حجاب را رعایت نکرده بودند،شناسایی می‌کرد.
پس از شناسایی، مسوولان با پیامک‌هایی این شهروندان را به پیگرد قانونی تهدید می‌کردند. جزییات این طرح‌ها و نوع فناوری‌های مورد استفاده در آنها کمتر شناخته شده‌است، اما همین نمونه نشان می‌دهد که چگونه فناوری‌های مربوط به کنترل ترافیک و دوربین‌های ناظر بر تخلفات رانندگی می‌توانند در خدمت نظارت و رصدِ رفتار شهروندان قرار گیرند.

شیوه‌های دیگر نظارت و رصد شهروندان

حقایق مربوط به استفاده از فناوری نظارت و کنترل در ایران هنوز در پرده ابهام است اما در جریان تظاهرات اخیر روزنه‌ای باز شد که بتوانیم از آن به ظرفیت‌های نظارت و سرکوب دیجیتالی نگاهی بیندازیم. سایت خبری «اینترسپت» در گزارشی مستند نشان داد که سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری) با استفاده از یک سیستم دیجیتال به نام «سیام» (SIAM) که کارکردهای نظارتی بسیاری دارد، از جمله می‌تواند به لاگ‌ها یا فایل‌های اطلاعاتی مربوط به تماس‌ها دسترسی پیدا کند، سرعت شبکه‌ها را کاهش دهد و از این طریق بر فعالیت آنلاین کاربران نظارت داشته باشد. این کارکردها به ویژه برای کسانی که در تظاهرات شرکت می‌کنند، تهدیدآمیز است. براساس اطلاعاتی که در اختیار فیلتربان قرار گرفته، تعداد قابل توجهی از دستگیری‌ها نه در هنگام وقوع تظاهرات بلکه زمانی که معترضان به خانه برگشته بودند، اتفاق افتاده است. باید نتیجه گرفت که برای شناسایی این معترضان از ابزارهای دیجیتال نظارت، شناسایی، و ردگیری استفاده شده است، هرچند جزییات دقیقی از روش‌های به کار رفته در دسترس نیست.

همان‌طور که پیش‌بینی می‌شد، در ماه آبان ۱۴۰۱ استفاده از انواع فیلترشکن به هنگام خاموشی‌های اینترنتی، برای مقابله با سانسور آنلاین افزایش پیدا کرد. دو پلتفرم بزرگ اینستاگرام و واتس‌اپ مشمول این سانسور شدند.

هنوز نمی‌دانیم در ماه‌های وقوع اعتراضات چه تعداد از کاربران داخل کشور موفق به دور زدن سانسور شده‌اند و دولت تا چه میزان توانسته دسترسی به محتوا و خدمات اینترنتی را محدود کند. در این مورد، کمبود اطلاعات از خصلت تکنیکی ابزارهای ضد سانسور ناشی می‌شود. اما همین که انبوهی از کاربران برای یافتن ابزار ضدسانسور هجوم می‌آورند، می‌تواند مورد سواستفاده مقامات امنیتی یا سودجویان قرار گیرد.



در دی‌ماه ۱۴۰۰، سایت «بیت‌دیفندر» (Bitdefender) در یک گزارش تحقیقی آشکار کرد که یک نرم‌افزار نظارت‌گر و ردیاب به نام «سِکندآی» (SecondEye) که در ایران تولید شده به طور مخفیانه داخل یک نرم‌افزارنصب‌کننده وی‌پی‌ان به نام «تونتی‌سپید وی‌پی‌ان» (۲۰SpeedVPN) ــ که آن‌هم در ایران تولید می‌شود ــ تعبیه شده است تا کسانی که از این طریق وی‌پی‌ان نصب می‌کنند، زیر نظارت رصدگر «سکند آی» قرار بگیرند. دراین‌باره در اردیبهشت ۱۴۰۱ کارزاری افشاگر به راه افتاد. بسیاری از قربانیان این دام ساکن ایران بودند و تعداد کمتری نیز در آمریکا و آلمان به سر می‌بردند. «سکندآی» یا همان نرم‌افزاری که مخفیانه تعبیه شده بود، می‌تواند به اطلاعات حساس و محرمانه نظیر اسناد، عکس‌ها، کیف‌پول‌های دیجیتالی و رمزهای عبور شبیخون بزند. محدودیت‌های روزافزون اینترنتی در ایران باعث شده که کاربران بیشتری به نصب وی‌پی‌ان و فیلترشکن روی بیاورند و یافتن وی‌پی‌ان‌های امن و قابل اعتماد برای کاربران چالش بزرگی به حساب می‌آید. آنها اکنون باید خطرات بیشتری را از سر بگذرانند تا بتوانند ابزاری کارآمد برای دور زدن سانسور بیابند و طبعاً ریسک بالاتری را در قبال آلوده شدن به نرم‌افزارهای جاسوسی بپذیرند.

سیاست جدید «حکومت نظامی دیجیتالی» و «قطع استراتژیک و منطقه‌ای اینترنت»

قطع اینترنت تاکتیکی است که دولت عموماً برای خنثی کردن اعتراضات و جلوگیری از تبادل اطلاعات در داخل کشور و میان داخل با خارج به کار می‌گیرد و از همین طریق نقض حقوق بشر را نیز لاپوشانی می‌کند. نخستین و تنها مرتبه‌ای که اینترنت در سراسر کشور تقریبا به صورت یکپارچه قطع شد، در آبان ۱۳۹۸ بود که به دنبال اعتراضات گسترده به افزایش بهای بنزین رخ داد. این خاموشیِ سراسری یک هفته طول کشید.

از آبان ۹۸ تاکنون دیگر شاهد قطع سراسری اینترنت نبوده‌ایم، اما قطع منطقه‌ای اینترنت بارها رخ داده است. قطع منطقه‌ای در محل وقوع اعتراضات و در مکان درگیری میان مردم و نیروهای امنیتی صورت می‌گیرد. این نوع از خاموشی اینترنتی را در سال‌های ۱۳۹۹، ۱۴۰۰، و ۱۴۰۱ در سیستان و بلوچستان، کردستان، و تهران شاهد بوده‌ایم. اعتراضات اخیر پس از مرگ ژینا امینی نیز به همین سرنوشت دچار شد.

اعتراضات حوالی ۲۵ شهریور ۱۴۰۱ شروع شد و از همان روز برای نخستین‌بار قطع اینترنت در ساعت‌های غروب مشاهده شد. تظاهرات غالبا در ساعات اول شب به اوج می‌رسید و در نتیجه قطع اینترنت از حوالی چهار بعد از ظهر به طور منظم به اجرا درمی‌آمد.

به همین دلیل این سیاست به نام «ساعات منع رفت و آمد دیجیتالی» شناخته شد.

خاموشی‌های منطقه‌ای در سایر مکان‌های وقوع اعتراضات مثل استان کردستان نیز ادامه پیدا کرد. این خاموشی‌های اینترنتی بیشتر دامنگیر گوشی‌های همراه متصل به شبکه‌های اصلی موبایل مثل ایرانسل، ام‌سی‌آی، و رایتل می‌شد. طبق تازه‌ترین آمارهای رگولاتوری، پوشش اینترنت موبایل در ایران بالای صد در صد است، در حالی‌که اینترنت ثابت خانگی زیر ۱۵ درصد جمعیت را پوشش می‌دهد. در جریان خاموشی‌های اینترنتی اخیر، محتوا و خدمات بعضی از شرکت‌ها از طریق «شبکه ملی اطلاعات» (اینترانت داخلی) آنلاین و در دسترس بودند.

به مرور زمان، بیشتر مشاهده می‌کنیم که ارتباطها به‌جای آنکه کاملا قطع شود، فقط از طریق خدمات شبکه ملی اطلاعات امکان‌پذیر می‌شود، اما این روند هنوز کند و نامنظم است.

می‌توانیم چند دلیل را نام ببریم که چرا خاموشی‌های منطقه‌ای و منحصرا موبایل جایگزین سیاست قطع سراسری اینترنت شده است؛

نخست هزینه‌ای است که خاموشی‌ها در بر دارند. با وجود این‌که شبکه ملی اطلاعات می‌تواند خسارت قطع اینترنت را پایین بیاورد، قطع سراسری اینترنت در کشور می‌تواند تأثیری فلج‌کننده بر اقتصاد کشور بگذارد. در زمان قطع سراسری سال ۹۸، با آنکه هنوز دسترسی محدودی میسر بود، طبق برآورد سایت «تاپ‌تِن‌وی‌پی‌ان» (Top۱۰VPN) در همان سال، خسارت قطع سراسری اینترنت در ایران بالغ بر ۶۱۱ ممیز ۷ میلیون دلار شد. منطقه‌ای کردن قطع اینترنت که فقط گوشی‌های همراه را دربرگیرد به احتمال زیاد هزینه‌ی این سیاست را برای اقتصاد کشور پایین می‌آورد. باید اضافه کنیم، در سال ۱۴۰۱، به ویژه به دنبال اعتراضات شهریور، به خاطر اختلال‌ها و خاموشی‌های اینترنتی، اقتصاد ایران خسارتی بالغ بر ۷۷۳ میلیون دلار به بار آورد. کمی پایین‌تر در این گزارش، به این موضوع می‌پردازیم که چگونه بخش فناوری و شرکت‌های خدمات اینترنتی در ایران از خاموشی‌های اینترنتی آسیب می‌بینند.

دومین دلیلی که می‌توان برای خاموشی‌های منطقه‌ای به جای قطع سراسری برشمرد، این است که رصد کردن خاموشی‌های محلی با ابزارهای موجود دیده‌بانی شبکه دشوارتر است و رصد کردن آنها معمولا وقت بیشتری می‌گیرد. از همین‌رو مقامات دولتی ترجیح می‌دهند با این گزینه اقدامات خود را از چشم‌های پژوهشگران پنهان نگه دارند.

چه کسانی دستور قطع اینترنت را می‌دهند؟

مقامات دولتی همیشه با توجیه «امنیت ملی» دست به قطع اینترنت می‌زنند یا به طور عمد سرعت اینترنت را کاهش می‌دهند با این ادعا که تنها از این طریق می‌توان «اغتشاشات» را پایان داد. مثلا رییس‌جمهور ابراهیم رییسی در سخنرانی ۱۶ آذر ۱۴۰۱ در دانشگاه تهران مدعی شد که، «دلیل محدودیت‌های اینترنتی ناامنی و اختلالی است که دشمن در کشور ایجاد کرده است.» همان‌طور که وزیر وقت ارتباطات، محمدجواد آذری جهرمی فاش کرد، قطع اینترنت در آبان ۹۸ به دستور شورای امنیت ملی صورت گرفت. در نتیجه چنین تصمیمی در سطح کشوری بر عهده همین نهاد است.

طبق اطلاعات رسیده به فیلتربان ، از آبان ۹۸ به بعد برای قطع اینترنت در سطح منطقه و استان، نخست فرماندار باید این تقاضا را به مرکز بفرستد، سپس وزیر کشور که ریاست شورای امنیت ملی را هم عهده‌دار است باید این تقاضا را تایید کند. اگر تقاضا برای قطع اینترنت همزمان از چند استان برسد، رییس جمهور باید دستور تیید بدهد. براساس اطلاعات منبع فیلتربان، قطع اینترنت در سیستان و بلوچستان در بهمن ۹۹ با همین روش اجرا شد.

ضرر مالی: هزینه خاموشی‌های اینترنت

بیشترین زیان قطع اینترنت متوجه حقوق بشر است، اما اختلال‌های دایمی در دسترسی به اینترنت باعث خسارت‌های هنگفت به بخش فناوری و کسب‌وکارهایی است که درآمدشان از راه خدمات آنلاین به دست می‌آید. همان‌طور که گفتیم، طبق تحقیق «تاپ‌وی‌پی‌ان»، در سال ۲۰۲۲ خاموشی‌های اینترنتی خسارتی معادل ۷۷۳ میلیون دلاربه اقتصاد ایران وارد کرد که پس از روسیه دومین کشور به لحاظ ضرر مالی از این بابت است. این ضرر در سال ۲۰۲۱ بالغ بر ۲ میلیون دلار بود.

اپراتورهای شبکه‌های تلفن همراه در ایران بیشترین ضربه‌های مالی را متحمل می‌شوند. از آذرماه ۱۴۰۱ به بعد، اپراتورهای شبکه‌بزرگی نظیر رایتل، شاتل، ایرانسل، و مبین‌نت در گزارش‌های خود به سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری) و وزیر ارتباطات خبر از زیان‌های مالی عظیم داده‌اند. این زیان‌ها شامل از دست دادن ۳۰ تا ۶۰ درصد پهنای باند مصرفی و دست‌کم ۲۰ درصد از درآمد بوده است.

> **در سال ۲۰۲۲ خاموشی‌های اینترنتی خسارتی معادل ۷۷۳ میلیون دلاربه اقتصاد ایران وارد کرد**

سایر کسب‌وکارهای آنلاین، مثل اپلیکیشن مسیریاب «بلد» نیز به فاصله‌ی کمی پس از اجرای محدودیت‌های اینترنتی از مشکلات بزرگ گزارش داده و سرزنش را متوجه «شرایط جاری» کرده‌اند. شرکت هزاردستان مالک مسیریاب بلد اعلام کرد که، ده‌ها نفر از کارکنان خود را اخراج کرده و تضمینی برای دوام این پلتفرم در آینده وجود ندارد. ما نمی‌دانیم پیش از محدودیت‌های اخیر اینترنتی، این پلتفرم تا چه اندازه موفق بوده است. اما تردیدی نیست که رخدادهای اخیر باعث دشوارتر شدن وضعیتی شده که پیش از این هم چندان پایدار نبود.

کسب‌وکارها و افرادی که برای درآمدزایی و بازاریابی به اینستاگرام متکی بودند نیز به احتمال زیاد از این محدودیت‌ها لطمه دیده‌اند. هرچند محاسبه دقیق خسارت بر کسب‌وکارهای اینستاگرام دشوار است، در بهمن ۱۳۹۹ علی ربیعی، سخنگوی وقت دولت متذکر شد که اگر اینستاگرام مسدود شود به درآمد حدود یک میلیون نفر آسیب خواهد رسید. در اسفند ۱۴۰۰، مرکز بررسی و تحلیل«بتا» نوشت، ۹ میلیون ایرانی از راه اینستاگرام کسب درآمد می‌کنند. آمار منتشرشده دراین‌باره با یکدیگر تفاوت آشکار دارند و فیلتربان نمی‌تواند به طور مستقل آنها را راستی‌آزمایی کند.

با این حال، حتی اگر آمارخوش‌بینانه دولت را هم در نظر بگیریم باید گفت که، مسدود کردن اینستاگرام در سال ۱۴۰۱ باعث قطع درآمد تعداد بی‌شماری از شهروندان ایرانی شد. هرچند دولت انکار می‌کند که از شهریور ۱۴۰۱ به این طرف دست به اخلال‌ها و محدودیت‌های اینترنتی گسترده‌ای زده، اما اعلام کرده است که به جبران خسارت‌های احتمالی، بسته‌های حمایتی برای «سکوها و کسب و کارهای اقتصاد دیجیتال»، از جمله وام و تسهیلات اهدایی دیگر در نظر گرفته است. تأثیر مالی منفی ناشی از خاموشی‌های اینترنتی بر افراد و کسب‌وکارها که درآمد و معیشت آنها به اینترنت وابسته است بدون شک مهم است، اما تاثیر محدودیت‌های اینترنتی بر حقوق دیجیتال نیز باید مورد توجه قرار گیرد. بخش خصوصی فناوری در کشور که تا اندازه‌ای استقلال خود را در قبال دولت حفظ کرده، فشار مالی زیادی را تحمل می‌کند. اما محدودیت‌های اخیر اینترنتی، به این معنی است که این شرکت‌ها به ناچار باید دست نیاز به سمت دولت دراز کنند و از طریق وام و بسته‌های حمایتی به بقای خود ادامه دهند. میزان تاثیرات منفی این وابستگی بر حقوق دیجیتال را نمی‌توان اکنون پیش‌بینی کرد، اما چنین رابطه‌ای دست دولت را برای زیر فشار گذاشتن شرکت‌های خدمات اینترنتی و دریافت اطلاعات کاربران باز می‌گذارد. برآیند دیگر این وابستگی آن است که این کسب‌وکارها و کارمندان آنها دست به خودسانسوری زده، از انتقاد به سیاست‌های دولت بپرهیزند مبادا که کمک‌ها و قراردادهای آنها به خطر بیفتد.

سرنوشت واتس‌اپ و اینستاگرام

اینستاگرام و واتس‌اپ که هر دو به شرکت متا تعلق دارند از معدود رسانه‌های اجتماعیِ بین‌المللی بودند که در ایران فیلتر نمی‌شدند. این وضعیت پس از اعتراضات اخیر و اختلال‌های اینترنتی تغییر کرد و شورای امنیت ملی تصمیم گرفت این دو پلتفرم را در ۳۰ شهریور ۱۴۰۱ مسدود کند. در توجیه مصوبه شورای امنیت، سردار غلامرضا جلیلی، عضو شورا و رییس سازمان پدافند غیرعامل، «همکاری این دو شبکه اجتماعی با دشمن در حوزه بی‌نظمی و به هم زدن امنیت کشور» به عنوان دلیل این انسداد مطرح کرد.

در سال‌های گذشته مقامات متعدد، از بستن اینستاگرام استقبال کرده بودند. این بحث ها در دولت حسن روحانی به جایی نرسید. در آخرین ماه‌های دولت روحانی، آذری جهرمی، وزیر وقت ارتباطات توسط دادسرای فرهنگ و رسانه به دادگاه احضار شد تا در مورد سرپیچی از دستور فیلتر کردن اینستاگرام توضیح دهد.

حمله‌های مداوم به اینستاگرام، به ویژه از سوی اصولگرایان تندرو به نگرانی در مورد سرنوشت این پلتفرم در ایران دامن می‌زد. اینستاگرام نه تنها یک ابزار مهم اجتماعی و ارتباطی است بلکه در تامین معاش بسیاری از شهروندان که کسب‌وکار و بازاریابی آنها وابسته به این پلتفرم است، نقش حیاتی داشته است.

در تیرماه ۱۴۰۱، عیسی زارع‌پور، وزیر ارتباطات و فناوری اطلاعات در واکنش به اخبار فیلتر شدن اینستاگرام و واتس‌اپ گفت، این موضوع تنها یک شایعه است و هیچ تصمیمی در این مورد گرفته نشده است.

اعتراضات شهریور ۱۴۰۱ فرصت خوبی بود تا به بهانه «اغتشاشات» و «دخالت خارجی» این پلتفرم‌های بین‌المللی زیر تیغ سانسور بروند. این همان الگوی آشنایی است که پیش‌تر دامنگیر محبوب‌ترین پیام‌رسان آن‌زمان شد. پلتفرم تلگرام یک بار در سال ۹۶ طی اعتراضات خیابانی مسدود شد اما کمی بعد از زیر سانسور بیرون آمد، تا سرانجام سال بعد به حکم دادگاه، به طور رسمی و برای آخرین‌بار مشمول فیلترینگ شود. اختیار مقامات قرار دهند.

داستان نامه مرکز ملی فضای مجازی به شرکت متا

در اکتبر ۲۰۲۲ دولت ایران مصمم شد از فرصت استفاده کرده و با شرکت متا، صاحب واتس‌اپ و اینستاگرام، ارتباط برقرار کند. در نامه‌ای از طرف مرکز ملی فضای مجازی از شرکت متا خواسته شده با همکاری در تعیین محتوا و همسو با قوانین جمهوری اسلامی کمک کند که دو پلتفرم از قید فیلتر آزاد شوند. چند هفته پیش از آن وزارت اطلاعات و سازمان اطلاعات سپاه پاسداران در یک بیانیه مشترک شرکت متا را متهم کردند از طریق «اخبار جعلی» و «محتوای خشونت آمیز» دست به فریب مردم ایران زده‌اند. این ادعاها زمانی مطرح شد که شرکت متا تصمیم داشت بخشی از محتوای کاربران را که در آنها شعار اعتراضیِ مرگ بر خامنه‌ای آمده بود حذف کند. این تصمیم سپس لغو شد.

> رییس سازمان پدافند غیرعامل، «همکاری این دو شبکه اجتماعی با دشمن در حوزه بی‌نظمی و به هم زدن امنیت کشور» به عنوان دلیل این انسداد مطرح کرد.

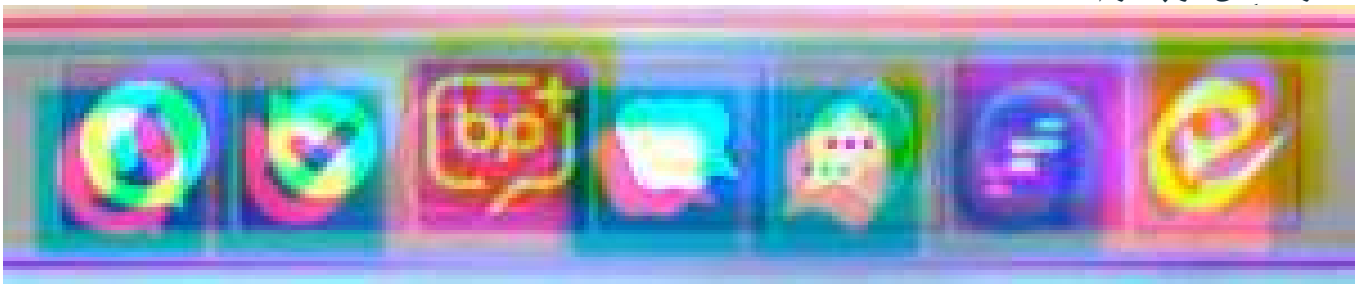
شرکت متا در برخی از کشورها دفتر نمایندگی دارد و در مواردی با دولت‌ها همکاری کرده است، اما در مورد ایران، این شرکت پیش‌شرط‌های جمهوری اسلامی را رد کرد و در بیانیه‌ای که از بی‌بی‌سی فارسی پخش شد اعلام کرد که، «باور دارد همگان، از جمله ایرانیان، باید به خدمات آنلاین دسترسی داشته باشند.» و شرکت متا، «افتخار می‌کند که مردم با استفاده از اینستاگرام اعتراضات را حمایت کرده و آن را مستند می‌نمایند.»

ایران پیش‌تر از طریق مصوبه‌های شورای عالی فضای مجازی و نسخه‌های متعدد «طرح صیانت» روشن کرده بود که می‌خواهد همانند برخی از کشورها در منطقه نمایندگانی از شرکت‌های مهم رسانه‌های اجتماعی در ایران داشته باشد که تضمین دهند عملکرد این پلتفرم‌ها با قوانین کشور هماهنگی دارد. البته، مجموعه‌ی تحریم‌های اقتصادی که فعالیت شرکت‌های رسانه‌ای بین‌المللی در ایران را دشوار کرد و بدتر شدن نقض حقوق بشر ایران را از سایر کشورها متمایز می‌کند و به همین جهت واکنش متا به تقاضای ایران جای شگفتی ندارد. اکنون، مقامات دولتی همین واکنش را بهانه خواهند کرد تا به فیلترینگ آن دو پلتفرم ادامه دهند.

دیرزمانی است که پیام‌رسان‌های داخلی در حال برنامه‌ریزی و توسعه بوده‌اند زیرا در پروژه شبکه ملی اطلاعات این نرم‌افزارها به طور مستقیم با کاربران سروکار دارند و از این بابت نقش مهمی ایفا می‌کنند. برخی از این پیام‌رسان‌ها برای رشد و توسعه خود از وام‌های دولتی بهره برده‌اند و با نهادهای دولتی ارتباط مستقیم و غیرمستقیم دارند. پیام‌رسان‌های بومی مثل روبیکا، بله، گپ ، ایتا، و سروش در سال‌های اخیر توجه بیشتری به خود جلب کرده‌اند زیرا کاربران مجبور بوده‌اند برای دسترسی به برخی خدمات، از جمله سرویس‌های بانکی و دولتی، این اپلیکیشن‌ها را دانلود و نصب کنند.

آنها در حالی‌که در رقابت با همتاهای بین‌المللی به طور ارگانیک رشد چندانی نداشته‌اند، از طریق ایجاد انگیزه و روش‌هایی مثل خدمات رایگان یا ترافیک ارزان در مقایسه با نمونه‌های خارجی توانسته‌اند تعداد مشتریان خود را افزایش دهند. این اپلیکیشن‌ها در برابر کنترل دولتی آسیب‌پذیرتر هستند و احتمال می‌رود که دسترسی به داده‌های مشتریانِ خود را در اختیار مقامات دولتی بگذارند.

موارد مستندی از نقض حق حریم خصوصی در رابطه با این اپلیکیشن‌ها وجود داشته؛ نظیر مورد روبیکا که اطلاعات کاربران در اینستاگرام را بدون اطلاع آنهاکپی کرده بود.



پس از چاپ پاسخ متا در آبان ۱۴۰۱، در دی‌ماه هیات نظارت بر محتوای متا تصمیم حذف شعار «مرگ بر خامنه‌ای» را لغو کرد و توضیح داد که آن فقط یک شعار سیاسی لفظی است و یک تهدید جدی محسوب نمی‌شود.

در واقع، اهمیت اپلیکیشن‌های داخلی برای حاکمیت در اکتبر ۲۰۲۲ مشهود شد؛ هنگامی که فروشگاه «گوگل پلی» پیام‌رسان روبیکا را به دلیل «نگرانی‌های امنیتی» حذف کرد و مقامات ایرانی در واکنش به این تصمیم سرویس‌های گوگل مثل نقشه، مترجم، فایربیس، APIها، گوگل‌پلی، چت، و حتی فونت را مسدود کردند.

به لحاظ منطقی، کاربران داخل کشور به خاطر مسایل امنیتی و حریم خصوصی، و همچنین ظرفیت‌های فنی و تعداد کاربران، رغبت چندانی به اپلیکیشن‌های داخلی ندارند و ترجیح می‌دهند از پیام‌رسان‌های قابل اعتماد بین‌المللی استفاده کنند.

پیام‌رسان‌های داخلی از پیدایش تا آلایش

محدودیت‌های اخیر اینترنتی در ایران و فیلترشدن واتس‌اپ و اینستاگرام این تنها بازمانده‌های پیام‌رسان‌های بین‌المللی را، برای آنها که وی‌پی‌ان ندارند، از دسترس خارج کرد. این فرصت مغتنمی بود برای مقامات تا اپلیکیشن‌های داخلی را تبلیغ کنند. کاربران نیز که دست‌شان از همتاهای خارجی کوتاه شده به ناچار این اپلیکیشن‌ها را دانلود و نصب می‌کنند. عیسی زارع‌پور وزیر ارتباطات هم خبر داد که طرح اتصال پیام‌رسان‌های داخلی در حال اجرا است به نحوی که بتوان میان انواع مختلف پیام رد و بدل کرد. این نیز تلاش دیگری برای ترغیب کاربران و بالا بردن تعداد مشتریان اپلیکیشن‌های داخلی است تا دولت به نام عرضه خدمات بیشتر عملا کنترل خود را بر کاربران افزایش دهد.

یافتن تعداد دقیق کاربران اپلیکیشن‌های داخلی دشوار است، اما در آذرماه ۱۴۰۱ سخنگوی روابط عمومی پیام‌رسان ایتا ادعا کرد که ۱۵ میلیون و هشتصد کاربر فعال در ماه و ۹ میلیون و ۲۰۰ هزار کاربر در روز در این پلتفرم حضور پیدا می‌کنند. روبیکا تعداد ۷۰ میلیون کاربر ثبت نام شده را گزارش داد ــ آماری بسیار بالا با توجه به اینکه در ایران تعداد کاربران اینترنت ۷۱ میلیون و ۹۴۰ هزار نفر تخمین زده می‌شود ــ و پیام‌رسان سروش‌پلاس ۳ و نیم میلیون کاربر، و پیام‌رسان بلد ۳ میلیون و ۳۰۰ هزار کاربر گزارش دادند. در مقایسه با آمار سال ۱۴۰۰ که مرکز ملی فضای مجازی منتشر کرد، این ارقام رشد چشمگیری را ارایه می‌کنند..

ارقام واقعی هرچه باشد، انتظار می‌رود که تعداد کاربران پیام‌رسان‌های داخلی بالا برود. این افزایش ناشی از نیازی است که مسدود کردن اپلیکیشن‌های خارجی ایجادکرده است. به دلایلی مثل ارزان‌تر بودن این پلتفرم‌ها یا این‌که هنگام اعتراضات و قطع اینترنت، این پیام‌رسان‌ها از طریق شبکه ملی اطلاعات در دسترس باقی می‌مانند، روند بومی کردن اینترنت سرعت بیشتری می‌گیرد.

در میان‌مدت یا درازمدت، با بالا رفتن تعداد متقاضیان پیام‌رسان‌های داخلی، تلاش برای کنترل و سانسور محتوای آنها نیز مطابق با قوانین موجود و به دست پلیس سایبری فتا یا صدا و سیما افزایش خواهد یافت. این دو سازمان سابقه‌ای طولانی در نظارت و سانسور پلتفرم‌های داخلی و خارجی دارند و در مواردی با شکایت قانونی و دادگاهی کردن خاطیان هدف‌های خود را جلو برده‌اند.

در آینده چه خواهد شد؟

معترضان همچنان به خیابان‌ها می‌آیند و با سرکوب خشن روبرو می‌شوندتا یکی از پرشمارترین و پایدارترین اعتراضاتی که ایران طی سالیان به خود دیده را شکل دهند. در دوره‌های بحرانی، ما دیده‌ایم که حاکمیت در پاسخ به بحران، یک فاز جدید یا یک جز تشکیل‌دهنده‌تازه را در مسیر استقرار نظام تمامیت‌خواه دیجیتالی به اجرا می‌گذارد.

در اعتراضات آبان ۹۸، ما شاهد بودیم که چطور شبکه ملی اطلاعات در حال شکل گرفتن است، چگونه خدمات داخلی آنلاین در دسترس باقی می‌مانند، درحالی‌که سرویس‌های بین‌المللی از دسترس خارج می‌شوند. از آن زمان تا کنون هر بار که اینترنت قطع شده، آزمون تازه‌ای برای کارآمدکردنِ سیاست خاموشی‌های اینترنتی و اِعمال محدودیت بیشتر برای شبکه‌ی جهانی اینترنت بوده است.

> در دوره‌های بحرانی، ما دیده‌ایم که حاکمیت در پاسخ به بحران، یک فاز جدید یا یک جز تشکیل‌دهنده‌تازه را در مسیر استقرار نظام تمامیت‌خواه دیجیتالی به اجرا می‌گذارد.

در طول اعتراضات اخیر، با مسدود کردن واتس‌اپ و اینستاگرام ما شاهد قدم‌های بعدی برای مجبور ساختن کاربران به استفاده از پیام‌رسان‌های داخلی بودیم. اما گام‌های مهم دیگری نیز در این مسیر در حال برداشته شدن است؛ مثل فیلترینگ غیرهمسان یا طبقه‌بندی شده. این نوع از فیلترینگ هدفش کنترل بیشتر دسترسی کاربران به خدمات بین‌المللی است. در این طرح، فقط افراد یا گروه‌هایی که مورد قبول دولت هستند به «وی‌پی‌ان‌های قانونی» دسترسی خواهند داشت. سایر شهروندان تنها به خدمات داخلی یا به شکل محدود به محتوا و سرویس‌های خارجی دسترسی پیدا می‌کنند. این تلاشی است در راه نهادینه کردن یک روش جامع و پایدار برای محدود کردن اینترنت که به طور گزینشی اجازه می‌دهد گروه‌های خاص به اینترنت بین‌المللی دسترسی داشته باشند و از منافع آن بهره‌مند شوند، اما کنترل و نظارت دولتی همواره بر میزان این دسترسی باقی خواهد ماند.

با آنکه وی‌پی‌ان‌های قانونی هنوز به طور رسمی به بازار وارد نشده‌اند ــ هرچند سالهاست که اجرای این طرح در دستور کار است ــ قدم حیاتی دیگری که برای محدود کردن اینترنت برداشته شده، تعقیب قانونی کسانی است که از فیلترشکن‌های موجود استفاده می‌کنند. طبق قانون جرایم رایانه‌ای، توزیع انواع وی‌پی‌ان و فیلترشکن ممنوع است. این قانون تا این زمان چندان جدی به اجرا گذاشته نشده بود، اما در دی‌ماه ۱۴۰۱ اعلام شد که وزارت ارتباطات و فناوری اطلاعات موظف شده است که فیلترشکن‌ها را شناسایی و از دسترس خارج کند. طبق این تصمیم، اشخاصی که دست به تولید، انتشار، توزیع، یا فروش «وی‌پی‌ان های غیرمجاز» بزنند به حبس یا جزای نقدی محکوم خواهند شد. جرم‌انگاریِ رسمی فروش فیلترشکن‌ها به روشنی گام مهمی برای استقرار وی‌پی‌ان‌های «قانونی» زیر نظارت و کنترل دولت و تثبیت سیاست فیلترینگ غیرهمسان یا طبقه‌بندی شده است.

فیلترینگ غیرهمسان یا طبقه‌بندی شده همین الان نیز د مقیاس کوچکی عملی شده است. برای مثال، هنگام قطع سراسری اینترنت در آبان ۹۸ که بیشتر کشور از دسترسی به پیام‌رسان‌ها و شبکه‌های اجتماعی محروم بود، عده‌ای از خبرنگاران هنوز به اینترنت و توییتر دسترسی داشتند. رهبر نظام، نمایندگان مجلس، و تعداد دیگری از دولتمردا در پلتفرم‌های مسدود شده مثل توییتر و اینستاگرام حضور دارند. اخیرا وزارت ارتباطات هم اعلام کرده که «اینترنت با کیفیت مناسب‌تر» را در دسترس برنامه‌نویسان قرار می‌دهد. احتمالا زمان بیشتری لازم است تا چنین نرم‌افزارهایی در اختیار عمومِ مردم قرار گیرد؛ زیرا باید سیستمی استقرار یابد که متقاضیان برای دریافت وی‌پی‌ان قانونی ثبت نام کنند، هویت آنها تایید شود، و قواعدی برای نظارت بر استفاده از این نرم‌افزارها تدوین شود. همه‌ی این اقدامات در نگاه اول جاه‌طلبانه و شاید ناممکن به نظر رسد. اما اگر از تجربه‌های گذشته در زمینه‌ی سیاست‌های اینترنتی – مثل طرح شبکه ملی اطلاعات – در ایران درس بگیریم،، خواهیم دید که همین طرح‌های بلندپروازانه هم به تدریج جامه عمل می‌پوشند و حرکت نظام به سمت تمامیت‌خواهی یا توتالیتاریسم دیجیتالی متوقف نخواهد شد.

لنترن؛
چراغی علیه خاموشی

لنترن چیست؟

لنترن ابزاری برای دور زدن سانسور است که بر روی سیستم‌عامل‌های MAC، WINDOWS، LINUX، ANDROID و IOS قابل استفاده است؛ این اپلیکیشن، دسترسی سریع، معتبر و امن را به وب‌سایت‌ها و برنامه‌های سانسورشده امکان‌پذیر می‌کند.
در یک دهه اخیر که اپلیکیشن لنترن شروع به فعالیت کرده است، بیش از ۱۵۰ میلیون بار در سراسر دنیا دانلود شده است. با وجود تداوم ساسنورهای پیچیده، تیم لنترن در طول این سال‌ها به اتکای دانش و تجربه‌ی خود، همواره پشتیبان کنار زدن سد سانسور دیجیتال بوده است. رسالت لنترن بر مبنای ممکن‌کردن دسترسی خصوصی، سریع، قابل اعتماد و امن تعریف شده است تا افراد، صرف‌نظر از محل سکونت خود در این سیاره بتوانند آزادانه به اطلاعات دسترسی داشته باشند.

چه چیزی لنترن را متمایز می‌کند؟

للنترن ، اغلب برای راحتی و هنگام ترجمه فیلترشکن نامیده می‌شود اما روش‌های عملکرد آن پیچیدگی بسیار بیشتری دارد. فیلترشکن‌ها از پروتکل‌های استاندارد و زیرساخت سرور استفاده می‌کنند تا ترافیک وب‌سایت نمایان خود برای ناظران شبکه را پردازش کنند. این کار شناسایی و مسدود کردن اتصال‌ها را برای سانسورچی‌ها نسبتاً آسان می‌سازد. لنترن از طیف وسیعی از تکنیک‌ها و پروتکل‌ها استفاده می‌کند تا شناسایی و مسدود نشود و اتصالی بدون قطعی داشته باشد.

حریم خصوصی و امنیت لنترن

لنترن ترافیکی را که به سرور خود ارسال می‌کند رمزگذاری می‌کند تا از داده‌ها و حریم خصوصی شما محافظت کند. لنترن دو حالت دارد. به‌طور پیش‌فرض، تنها در صورتی ترافیک را از طریق سرورهای لنترن ارسال می‌کند که آن ترافیک سانسور شده باشد، در حالی که سایر ترافیک‌ها را مستقیماً ارسال می‌کند. این حالت همچنین اقتصادی‌تر است چرا که به جز موارد سانسور شده بقیه موارد از ترافیک داخلی استفاده کرده و نیم‌بها باقی می‌ماند. با این حال، اگر "پراکسی همه" را در تنظیمات لنترن انتخاب کنید، لنترن تمام ترافیک شما را از طریق سرورهای خودارسال می‌کند.
وقتی کاربران برای اهداف عیب‌یابی و تجزیه‌وتحلیل به طور ناشناس در برنامه‌ها و وب‌سایت این برنامه، بازخوردشان را به اشتراک می‌گذارند، لنترن اطلاعات عیب‌یابی را جمع‌آوری می‌کند تا تجربه کاربری بهتری به شما ارائه دهد، اما این اطلاعات را بیشتر از ضرورت نگه نمی‌دارد. اگر ارسال داده‌های استفاده و عیب‌یابی به لنترن را انتخاب کنید، این داده‌ها را با اشخاص ثالث به اشتراک نمی‌گذارد، به آن‌ها نمی‌فروشد یا کرایه نمی‌دهد و به گفته‌ی توسعه‌دهندگان این برنامه، از این داده‌ها جز برای بهبود سرویس‌های لنترن برای کاربران استفاده نمی‌شود. تنظیمات لنترن به شما اجازه می‌دهد این مورد را مطابق با اولویت‌های شخصی‌تان پیکربندی کنید.

چگونه لنترن را دانلود کنیم؟

شما می‌توانید لنترن را از طریق گوگل‌پلی و یا اپل‌استور دانلود کنید.
یکی دیگر از راه‌ها ارسال یک ایمیل خالی به آدرس زیر است تا همراه با لینک‌های دانلود، دستورالعمل نصب به زبان فارسی را هم دریافت کنید. IRANDOWNLOADS@GETLANTERN.ORG
شما در عین حال می‌توانید از طریق وبسایت گیت‌هاب به دانلود نسخه ثابت لنترن درسترسی پیدا کنید.

گزارش تحقیقی

از فیلترینگ تا اینترنت طبقاتی؛ تاریخچه نقض حق دسترسی به اینترنت

لویی شکیبایی

مدل اینترنت طبقاتی برای دسترسی به اینترنت، بزرگترین تهدید علیه حق دسترسی به اینترنت است

از حدود سال ۱۳۸۰ تا ۱۴۰۰ ما شاهد اعمال سانسور اینترنتی به روشی بودیم که می‌توان آن را سانسور سنتی نامید. اما طی سال‌های اخیر و با توسعه شبکه ملی اطلاعات، و همچین شکل‌گیری نهادهای سیاستگذار اینترنتی مانند شورای عالی فضای مجازی، شاهد هستیم که مقامات ایرانی روش سنتی را برای کنترل اینترنت کافی نمی‌دانند.

بر همین اساس آنها در حال حرکت به سمت پیاده‌سازی پروژه اینترنت طبقاتی هستند که در آن دسترسی شهروندان ایرانی به محتوای اینترنت بر اساس طبقه اجتماعی، سن و جنسیت آنها متفاوت خواهد بود. این مدل از دسترسی به اینترنت، بزرگترین تهدید علیه حق دسترسی به اینترنت است که در مصوبه غیرالزام‌آور تابستان ۲۰۱۶ سازمان ملل تصویب شد.
در ادامه روند شکل‌گیری این بزرگترین تهدید نقض حق دسترسی به اینترنت شهروندان ایرانی را بررسی می‌کنیم.

تاریخچه فیلترینگ

در فاصله سال ۱۳۷۲ که برای اولین‌بار اینترنت در ایران در دسترس قرار گرفت تا ۱۳۸۰ سیاست و برنامه‌ی روشنی برای ایجاد سانسور و محدودیت اینترنت وجود نداشت. در سال ۱۳۸۰ برای اولین بار «سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای» توسط آیت‌الله علی خامنه‌ای، رهبر ایران اعلام شد و پس از آن بود حکومت جمهوری اسلامی نهادهایی برای نظارت بر محتوای اینترنت و عملکرد کاربران را ایجاد کرد.

در سال ۱۳۸۵ دولت محمد احمدی‌نژاد آیین‌نامه «ساماندهی فعالیت سایت‌های اینترنتی» را ابلاغ کرد که بر اساس آن تمام وب‌سایت‌ها باید در وزارت فرهنگ و ارشاد اسلامی ثبت می‌شدند.

روند تشکیل نهادهای سیاست‌گذاری و برخورد با محتوای که مورد تایید حکومت نبود با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ و در پی آن با تشکیل «کمیته‌ی تعیین مصادیق محتوای مجرمانه» شدت بیشتری پیدا کرد.

تا این زمان ما شاهد سیاست‌گذاری اینترنتی نبودیم و هدف نهادهای ایجاد شده صرفا به برخورد قهری و قضایی، همچنین سانسور و محدودیت دسترسی به محتوای اینترنتی محدود می‌شد. از سال ۱۳۹۰ جمهوری اسلامی با تشکیل «شورای عالی فضای مجازی» به صورت جدی وارد مرحله سیاستگذاری اینترنتی شد.

آیت‌الله علی خامنه‌ای طی حکمی در ۱۷ اسفند ۱۳۹۰ اعضای این شورا که عالی‌ترین نهاد سیاستگذاری اینترنتی هستند را منصوب کرد. از این تاریخ ما شاهد سیاست‌گذاری مرکزی تحت نظارت رهبر ایران برای کنترل دسترسی به اینترنت و اجرای عملی پروژه شبکه ملی اطلاعات هستیم.

از سال ۱۳۹۰ جمهوری اسلامی با تشکیل «شورای عالی فضای مجازی» به صورت جدی وارد مرحله سیاستگذاری اینترنتی شد.

با وجود آنکه گام‌های نخست این شبکه از سال ۱۳۸۵ برداشته شده بود، اما چیزی که امروز ما به اسم‌های مانند اینترنت ملی یا اینترانت و اسم رسمی «شبکه ملی اطلاعات» می‌شناسم، در جلسه ۳ دی ۱۳۹۲ شورای عالی فضای مجازی تصویب شد.

روند تصمیم‌گیری کارگروه تعیین مصادیق محتوای مجرمانه

در زمان ریاست‌جمهوری حسن روحانی (از سال ۱۳۹۲ تا ۱۴۰۰) و تا نیمه های وزارت محمدجواد آذری جهرمی (از مرداد ۱۳۹۶ تا شهریور ۱۴۰۰) فیلترینگ با همان شیوه قبلی یعنی برگزاری جلسه کارگروه تعیین مصادیق محتوای مجرمانه اعمال می‌شد. اما از میانه دولت دهم و وزارت محمدجواد آذری‌جهرمی تغییر پیدا کرد.

آذری‌جهرمی در یک جلسه که به صورت عمومی در اپلیکیشن کلاب‌هاوس در اردیبهشت ۱۴۰۰ برگزار شد، خبر از آیین‌نامه داخلی در این کارگروه داد که بر اساس آن تغییراتی در شیوه برگزاری جلسات ایجاد شده است. بر اساس آنچه آذری‌جهرمی در یک جلسه کلاب‌هاوس در اردیبهشت ۱۴۰۰ گفت، بر اساس قانون جرایم رایانه‌ای جلسات این کارگروه باید حضوری برگزار می‌شد

اما بر اساس یک آیین‌نامه داخلی این کارگروه، اعضا رای به آنلاین برگزار کردن جلسات دادند. به همین دلیل پلتفرمی آنلاین برای رای گیری ساخته شده است. فهرست سایت‌ها و محتوای که باید برای فیلتر شدن‌شان تصمیم گیری می‌شد، روی این پلتفرم وارد می‌شد و اعضا به صورت آنلاین و بدون برگزاری جلسه و گفتگو در مورد آنها تصمیم می‌گرفتند.

جهرمی در ادامه با ذکر یک مثال توضیح داد که چنین اقدامی در عمل باعث می‌شد تا اعضا بدون بحث و بررسی و با سرعت بالا رای بدهند به صورتی که به گفته او، برای نشان دادن ناکارآمدی این سیستم، او درخواست فیلترینگ سایت پیوندها (سایتی که در زمان فیلتر شدن یک پلتفرم به کاربران نمایش داده می‌شود) را ثبت کرده است.

به گفته او، پنج رای مثبت به سایت پیوندها در جلسه کمیته فیلترینگ ثبت شده بود و یکی از رای‌دهنده‌ها نیز مدعی شده بود، سایت پیوندها قبلا فیلتر شده است.

فروردین ۱۴۰۰ امیر ناظمی، معاون وقت وزیر ارتباطات، درباره چگونگی کارکرد این جلسات یک یادداشت نوشته که جزییات آن را بیشتر بازگو می‌کند.

بنا بر این یادداشت، مکانیزمی از سال ۱۳۹۰ پیاده می‌شود که براساس آن «فیلترینگ سایت‌ها به صورت تک‌تک مورد رای‌گیری قرار نمی‌گیرند.

بر اساس یک مصوبه یا بهتر بگوییم یک توافق در سال ۹۰ راه‌های میان‌بری برای فیلترینگ ایجاد شده است که بر اساس ۵ عضو (که ۳ مورد از خارج از دولت و ۲ مورد از طرف دولت است) با تطبیق مصادیق کلی به سایت‌ها، برای فیلترینگ راه ساده‌تر و میان‌بری دارند.»

در همین یادداشت اشاره شده است که، «اجرای فیلترینگ به صورت توزیع‌یافته در دست اپراتورها و شرکت‌های مخابراتی ارائه‌دهنده خدمات اینترنتی است. ابتدا حکم صادرشده از طریق مراجع فوق (خارج از وزارت ارتباطات) به این شرکت‌ها (خارج از وزارت ارتباطات) ابلاغ شده، سپس آنها موظف به پیاده‌سازی سیاست هستند.»

حکم قضایی:
راهی برای فیلترینگ فوری

ارایه حکم قضایی یکی دیگر از راه‌های اجرای فیلترینگ در ایران است. این شیوه از زمانی که فیلترینگ آغاز شد، پیش‌بینی شده بود. همان طور که قبل‌تر در همین مقاله اشاره شد، حکومت در این مورد سایت را به منزله یک کسب‌وکار یا موجودیت حقیقی در نظر می‌گرفته که حکم قضایی آن را پلمب می‌کند.

یک نمونه مهم برای بررسی اعمال سانسور اینترنتی به حکم قضایی، مسدود شدن اپلیکیشن محبوب تلگرام است.

در اردیبهشت ۱۳۹۷ تلگرام با حکم بیژن قاسم زاده سنگرودی، بازپرس دادسرای فرهنگ و رسانه تلگرام برای تمام کاربران ایرانی فیلتر شد.

این اتفاق باعث واکنش منفی حقوق‌دانان شد چرا که چنین اقدامی را غیرقانونی می‌دانستند.

آرش کیخسروی،، ابوذر نصراللهی، جواد پارسا، سعید دهقان، محمد مقیمی و پیام درفشان از جمله وکلایی بودند که ۱۶ اردیبهشت ۱۳۹۷ با حضور در دادسرای رسیدگی به جرائم کارکنان دولت از بازپرس شعبه دوم دادسرای فرهنگ و رسانه با اعلام غیرقانونی بودن فیلترینگ تلگرام، از از بازپرس صادر کننده این حکم شکایت کردند که راه به جایی نبرد.

فیلترینگ با دستور امنیتی:
فیلترینگ غیر شفاف و غیرقابل بازگشت

یکی دیگر از فرایندهایی که به بسته شدن دسترسی شهروندان به اینترنت یا پلتفرم‌های اینترنتی منجر می‌شود، دستورات امنیتی است. این تصمیمات را منصوب به شورای عالی امنیت ملی یا شورای عالی فضای مجازی می‌دانند و بهانه‌ای که برای ایراد محدودیت بازگو می‌شود، شرایط خاص و امنیتی در کشور است.

قطعی شدید اینترنت در آبان ۱۳۹۸ و فیلتر شدن واتس‌آپ و اینستاگرام همزمان با رخ دادن جنبش مهسا امینی در ایران از محدودیت‌هایی است که وقوع آن را به دستگاه‌های امنیتی مرتبط می‌کنند.

در زمان‌هایی که محدودیت اینترنتی توسط امنیتی‌ها اعمال می‌شود، مسوولان دیگر مثل وزیر ارتباطات از قبول کردن هر گونه مسوولیتی در این باره شانه خالی می‌کنند و رفع محدودیت را منوط به تصمیم مقامات امنیتی می‌دانند.

پس از خاموشی‌های آبان، در آذرماه جهرمی اعلام کرد به منظور شفاف‌سازی و دقیق‌تر کردن سیاست‌های قطع اینترنت در کشور، در حال تنظیم یک لایحه است. با این‌همه، بر اساس خبری که از یک منبع نزدیک به وزارت ارتباطات، که از فیلتربان خواسته اسم او محفوظ بماند، این لایحه زیر فشار نهادهای امنیتی و شورای امنیت کشور هرگز به مجلس فرستاده نشد. این طرح فقط به عنوان یکی از اسناد بسیار محرمانه در شورای امنیت بایگانی شد.

قطعی شدید اینترنت در آبان ۱۳۹۸ و فیلتر شدن واتس‌آپ و اینستاگرام همزمان با رخ دادن جنبش مهسا امینی در ایران از محدودیت‌هایی است که وقوع آن را به دستگاه‌های امنیتی مرتبط می‌کنند.

طبق اطلاعات منابع داخلی فیلتربان، در لایحه مذکور روند تصمیم‌گیری و عملی کردن خاموشی‌های اینترنتی را طراحی شده است. این اقدام به احتمال زیاد پس از اعتراضات آبان صورت گرفت.

در آن زمان مقامات دولتی را به این فکر افتادند که از این پس برای سرکوب و ساکت کردن معترضان، خاموشی اینترنت بیشتر از قبل لازم است. بر اساس اطلاعات رسیده به فیلتربان، تقاضا برای خاموشی‌های اینترنتی در سطح استان می‌تواند از طرف فرماندار استان به وزیر کشور ارائه شود تا مهر تأیید بگیرد. وزیر کشور خود رئیس شورای امنیت است. چنانچه تقاضا برای انسداد اینترنت همزمان از سوی چند استان به وزارت کشور برسد، آنگاه مهر تأیید باید از رییس جمهور دریافت شده است.

آن‌چه تا به حال گفته شد، روش‌هایی است شاید بتوان از آنها به عنوان روش‌ها و برنامه‌های سنتی برای سانسور و محدودیت اینترنت یاد کرد که نمونه های مشابه آن در سایر کشورها هم دیده می‌شوند. اما از آنجایی که این روش ها تا امروز پاسخ مورد نظر حکومت را نداده است و شهروندان ایرانی توانسته‌اند به محتوای اینترنت دسترسی پیدا کنند، ما شاهد این هستیم که برنامه‌های جدیدی در دست اجرا وجود دارد که دسترسی به محتوای اینترنتی را به شکل منحصربه‌فردی محدود و سانسور می‌کند.

این طرح‌های بانام‌های «وی‌پی‌ان قانونی»، «فیلترینگ غیرهمسان» یا «اینترنت طبقاتی» شناخته می‌شود.

تمام این طرح های درواقع بخشی از سیاست‌های کلان شبکه ملی اطلاعات شناخته می شوند.

در اینترنت طبقاتی، دسترسی کاربران به محتوای اینترنت بر اساس جنسیت، سن، شغل، طبقه بندی می‌شود و بر اساس این طبقه بندی محتوای اینترنت در دسترس برای هر طبقه با سایر طبقات فرق خواهد داشت. درواقع در این مدل از دسترسی به اینترنت برای دسترسی به محتوای اینترنتی هر شخص باید احراز هویت شود و اطلاعاتش را در یک بانک اطلاعاتی ثبت کند و مشخص بکند به چه بخشی از محتوای اینترنت نیاز به دسترسی .

> **در اینترنت طبقاتی، دسترسی کاربران به محتوای اینترنت بر اساس جنسیت، سن و شغل طبقه بندی می‌شود**

دارد، سپس بر اساس شغلی، جنس یا موقعیت اجتماعی‌اش ممکن است به بخشی از فهرست درخواست خود دسترسی داشته یا نداشته باشددر این روش، انواع فیلترشکن غیرقانونی می‌شود، کاربر پس از احراز هویت باید با استفاده از وی‌پی‌انی که حکومت تحت عنوان وی‌پی‌ان قانونی به او ارایه می‌کند به محتوای مورد نظر خود دسترسی داشته باشد.

به عنوان نمونه یک خبرنگار می‌تواند با ثبت اطلاعات هویتی خود فهرستی از سایت‌ها و یا اپلیکیشن های که فیلتر شدند اما او نیاز به دسترسی دارد را اعلام کند. از بین این فهرست، آن بخشی که مورد تایید حکومت قرار بگیرد به وسیله‌ی وی‌پی‌ان قانونی در دسترس این خبرنگار خواهد بود.

طرح اینترنت طبقاتی هنوز به این شکل اجرایی نشده، اما نشانه‌های بسیاری وجود دارد که نشان می‌دهد حاکمیت برای اجرای آن عزم جدی دارد.

اینترنت طبقاتی؛ بزرگترین تهدید علیه حق دسترسی به اینترنت

به عنوان نمونه، عیسی زارع‌پور ، وزیر ارتباطات ۳۰ آذر ۱۴۰۱ از ارایه سرویس خاصی برای گیمرها خبر داد که می‌تواند پینگ بازی‌ها را کاهش دهد.

در عین حال، ۸ دی ۱۴۰۱ ، امیر محمدزاده لاجوردی، رییس شرکت ارتباطات زیرساخت (رگولاتوری) از ارایه سرویس اینترنت خاص برنامه‌نویسان صحبت کرد که در آن، دسترسی به برخی سایت‌های تحریم‌شده بدون فیلترشکن فراهم شده است.

وزیر ارتباطات ۲۱ دی ۱۴۰۱ در واکنش به ارایه اینترنت طبقاتی برای گیمرها و برنامه‌نویسان گفت: «اینترنت طبقاتی بدین معنی است که یک طبقه خاصی بخواهند اینترنت پرسرعت بگیرند که چنین چیزی صحت ندارد و همه مردم برای ما خاص هستند.» این حرف در حالی بازگو می‌شود که، منظور کارشناسان از اینترنت طبقاتی، «دسترسی خاص یک عده» به محتوای اینترنت است و حرفی از سرعت نیست.

دیده بان شبکه

وضعیت اینترنت ایران در سال ۲۰۲۲ میلادی؛ سالی که پرده‌ها کنار زده شد

امیر رشیدی

با در نظر گرفتن انواع مختلف اختلال اینترنتی ازقطع دیتای موبایل، قطع اینترنت سراسری و اختلال تا اخلال در شبکه‌های اجتماعی مثل اینستاگرام، به جرات می‌توان سال ۲۰۲۲ میلادی را تاریک‌ترین سال در تاریخ اینترنت ایران برشمرد.

کاربران ایرانی در سال ۲۰۲۲ میلادی موج‌های متعددی از قطعی اینترنت، اختلال، محدودیت عمدی پهنای باند و البته فیلترینگ روی پلتفرم‌ها و وب‌سایت‌ها تجربه کردند.

پس از مرگ دلخراش مهسا (ژینا) امینی در شهریور ۱۴۰۱ و با شدت گرفتن اعتراضات به مرگ وی، در طی دست‌کم ٤ ماه شبکه دیتای موبایل در سطح استانی و ملی قطع شد. همچنین، ۲۰ پلتفرم شبکه اجتماعی، ابزار ارتباطی، بازی آنلاین و موتور جست‌وجو در همین سال فیلتر شدند.با در نظر گرفتن انواع مختلف اختلال اینترنتی ازطع دیتای موبایل، قطع اینترنت سراسری و اختلال تا اخلال در شبکه‌های اجتماعی مثل اینستاگرام، به جرات می‌توان سال ۲۰۲۲ میلادی را تاریک‌ترین سال در تاریخ اینترنت ایران برشمرد. در چنین فضایی، حقوق دیجیتال با اعمال نظارت‌های اطلاعاتی شدیدتر نقض می‌شد.

قطع اینترنت چطور اتفاق افتاد؟

دستور مستقیم مسوولان

ررسی داده‌های مرتبط با قطع اینترنت، براساس داده‌ها و اطلاعات عمومی، همچنین مستنداتی که در گزارش‌های شبکه‌ی فیلتربان به صورت ماهیانه در سال میلادی ۲۰۲۲ منتشر شده، نشان می‌دهد که حدود ٦٠ درصد از محدودیت‌ها در پی دستور مقامات ایرانی اعمال شده‌اند؛ این اختلال‌ها شامل قطعی اینترنت در استان خوزستان در ماه می و قطعی سراسری اینترنت در شهریور ماه – که به مدت سه ماه ادامه پیدا کرد– می‌شود.

با توجه به مستندات، دستورهای قطع اینترنت تقریبا همیشه در طول زمان برگزاری تظاهرات یا شرایط حساس سیاسی، به «دلایل امنیتی» گرفته می‌شود؛ زمان‌هایی که حکومت به اعمال خشونت و زور علیه معترضان مبادرت می‌کند.

با چنین رویکردی، عجیب نیست که با بالا گرفتن موج اعتراضات بعد از مرگ مهسا (ژینا) امینی در شهریور ماه ۱۴۰۱ قطعی اینترنت در ایران به اوج برسد. این در حالی است که، ما از آبان ۱۳۹۸ به این سو، شاهد قطعی سراسری اینترنت نبوده‌ایم و قطعی محلی اینترنت جایگزین آن شده است.

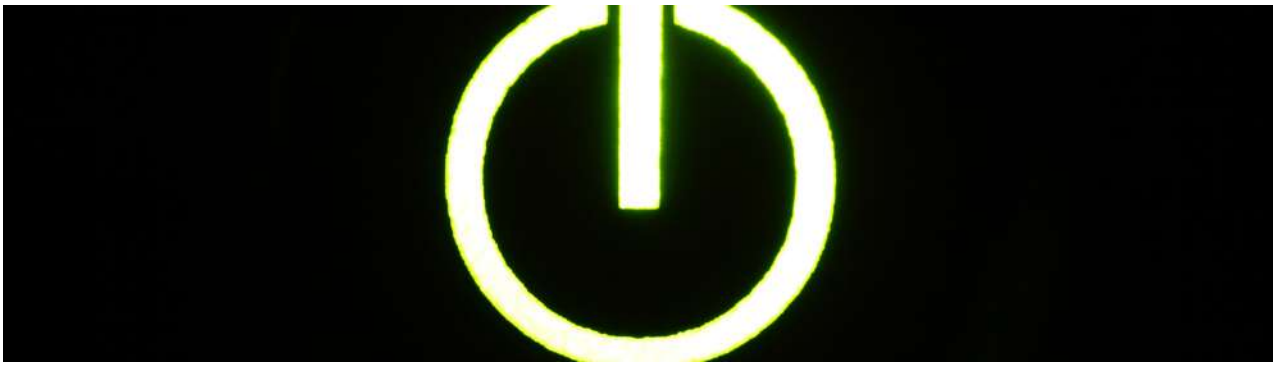
یکی از دلایل این امر را می‌توان هزینه بالای قطعی اینترنت دانست. در عین حال، تشخیص قطعی محلی اینترنت برای کسانی که وضعیت اینترنت ایران را بررسی می‌کنند، بسیار دشوارتر است.

درباره این‌که دستور قطع اینترنت چطور اعمال می‌شود، اطلاعات محدودی وجود دارد. در آبان ۱۳۹۸ ، همزمان با قطعی سراسری اینترنت در ایران بعد از اعتراضات به افزایش قیمت بنزین، محمدجواد آذری‌جهرمی، وزیر وقت ارتباطات اعلام کرد که، قطعی اینترنت به دستور شورای امنیت کشور (مخفف شاک) قطع شده است. ریاست «شاک» بر عهده وزیر کشور است و نمایندگانی از وزارتخانه‌های ارتباطات، اطلاعات، سپاه پاسداران و نیروهای نظامی از اعضای آن هستند.

در پی قطعی‌های آبان ۱۳۹۸، محمدجواد آذری جهرمی در آذر ۱۳۹۸ از تهیه لایحه‌ای خبر داد که قطعی اینترنت در ایران را درجه‌بندی و فرمول‌بندی می‌کند. یک منبع نزدیک به وزارت ارتباطات که خواست نامش فاش نشود، دراین‌باره به فیلتربان گفت که، در پی مخالفت نهادهای امنیتی و شورای امنیت ملی (شاک) این لایحه هرگز به مجلس نرسید. اما به یک لایحه فوق‌سری در شورای امنیت ملی تبدیل شد.

بنابر اطلاعات منبع فیلتربان، این لایحه روند اجرا و اعمال دستور قطعی اینترنت را مشخص می‌کند. محتمل است که چنین قانونی در نتیجه قطعی اینترنت در آبان ۱۳۹۸ رخ داده باشد؛ در شرایطی که مقامات حکومت احساس کردند، نیاز به قطعی مکرر اینترنت – برای خاموش کردن و اعمال فشار بر معترضان – وجود دارد. براساس اطلاعات رسیده به فیلتربان، استاندار می‌تواند درخواست قطعی اینترنت در سطح استان را برای بررسی و تایید به وزیر کشور (رییس شورای امنیت کشور) بفرستد. اگر چند درخواست قطع اینترنت در چند استان به صورت همزمان ارایه شده باشند، رییس‌جمهور باید دستور نهایی را تایید کند.

با توجه به مستندات، دستورهای قطع اینترنت تقریبا همیشه در طول زمان برگزاری تظاهرات یا شرایط حساس سیاسی، به «دلایل امنیتی» گرفته می‌شود؛ زمان‌هایی که حکومت به اعمال خشونت و زور علیه معترضان مبادرت می‌کند.



قطع اینترنت چطور اتفاق افتاد؟

دستور مستقیم مسوولان

در سال ۱۴۰۱ (۲۰۲۲ میلادی) قطعی برق دست‌کم باعث رخ دادن دو اختلال اینترنت شد. همچنین، آتش‌سوزی در مرکز داده مخابرات تهران مشهور به ساختمان ال‌سی‌تی (مخفف Large Capacity Tandem) باعث یک اختلال دیگر در دسترسی به اینترنت شد. ساختمان «ال.سی.تی» وظیفه توزیع اینترنت بین شرکت‌های ارایه دهنده خدمات اینترنت و شرکت‌های دیگر در ایران را برعهده دارد. اوایل سال گذشته میلادی (اواخر سال خورشیدی) مشکلات برقی باعث آتش‌سوزی دیگری در همین ساختمان شده بود.

جستجوی ایمن اجباری در موتورهای جست‌وجو

مقامات حکومت در اقدامی صریح در مرداد ماه امسال سرویس «جست‌وجوی امن» روی تمام موتورهای جست‌وجو شامل «گوگل»، «داک‌داک‌گو»، «بینگ» و «یاندکس» فعال کردند. جست‌وجوی امن سرویسی است که سایت‌ها با محتوای حساس را از دسترس کودکان دور نگه می‌دارد.
از آن‌جایی که بسیاری از محتوای مرتبط با راهپیمایی‌ها به عنوان محتوای خشونت‌آمیز طبقه‌بندی می‌شود، با این روش می‌توان بر محتوایی که در دسترس کاربران قرار می‌گیرد، سانسور اعمال کرد.

تاثیر جنگ روسیه و اوکراین

ایران در فروردین ماه اختلالات سراسری اینترنت را تجربه کرد. این اتفاق به دلیل از دست دادن ٤ هزار گیگابایت از پهنای باند در مسیر دروازه اکسپرس ایران-اروپا (مخفف EPEG) رخ داد. این دروازه یک سامانه پرسرعت کابل فیبر نوری است که ارتباطات اضافه‌ای را بین اروپا و خاورمیانه قرار دارد. این کابل فیبر نوری ظرفیت ۳ ممیز ۲ ترابیت بر ثانیه را دارد و کل طول آن به ۱۰ هزار کیلومتر می‌رسد. این خط ارتباطی از فرانکفورت در آلمان آغاز می‌شود و از اروپای شرقی و اوکراین به سمت روسیه، جمهوری آذربایجان و ایران گذر می‌کند. این مسیر به سمت خلیج فارس و شهر برکاء در سلطان‌نشین عمان ادامه دارد.
این اختلال که کمی بیشتر از ٤ ساعت طول کشید، می‌تواند به قطع ارتباط در مسیر اوکراین مرتبط باشد. وزیر ارتباطات ایران در حساب کاربری‌اش در اینستاگرام این اختلال را تایید کرد. پس از آن، سایت شرکت ارتباطات زیرساخت گزارش داد، بعد از دستور وزیر ارتباطات برای پیدا کردن مسیر ارتباطی جایگزین،این مشکل رفع شده است.

دلایل نامشخص

به خاطر نبود شفافیت در حاکمیت ایران پیرامون دلایل پشت‌پرده قطع و اختلال اینترنت، ما نمی‌توانیم برای ۱۲ درصد از مشکلات شبکه در سال ۲۰۲۲ دلیلی پیدا کنیم.

سیاست‌گذاری‌هایی که بر افزایش قطعی اینترنت تاثیر می‌گذارند

براساس داده‌های سال ۲۰۲۲ باید انتظار داشت که در سال ۲۰۲۳ اینترنت و حقوق دیجیتال همچنان وضعیت بدتری را تجربه کند. این موضوع تنها به توانایی فنی حکومت در اعمال قطعی اینترنت و انسداد محتوا و پلتفرم‌ها برنمی‌گردد. بلکه، سیاست‌ها و بستر آماده برای اعمال فشارهای حکومت نیز بر آن تاثیرگذار خواهند بود.

اکنون با حضور ابراهیم رییسی به عنوان رییس‌جمهور،عیسی زارع‌پور، به عنوان وزیر ارتباطات و چهره‌های دیگری مثل رسول جلیلی، از چهره‌های تاثیرگذار ارتباطات ایران – هر سه عضو شورای عالی فضای مجازی) این سیاست‌گذاری‌ها مجال بیشتری برای اعمال می‌یابند.

جلیلی و زارع پور در «جمعیت توسعه‌گران فضای مجازی پاک» – که اغلب با نام اختصاری «فمپ » شناخته می‌شود، با یکدیگر همکاری داشته‌اند. این سازمان توسط گروهی از سیاست‌گذاران تندرو ایجاد شده که مدعی هستند فعالیت‌هایشان منطبق با سیاست‌های اینترنتی ایران و در راستای «ارزش‌ها و آرمان‌های انقلاب اسلامی» است.

این فعالیت‌ها در نهایت به شکل‌گیری «طرح صیانت» منجر شد؛ طرحی که مجلس شورای اسلامی ایران ارایه کرد و هم‌اکنون تقریبا به طور کامل توسط نمایندگان تندرو اداره می‌شود. طرح صیانت تاکنون با برخوردهای منفی زیادی از سوی جامعه مدنی و فعالان آزادی اینترنت در ایران روبرو شده است. در همین رابطه، بیش از یک میلیون نفر نامه‌ای را در مخالفت با آن امضا کرده‌اند. همچنین بیش از ٤٠ استارتاپ و شرکت حوزه فناوری نیز بیانیه‌ای بر ضد آن منتشر کرده‌اند.این لایحه به خاطر فشار جامعه مدنی تصویب نشد. با این وجود، بررسی‌های فیلتربان نشان می‌دهد که بخش‌های مختلف این لایحه برای اجرا بین ارگان‌های مختلف دولتی تقسیم شده است. اجرای این فرایند از نگاه عمومی دور نگه داشته شده تا حساسیت‌برانگیز نباشد.

به عنوان نمونه، در سه بند از مصوبه شورای عالی فضای مجازی که اخیرا تصویب شده، به کمیسیون عالی تنظیم مقررات امکان می‌دهد که برای رگولاتوری در هر زمینه‌ای در فضای آنلاین دخالت کند.

سیاست‌های سرکوبگرانه اینترنتی ایران فقط به بزرگسالان محدود نمی‌شود. در اردیبهشت‌ماه، شورای عالی امنیت ملی به ریاست ابراهیم رییسی – رییس‌جمهوری ایران– لایحه «کمیته راهبردی صیانت از کودکان و نوجوانان در فضای مجازی» را تصویب کرد که در آن سیاست‌های کلی دسترسی به اینترنت برای کودکان مورد اشاره قرار گرفته است.

سال ۲۰۲۲ میلادی در ایران با دو قطع اینترنت بزرگ در ایران همراه بود که در پی اعتراضات «زن، زندگی،آزادی» در شهریورماه به اوج رسید و به دنبال آن، تقریبا تمام کانال‌ها و پلتفرم‌های ارتباطی مسدود شدند.

سایفون؛
به سمت اینترنت بدون محدودیت و فراتر از آن

سایفون چیست؟

«سایفون» یک فیلترشکن رایگان و متن باز، برای دور زدن فیلترینگ در اینترنت است. این برنامه از فناوری‌های متعدد استفاده می‌کند تا دسترسی بدون سانسور به اینترنت را برای شما فراهم کند. این فیلترشکن از ابتدای تاسیس در سال ۲۰۰۶ تاکنون ازهمراهان ثابت کاربران ایرانی به شمار می‌رود. کاربرانی که از آغاز فراگیری اینترنت در ایران، همواره با فیلترینگ گسترده مواجه بوده‌اند. درباره سایفون این نکته قابل توجه است که کاربران در ایران در واقع از نسخه‌ای از فیلترشکن بهره می‌برند که در دیگر نقاط جهان نسخه‌ی پولی به حساب می‌آید.

سایفون چگونه کار می‌کند؟

سایفون از سیستم رمزگذاری بهره می‌برد، آدرس آی‌پی شما را مخفی نگه می‌دارد و شما را از مسیر یک تونل امن به اینترنت آزاد متصل می‌کند. . در این برنامه ابزارهای مختلفی برای عبور از سانسور و دور زدن انواع مسدودیت‌های آنلاین تعریف شده است. فیلترشکن‌ها و پراکسی‌های مختلف معمولا با منحرف کردن ترافیک یا مخفی کردن آن به شکل ترافیکی که فیلتر نیست، فیلترینگ را برای کاربران دور می‌زنند. برنامه سایفون اما هردوی این کارها را انجام می‌دهد.

سایفون سرورهای شناخته‌شده‌ی مختلفی دارد و با بهره‌گیری از شیوه‌های متفاوت به این سرورها متصل می‌شود. یکی دیگر از شیوه‌های دور زدن فیلترینگ توسط سایفون «ترافیک مبهم» است. در این شیوه ترافیک سایفون، به اشکال متفاوت و کمتر شناخته‌شده تغییر شکل می‌یابد.

ابزارهای فیلترینگ قادر به رصد محتوایی که از تونل سایفون می‌گذرند نیستند چراکه این داده‌ها از پیش و توسط این برنامه رمزگذاری شده‌اند. هرچند ممکن است که همچنان و با استفاده از پروتکل‌های ارتباطی قادر به مسدود ساختن ترافیک رمزگذاری شده باشند. پروتکل‌های ارتباطی، مجموعه‌ای از قوانینی هستند که برای مسیریابی داده‌ها و اطمینان از رسیدن آن‌ها به مقصد مورد نظر استفاده می‌شوند.
در نسخه‌ی ۵.۰ و بالاتر اندروید فیلترشکن سایفون، امکان غیر فعال کردن برنامه‌هایی که نمی‌خواهید از تونل سایفون رد شوند را دارید. بدین ترتیب می‌توانید از این فیلترشکن، هدفمندتر استفاده کرده و در مصرف حجم اینترنت نیز صرفه‌جویی کنید.

> کاربران در ایران در واقع از نسخه‌ای از سایفون بهره می‌برند که در دیگر نقاط جهان نسخه‌ی پولی به حساب می‌آید

سایفون برای چه کسانی مفید است؟

سایفون برای عموم مردم، فعالان اجتماعی، روزنامه‌نگاران و تمام کسانی که به دنبال دسترسی به انواع محتوای مسدودشده در اینترنت هستند و با مشکل فیلترینگ مواجهند، مفید است. این ابزارهرچند با کارایی کمتر اما در زمان کندی اینترنت نیز می‌تواند به کار بیاید. البته نباید فراموش کنیم که «سایفون»، امکان گمنام ماندن کاربران و فاش نشدن هویتشان را فراهم نمی‌کند، پس زمانی که با اطلاعات حساس سروکار دارید، باید با احتیاط از این اپلیکیشن استفاده کنید

آیا می‌توانید در زمان قطع اینترنت یا زمانی که اینترنت مختل شده است از سایفون استفاده کنید؟

وقتی اتصال به شبکه جهانی اینترنت مختل می‌شود، اتصال وی‌پی‌ان‌ها نیز دچار اختلالاتی می‌شود. تنها فیلترشکنی که ادعا می‌کند در آبان ۱۳۹۸ ایرانیان را به اینترنت جهانی متصل نگه داشته، اپلیکیشن «سایفون» است و طبق گزارش‌ها قادر بوده تا از شکاف‌های موجود در اجرای پروژه قطع اینترنت ایران بهره‌برداری کرده و برخی کاربران را به اینترنت جهانی متصل نگه دارد. به عبارت دیگر چون این قطعی اینترنت، قطع صد در صدی نبوده همچنان راهی برای اتصال گروهی از کاربران وجود داشته است.

> در آبان ۱۳۹۸ و طبق گزارش‌ها، اپلیکیشن «سایفون» قادر بوده تا از شکاف‌های موجود در اجرای پروژه قطع اینترنت ایران بهره‌برداری کرده و برخی کاربران را به اینترنت جهانی متصل نگه دارد.

حریم خصوصی و امنیت سایفون

همانطور که پیشتر اشاره شد، سایفون یک برنامه متنِ باز است. این یعنی هر کسی می‌تواند برای بررسی نحوه‌ی پیاده‌سازی سیستم و فناوری‌های رمزنگاری و اساسا هر جز زیربنایی این برنامه، اقدام کند. در عین حال سایفون نه تنها به‌طور منظم به بازبینی کدهای داخلی پرداخته است، بلکه از شرکت‌های معتبر خارجی برای ارزیابی امنیتی و انجام تست‌های نفوذ کمک گرفته است.

خطرات احتمالی کار با سایفون چیست؟

اگر دنبال دست یافتن به اطلاعات حساس یا به اشتراک گذاشتن آن هستید، نباید فقط به این اپلیکیشن متکی باشید. هرچند که با استفاده از «سایفون»، ISP شما قادر به دیدن محتوای در حال داد و ستد شما نخواهد بود، اما این اپلیکیشن مانع دخیره شدن تاریخچه مرورگر و کوکی‌ها بر روی دستگاه شما نمی‌شود.

توجه داشته باشید که اطلاعات مربوط به مکان، شبکه و فعالیت مرورگرها می تواند توسط فیلترشکن یا وی‌پی‌ان‌ها رویت شود. سایفون اطلاعاتی که منجر به افشای هویت افراد شود را نگه نمی‌دارد و جزییات اطلاعات، تنها برای مدت کوتاهی ذخیره می‌شود و پس از آن صورت تجمیع‌شده ذخیره می‌شود و قابل انتساب به افراد نخواهد بود. اطلاعات شبکه با هدف اطمینان از وضعیت شبکه و کارآیی سایفون جمع‌آوری و تحلیل می‌شود. خط مشی «سایفون» در رابطه با حفظ حریم خصوصی به زبان فارسی در اینجا موجود است، که در مورد جمع‌آوری داده‌ها و نحوه‌ی به اشتراک گذاشتن آن‌ها با طرف ثالث در آن توضیح داده شده است.

نصب، اجرا و استفاده از سایفون

سایفون رابط کاربری بسیار ساده‌ای دارد که سهولت استفاده از این برنامه را برای کاربران فراهم کرده است. برای دریافت این برنامه می‌توانید به گوگل پلی و اپ استور مراجعه کنید و نسخه‌ی ویندوز آن نیز از اینجا قابل دانلود است.

سایفون همچنین راه‌های متنوع دیگری نیز در نظر گرفته تا کاربران بتوانند در مواقعی که گوگل پلی و اپ استور هم فیلتر هستند، به این برنامه دسترسی پیدا کنند.

یک راه برای دریافت فایل این فیلترشکن، ارسال یک ایمیل خالی به این آدرس است:
get@psiphon۳.com

شما همچنین می‌توانید با استفاده از بات تلگرامی سایفون به این برنامه دسترسی داشته باشید.

سایفون در روزهای آخر اسفند ۱۴۰۱ برای کاربران اندروید به روزرسانی شده است.

مقدمه

با گسترش استفاده از گوشی‌های هوشمند در ایران، متهم کردن مخالفان، معترضان و دگراندیشان براساس مستندات به دست آمده از تلفن همراه به روندی معمول برای نیروهای امنیتی بدل شده است.
از شروع اعتراضات سراسری به مرگ مهسا امینی و فراگیر شدن جنبش برآمده از آن «زن، زندگی، آزادی» و به تبع آن بازداشت و سرکوب گسترده‌ی معترضان توسط حکومت ایران، این موضوع مجددا مورد توجه قرار گرفته است.
هرچند گزارش‌های غیررسمی بسیاری از اتهامات مبتنی بر مستندات به دست آمده از تلفن همراه حکایت دارد، کمیته پیگیری وضعیت زندانیان در گزارش سوم خود اعلام کرده که دست‌کم یک نفر براساس فیلم‌هایی که از گوشی موبایل او استخراج شده و همچنین محتویات اینستاگرامش به محاربه متهم و به اعدام محکوم شده است.

ما در «ایران در خاموشی»، در مجموعه‌ی پیش رو، تعدادی از اپلیکیشن‌های کاربردی را گردآوری کردیم تا به بالا بردن امنیت دیجیتال شما برای شرکت در تظاهرات یا برنامه‌های اعتراضی کمک کند. جز این، توصیه‌هایی جمع‌آوری کرده‌ایم تا احتمال دسترسی دیگران به داده‌های شخصی و اکانت‌های شبکه‌های اجتماعی‌تان را تا حد ممکن پایین بیاورید.
ضرورت رعایت این نکات از آن روست که می‌توان گفت، تقریبا تمام داده‌های موجود در تلفن همراه نظیر ویدیو، عکس، نوشته، تاریخچه‌ی مرورگر و سایت‌های بازدیدشده، تاریخچه‌ی موتور جستجو، گفتگوهای ذخیره شده در برنامه‌های پیام‌رسان، ایمیل‌های تبادل شده، موقعیت مکانی و اطلاعاتی از این دست می‌توانند برای پرونده‌سازی علیه شرکت‌کنندگان در اعتراضات و فعالین سیاسی و مدنی، مورد استفاده قرار بگیرند.
توصیه‌ها و ابزارهای این مجموعه در سه بخش کلی ارائه شدند. بخش اول ارتباط امن و آمادگی پیش از حضور در تجمع‌ها، بخش دوم ابزارها و توصیه‌هایی برای شرکت در تظاهرات و بخش سوم اقداماتی در صورت دستگیری احتمالی یا ضبط تلفن همراه.
شما می‌توانید با به اشتراک گذاشتن این توصیه‌ها با دوستان و اطرافیانتان به امنیت دیجیتال آن‌ها کمک کنید.

جعبه ابزار همراه

ابزار و توصیه‌های کاربردی برای حفاظت از امنیت دیجیتال هنگام شرکت در اعتراضات

برای دانلود ابزار معرفی شده در این پست به وبسایت ما مراجعه کنید

WWW.IRANDARKHAMOOSHI.NET

بخش اول: ارتباط امن و آمادگی پیش از حضور در تجمعات

این بخش که شامل اصول پایه‌ای امنیت دیجیتال است، برای فعالیت‌های مجازی روزمره مفید و برای آمادگی پیش از حضور در تجمعات ضروری است.

این توصیه‌ها شامل برقراری ارتباط از طریق پیام رسان‌های امن، رمزگذاری پیام‌ها و تصاویر ارسالی، پاک سازی و خروج از حساب‌های کاربری شبکه‌های اجتماعی، پاک‌سازی داده‌های مهم از روی گوشی و استفاده از رمزهای دو مرحله‌ای و پیچیده برای جلوگیری از بازگشایی حساب‌های کاربری شما توسط نیروهای امنیتی است.

اینها نکات ساده‌ای هستند که سهل‌انگاری در رعایت کردن آن‌ها می‌تواند نه تنها امنیت شما بلکه دوستان و همراهانتان را به خطر بیندازد.

در مورد دو پیام‌رسان رایج واتساپ و تلگرام نیز بهتر است در به اشتراک گذاشتن موارد امنیتی و مهم، جانب احتیاط را رعایت کنید.

تلگرام به صورت پیش‌فرض پیام‌های شما را رمزنگاری نمی‌کند و برای این کار حتما باید گزینه‌ی سکرت چت (چت امن) را انتخاب کنید. پاک کردن خودکار پیام‌ها نیز تنها در صورت استفاده از این گزینه فراهم است. همچنین این برنامه فراداده‌های (متا دیتا) زیادی را حداقل تا دوازده ماه در برنامه حفظ می‌کند.

هرچند واتس‌اپ به صورت پیش‌فرض پیام‌های شما را رمزگذاری و از پروتکل‌های امنی پیروی می‌کند اما همواره میزان داده‌ای که این برنامه با شرکت اصلی خود «متا» و به واسطه‌ی آن دلالان داده به اشتراک می‌گذارد، نگرانی‌هایی وجود دارد.

همچنین گزارش‌های غیررسمی وجود دارد که ممکن است برخی از پیام‌ها حتی بعد از پاک شدن در این اپلیکیشن قابل بازیابی باشند.

استفاده از پیام‌رسان امن

برای برنامه‌ریزی و هماهنگی با دیگران از پیام‌رسان‌های امن یا برنامه‌هایی که امکان رمزگذاری پیام را فراهم می‌کنند، استفاده کنید. بارها شاهد بوده‌ایم که با استخراج محتوای رد و بدل شده در پیام‌رسان‌های یک شخص، تنها به خاطر یک قرار ساده در محل اعتراضات، او را به جرم اجتماع و تبانی یا حتی جلوداری (لیدری) اعتراضات متهم کرده‌اند.

پیامک تلفنی و پیام‌رسان‌های بومی هرگز راه‌های ارتباطی امنی نیستند. بنابراین تحت هیچ شرایطی از پیام‌رسان‌های داخلی استفاده نکنید.

از نگاه کارشناسان ما، پیام‌رسان‌های زیر امن‌ترین امکان تبادل اطلاعات را فراهم می‌کنند:

پیام‌رسان سیگنال

این پیام‌رسان برای ویندوز، اندروید و آی‌اواس قابل استفاده است و پیام‌ها در هر دو طرف مکالمه رمزگذاری می‌شوند. به عبارت ساده‌تر، اگر خط شما شنود شود، نهاد شنود کننده – در پیشرفته‌ترین حالت– به یک سری اطلاعات رمز شده دسترسی دارد و عملا نمی‌تواند پیام را بخواند. اگر امکان حذف خودکار پیام‌ها را فعال کرده باشید، پیام‌تان مدتی پس از ارسال به مخاطب، پاک شده و در دسترس کسی نخواهد بود. این پیام رسان البته تنها از طریق اینترنت قابل استفاده است و بدون آن کارایی ندارد.

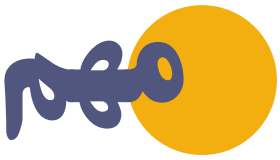
پیام‌رسان سشن

این پیام‌رسان امکان نصب روی ویندوز،ا ندروید و ای‌آواس را دارد. تفاوت این پیام‌رسان با سیگنال این است که، برای راه‌اندازی به شماره تلفن کاربر نیازی ندارد. در نتیجه، بلاک یا شنود شدن پیامک فعال‌سازی تاثیری روی دسترسی شما به این سامانه ندارد. هیچ داده و ابرداده (متا دیتا) در این برنامه نگهداری نمی‌شود. در نتیجه، حتی اگر تلفنتان به دست نهادهای امنیتی افتاده و رمز ان را هم داشته باشند، عملا نمی‌توانند به اطلاعات خاصی دسترسی پیدا کنند.

به خصوص اگر امکان حذف خودکار پیام‌ها را فعال کرده باشید، پیام‌تان مدتی پس از ارسال به مخاطب، پاک شده و در دسترس کسی نخواهد بود.

ابزار رمزگاری نهفت

نهفت پیام رسان نیست اما با کمک آن می‌توانید پیام‌هایتان را پیش از ارسال رمزگذاری کنید. این برنامه که توسط گروه «همبستگی برای ایران» تهیه شده، فعلا فقط روی سیستم عامل اندروید قابل پیاده‌سازی است. با کمک این سامانه می‌توانید پیام‌هایتان را پیش از فرستادن برای دیگران رمزگذاری کنید تا محتوای آن قابل شناسایی نباشد. برای راه‌اندازی این برنامهبه ارتباط اینترنتی یا شماره تلفن نیازی ندارید. شما همچنین می‌توانید اطلاعات رمزگذاری شده را از طریق هر پیام‌رسانی، حتی بر روی شبکه ملی اطلاعات ارسال کنید. اطلاعاتی مربوط به شما یا تلفن همراه‌تان نیز روی سرورهای «نهفت» ذخیره نمی‌شود.



در تمام اپلیکیشن‌های پیام‌رسان حتما امکان حذف پیام خودکار را فعال کنید. با این تنظیمات، پیام‌های شما برای دیگران بعد از زمان مشخصی (مثلا یک ساعت بعد از خوانده شدن) پاک می‌شود.

ضمنا توجه داشته باشید که، پیام‌رسان‌هایی که از آنها نام بردیم زمانی کار می‌کنند که ارتباط اینترنتی برقرار باشد. بدون اینترنت این نرم‌افزارها کارایی ندارند. در ادامه همین مطلب به پیام‌رسان‌هایی نیز اشاره کرده‌ایم که در صورت قطع اینترنت احتمالا کار می‌کنند و می‌توانند ارتباط شما با اطرافیان را برقرار کنند.

حفاظت از داده‌ها، قبل از شرکت در تجمع

اما اگر ناچار به همراه بردن تلفن خود هستید، به این نکته‌ها توجه کنید:

۱ حساب‌های کاربری‌تان را خصوصی/پرایوت کنید

تمام حساب‌های کاربری‌تان در تمام شبکه‌های اجتماعی را از حالت عمومی خارج کنید و به حالت پرایوت یا خصوصی در بیاورید. در این حالت، دیدن محتوایی که در حسابتان – مثلا در اینستاگرام – منتشر می‌کنید، برای عموم مردم و کسانی که در لیست دوستان شما نیستند، امکان‌پذیر نیست.

برای انجام این‌کار می‌توانید به بخش تنظیمات حساب کاربری‌تان بروید و گزینه «پرایوت» را انتخاب کنید. برای دسترسی به بخش «تنظیمات» باید روی آیکون چرخ‌دنده یا سه‌نقطه کلیک کنید. ممکن است عبارت «تنظیمات حساب کاربری» یا Setting در بعضی حساب‌های کاربری درج شده باشد.

۲ از تمام حساب‌های کاربری‌تان خارج شوید

از تمام حساب‌های کاربری‌تان اعم از ایمیل، شبکه‌های اجتماعی و پیام‌رسان‌ها- خارج شوید. به خصوص اگر احتمال دستگیری‌تان وجود دارد، حتما این‌کار را انجام دهید.

۳ رمز دو مرحله ای را از پیامک به ایمیل تغییر دهید

امکان ورود با رمز دو مرحله‌ای یا ۲FA را برای همه حساب‌های کاربری‌تان – ایمیل و شبکه‌های اجتماعی – فعال کنید. در این صورت، بعد از وارد کردن رمز عبور (پسورد) از شما یک کد یکبار مصرف درخواست خواهد شد.

امکان دریافت این رمز با پیامک را غیرفعال کنید چون نهادهای امنیتی امکان شنود و دسترسی به پیامک‌های ارسالی را دارند. در عوض، امکان دریافت کد ورود دومرحله‌ای با اپلیکیشن‌های Authenticator را فعال کنید. این برنامه‌ها، همان رمز دوم را برایتان نمایش خواهند داد.

۴ رمزهای قوی استفاده کنید

برای تلفن همراه‌تان رمزهای قوی (شامل اعداد و حروف بزرگ و کوچک و نشانه‌های مختلف) انتخاب کنید تا بازیابی آن برای نیروهای امنیتی و افرادی که ممکن است تلفن شما را تحت نظر بگیرند، دشوارتر باشد. همچنین این اصل را در مورد رمز شبکه‌های اجتماعی و ایمیلتان هم مراعات کنید. سال تولد، یک سری عدد پشت سر هم، نام خودتان یا اطرافیان‌تان و... رمزهای ضعیفی هستند. همچنین اگر تلفن همراه‌تان از قابلیت قفل تشخیص چهره یا اثر انگشت پشتیبانی می‌کند، حتما آن را فعال کنید.

۵ اپلیکیشن‌های داخلی را حذف کنید

بهتر است تمام اپلیکیشن‌های داخلی را از گوشی‌تان حذف کنید. به دلیل دسترسی این اپلیکیشن‌ها به داده‌های گوشی ممکن است نیروهای امنیتی بتوانند به این اطلاعات دسترسی پیدا کرده و برایتان پرونده‌سازی کنند.

۶ اطلاعات مهم را پاک کنید

اگر روی اکانت‌های شخصی شبکه‌های اجتماعی، ایمیل یا داخل تلفن همراه‌تان محتوای حساسیت‌برانگیز و مهمی دارید، آن را حذف کنید. محتوای خطرناک یعنی هرچیزی که بتواند امکان پرونده‌سازی برای شما را فراهم کند یا موقعیت و سلامت دوستان‌تان را به خطر بیندازد.

مراقب باشید که داده‌هایتان از همه‌جا پاک شده باشند. بعضی از عکس‌ها و داده‌ها به طور خودکار توسط تلفن همراه‌تان پشتیبان‌گیری شده و در جای دیگری – مثلا یک فضای ابری- ذخیره می‌شوند. اگر داده مهمی را دارید که نمی‌خواهید به دست کسی بیفتد، مطمئن باشید که نسخه‌های پشتیبان نیز پاک شده‌اند.

توصیه‌ی کارشناسان ما در این زمینه روشن است:

درهیچ برنامه اعتراضی تلفن‌تان را با خود نبرید.

بخش دوم-ابزارها و توصیه‌هایی برای شرکت در اعتراضات

تکرار این نکته ضروری است که کارشناسان ما معتقند، همراه نبردن تلفن همراه بهترین گزینه برای شرکت در تجمعات و مکان‌هایی با خطر دستگیری است.

اما اگر ناچار به بردن گوشی خود شدید می‌توانید با رعایت چند نکته خطرات آن را کاهش دهید و یا برنامه‌هایی نصب کنید که ممکن است در موقعیت‌های پرخطر به کارتان بی‌آید.

این بخش شامل توصیه‌هایی برای جلوگیری از ردگیری شما چه به وسیله تلفن همراه و چه به وسیله تکنولوژی شناسایی چهره است. همچنین ما ابزارهایی را برای ایجاد ارتباط امن بدون اینترنت و در فواصل کوتاه معرفی میکنیم. دراین بخش ابزارهایی نیز برای فرستادن پیام اضطراری یا آخرین موقعیت مکانی شما قبل از بازداشت ارائه شده است.

حالت هواپیما را فعال کنید

پیش از رسیدن به مقصد گوشی را خاموش کنید یا روی حالت هواپیما قرار دهید. مطمئن شوید که همه دسترسی‌های داده – از جمله جی‌پی‌اس و آنتن موبایل، بلوتوث و ... – خاموش شده است.

برای این‌که بدانید از چه محلی به بعد باید تلفن همراه‌تان را خاموش کنید،به شیوه کارکرد و ردیابی آنتن‌های تلفن همراه دقت کنید. دکل‌های زمینی تلفن همراه موسوم به BTS به تلفن‌هایی که در محدوده ۵۰۰ مترمربعی‌شان در یک مساحت شش ضلعی قرار داشته‌باشند، خدمات ارایه می‌کنند. در نتیجه، حداکثر ۵۰۰ متر قبل از محل تجمع باید گوشی‌تان از دسترس خارج شده باشد.

اپلیکیشن Panic Button را نصب کنید

این برنامه به شما کمک می‌کند که در لحظه دستگیری – یا موارد مشابه- اطرافیان‌تان را از محل جغرافیایی‌تان در آن لحظه مطلع کرده و آنها را از شرایط‌تان باخبر کنید. این برنامه یک پیامک حاوی موقعیت جغرافیایی لحظه‌ای شما را به شماره تلفن‌هایی که از پیش تعیین کرده‌اید، پیامک می‌کند. شخص گیرنده برای دریافت پیام شما نیازی به نصب برنامه ندارد. این برنامه فعلا برای سیستم عامل اندروید در دسترس است.

نسخه‌ی مشابه و قابل استفاده برای کاربرانی که از گوشی‌های اپل استفاده می‌کنند برنامه‌ی Silent beacon است.

زمان شرکت در اعتراضات: مراقب سیستم‌های شناسایی چهره دیجیتال باشید

سیستم‌های شناسایی چهره می‌توانند از روی چهره شما به هویت‌تان پی ببرند. این سامانه چهره اشخاص را آنالیز کرده و محتوای آن را با یک بانک اطلاعاتی - مثلا داده‌های مربوط به کارت ملی هوشمند- می‌سنجد و آنها را شناسایی می‌کند. چنین سامانه‌هایی در حال حاضر در چین استفاده می‌شود و با کمک آن تا به حال فعالان مدنی بسیاری تحت فشار قرار گرفته‌اند. درباره چگونگی کارکرد سیستم مشابه در ایران، اطلاعات اندکی وجود دارد اما در عین حال شواهدی وجود دارد که از این سیستم در ایران استفاده می‌شود. در نتیجه بهتر است، نکات ایمنی در این باره را رعایت کنید:

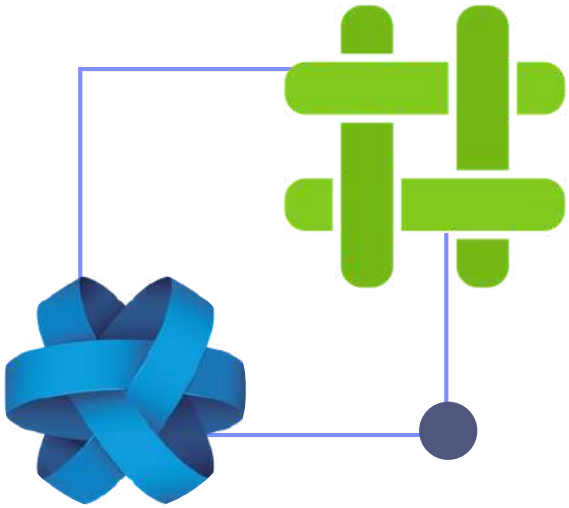
از پوشیدن هر لباس یا در معرض دید قرار دادن هر چیزی که شما را قابل‌شناسایی کند مثل لباس‌های مارک‌دار، رنگی، طرح‌دار، مدل موی خاص و... اجتناب کنید.

چهره‌تان را با ماسک بپوشانید. به جز تشخیص چهره، ماسک می‌تواند در زمان شلیک اشک‌آور نیز به شما کمک کند.

موقعیت جغرافیایی‌تان را با نزدیکان‌تان به اشتراک بگذارید

با استفاده از سرویس «نقشه گوگل» می‌توانید موقعیت جغرافیایی‌تان را با نزدیکان‌تان به اشتراک بگذارید. در نظر داشته باشید که، ممکن است سرویس‌های گوگل در ایران فیلتر شوند. در این صورت، انجام این کار منوط به باز ماندن فیلترشکن شماست. ضمن این‌که، استفاده از سرویس‌های نقشه روی موبایل، باتری زیادی مصرف می‌کنند.

اپلیکیشن‌های مهم برای حضور در تجمع



اگر تلفن همراه‌تان را در اعتراضات همراه می‌برید، حتما این اپلیکیشن‌ها را نصب کنید. با این روش، می‌توانید با افراد دیگری که در تجمع حضور دارند، با یک راه امن در تماس باشید. ضمنا اگر توسط نیروهای امنیتی تهدید یا بازداشت شدید، می‌توانید این موضوع را به دیگران اطلاع دهید.

اپلیکیشن‌های Briar و Jami را نصب کنید

این برنامه‌ها به شما کمک می‌کنند که با اطرافیان‌تان ارتباط امن داشته باشید. با این برنامه‌ها می‌توانید به یک شبکه محلی امن – مثلا یک شبکه وای‌فای بدون اینترنت– متصل شوید و در یک فاصله حداکثر شش متری با یکدیگر در ارتباط بمانید.
توجه داشته باشید، برای این‌که بتوانید با دیگر اطرافیان و دوستان‌تان در تماس بمانید، باید آنها هم این نرم‌افزارها را نصب کنند. پس حتما به صورت گروهی این برنامه‌ها را نصب و استفاده کنید.

جمی یک برنامه پیام‌رسانی و تماس ویدیویی رمزگذاری‌شده است که به کاربران امکان می‌دهد پیام ارسال کنند، تماس برقرار کنند، تماس ویدیویی با یک یا چند نفر داشته باشند و کارهایی مانند اشتراک‌گذاری صفحه نمایش و اشتراک‌گذاری فایل‌ها مانند تصاویر را انجام دهند.

برایر به کاربران خود امکان می‌دهد تا بدون اینترنت و با استفاده از شبکه‌ای که توسط بلوتوث یا وای‌فای ایجاد می‌شود، با هم در ارتباط باشند. این به شما امکان می‌دهد تا در مواقع قطع یا اختلال در اینترنت بتوانید از این برنامه استفاده کنید. به دلیل این که شبکه‌های مانند بلوتوث و وای‌فای فقط توانایی ارتباط در فاصله مشخصی که چندان زیاد نیست را دارند، کاربران این اپلیکیشن باید در نزدیکی هم قرار داشته باشند. بلافاصله بعد از اتصال به اینترنت، امکان به اشتراک گذاشتن این اطلاعات با مخاطبینی که نزدیک شما نیستند نیز فراهم می‌شود.

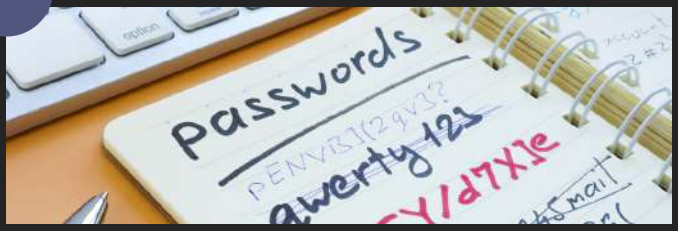
از آنجایی که استفاده از این دو برنامه به ارتباط اینترنتی نیاز ندارد، در صورت قطع اینترنت یا از بین رفتن آنتن موبایل می‌توانید همچنان از آن استفاده کنید.

بخش سوم– اقداماتی برای دستگیری احتمالی و یا ضبط تلفن همراه

بخش سوم- اقداماتی برای دستگیری احتمالی و یا ضبط تلفن همراه اگر توسط نیروهای امنیتی دستگیر شدید و تلفن‌تان در دست بازجوها ماند، می‌توانید به چند توصیه عمل کنید. توجه داشته باشید که برای انجام بخشی از کارهایی که در اینجا پیشنهاد می‌شوند، به افراد معتمد یا نزدیک نیاز خواهید داشت و خودتان احتمالا نمی‌توانید آنها را به تنهایی انجام دهید.

به همین دلیل، پیشنهاد می‌کنیم، حتما این بخش از توصیه‌های ما را با یکی از افراد معتمد خودتان مرور کنید.

در این بخش همچنین توصیه‌هایی برای ارائه‌ی امن محتوای تهیه شده در اعتراضات اعم از عکس و ویدئو وجود دارد.



عوض کردن رمزهای عبور

اگر تلفن همراه‌تان دست نیروهای امنیتی باقی ماند، خودتان یا نزدیکان‌تان باید بتوانند رمز عبورتان را تغییر بدهید . این کار در صورتی امکان‌پذیر است که آنها راه دسترسی به حساب کاربری شما را بلد باشند.اگر شخص قابل اعتمادی در دسترس دارید می‌توانید ایمیلی که بر اساس آن حساب کاربری در شبکه‌های اجتماعی ساخته‌اید را در اختیار او قرار دهید تا در صورت ضرورت، به بازیابی حساب شما و کنترل و پاک سازی محتوای درون حساب اقدام کند.

تغییر رمز عبور با رفتن به بخش «تنظیمات حساب کاربری» یا «تنظیمات امنیتی» امکان‌پذیر است. (بنا به نوع شبکه اجتماعی یا ایمیل نام این بخش می‌تواند اندکی متفاوت باشد)

غیرفعال کردن امکان «دانلود اطلاعات» در فیسبوک

اگر عضو فیسبوک هستید، باید امکان دانلود اطلاعات را غیرفعال کنید. این‌کار با حذف یا غیرفعال کردن اکانت تفاوت دارد. در این‌حالت شما به کاربری که وارد حساب کاربری‌تان نمی‌شود اجازه نمی‌دهید که اطلاعات شخصی و محتوای فیسبوک شما را دانلود کند. برای انجام این‌کار از راهنمای فیسبوک استفاده کنید.

پاک کردن اطلاعات گوشی در اندروید

برای پاک کردن اطلاعات گوشی‌های اندروید باید به بخش تنظیمات یا Setting تلفن بروید. گزینه Allow Remote Lock and Factory Reset را انتخاب کنید. در پنجره جدیدی که باز می‌شود، گزینه «پیدا کردن دستگاه از راه دور» را انتخاب کنید. اکنون گزینه Allow remote lock and Factory reset را انتخاب کنید.

در مرحله بعد، یک صفحه جدید باز می‌شود که از شما اجازه می‌گیرد، داده‌های دستگاه‌تان را پاک کند. این صفحه را تایید کنید.

توجه داشته باشید، هنوز داده‌ای پاک نشده است. بلکه در اینجا شما به گوگل اجازه می‌دهید که، در آینده اگر نیاز شد، اطلاعات تلفن‌تان را از راه دور پاک کند.

برای پاک کردن داده‌های تلفن‌همراه اندرویدی باید به سایت «پیدا کردن» گوگل بروید. نام کاربری و کلمه عبورتان را وارد کنید. در این مرحله، موقعیت جغرافیایی تلفن شما را نشان می‌دهد. بعد از پیدا شدن تلفن، شما می‌توانید آن را قفل یا داده‌هایش را پاک کنید. اگر عبارت Erase را انتخاب کنید، داده‌ها – بعد اا‌ز تایید شما– از روی تلفن‌تان پاک می‌شوند. توجه داشته باشید که بعد از اعلام موافقت، از شما خواسته می‌شود تا یک‌بار رمزعبورتان را وارد کنید.

شما باید این تنظیمات را قبل از رفتن به تجمعات و مناطق پرخطر انجام دهید.

برای پاک کردن اطلاعات موبایل آیفون‌تان باید این مراحل را طی کنید:

با اپل‌آی‌دی و رمز عبور وارد حساب کاربری‌تان در سایت آی‌کلاود شوید. گزینه Find my phone را انتخاب کرده و از بین گزینه‌های موجود، Erase را انتخاب کنید. با تایید این مرحله تمام داده‌هایتان از روی گوشی پاک می‌شوند. اگر تلفن‌تان در آن لحظه به اینترنت وصل نباشد، در اولین زمانی که به اینترنت متصل شود، داده‌ها پاک می‌شوند.

یک راه دیگر هم برای محافظت از داده‌های شخصی‌تان در آیفون وجود دارد. در این‌صورت، حتی اگر تلفن‌تان به اینترنت متصل نشود، باز هم می‌توان امید داشت که اطلاعاتش پاک شود. در این حالت، وقتی شخص ثالث به گوشی شما دسترسی داشته باشد و ده بار پسورد اشتباه وارد کند، تمام اطلاعات داخل تلفن پاک می‌شود. برای فعال کردن این امکان در آیفون باید وارد بخش تنظیمات یا Setting شوید و گزینه Face ID and Passcode را انتخاب کنید. در پنجره تازه گزینه Turne passcode را انتخاب کرده و یک پسورد جدید بسازید.

اگر قبلا پسورد ایجاد کرده‌اید، در همین صفحه گزینه Erase Date را فعال می‌کنید. در این‌صورت، همان‌طور که قبلا هم گفته شد، بعد از ده‌بار تلاش ناموفق در دسترسی به تلفن‌تان، تمام اطلاعات آن پاک می‌شود. برای این‌که چنین اتفاقی رخ بدهد، نیازی به اتصال اینترنتی نیست.

بعد از شرکت در اعتراضات؛ چطور اطلاع‌رسانی کنیم؟

مهم

تمام «متا دیتا» موجود روی عکس و ویدیوهایی که می‌خواهید در شبکه‌های اجتماعی به اشتراک بگذارید را پاک کنید. اینجا یک آموزش کوتاه وجود دارد. به عنوان یک راه‌حل برای حذف «ابر داده» یا «متا دیتا»، اگر از عکس‌هایتان اسکرین‌شات بگیرید، متادیتا حذف خواهد شد.
در پست‌هایی که در شبکه‌های اجتماعی منتشر می‌کنید، بخشی مربوط به چهره‌ها و لباس‌ها را محو کنید. برای انجام این‌کار در نرم‌افزارهای ویرایش ویدیو و عکس، یک فیلتر اختصاصی وجود دارد. (در منو دنبال گزینه‌ای به نام Blur بگردید.) وقتی عکسی را در پیام‌رسان سیگنال می‌فرستید، می‌توانید پیش از ارسال، محتوای آن را محو کنید. برای این‌کار عکس‌تان را انتخاب کنید. گزینه «ویرایش/Edit » را انتخاب کنید. گزینه blur option را انتخاب کنید. پیشنهاد ما این است که چهره‌ها، مارک لباس‌ها، نام خیابان‌ها و مکان‌های خاص و به طور کلی، هرچیزی که به شناسایی و دستگیری افراد کمک می‌کند را محو کنید.

سخن آخر

ما ویدیوهای کوتاهی از آموزش گام به گام ابزاری که در این مجموعه معرفی شده‌اند تهیه کرده‌ایم. برای بازدید این ویدیوها می‌توانید به صفحه‌ی ما در شبکه‌های اجتماعی مراجعه کنید

به یاد داشته باشید که با تمام دقت و کارشناسی که در مورد ابزار موجود در این مجموعه شده است، وجود باگ و حفره‌های امنیتی، بخشی از طبیعت ابزار دیجیتال و دنیای مجازی به حساب می‌آید. شما قبل از هر اقدامی در فضای مجازی باید بدانید که امنیت در این فضا صد درصدی نیست و همواره احتمالی را برای درز اطلاعات و رصد شدن در نظر بگیرید.

شما می‌توانید با درمیان گذاشتن تجربیات شخصی، ملاحظات منطقه‌ای و به اشتراک گذاشتن دانش فنی خود در به روزرسانی و کاربردی‌تر کردن این جعبه ابزار همراه به ما کمک کنید.