



سیاست‌گذاری و نگاشت نهادی «نظارت و تجسس» از شهروندان در جمهوری اسلامی ایران

ژانویه ۲۰۲۵ - بهمن ۱۴۰۴



RaazNet

فهرست مطالب

۴	۱. جایگاه نظارت و تجسس در قوانین اینترنت در ایران
۴	۱.۱. نظارت و تجسس در طرح «صیانت»
۵	۱.۲. اشراف بر «فضای مجازی» و شنود قانونی در قوانین اینترنت در ایران
۶	۱.۳. نظام هویت معتبر در «فضای مجازی»
۷	۱.۴. برنامه هفتم پیشرفت جمهوری اسلامی
۸	۲. سامانه‌های حکومتی نظارت و تجسس از شهروندان در جمهوری اسلامی ایران
۹	۲.۱. سامانه‌های زیرساختی و پنهان نظارت، تجسس و کنترل شهروندان
۱۰	۲.۱.۱. سامانه «اشراف بر فضای مجازی»
۱۲	۲.۱.۲. شاهکار؛ شبکه احراز هویت کاربران ارتباطی
۱۲	۲.۱.۳. سیام؛ سامانه یکپارچه استعلامات مخابراتی
۱۴	۲.۱.۴. سامانه رصد و سنجش سبک زندگی مردم
۱۵	۲.۲. سامانه‌های رسمی و آشکار نظارت و احراز هویت در تعاملات روزمره شهروندان
۱۵	۲.۲.۱. سماوا؛ سامانه ملی احراز هویت و استعلامات
۱۶	۲.۲.۲. هدا؛ سامانه احراز هویت دیجیتال ایرانیان
۱۷	۲.۲.۳. ثنا؛ سامانه احراز هویت قضایی آنلاین
۱۸	۲.۲.۴. همتا؛ سامانه هوشمند مدیریت تجهیزات ارتباطی
۱۹	۲.۲.۵. ام‌تا؛ سامانه احراز مشتریان تجارت الکترونیکی
۱۹	۲.۲.۶. سخا؛ سامانه خدمات انتظامی (پلیس)
۲۰	۲.۲.۷. میخک؛ سامانه مدیریت یکپارچه خدمات کنسولی
۲۲	۳. ابزارهای مخفی حکومت برای نظارت و تجسس
۲۳	۳.۱. شنود مرد میانی در سیاست‌های نظارتی حکومت
۲۳	۳.۱.۱. نهادهای پیشران شنود مرد میانی در ایران
۲۴	۳.۱.۲. جایگاه شنود مرد میانی در معماری شبکه ملی اطلاعات
۲۴	۳.۱.۳. اهداف و کارکردهای مرد میانی
۲۶	۳.۱.۴. ربایش نشست به‌عنوان ابزار کنترل در سطح پلتفرم
۲۷	۳.۱.۵. انحراف‌های حقوقی و فنی از استانداردهای جهانی
۲۸	۳.۲. ابزارهای فریب و تبدیل تقاضای دسترسی به زیرساخت نظارت
۲۸	۳.۲.۱. کارزارهای فریبده VPN همان‌زمان با اختلال و قطع اینترنت در هنگامه اعتراضات مردمی علیه حکومت
۲۹	۳.۲.۲. طعمه‌های استارلینک و توزیع جاسوس‌افزار از مسیر ابزارهای اتصال جعلی
۳۰	۳.۲.۳. جاسوس‌افزاری فریبده در پوشش یک ابزار پی‌خطر
۳۰	۳.۳. چارمینگ کیتن (APT۳۵)؛ دسترسی فریبده، زنجیره ابزارهای جاسوسی و کنترل دولتی
۳۲	۳.۳.۱. تروجان دسترسی از راه دور ویندوزی مازولار با سامانه فرماندهی و کنترل مبتنی بر رله
۳۳	۳.۳.۲. بلا چاو (BellaCiao)؛ بارگذار مازولار ویندوزی مرکزی در زنجیره عملیات‌های چارمینگ کیتن

۳۴	۳.۳.۳. ابزار دسترسی از راه دور ماژولار PACP-RAT
۳۵	۳.۳.۴. زیرساخت فریب و تحویل مبتنی بر طعمه ای تصویری
۳۶	۳.۳.۵. ثاقب؛ تروجان دسترسی از راه دور در معماری نظارت نهادی
۳۷	۳.۴. تسخیر پلتفرم‌ها: شبیه‌سازی، پوسته‌های حاکمیت‌پذیر و کنترل در سطح اپلیکیشن
۳۸	۳.۴.۱. پوسته‌های حاکمیت‌پذیر و برنامه‌های نظارتی ثالث
۳۹	۳.۴.۲. سوءاستفاده از پیام‌رسان‌ها و نظارت در سطح پلت‌فرم
۴۰	۳.۵. داده‌های کاربران به‌عنوان دارایی اطلاعاتی: پلت‌فرم‌ها، درهای پشتی و اپلیکیشن‌های همسو با حکومت
۴۳	۳.۶. شبکه کاشف: همجوشی داده‌ها، ترسیم روابط و نظارت عملیاتی
۴۶	۴. نظارت خیابانی در جمهوری اسلامی و کشف هویت شهروندان در فضای عمومی
۴۷	۴.۱. اقتدارگرایی و ایدئولوژی دینی در راهبردهای نظارت و احراز هویت
۴۸	۴.۱.۱. تحول راهبردی در کنترل پوشش: از تبلیغ فرهنگی تا رصد امنیتی
۴۹	۴.۱.۲. قانون عفاف و حجاب؛ چارچوب قانونی برای نظارت دیجیتال در فضاهای عمومی
۵۰	۴.۲. پیاده‌سازی تشخیص چهره در فضای عمومی: سیاست، فناوری و واقعیت میدانی
۵۱	۴.۲.۱. ادعاها درباره استفاده از الگوریتم‌های چهره‌نگاری و میزان تحقق آن در ایران
۵۱	۴.۲.۲. واردات تجهیزات از چین با قابلیت اتصال به سامانه‌های چهره‌نگاری
۵۳	۴.۲.۳. توسعه بومی تشخیص چهره: پروژه‌ها، بازیگران و آزمون‌های میدانی
۵۴	۴.۲.۴. زیرساخت‌های هویتی و نظارت شهری؛ اتصال داده‌ها، دوربین‌ها و پایگاه‌های ملی
۵۵	۴.۳. شیوه‌های ترکیبی و اجرای میدانی؛ شبکه‌های داده‌ای متصل به هویت دیجیتال
۵۶	۴.۳.۱. نقش قرارگاه ۲۱ تیر و اقدامات میدانی سپاه و بسیج
۵۷	۴.۳.۲. اپلیکیشن ناظر؛ جمع‌سپاری نظارت
۵۷	۴.۳.۳. چهره‌نگاری به‌عنوان مکمل سامانه‌های داده‌محور
۵۸	۴.۴. اتصال‌پذیری پایگاه‌های داده؛ زیرساختی برای مهندسی هویت
۵۹	۴.۵. تحلیل پیامدها و سطح بلوغ این مدل‌ها برای شناسایی معترضان در آینده
۶۰	۵. اشاعه جهانی فناوری‌های نظارت، تجسس، سانسور و سرکوب اینترنت
۶۰	۵.۱. بستر راهبردی و انگیزه‌های صدور
۶۱	۵.۲. شرکت‌ها و پیمانکاران ایرانی صادرکننده فناوری‌های سرکوب اینترنت
۶۴	۵.۳. ارزیابی تشدید خطر روند چندپارگی اینترنت
۶۵	۵.۳.۱. نظام هویت معتبر در «فضای مجازی»
۶۶	۵.۳.۲. برنامه هفتم پیشرفت جمهوری اسلامی



۱. جایگاه نظارت و تجسس در قوانین اینترنت در ایران

۱.۱. نظارت و تجسس در طرح «صیانت»

در سال‌های اخیر در مجلس شورای اسلامی طرح «نظام تنظیم مقررات خدمات فضای مجازی»^۱ که در افکار عمومی به صیانت مشهور است، در روند تصویب قرار گرفت و چون با انتقاد جدی افکار عمومی و جامعه مدنی مواجه شد، با مکانیزمی پیچیده و نسبتاً مخفیانه (با استفاده از اصل ۸۵ قانون اساسی جمهوری اسلامی) در روند اجرا قرار گرفت.^۲ طرح «صیانت» در نظر کارشناسان منتقد، به‌عنوان ابزاری قانونی در دست حکومت برای محدودسازی اینترنت در ایران معرفی شده است. اما نگاهی به روند مطرح‌شدن این طرح در مجلس نشان می‌دهد «نظارت و تجسس» هم همواره از خواست‌های اصلی و کلیدی حکومت جمهوری اسلامی در این طرح بوده است.

در اعتراضات شهروندان علیه حکومت جمهوری اسلامی در دی ۱۳۹۶، شورای عالی امنیت ملی، نهادی در کنترل رهبری جمهوری اسلامی ایران و متشکل از سران نظامی و امنیتی، با ادعای نقش پیام‌رسان «تلگرام» در اعتراضات، دسترسی به آن را مسدود کرد.^۳ خواسته جمهوری اسلامی که در مذاکره با مدیران شرکت تلگرام مطرح شده بود^۴ صراحتاً «جاسوسی و سانسور» بود.^۵

این خارج شدن کنترل ارتباطات و در ادامه نفوذ رسانه‌ای از سیطره زیرساخت‌های حکومتی بود که منجر به ارائه

حکومت جمهوری اسلامی ایران قابلیت‌هایش در «نظارت و تجسس» از شهروندان را با استفاده از فناوری‌های نوین توسعه داده است؛ دوربین‌های مدار بسته، سیستم‌های تشخیص چهره، اپلیکیشن‌هایی برای ثبت محتوای پیام‌های خصوصی کاربران، سیستم‌های ارزیابی وضعیت سبک زندگی شهروندان و ... امکان نظارت گسترده و دقیق بر شهروندان ایرانی را برای دستگاه‌های امنیتی جمهوری اسلامی فراهم کرده‌اند.

یکی از اجزای محوری سیستم‌های نظارت و تجسس در جمهوری اسلامی «شبکه ملی اطلاعات» (NIN)^۱ است که در افکار عمومی به «اینترنت ملی» معروف است. «نقض آزادی بیان با فیلترینگ و سانسور اینترنت» و «ممانعت از جریان آزاد اطلاعات با ایجاد اختلال در ارتباطات، مسدودسازی سکوهای ارتباطی یا قطع کامل سراسری و محلی اینترنت» مهم‌ترین موارد نقض حقوق بشر در این شبکه است.

اما از همه بدیع‌تر توسعه قابلیت‌های «نظارت و تجسس» شبکه ملی اطلاعات در سطوح فنی مختلف با اهداف و چشم‌اندازهای متفاوت در دستگاه‌های مختلف حکومتی جمهوری اسلامی است. بعضی از این سیستم‌ها برای نظارت فراگیر (Mass Surveillance) به‌کار می‌روند و بعضی دیگر قابلیت ردیابی، جاسوسی و شنود از اهداف خاص (Spying, Tracking, and Interception) دارند که در ادامه آنها را بررسی می‌کنیم.

امنیت و مدل اقتصادی». بخش «امنیت» هسته اصلی سند است که بسیاری از جزئیات آن طبقه‌بندی شده و غیرقابل انتشار است.^۹ عباراتی مانند «امکان رصد، اشراف و اعمال سیاست‌های حاکمیتی»، «نظام مدیریت شناسه و هویت قابل اعتماد و یکپارچه»، «پالایش جامع محتوا» و ... نشان‌دهنده برنامه‌ریزی برای توسعه ابزارهایی است که در سال‌های بعد که به نهادهای امنیتی حکومتی و همین طور سپاه پاسداران انقلاب اسلامی، امکان نظارت و تجسس بر فعالیت‌های شهروندان عادی را می‌دهد (تصویر پایین).

تقارن زمانی میان شکل‌گیری نهادهای عالی حکمرانی دیجیتال در چین و ایران معنادار است. اداره فضای مجازی چین (Cyberspace Administration of China) در سال ۲۰۱۱ تأسیس شد^{۱۰} و تنها چند ماه بعد، در اسفند ۱۳۹۰، مرکز ملی فضای مجازی در ایران ایجاد شد.^{۱۱} هر دو نهاد با هدف متمرکزسازی کنترل دولت بر زیرساخت‌های دیجیتال، مقررات‌گذاری فراگیر و ایجاد مرجع واحد برای سیاست‌گذاری اینترنت شکل گرفتند. نکته مهم‌تر این است که هر دو حکومت، به جای استفاده از واژه «اینترنت»، از اصطلاحی با بار معنایی خاص یعنی «فضای مجازی» بهره می‌برند؛

نسخه اول طرح «صیانت» شد. این طرح، پلت‌فرم‌های خارجی را ملزم به انتقال سرورهای حاوی اطلاعات کاربران ایرانی، به داخل کشور می‌کند. مهم‌ترین مستمسک حکومت جمهوری اسلامی ایران برای این منظور مفهوم «دیتا رزیدنسی» است. با این حال حداقل در مذاکرات با تلگرام می‌بینیم که خواست نهایی جمهوری اسلامی از این شرکت‌ها، دسترسی‌هایی برای نظارت، تجسس و سانسور کاربران ایرانی بوده و هست.

۲.۱. اشراف بر «فضای مجازی» و شنود قانونی در قوانین اینترنت در ایران

درخواست حکومت جمهوری اسلامی برای چنین دسترسی‌هایی موضوع جدیدی نیست. شورای عالی انقلاب فرهنگی، نهاد سیاست‌گذار فرهنگی در ایران که تحت کنترل رهبری جمهوری اسلامی است، در سال ۲۰۰۱ «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» را تصویب کرد.^{۱۲} این قانون از نخستین سنگ‌بناهای حکمرانی اینترنت در ایران است. در این قانون توزیع‌کنندگان اینترنت موظف شدند «داده‌های مربوط به فعالیت کاربران را در اختیار وزارت ارتباطات قرار دهند تا در صورت درخواست و با تایید مقام قضایی مربوطه در اختیار وزارت اطلاعات قرار گیرد». با این حال مواردی مانند نشت اطلاعات از سرورهای ای‌میل «کمپته فیلترینگ» در قوه قضاییه جمهوری اسلامی نشان می‌دهد بسیاری از اطلاعات و درخواست‌ها مستقیماً از طریق دادستانی به شرکت‌های اینترنتی ارائه شده‌است (فصل سوم). این قانون، پشتوانه مهمی برای سیستم شنود قانونی (Lawful Intercept) در جمهوری اسلامی یا آنچه «اشراف اطلاعاتی» خوانده می‌شود، فراهم کرده‌است. سیستمی که از نظر فنی، انحراف قابل توجهی از استانداردهای جهانی برای حفظ حریم خصوصی دارد (بخش ۵ از همین فصل).

علی خامنه‌ای، رهبری جمهوری اسلامی ایران، همچنین شورای عالی فضای مجازی را تأسیس کرده و در کنترل دارد. این شورا سیاست‌گذار اصلی اینترنت در ایران است. در این شورا سندی با عنوان «تعیین الزامات شبکه ملی اطلاعات»^{۱۳} تصویب شده که تعاریف اولیه و اصول کلی را برای شش حوزه کلیدی شبکه در ایران ترسیم می‌کند: «زیرساخت‌های ارتباطی، استقلال، مدیریت، خدمات،



تأمین‌کنندگان شناسه، دوره گذار ۳ ساله در نظر گرفته شده است. با وجود گذشتن این زمان هنوز «نظام هویت معتبر در فضای مجازی» به‌طور کامل و فراگیر پیاده‌سازی نشده است. جمهوری اسلامی ایران با تکمیل «نظام هویت معتبر در فضای مجازی» زیرساخت‌های جامع برای مدیریت هویت کاربران در فضای دیجیتال را به‌دست می‌آورد. هدف اصلی این طرح در ظاهر «تضمین شناسایی کامل کاربران و تعاملات آنان در فضای مجازی» است اما در نهایت به «تسهیل در رهگیری، کنترل محتوا و اقتدار لازم برای اعمال سیاست‌های حاکمیتی» منجر می‌شود.

۴.۱. برنامه هفتم پیشرفت جمهوری اسلامی

«برنامه هفتم پیشرفت جمهوری اسلامی ایران»^{۱۳} که نقشه راه توسعه کشور برای پنج سال است و در سال ۲۰۲۴ تصویب شده است، تأکید ویژه‌ای بر توسعه زیرساخت‌های دیجیتال، دولت الکترونیک و هوشمندسازی خدمات عمومی در سال‌های پیش رو دارد. این برنامه نقش کلیدی در تسریع روند گسترش سامانه‌های احراز هویت در ایران دارد. عدم قوانین شفاف، نظارت مستقل و رعایت حقوق شهروندی در جمهوری اسلامی ایران احتمال اینکه این سامانه‌ها را به ابزارهای نقض حریم خصوصی و کنترل اجتماعی تبدیل کند بسیار بالا می‌برد. این ابزارها هنوز در مرحله طراحی هستند. مشهورترین سامانه که در زمان تصویب این برنامه توجه افکار عمومی را به‌خود جلب کرد «سامانه رصد و سنجش سبک زندگی مردم» بود.

در بخش بعدی به بررسی جزئی‌تر سیستم‌ها و سازوکارهای سامانه‌های «اشراف بر فضای مجازی» خواهیم پرداخت. هر سیستم، معمولاً یک نهاد سفارش‌دهنده در حکومت از نهادهای انتصابی و غیرانتخابی دارد و یک اپراتور یا توسعه‌دهنده دارد که بخشی از دولت، یا شرکت‌های وابسته به سرمایه‌گذاران حکومتی یا حتی بخش خصوصی است.

اصطلاحی که به حکومت‌ها اجازه می‌دهد عرصه ارتباطات دیجیتال را نه به‌عنوان یک شبکه جهانی باز، بلکه به‌مثابه «قلمرو» قابل حکمرانی، تنظیم، تصرف و کنترل بازنمایی کنند.

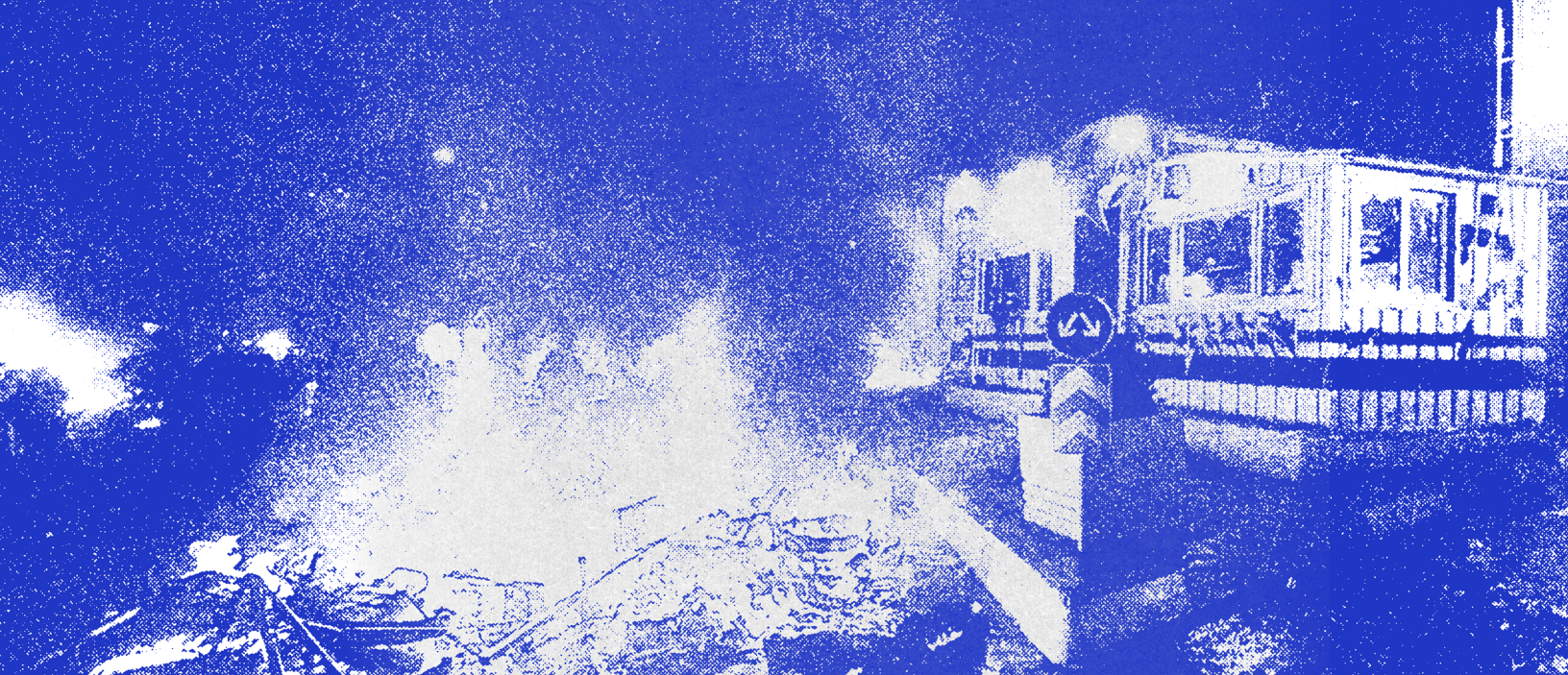
۳.۱. نظام هویت معتبر در «فضای مجازی»

«احراز هویت» در کنار «مجوز» و «مدیریت حساب» (AAA; Authentication, Authorization, Accounting) اجزای اصلی هر چارچوب امنیتی برای دسترسی به منابع و خدمات در یک شبکه است. اما این مساله آنجا تبدیل به پتانسیلی برای «نظارت و تجسس» شهروندان می‌شود که همه این خدمات از درگاه‌های واحد مرکزی (SSO; Single Sign-on)، یکپارچه و فراگیر «احراز هویت» که تحت کنترل حکومت است در دسترس قرار بگیرند. «احراز هویت» در مرکز و هسته اصلی هر سامانه «نظارت و تجسس» قرار دارد.

در سپتامبر ۲۰۱۹ در شورای عالی فضای مجازی مصوبه «نظام هویت معتبر در فضای مجازی کشور» تصویب شد که در توضیح آن آمده که هدفش «ایجاد زیرساخت‌های لازم برای تعاملات امن و قابل اطمینان در فضای مجازی» است.^{۱۴} این مصوبه «تمامی تعاملات فنی، اقتصادی، فرهنگی، اجتماعی، سیاسی و اداری» را ملزم به استفاده از شناسه‌های معتبر می‌کند.

بر اساس این مصوبه، تمامی موجودیت‌ها در شبکه ملی اطلاعات و شبکه‌های مرتبط با آن باید هویت احراز شده داشته باشند و ارائه‌دهندگان خدمات موظفند از پذیرش تعاملات فاقد هویت معتبر خودداری کنند. ماده ۳ تأکید می‌کند که، تمام تعاملات کاربران با شبکه ملی اطلاعات یا سامانه‌های داخلی مثل پنجره دولت هوشمند باید از کانال احراز هویت بگذرند. براساس این ماده (بند ۶) این شناسه برای «هر شخص» منحصر به فرد است و «هر تعامل» [در شبکه ملی اطلاعات] باید به شخصی منحصر به فرد منتهی شود. براساس ماده ۴، وزارت ارتباطات، زیرساخت تأمین شناسه را توسعه می‌دهد. سایر دستگاه‌های اجرایی در لایه‌های کاربردی شبکه ملی اطلاعات، تحت نظر مرکز ملی فضای مجازی از این سیستم برای توسعه سیستم تأمین شناسه‌های لایه کاربرد خود استفاده می‌کنند.

در ماده ۴ این مصوبه برای توسعه «درگاه واحد» برای



۲. سامانه‌های حکومتی نظارت و تجسس از شهروندان در جمهوری اسلامی ایران

خصوصی کاربران و شیوه جمع‌آوری پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوه‌ای فضای مجازی^{۱۵} را تصویب کرد. این دستورالعمل اجرایی، همه خدمات اینترنتی داخلی را ملزم می‌کند که دسترسی‌های اجباری و اختیاری که از کاربر می‌گیرند را به اطلاع او رسانده، اطلاعات کاربر را رمزنگاری کرده و امکان «حذف حساب کاربری» را فراهم کنند. اما در بند ۱-۳ می‌نویسد:

«در صورت درخواست کاربر برای حذف داده‌های مرتبط از قبیل حذف حساب کاربری ... بلافاصله انجام پذیرفته و داده‌های حذف شده از سامانه، به منظور رعایت مقررات قانونی از جمله مقررات مواد ۷۶۶ تا ۷۶۷ قانون آیین دادرسی کیفری (جرایم رایانه‌ای) به پایگاه پشتیبان مستقر در بخش غیر برخط و منفصل از شبکه ... نگهداری و پس از خاتمه مواعد قانونی یا قضایی به‌طور کامل امحا شود».

به عبارت بهتر، پس از درخواست کاربر برای «حذف اکانت» از سکوه‌ای مختلف داخلی، اطلاعات حساب کاربری او حذف

استفاده سیستم‌های ارائه‌دهنده خدمات عمومی از سامانه‌های احراز هویت برای مدیریت و تسهیل خدمات دیجیتال به شهروندان، در دولت‌ها یا سایر بخش‌های خدمات عمومی مزایای مهمی مانند افزایش شفافیت، کاهش تقلب، و تسهیل فرآیندهای دیجیتال دارد. اما در جمهوری اسلامی ایران که آزادی‌های شهروندی تحت فشار است نگرانی‌هایی جدی درباره استفاده از این سامانه‌ها برای نظارت و تجسس شهروندان مطرح است. این سامانه‌ها می‌توانند ابزاری قدرتمند برای ردیابی و جمع‌آوری اطلاعات گسترده از فعالیت‌های آنلاین و آفلاین کاربران باشند. اگرچه هدف رسمی آنها ایجاد اعتماد در فضای مجازی است، اما در عمل می‌توانند برای شناسایی مخالفان سیاسی، محدود کردن آزادی بیان و اعمال کنترل اجتماعی مورد استفاده قرار گیرند. این نگرانی هم وجود دارد که ترکیب این سامانه‌ها با فناوری‌هایی نظیر یادگیری ماشینی با هدف تحلیل رفتار کاربران منجر به سطح جدیدی از نقض حریم خصوصی افراد در جمهوری اسلامی ایران شود.

«کمیسیون عالی تنظیم مقررات»^{۱۶} بخشی از مرکز ملی فضای مجازی و بالاترین نهاد تنظیم‌گر (Regulator) در ایران در ژانویه ۲۰۲۴ «دستورالعمل اجرایی بهبود حفاظت از حریم

اطلاعات هویتی از کاربران [توسط سکوها و پلتفرم‌ها] اعلام شده‌است.

اما بر اساس اسناد افشا شده در سال ۲۰۲۳ سیستم ذخیره‌سازی شمس‌ا به‌عنوان بستری برای نگهداری اطلاعات این سیستم شنود قانونی (Lawful Intercept) استفاده می‌شود (دی‌گرام پایین).^{۱۶} سیستم شنود قانونی شرح داده شده به طور قابل توجهی از استانداردهای شنود قانونی توسعه‌یافته در گروه‌های کاری ۳GPP^{۱۷} و کمیته‌های استاندارد ETSI^{۱۸} انحراف دارد. این استانداردها فرآیندها و رابط‌هایی را برای تبادل ضمانت‌های قانونی، امکان شنود ارتباطات و ارائه محتوای ارتباطی به یک مرجع قانونی تعریف می‌کنند. اما سیستم شنود قانونی در جمهوری اسلامی ایران به هیچ‌کدام از این استانداردها پایبند نیست و تحلیل اسناد فنی به‌دست آمده در تحقیقات مختلف و مطابقت آنها با قوانین تصویب شده، نشان می‌دهد این سامانه، ضمانت‌های قانونی، تحویل کامل اطلاعات کاربر در حین فعال‌سازی و ادغام عمیق در سیستم‌های کسب‌وکار تلفن همراه برای بازیابی محتوای کاربر و تغییر دسترسی به خدمات را ارائه نمی‌کند.

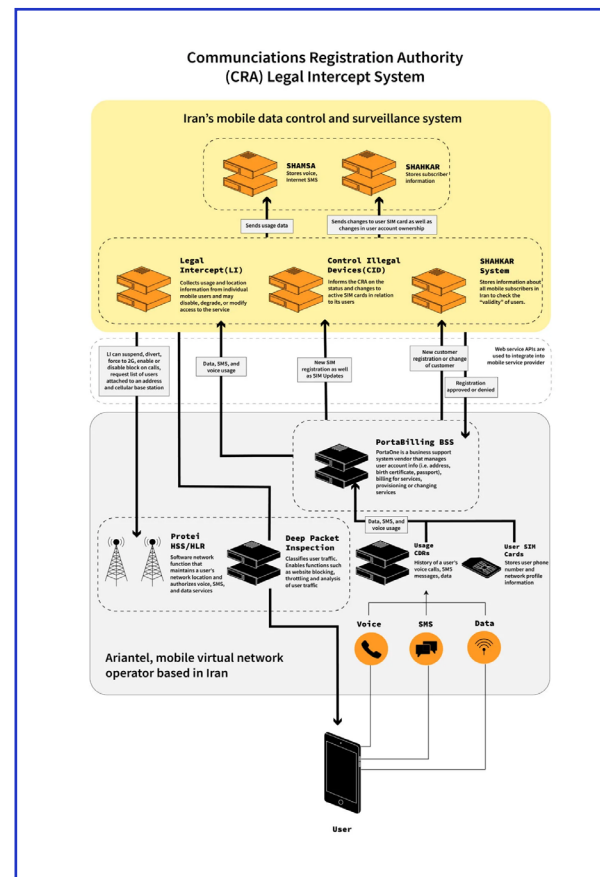
۱.۲. سامانه‌های زیرساختی و پنهان نظارت، تجسس و کنترل شهروندان

این دسته از سامانه‌ها به‌طور ذاتی و از ابتدا با کارویژه نظارت، شنود، ردیابی و تجسس طراحی شده‌اند و وجود و عملکرد آنها عموماً خارج از دید مستقیم شهروندان است. این سامانه‌ها در لایه‌های زیرساختی شبکه، مخابرات، مدیریت ترافیک، احراز هویت ارتباطی و تجمیع داده عمل می‌کنند و بدون تعامل مستقیم کاربر، امکان دسترسی گسترده و پیوسته به داده‌های ارتباطی و رفتاری شهروندان را فراهم می‌سازند. سامانه‌هایی مانند شاهکار، سیام، هم‌تا، اشراف، شمس‌ا و سیستم پایش سبک زندگی، نه به‌عنوان ابزار ارائه خدمت عمومی، بلکه به‌مثابه اجزای اصلی معماری کنترل دیجیتال در جمهوری اسلامی عمل می‌کنند. کارکرد این سامانه‌ها از نظر فنی به‌گونه‌ای است که شنود، ردیابی، تجمیع داده و اعمال محدودیت بر دسترسی کاربران را به‌صورت ساختاری و متمرکز ممکن می‌سازد و در عمل، ستون فقرات زیرساخت نظارتی و امنیتی حکومت را تشکیل می‌دهد.

نمی‌شود، بلکه به سرورهای آف‌لاین منتقل می‌شود.

براساس مواد ۶۶۷ و ۶۶۸ قانون آیین دادرسی کیفری^{۱۹} داده‌های ترافیک و اطلاعات کاربران حداقل شش ماه نگهداری می‌شود؛ اطلاعاتی از قبیل «مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات». همچنین «هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت (IP)، شماره تلفن و سایر مشخصات فردی» ذخیره می‌شود.

در ماده دوم این دستورالعمل اجرایی، از سکوها خواسته شده «برای احراز هویت کاربران، پس از فراهم‌شدن سازوکار لازم براساس قابلیت «زیست بوم هویت معتبر» توسط سازمان ثبت احوال کشور، سامانه‌های خود را با فرآیندهای مربوطه منطبق کنند.» یعنی از همه ارائه‌دهندگان خدمات اینترنتی می‌خواهد از یک سامانه واحد که هویت کاربران را با ثبت احوال (وزارت کشور) چک می‌کند، فرآیند احراز هویت را انجام دهند. هدف این بخش «به حداقل رساندن جمع‌آوری



سامانه‌های جامع حکومتی	Category	دسته
سامانه اشراف بر فضای مجازی	Name	نام
وزارت ارتباطات و فناوری اطلاعات	Operation by	اوپراتور
وزارت ارتباطات و فناوری اطلاعات (سازمان تنظیم مقررات / شرکت ارتباطات زیرساخت)، معاونت فضای مجازی دادستانی کل کشور، مرکز آمار و فناوری اطلاعات قوه قضاییه	Developer	توسعه‌دهنده
معاونت فضای مجازی دادستانی کل کشور	Ordered By	سفارش‌دهنده
بودجه‌های دستگاهی؟	Paid By	محل تامین بودجه
طراحی	Vision	چشم‌انداز
سراسری	Coverage	گسترده‌ی پوشش
خاص (شخصی)	Target	هدف
عمومی	Distribution	توزیع
پیش‌نویس آیین‌نامه اجرایی	Documents	اسناد

۱.۱.۲. سامانه «اشراف بر فضای مجازی»

بر فضای مجازی، موضوع بند ۲-۲-۱-۲۸ سند طرح کلان و معماری شبکه ملی اطلاعات مصوب شورای عالی فضای مجازی» است. این همان هدف بیست‌وهشتم است که دو سال قبل‌تر و در زمان انتشار سند طرح کلان و معماری شبکه ملی اطلاعات «غیر قابل انتشار» ذکر شده بود.

در این پیش‌نویس ذکر شده که هر نوع «داده ترافیکی از قبیل مبدا و مقصد و تاریخ» ارتباطات و هر نوع «اطلاعات کاربر» ذخیره شده و سپس در مواردی که «ظن قوی به کشف جرم ...» وجود داشته باشد با «اخذ دستور مقام قضایی» قابل ارائه به «متقاضی» است. براساس این اسناد، آنچه از عملکرد سامانه «اشراف بر فضای مجازی» انتظار می‌رود بر سیستم «شنود قانونی» منطبق است. بنابراین برای نخستین‌بار به سندی دست پیدا کرده‌ایم که بخشی از

یکی از مهم‌ترین مصوبه‌های تاثیرگذار در ساختار و چشم‌انداز توسعه شبکه ملی اطلاعات و آینده وضعیت اینترنت و حکمرانی دیجیتال جمهوری اسلامی ایران «طرح کلان و معماری شبکه ملی اطلاعات»^{۲۸} است که سال ۲۰۲۰ در شورای عالی فضای مجازی تصویب شد. این سند به عنوان نقشه راه توسعه شبکه در ایران تلاش دارد چارچوب کلی، اهداف، و الزامات فنی، حقوقی، و اجرایی مربوط به توسعه و مدیریت شبکه ملی اطلاعات را مشخص کند. در بخشی از این سند سی هدف برای این شبکه ذکر شده است. در این فهرست هدف بیست‌وهشتم «غیر قابل انتشار» ذکر شده است.

اما پس از حمله سایبری به سرور ای‌میل معاونت فضای مجازی دادستانی کل کشور^{۲۹} اطلاعات بی‌نظیری از جزئیات عملکرد و برنامه‌های توسعه‌ای برای سیستم سانسور و فیلتر در جمهوری اسلامی ایران با محوریت «کارگروه تعیین مصادیق محتوای مجرمانه» (کمیته فیلترینگ) به دست آمد. این نهاد، مهم‌ترین نهاد سانسور و فیلترینگ اینترنت در ایران است. این کارگروه متشکل از نمایندگان دوازده نهاد است و زیر نظر دادستانی کل کشور، معاونت فضای مجازی عمل می‌کند.

در بین این اسناد، پیش‌نویس سندی قرار داشت که عنوانش «آیین‌نامه بهره‌برداری از سامانه اشراف وزارت ارتباطات» نام دارد. در ماده ۱ این پیش‌نویس قید شده که «سامانه اشراف



عملکرد سیستم شنود قانونی را تحت عنوان «سامانه اشراف بر فضای مجازی» شرح می‌دهد.

هرچند بند اصلی سامانه اشراف از «اهداف شبکه ملی اطلاعات» منتشر نشده‌است، اما همین آیین‌نامه اجرایی هم جزییات دارد که سطح این «اشراف اطلاعاتی» را آشکار می‌کند. برای مثال در ماده ۱ در توصیف متقاضیان استفاده از سامانه اشراف در باره کاربران این سیستم می‌نویسد:

«مقامات قضایی، ضابطان دادگستری (فرماندهان، افسران و درجه‌داران نیروی انتظامی که کارت ضابط دریافت نموده‌اند) ... کارکنان وزارت اطلاعات در کشف مفاصد کلان اقتصادی و کارکنان سپاه پاسداران در ماموریت‌های موضوع مواد ۲ تا ۵ اساسنامه سپاه پاسداران و بند ۲ ماده ۶ قانون تأسیس وزارت اطلاعات، ضابط قوه قضائیه».

ماده ۲ اساسنامه سپاه «مبارزه با جمهوری اسلامی»^{۲۳} ارجاع داده‌است که جرمی امنیتی است. این موضوع، اهمیت «سامانه اشراف» در سیستم امنیتی جمهوری اسلامی را نشان می‌دهد. اما نکته قابل توجه، اشراف وزارت ارتباطات به «همه» داده‌های مبادله شده در کشور است. در ماده ۴ پیش‌نویس آمده:

«درخصوص استعلامات موردی داده ترافیک یا اطلاعات کاربران، متقاضی درخواست خود را با ذکر دلایل و قرائن مربوطه و اطلاعات پایه نظیر PI مبدأ یا مقصد، تاریخ، زمان، نوع خدمت، نشانی سایت مقصد، از طریق سامانه به مقام قضایی رسیدگی کننده به پرونده ارائه و در صورت موافقت مقام قضایی، دستور ارائه داده‌های موردنظر در اجرای ماده ۷۶ قانون آیین دادرسی کیفری از طریق سامانه ثبت شده و پاسخ بطور خودکار از سامانه دریافت و به متقاضی مربوطه ارائه می‌گردد.»

جزئیات فنی دیگری از سامانه «اشراف» یا قابلیت «اشراف بر فضای مجازی» در شبکه ملی اطلاعات در دسترس نیست

آیین نامه بهره برداری از سامانه اشراف وزارت ارتباطات

بخش اول: تعاریف و اختصارات

ماده ۱- تعاریف و اختصارات بکاررفته شده در این دستورالعمل به شرح ذیل است:

- سامانه: سامانه اشراف بر فضای مجازی موضوع بند ۲-۱-۲۸ سند طرح کلان و معماری شبکه ملی اطلاعات مصوب شورای عالی فضای مجازی

- قانون: قانون آیین دادرسی کیفری

- داده ترافیک: هرگونه داده‌ای که سامانه‌های رایانه‌ای و مخابراتی در زنجیره ارتباطات تولید می‌کنند تا امکان ردیابی آن‌ها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مقصد، مسیر، تاریخ، زمان، مدت، حجم و نوع ارتباط و خدمات می‌باشد

- اطلاعات کاربر: هرگونه اطلاعاتی راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده، مدت زمان آن، اطلاعات هویتی کاربر، نشانی جغرافیایی یا پستی، IP، شماره تلفن و سایر مشخصات فردی وی.

- کنترل ارتباطات: دسترسی به داده‌های در حال انتقال یا ذخیره شده ارتباطات خصوصی نظیر محتوای ایمیل، پیامک، گفتگوی خصوصی در شبکه‌های اجتماعی و پیام‌رسان و ارتباطات مخابراتی.

- متقاضی: مقامات قضایی، ضابطان دادگستری (فرماندهان، افسران و درجه داران نیروی انتظامی که کارت ضابط دریافت نموده‌اند) که در اساسنامه، اساسنامه سپاه پاسداران، اساسنامه وزارت اطلاعات، اساسنامه قوه قضائیه یا اساسنامه

اما شواهد دیگری که از سامانه‌های سیام، همتا، شاهکار و ... به‌دست آمده نشان می‌دهد وزارت ارتباطات و فناوری اطلاعات، در حال توسعه زیرساخت‌هاییست که امکان کامل شنود شهروندان و نظارت و تجسس از داده‌های ترافیکی کاربران را مطابق مصوباتی که دو دهه پیش در شورای عالی انقلاب فرهنگی تصویب شده‌بود، فراهم می‌کند.

۲.۱.۲. شاهکار؛ شبکه احراز هویت کاربران ارتباطی

سامانه شاهکار (شبکه احراز هویت کاربران ارتباطی)^{۲۴} به‌منظور احراز هویت کاربران در خدمات ارتباطی و اینترنتی به کار می‌رود. این سامانه با تطبیق شماره ملی افراد با شماره تلفن‌های همراه آن‌ها، هویت کاربران را تایید کرده و از استفاده ناشناس از خدمات دیجیتال جلوگیری می‌کند.^{۲۵} این امر به دولت امکان می‌دهد تا فعالیت‌های آنلاین شهروندان را به‌دقت رصد کند. کسب و کارها می‌توانند با ارسال کد ملی و شماره موبایل کاربر به سامانه شاهکار، بررسی کنند که شماره موبایل متعلق به صاحب کد ملی است یا خیر.

اسناد داخلی نشان می‌دهد که سازمان تنظیم مقررات و ارتباطات رادیویی، در حال ایجاد دسترسی مستقیم از طریق API ها به سیستم‌های پشتیبان اپراتورهای تلفن همراه (صورت‌حساب، فعال‌سازی سرویس و پشتیبانی) برای شاهکار است. این امر وزارت ارتباطات را قادر می‌سازد تا ثبت‌نام‌ها را مسدود کند، تایید هویت را به صورت بلادرنگ اجرا کند و یک رجیستری متمرکز از کاربران تلفن همراه را به عنوان یک جز اصلی معماری رهگیری قانونی گسترده‌تر جمهوری اسلامی ایران حفظ کند.

شاهکار اطلاعات هویتی کاربران، شامل کد ملی، شماره

دسته	Category	سامانه‌های جامع حکومتی
نام	Name	سامانه شاهکار (شبکه احراز هویت کاربران ارتباطی)
اوپراتور	Operation by	وزارت ارتباطات و فناوری اطلاعات (سازمان تنظیم مقررات و ارتباطات رادیویی؟)
توسعه‌دهنده	Developer	داخلی
سفارش‌دهنده	Ordered By	مرکز ملی فضای مجازی
محل تامین بودجه	Paid By	بودجه‌های دستگاهی؟
چشم‌انداز	Vision	پیاده‌سازی‌شده
گسترده پوشش	Coverage	سراسری
هدف	Target	شخصی
توزیع	Distribution	عمومی (همه افراد دارای سیم کارت یا خط تلفن)
اسناد	Documents	مستندات ipa

می‌کند. دسترسی به این داده‌ها برای نهادهای نظارتی و امنیتی به‌صورت بی‌درنگ (Real-Time) امکان‌پذیر است. سامانه سیام این قابلیت را دارد که سرعت اینترنت کاربران را کاهش داده یا دسترسی آن‌ها را به‌طور کامل قطع کند. همچنین، این سامانه می‌تواند کاربران را از شبکه‌های امن‌تر ۳G و LTE به فناوری GPRS منتقل کند که امکان شنود و نظارت بیشتری فراهم می‌سازد. داده‌های ذخیره‌شده بر روی این سامانه شامل تماس‌ها، پیام‌ها و حق محتوای ارتباطات آنلاین کاربران می‌شود (تصویریلاً؛ بخش Data در سند افشا شده^{۲۴}) که نشان‌دهنده میزان گسترده و عمیق

تلفن، و داده‌های مرتبط با ثبت‌نام آن‌ها را جمع‌آوری و ذخیره می‌کند. این موضوع خطر نقض حریم خصوصی کاربران را افزایش می‌دهد، به‌ویژه اگر مدیریت داده‌ها به‌درستی انجام نشود یا دسترسی غیرمجاز رخ دهد. کاربران اغلب از نحوه ذخیره‌سازی، استفاده و به‌اشتراک‌گذاری داده‌های خود در سامانه شاهکار آگاه نیستند.

۳.۱.۲. سیام؛ سامانه یکپارچه استعلامات مخابراتی

سیام (سیستم یکپارچه استعلامات مخابراتی) به‌عنوان یکی از ابزارهای کلیدی نظارت، تجسس و حق سرکوب دیجیتال شهروندان در جمهوری اسلامی، نمایانگر میزان سیطره حکومت بر زندگی دیجیتال شهروندان است. این سامانه تحت نظارت سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری) و از زیرمجموعه وزارت ارتباطات فعالیت می‌کند. سازمان تنظیم مقررات وظیفه ارائه مجوز فعالیت برای اپراتورها را برعهده دارد. اطلاعات مربوط به یکی از ورژن‌های این سامانه (مربوط به سال ۲۰۱۸) در سال ۲۰۲۲ افشا شد.^{۲۵}

براساس سند مشخصات فنی api سیام، این سیستم چهل قابلیت در زمینه شنود، نظارت، تجسس، ردیابی و سرکوب شهروندان را دارد. یکی از مهم‌ترین ویژگی‌های سیام، توانایی ردیابی موقعیت جغرافیایی دقیق کاربران از طریق سیم‌کارت است. این سیستم کلیه اطلاعات تماس‌های کاربران را ثبت

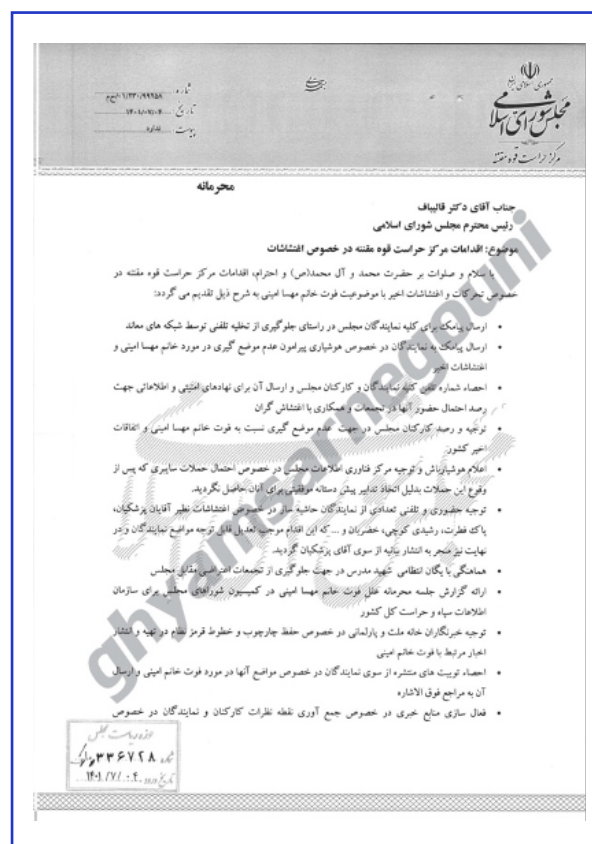
محل درج لوگوی اپراتور		سامانه یکپارچه استعلامات مخابراتی (سیام)		اداره کل امنیت سیستم‌های ارتباطی	
نام سند		۴-۵. استعلام ریز ارتباطات ترکیبی (GetIPDR)		تایید ریز ارتباطات ترکیبی	
فارسی		انگلیسی		فارسی	
شماره		شماره تلفن		۱. شماره تلفن	
TelNum		IPAddr		۲. آدرس IP	
Cid		FDdate		۳. تاریخ	
TDate		Uname		۴. نام کاربری	
AuthStr		AuthStr		۵. رمز عبور	
GetIPDR		AuthStr		۶. تاریخ و ساعت شروع ارتباط (Session)	
AuthStr		AuthStr		۷. تاریخ و ساعت پایان ارتباط (Session)	
AuthStr		AuthStr		۸. آدرس IP مبدأ	
AuthStr		AuthStr		۹. آدرس IP مقصد	
AuthStr		AuthStr		۱۰. پورت مبدأ	
AuthStr		AuthStr		۱۱. پورت مقصد	
AuthStr		AuthStr		۱۲. حجم Upload	
AuthStr		AuthStr		۱۳. حجم Download	
AuthStr		AuthStr		۱۴. MacAddress	
AuthStr		AuthStr		۱۵. Layer3 Protocol	
AuthStr		AuthStr		۱۶. Layer4 Protocol	
AuthStr		AuthStr		۱۷. آدرس سبب مقصد	
AuthStr		AuthStr		۱۸. پورت سبب مقصد	
AuthStr		AuthStr		۱۹. پورت سبب مقصد	
AuthStr		AuthStr		۲۰. پورت سبب مقصد	
AuthStr		AuthStr		۲۱. پورت سبب مقصد	
AuthStr		AuthStr		۲۲. پورت سبب مقصد	
AuthStr		AuthStr		۲۳. پورت سبب مقصد	
AuthStr		AuthStr		۲۴. پورت سبب مقصد	
AuthStr		AuthStr		۲۵. پورت سبب مقصد	
AuthStr		AuthStr		۲۶. پورت سبب مقصد	
AuthStr		AuthStr		۲۷. پورت سبب مقصد	
AuthStr		AuthStr		۲۸. پورت سبب مقصد	
AuthStr		AuthStr		۲۹. پورت سبب مقصد	
AuthStr		AuthStr		۳۰. پورت سبب مقصد	
AuthStr		AuthStr		۳۱. پورت سبب مقصد	
AuthStr		AuthStr		۳۲. پورت سبب مقصد	
AuthStr		AuthStr		۳۳. پورت سبب مقصد	
AuthStr		AuthStr		۳۴. پورت سبب مقصد	
AuthStr		AuthStr		۳۵. پورت سبب مقصد	
AuthStr		AuthStr		۳۶. پورت سبب مقصد	
AuthStr		AuthStr		۳۷. پورت سبب مقصد	
AuthStr		AuthStr		۳۸. پورت سبب مقصد	
AuthStr		AuthStr		۳۹. پورت سبب مقصد	
AuthStr		AuthStr		۴۰. پورت سبب مقصد	
AuthStr		AuthStr		۴۱. پورت سبب مقصد	
AuthStr		AuthStr		۴۲. پورت سبب مقصد	
AuthStr		AuthStr		۴۳. پورت سبب مقصد	
AuthStr		AuthStr		۴۴. پورت سبب مقصد	
AuthStr		AuthStr		۴۵. پورت سبب مقصد	
AuthStr		AuthStr		۴۶. پورت سبب مقصد	
AuthStr		AuthStr		۴۷. پورت سبب مقصد	
AuthStr		AuthStr		۴۸. پورت سبب مقصد	
AuthStr		AuthStr		۴۹. پورت سبب مقصد	
AuthStr		AuthStr		۵۰. پورت سبب مقصد	
AuthStr		AuthStr		۵۱. پورت سبب مقصد	
AuthStr		AuthStr		۵۲. پورت سبب مقصد	
AuthStr		AuthStr		۵۳. پورت سبب مقصد	
AuthStr		AuthStr		۵۴. پورت سبب مقصد	
AuthStr		AuthStr		۵۵. پورت سبب مقصد	
AuthStr		AuthStr		۵۶. پورت سبب مقصد	
AuthStr		AuthStr		۵۷. پورت سبب مقصد	
AuthStr		AuthStr		۵۸. پورت سبب مقصد	
AuthStr		AuthStr		۵۹. پورت سبب مقصد	
AuthStr		AuthStr		۶۰. پورت سبب مقصد	
AuthStr		AuthStr		۶۱. پورت سبب مقصد	
AuthStr		AuthStr		۶۲. پورت سبب مقصد	
AuthStr		AuthStr		۶۳. پورت سبب مقصد	
AuthStr		AuthStr		۶۴. پورت سبب مقصد	
AuthStr		AuthStr		۶۵. پورت سبب مقصد	
AuthStr		AuthStr		۶۶. پورت سبب مقصد	
AuthStr		AuthStr		۶۷. پورت سبب مقصد	
AuthStr		AuthStr		۶۸. پورت سبب مقصد	
AuthStr		AuthStr		۶۹. پورت سبب مقصد	
AuthStr		AuthStr		۷۰. پورت سبب مقصد	
AuthStr		AuthStr		۷۱. پورت سبب مقصد	
AuthStr		AuthStr		۷۲. پورت سبب مقصد	
AuthStr		AuthStr		۷۳. پورت سبب مقصد	
AuthStr		AuthStr		۷۴. پورت سبب مقصد	
AuthStr		AuthStr		۷۵. پورت سبب مقصد	
AuthStr		AuthStr		۷۶. پورت سبب مقصد	
AuthStr		AuthStr		۷۷. پورت سبب مقصد	
AuthStr		AuthStr		۷۸. پورت سبب مقصد	
AuthStr		AuthStr		۷۹. پورت سبب مقصد	
AuthStr		AuthStr		۸۰. پورت سبب مقصد	
AuthStr		AuthStr		۸۱. پورت سبب مقصد	
AuthStr		AuthStr		۸۲. پورت سبب مقصد	
AuthStr		AuthStr		۸۳. پورت سبب مقصد	
AuthStr		AuthStr		۸۴. پورت سبب مقصد	
AuthStr		AuthStr		۸۵. پورت سبب مقصد	
AuthStr		AuthStr		۸۶. پورت سبب مقصد	
AuthStr		AuthStr		۸۷. پورت سبب مقصد	
AuthStr		AuthStr		۸۸. پورت سبب مقصد	
AuthStr		AuthStr		۸۹. پورت سبب مقصد	
AuthStr		AuthStr		۹۰. پورت سبب مقصد	
AuthStr		AuthStr		۹۱. پورت سبب مقصد	
AuthStr		AuthStr		۹۲. پورت سبب مقصد	
AuthStr		AuthStr		۹۳. پورت سبب مقصد	
AuthStr		AuthStr		۹۴. پورت سبب مقصد	
AuthStr		AuthStr		۹۵. پورت سبب مقصد	
AuthStr		AuthStr		۹۶. پورت سبب مقصد	
AuthStr		AuthStr		۹۷. پورت سبب مقصد	
AuthStr		AuthStr		۹۸. پورت سبب مقصد	
AuthStr		AuthStr		۹۹. پورت سبب مقصد	
AuthStr		AuthStr		۱۰۰. پورت سبب مقصد	

دسته	Category	سامانه‌های جامع حکومتی
نام	Name	سیام (سیستم یکپارچه استعلامات مخابراتی)
اوپراتور	Operation by	سازمان تنظیم مقررات و ارتباطات رادیویی
توسعه‌دهنده	Developer	اپراتورهای تلفن همراه / داخلی
سفارش‌دهنده	Ordered By	سازمان تنظیم مقررات و ارتباطات رادیویی وزارت ارتباطات و فناوری اطلاعات
محل تامین بودجه	Paid By	بودجه‌های دستگاهی؟
چشم‌انداز	Vision	پیاده‌سازی‌شده
گسترده‌گی پوشش	Coverage	سراسری
هدف	Target	شخصی / عمومی
توزیع	Distribution	عمومی (همه شهروندان دارای تلفن همراه)
استاد	Documents	لینک مستندات افشاشده (نسخه انگلیسی)

استفاده از امکانات فنی شبکه همراه برای ردیابی اهداف خاص نکته جدیدی نیست. هم پیش از این در برخی رسانه‌های داخلی نیروی انتظامی شواهد پژوهش و کار روی آن دیده شده بود،^{۲۷} هم شواهدی از آن در حملات سایبری اخیر به سرورهای مختلف حکومت آشکار شده بود. برای مثال نامه‌ای از رئیس مرکز حراست قوه مقننه به محمداقبر قالیباف، رئیس مجلس افشا شد که او گزارش می‌دهد که یکی از اقدامات آنها پس از آغاز اعتراضات سال ۲۰۲۲ «احصا شماره تلفن نمایندگان و کارکنان مجلس برای نهادهای امنیتی و اطلاعاتی جهت رصد احتمال حضور آنها در تجمعات» بوده است.^{۲۸} این نامه نشان می‌دهد رصد مکان فیزیکی نمایندگان مجلس به صورت Real-time فراهم است زیرا اعتراضات به صورت سیال در ساعات نامشخص و مکان‌های از پیش تعیین نشده و صرفاً با اجتماع و تشکیل هسته‌های اولیه معترضین شکل می‌گرفت.

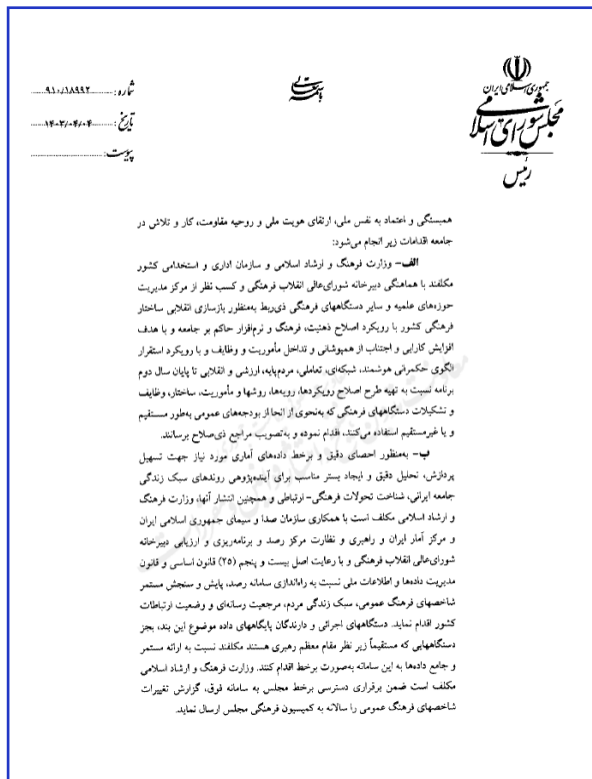
۴.۱.۲. سامانه رصد و سنجش سبک زندگی مردم

«برنامه هفتم پیشرفت جمهوری اسلامی ایران» که نقشه راه توسعه کشور برای پنج سال آینده است و در سال ۲۰۲۴ تصویب شده است، تاکید ویژه‌ای بر توسعه زیرساخت‌های دیجیتال، دولت الکترونیک و هوشمندسازی خدمات عمومی در سال‌های پیش رو دارد. این برنامه نقش کلیدی در تسریع روند گسترش سامانه‌های احراز هویت در ایران دارد. عدم قوانین شفاف، نظارت مستقل و رعایت حقوق شهروندی



نقض حریم خصوصی است. سیام اطلاعات کاربران را به سامانه‌های ابری داخلی منتقل می‌کند که به‌طور متمرکز مدیریت می‌شوند.

دسته	Category	سامانه‌های جامع حکومتی
نام	Name	سامانه رصد و سنجش سبک زندگی مردم
اوپراتور	Operation by	وزارت فرهنگ و ارشاد اسلامی
توسعه‌دهنده	Developer	وزارت فرهنگ و ارشاد اسلامی، صدا و سیما، جمهوری اسلامی ایران، مرکز آمار ایران
سفارش‌دهنده	Ordered By	قانون برنامه هفتم توسعه
محل تامین بودجه	Paid By	بودجه‌های دستگاهی؟
چشم‌انداز	Vision	طراحی
گسترده‌ی پوشش	Coverage	سراسری
هدف	Target	عمومی
توزیع	Distribution	عمومی
اسناد	Documents	قانون برنامه هفتم توسعه



در جمهوری اسلامی ایران احتمال اینکه این سامانه‌ها را به ابزارهای نقض حریم خصوصی و کنترل اجتماعی تبدیل کند بسیار بالا می‌برد. این ابزارها هنوز در مرحله طراحی هستند.

مشهورترین سامانه که در زمان تصویب این برنامه توجه افکار عمومی را به خود جلب کرد^{۲۵} «سامانه رصد و سنجش سبک زندگی مردم» است.^{۲۶} هدف این سامانه جمع‌آوری و تحلیل داده‌هایی از رفتارها، گرایش‌ها و الگوهای زندگی شهروندان است. مسئولیت اجرای این طرح به وزارت فرهنگ و ارشاد اسلامی با همکاری مرکز آمار ایران محول شده و قرار است از سال ۲۰۲۵ عملیاتی شود. در پیش‌نویس اولیه لایحه برنامه عنوان «سامانه رصد پایش و سنجش مستمر شاخص‌های فرهنگ عمومی سنجش دینداری و سطح معنویت و اخلاق و سبک زندگی مردم» برای آن انتخاب شده بود ولی در لایحه تقدیمی به مجلس به «سامانه رصد، پایش و سنجش مستمر شاخص‌های فرهنگ عمومی و سبک زندگی مردم» تغییر نام داد.

بر اساس ماده ۷۵ لایحه برنامه هفتم توسعه، وزارت فرهنگ و ارشاد اسلامی موظف است سیستمی برای «رصد، پایش و سنجش مستمر شاخص‌های فرهنگ عمومی و سبک زندگی مردم» ایجاد کند. این سامانه با رویکرد اسلامی-ایرانی طراحی شده و به دنبال سنجش مستمر ارزش‌ها، گرایش‌ها، رفتارها و نهادهای فرهنگی-اجتماعی جامعه ایرانی است. تمامی دستگاه‌های اجرایی و دارندگان پایگاه‌های داده

موظف به ارائه مستمر و جامع داده‌ها به این سامانه به صورت برخط هستند. جزئیات دقیق عملکرد این سامانه هنوز مشخص نشده اما پیش‌بینی می‌شود داده‌های متنوعی از منابع مختلف جمع‌آوری شود. این داده‌ها می‌تواند شامل اطلاعات مربوط به خریدهای اینترنتی، استفاده از خدمات آنلاین، الگوهای مصرف، فعالیت‌های فرهنگی و اجتماعی و

سامانه‌های جامع حکومتی	Category	دسته
سامانه سماوا (سامانه ملی احراز هویت و استعلامات)	Name	نام
درگاه ملی خدمات الکترونیکی ایران	Operation by	اوپراتور
داخلی	Developer	توسعه‌دهنده
سازمان فناوری اطلاعات ایران (فاوا)	Ordered By	سفارش‌دهنده
بودجه‌های دستگاهی؟	Paid By	محل تامین بودجه
پیاده‌سازی شده	Vision	چشم‌انداز
سراسری	Coverage	گسترده پوشش
شخصی	Target	هدف
عمومی (همه شهروندان)	Distribution	توزیع
لینک سامانه، مستندات فنی	Documents	اسناد

۲.۲.۱. سماوا؛ سامانه ملی احراز هویت و استعلامات

سماوا (سامانه ملی احراز هویت و استعلامات) را سازمان فناوری اطلاعات ایران (فاوا) زیرمجموعه وزارت ارتباطات توسعه داده است. این سامانه یک تامین کننده شناسه ارتباطی در «نظام هویت معتبر» است. براساس ادعای منابع جمهوری اسلامی ایران، سماوا با هدف ایجاد یکپارچگی در فرآیند احراز هویت و ارائه خدمات هویتی به دستگاه‌های دولتی و غیردولتی (سکوها و خدمات اینترنتی) فعالیت می‌کند.

اسناد رسمی، سماوا را به عنوان یک زیرساخت اعتماد دیجیتال بنیادی توصیف می‌کنند که به عنوان دروازه احراز هویت ملی فعالیت می‌کند. سماوا به جای ذخیره داده‌های هویتی حساس در یک پایگاه داده متمرکز، به عنوان یک هماهنگ‌کننده امن عمل می‌کند که از منابع معتبری مانند سازمان ثبت احوال یا سازمان تنظیم مقررات ارتباطات برای تأیید بلادرنگ درخواست می‌کند. این معماری که به عنوان «حریم خصوصی از طریق طراحی» تعریف شده است، به سرویس‌های دولتی اجازه می‌دهد تا هویت کاربران را از طریق پاسخ‌های توکن‌بله/خبر و بدون دسترسی مستقیم به پایگاه‌های داده اصلی تأیید کنند. در حالی که این مدل خطر حمله سایبری را کاهش می‌دهد و قابلیت همکاری بین نهادهای دولتی را افزایش می‌دهد، اما یک وابستگی

حق ترجیحات غذایی باشد. ادغام این اطلاعات در یک پایگاه داده مرکزی، امکان تحلیل جامع و دقیق‌تری از سبک زندگی شهروندان را فراهم می‌کند.

۲.۲. سامانه‌های رسمی و آشکار نظارت و احراز هویت در تعاملات روزمره شهروندان

دسته دوم شامل سامانه‌هایی است که در ظاهر و در تعریف رسمی، کارویژه‌ای مدنی، خدماتی و اداری دارند و شهروندان برای انجام امور روزمره ناگزیر از استفاده از آن‌ها هستند. سامانه‌هایی مانند سماوا، ثنا، ام‌تا و هدا، در بسیاری از حکومت‌ها نیز معادل‌هایی دارند و اصولاً برای تسهیل ارائه خدمات عمومی، احراز هویت، کاهش ثقل و دیجیتالی‌سازی فرآیندهای اداری طراحی می‌شوند. با این حال، در جمهوری اسلامی ایران، این سامانه‌ها در چارچوبی قرار گرفته‌اند که به‌طور سیستماتیک آن‌ها را به ابزارهای نظارت، شنود و تجسس تبدیل می‌کند. اتصال این سامانه‌ها به زیرساخت‌های متمرکز هویتی، الزام به عبور تعاملات از درگاه‌های واحد، و هم‌پوشانی آن‌ها با سامانه‌های امنیتی و قضایی، باعث شده است که داده‌های تولیدشده در فرآیندهای عادی شهروندی، به‌راحتی در خدمت پایش، ردیابی و کنترل افراد قرار گیرد. در نتیجه، آنچه در ظاهر «خدمت عمومی دیجیتال» است، در عمل به بخشی از زنجیره نظارت و اشراف اطلاعاتی حکومت بدل شده است.

سامانه‌های جامع حکومتی	Category	دسته
هدا (هویت دیجیتال ایرانیان)	Name	نام
سازمان ثبت احوال کشور	Operation by	اوپراتور
داخلی	Developer	توسعه‌دهنده
سازمان ثبت احوال وزارت کشور	Ordered By	سفارش‌دهنده
بودجه‌های دستگاهی؟	Paid By	محل تامین بودجه
پیاده‌سازی شده	Vision	چشم‌انداز
سراسری	Coverage	گسترده پوشش
شخصی	Target	هدف
عمومی (همه شهروندان)	Distribution	توزیع
لینک سامانه، لینک دانلود فایل اپلیکیشن اندروید	Documents	اسناد

۲.۲.۲. ثنا؛ سامانه احراز هویت قضایی آنلاین

سامانه ثنا (احراز هویت قضایی آنلاین)^{۳۵} در مرکز آمار و فناوری اطلاعات قوه قضائیه، در زیر مجموعه معاونت خدمات الکترونیک قضایی توسعه پیدا کرده‌است. این سامانه یک پلتفرم رسمی تایید هویت برای خدمات قضایی، دسترسی آنلاین به پرونده‌ها و سایر تعاملات دیجیتال مرتبط با قوه قضاییه در نظر گرفته شده‌است.

اسناد داخلی نشان می‌دهد که ثنا از کاربران می‌خواهد با استفاده از شماره ملی، شماره تلفن همراه و در برخی موارد تایید اطلاعات شخصی (نام، آدرس) خود در برابر ثبت احوال ملی یا سوابق دادگاه، احراز هویت کنند. منابع رسمی تاکید می‌کنند افرادی که از طریق ثنا احراز هویت نشوند، ممکن است از دسترسی به خدمات الکترونیکی قضایی، از جمله احضاریه‌های دادگاه و اعلان‌های مربوط به پرونده، که اکنون منحصر از طریق این پلتفرم ارائه می‌شوند، محروم شوند.

ثنا شناسه‌های شخصی مورد استفاده در هنگام ثبت نام و سوابق تلاش‌های احراز هویت را جمع‌آوری و ذخیره می‌کند. این امر نگرانی‌هایی را در مورد شفافیت، به ویژه در مورد مدت زمان نگهداری داده‌ها، چه کسی به آنها دسترسی دارد و نحوه اشتراک‌گذاری آنها با نهادهای قضایی یا امنیتی ایجاد می‌کند. بسیاری از کاربران از این رویه‌ها بی‌اطلاع هستند یا گزینه‌های معناداری برای کنترل یا حذف داده‌های خود تحت

استراتژیک نیز ایجاد می‌کند: هرگونه خرابی در سیستم‌های متصل، مانند پایگاه داده سازمان ثبت احوال، می‌تواند دسترسی به همه خدمات دولتی دیجیتال را مختل کند.

سماوا از یک سو در تسهیل خدمات دولت الکترونیک نقش مثبتی ایفا می‌کند، اما از سوی دیگر، پتانسیل این را دارد که به ابزاری قدرتمند برای کنترل اجتماعی و محدودیت آزادی‌های شهروندی تبدیل شود.

۲.۲.۲. هدا؛ سامانه احراز هویت دیجیتال ایرانیان

سامانه هدا (هویت دیجیتال ایرانیان)^{۳۶} را سازمان ثبت احوال کشور راه‌اندازی کرده و جایگزین ارائه کپی شناسنامه و کارت ملی است.^{۳۷} این پلتفرم به سازمان‌های دولتی و مؤسسات مجاز اجازه می‌دهد تا هویت فرد را به صورت الکترونیکی از طریق پرس‌وجوهای امن مبتنی بر API تأیید کنند.

اما تمرکز بالای این سامانه بر اطلاعات حساس هویتی، پتانسیل استفاده از این پایگاه داده‌ای جامع و قدرتمند برای ردیابی و نظارت گسترده را برای نظارت و تجسس، بیشتر می‌کند. ساختار متمرکز و انباشت داده‌های هویتی بسیار حساس آن، نگرانی‌هایی را در میان مدافعان حریم خصوصی ایجاد کرده‌است. در رسانه‌های حکومتی ایران، از «هدا» به‌عنوان «ابر پروژه احراز هویت اشخاص» نام برده شده‌است.^{۳۸}

سامانه‌های جامع حکومتی	Category	دسته
سامانه ثنا (احراز هویت قضایی آنلاین)	Name	نام
معاونت خدمات الکترونیک قضایی قوه قضائیه	Operation by	اوپراتور
داخلی (مرکز آمار و فناوری اطلاعات قوه قضائیه)	Developer	توسعه‌دهنده
دادگستری	Ordered By	سفارش‌دهنده
بودجه‌های دستگاهی؟	Paid By	محل تامین بودجه
پیاده‌سازی‌شده	Vision	چشم‌انداز
سراسری	Coverage	گسترده‌ی پوشش
شخصی	Target	هدف
عمومی (همه شهروندان)	Distribution	توزیع
لینک سامانه	Documents	اسناد

ساختارهای قانونی موجود ندارند.

صورت پیشرفت سرمایه‌گذاری‌ها در طرح‌های «گوشی ملی» و «سیستم عامل ملی» پتانسیل جدی پیاده‌سازی برای کاربردهای محدودکننده دیگری هم پیدا کند که مستقیماً حریم خصوصی افراد را تهدید کند.

۴.۲.۲. هم‌تا؛ سامانه هوشمند مدیریت تجهیزات ارتباطی

۵.۲.۲. ام‌تا؛ سامانه احراز مشتریان تجارت الکترونیکی

سامانه ام‌تا (احراز مشتریان تجارت الکترونیکی)^{۳۸} را مرکز توسعه تجارت الکترونیکی وزارت صنعت، معدن و تجارت (صمت) راه‌اندازی کرده‌است. هدف اصلی ام‌تا، احراز هویت و اعتبارسنجی «فروشنده‌گان» به صورت بلادرنگ برای پایگاه‌های داده دولتی در حوزه تجارت الکترونیکی است. این سامانه با استعلام آنلاین از پایگاه‌های اطلاعاتی نهادهای مختلف، صحت اطلاعات اظهارشده مشتریان را بررسی می‌کند.

در حالی که این سامانه به طور رسمی به دنبال کاهش تقلب در تجارت الکترونیک است، می‌تواند اطلاعات ارزشمندی درباره جزئیات فعالیت‌های اقتصادی افراد در اختیار نهادهای نظارتی قرار دهد. ام‌تا، به عنوان یک مرکز جمع‌آوری داده تحت کنترل دولت عمل می‌کند که نهادهای نظارتی را قادر می‌سازد تا فعالیت‌های تجاری افراد را رصد کنند. یعنی مأموریت دوگانه‌ای دارد: هم به عنوان یک پلتفرم خدماتی طراحی شده برای تسهیل تجارت الکترونیک (مشوقی برای

سامانه هم‌تا (سیستم هوشمند مدیریت تجهیزات ارتباطی)^{۳۹} برای مدیریت و نظارت بر واردات و استفاده از دستگاه‌های تلفن همراه در ایران (رجیستری)^{۳۷} ایجاد شده است. این سامانه با ثبت و ردیابی IMEI دستگاه‌ها از ورود و استفاده غیرمجاز از تلفن‌های همراه جلوگیری می‌کند و به گمرک جمهوری اسلامی و وزارت صمت امکان می‌دهد تا کنترل دقیقی بر توزیع و استفاده از این تجهیزات داشته‌باشد.

سامانه هم‌تا کاربران را مجبور به استفاده از گوشی‌هایی می‌کند که به صورت رسمی وارد کشور شده‌اند، یعنی اگر یک گوشی با هر سیم‌کارتی برای اولین بار به شبکه همراه وصل شود، به محض اینکه شبکه ارتباطی کشور این IMEI جدید را شناسایی کرد، صاحب دستگاه ۳۰ روز مهلت دارد اطلاعات خود را در سامانه هم‌تا وارد کرده تا هویت دارنده آن دستگاه برای حکومت مشخص شود، در غیر این صورت ارتباطات Data دستگاه قطع می‌شود. فرآیند «رجیستری» برای گوشی‌هایی مختلف، هزینه‌های متفاوتی دارد. جمهوری اسلامی، با استفاده از این سیستم مانع استفاده کاربران ایرانی از مدل‌های آی‌فون ۱۴ به بعد شده‌بود. این الزام نه تنها آزادی انتخاب افراد را محدود می‌کند بلکه در آینده در

دسته	Category	سامانه‌های جامع حکومتی
نام	Name	همتا (سیستم هوشمند مدیریت تجهیزات ارتباطی)
اوپراتور	Operation by	سامانه جامع تجارت ایران (وزارت صنعت، معدن و تجارت)
توسعه‌دهنده	Developer	وزارت ارتباطات و فناوری اطلاعات / داخلی
سفارش‌دهنده	Ordered By	ستاد مرکزی مبارزه با قاچاق کالا و ارز، گمرک جمهوری اسلامی ایران
محل تامین بودجه	Paid By	بودجه‌های دستگاهی؟
چشم‌انداز	Vision	پیاده‌سازی شده
گسترده‌ی پوشش	Coverage	سراسری
هدف	Target	شخصی / عمومی
توزیع	Distribution	عمومی (همه شهروندان دارای تلفن همراه)
اسناد	Documents	لینک سرویس

الزامی کردن استفاده از ام‌تا در بخش‌های خاصی از اقتصاد، تایید می‌کند که نقش آن فراتر از فعال کردن تجارت الکترونیک است. این سیستم همچنین ابزاری برای اجرای قانون و تنظیم مقررات اقتصادی است.

مشاغل) و هم به عنوان یک ابزار نظارتی که توسط دولت برای اعمال کنترل بر بازار دیجیتال (منبع فشار) استفاده می‌شود، عمل می‌کند. این دوگانگی درونی، جنجال‌ها و مقاومت‌های مداوم در مورد اجرای آن را دامن زده است.

این سیستم سوابق دقیقی از کالاها و خدمات معامله شده (داده‌های سطح SKU)، تاریخچه تراکنش‌ها و تعاملات مرتبط با هویت را جمع‌آوری می‌کند. با توجه به ادغام آن در زیرساخت حاکمیت دیجیتال دولت، حتی رسانه‌های دولتی نیز از ام‌تا به دلیل فرآیند تایید هویت مبهم و احتمال

روایت رسمی مرکز توسعه تجارت الکترونیک بر راحی کاربر، امنیت و پشتیبانی از مشاغل تأکید دارد. با این حال، برجسته‌ترین و اجباری‌ترین موارد استفاده این سیستم در پاسخ به بحران‌های اقتصادی، مانند تورم قیمت در بازار خودرو، پدیدار شده است. دخالت دادستانی کل کشور در

دسته	Category	سامانه‌های جامع حکومتی
نام	Name	ام‌تا (احراز مشتریان تجارت الکترونیکی)
اوپراتور	Operation by	پنجره واحد تجارت الکترونیکی
توسعه‌دهنده	Developer	داخلی
سفارش‌دهنده	Ordered By	مرکز توسعه تجارت الکترونیکی وزارت صنعت، معدن و تجارت (صمت)
محل تامین بودجه	Paid By	بودجه‌های دستگاهی؟
چشم‌انداز	Vision	پیاده‌سازی شده
گسترده‌ی پوشش	Coverage	سراسری
هدف	Target	شخصی
توزیع	Distribution	خاص (فعالان تجارت الکترونیکی)
اسناد	Documents	لینک سامانه

سامانه‌های جامع حکومتی	Category	دسته
سَخا (سامانه خدمات الکترونیک انتظامی)	Name	نام
فرماندهی انتظامی جمهوری اسلامی (پلیس ایران)	Operation by	اوپراتور
داخلی	Developer	توسعه‌دهنده
فرماندهی انتظامی جمهوری اسلامی (پلیس ایران)	Ordered By	سفارش‌دهنده
بودجه‌های دستگاهی؟	Paid By	محل تامین بودجه
پیاده‌سازی‌شده	Vision	چشم‌انداز
سراسری	Coverage	گسترده‌ی پوشش
شخصی	Target	هدف
عمومی (همه شهروندان)	Distribution	توزیع
لینک سامانه	Documents	اسناد

دسترسی بیش از حد به اطلاعات، انتقاد کرده‌اند.^{۳۹}

۶.۲.۲. سَخا؛ سامانه خدمات انتظامی (پلیس)

سَخا داده‌هایی از حوزه‌های متفاوت و حساس را به‌طور هم‌زمان گردآوری و یکپارچه می‌کند؛ از جمله اطلاعات هویتی، نشانی دقیق محل سکونت، سوابق نظام وظیفه، وضعیت گذرنامه و وثیقه خروج از کشور و سوابق انتظامی و ترافیکی.^{۴۰} این تجمیع داده‌ها، امکان پیوند میان حوزه‌های مدنی، انتظامی و قضایی را فراهم می‌سازد و به نهاد انتظامی اجازه می‌دهد دسترسی شهروندان به برخی حقوق اداری را به تکمیل یا تایید داده‌ها در سامانه مشروط کند.

سامانه سَخا (سامانه خدمات الکترونیک انتظامی یا پلیس)^{۴۱} درگاه متمرکز ارائه خدمات الکترونیک فرماندهی انتظامی جمهوری اسلامی ایران (فراجا) است که به‌عنوان یکی از زیرساخت‌های اصلی دولت الکترونیک، مجموعه‌ای گسترده از خدمات انتظامی و اداری را به‌صورت غیرحضوری در اختیار شهروندان قرار می‌دهد. این سامانه خدماتی نظیر امور نظام وظیفه، صدور و تمدید گذرنامه، احراز محل سکونت، خدمات شماره‌گذاری و تعویض پلاک خودرو، استعلام و اعتراض به تخلفات رانندگی، و مدیریت برخی فرآیندهای خروج از کشور را پوشش می‌دهد.

از منظر نظارت، سَخا فراتر از یک سامانه خدماتی عمل می‌کند و به ابزاری برای «کنترل اداری دیجیتال» بدل می‌شود؛ به‌گونه‌ای که اعمال محدودیت‌هایی مانند جلوگیری از تعویض پلاک، تعلیق برخی خدمات، یا اعمال محدودیت‌های خروج از کشور می‌تواند به‌صورت سیستمی و بدون مواجهه فیزیکی انجام شود. تمرکز این حجم از داده‌های حساس در یک سامانه تحت مدیریت مستقیم فراجا، در غیاب یک قانون جامع حفاظت از داده‌های شخصی، ریسک‌های جدی نقض حریم خصوصی و استفاده ثانویه از داده‌ها برای مقاصد نظارتی و امنیتی را به‌همراه دارد.

۷.۲.۲. میخک؛ سامانه مدیریت یکپارچه خدمات کنسولی

سامانه میخک (مدیریت یکپارچه خدمات کنسولی)^{۴۲} درگاه متمرکز ارائه خدمات کنسولی وزارت امور خارجه جمهوری

کارویژه رسمی سَخا، تسهیل دسترسی شهروندان به خدمات انتظامی و کاهش مراجعات حضوری اعلام شده است. با این حال، ماهیت متمرکز سامانه و الزام شهروندان به ثبت‌نام و احراز هویت برای انجام طیف وسیعی از امور حیاتی، سَخا را به یکی از گره‌های اصلی تجمیع داده‌های حساس شهروندی تبدیل کرده است. احراز هویت در این سامانه بر پایه اتصال کد ملی، شماره تلفن ثبت‌شده در سازمان ثبت احوال، و اطلاعات هویتی پایه انجام می‌شود و عملاً یک هویت دیجیتال غیرقابل انکار برای کاربران ایجاد می‌کند.

دسته	Category	سامانه‌های جامع حکومتی
نام	Name	میخک (مدیریت یکپارچه خدمات کنسولی)
اوپراتور	Operation by	وزارت امور خارجه جمهوری اسلامی ایران
توسعه‌دهنده	Developer	داخلی
سفارش‌دهنده	Ordered By	وزارت امور خارجه جمهوری اسلامی ایران
محل تامین بودجه	Paid By	بودجه‌های دستگاهی؟
چشم‌انداز	Vision	پیاده‌سازی شده
گسترده پوشش	Coverage	خارج از کشور
هدف	Target	شخصی
توزیع	Distribution	عمومی (همه شهروندان ساکن خارج از کشور)
اسناد	Documents	لینک سامانه

امکان می‌دهد ارائه یا تعلیق خدمات را به صورت سیستمی مدیریت کند. تمرکز این حجم از داده‌های حساس درباره جامعه ایرانیان خارج از کشور، در غیاب شفافیت درباره نحوه اشتراک‌گذاری داده‌ها با سایر نهادهای حکومتی، نگرانی‌های جدی درباره استفاده ثانویه از اطلاعات، ردیابی کنسولی، و اعمال فشار اداری یا امنیتی بر شهروندان را تقویت می‌کند.

معماری نظارت و تجسس در جمهوری اسلامی ایران صرفاً متکی بر ابزارهای پنهان امنیتی نیست، بلکه بر ترکیبی از سامانه‌های زیرساختی نامرئی و سامانه‌های رسمی و خدمات‌محور استوار است. در این ساختار، سامانه‌هایی که کارویژه‌های مدنی یا اداری دارند، از طریق اتصال به پایگاه‌های متمرکز هویتی و قضایی، به اجزایی از زنجیره نظارت و کنترل بدل می‌شوند. هم‌زمان، سامانه‌های زیرساختی پنهان، امکان شنود، ردیابی و تجمیع داده را در مقیاس کلان فراهم می‌کنند. نتیجه، شکل‌گیری نظامی است که در آن تعاملات روزمره شهروندان به صورت سیستماتیک به داده‌های قابل پایش و اعمال قدرت حکومتی تبدیل می‌شود.

اسلامی ایران برای شهروندان ایرانی خارج از کشور است. این سامانه با هدف دیجیتالی‌سازی و تسهیل خدمات کنسولی طراحی شده و فرایندهایی مانند ثبت و به‌روزرسانی اطلاعات هویتی، امور گذرنامه، وکالت‌نامه‌های کنسولی، تایید اسناد، امور سجلی، و برخی خدمات مرتبط با تابعیت و اقامت را به صورت غیرحضوری پوشش می‌دهد. در بسیاری از کشورها، سامانه‌های مشابهی برای ارائه خدمات کنسولی به اتباع مقیم خارج وجود دارد و کارویژه رسمی میخک نیز در همین چارچوب تعریف می‌شود.

با این حال، در جمهوری اسلامی ایران، میخک به یکی از گره‌های اصلی تجمیع داده‌های هویتی و کنسولی ایرانیان خارج از کشور تبدیل شده است. استفاده از این سامانه مستلزم ثبت اطلاعات دقیق هویتی، اقامتی و تماس است و احراز هویت کاربران به گونه‌ای طراحی شده که داده‌های کنسولی را به سامانه‌های هویتی داخلی متصل می‌کند. این اتصال، امکان هم‌پوشانی داده‌های کنسولی با پایگاه‌های اطلاعاتی داخل کشور را فراهم می‌سازد و یک پروفایل دیجیتال قابل پیگیری از شهروندان خارج از کشور ایجاد می‌کند.

از منظر نظارت، میخک فراتر از یک ابزار خدماتی عمل می‌کند و به بستری برای پایش اداری و کنسولی شهروندان در خارج از کشور بدل شده است. وابستگی دسترسی به خدمات کنسولی به ثبت و صحت‌سنجی داده‌ها در این سامانه، به دولت

۳. ابزارهای مخفی حکومت برای نظارت و تجسس

شهروندان در پلت فرمی به نام «کاشف» را آشکار کرد.^{۴۵}

این دسته از روش‌های حکومت جمهوری اسلامی ایران در پیاده‌سازی سیستم‌های نظارتی و تجسسی، ماهیتی پویا دارند و ابزارهای آن‌ها به مرور زمان تغییر می‌کنند. برخلاف روش‌هایی که توسط وزارت ارتباطات هدایت می‌شوند، توسعه این سیستم‌ها عمدتاً تحت نظر نهادهای امنیتی و نظامی مانند وزارت اطلاعات و سازمان اطلاعات سپاه پاسداران انقلاب اسلامی انجام می‌گیرد. شناسایی اهداف جدید و تحلیل عمیق‌تر فعالیت‌های این سیستم‌ها نیازمند ابزارهای پیشرفته‌تر و به‌روزتر است. در ادامه، به معرفی تعدادی از ابزارهایی که پیش‌تر توسط محققان امنیت سایبری افشا شده‌اند و در راستای این تکنیک‌ها برای نظارت و تجسس در زندگی شهروندان مورد استفاده قرار گرفته‌اند، خواهیم پرداخت.

۱.۳. شنود مرد میانی در سیاست‌های نظارتی حکومت

از نظر فنی، «حمله یا ترفند مرد میانی» (Man-in-the-Middle یا MITM) به نوعی شنود فعال اطلاق می‌شود که در آن یک بازیگر ثالث، بدون اطلاع یا رضایت طرفین ارتباط، خود را میان دو نقطه ارتباطی قرار می‌دهد تا داده‌های ردوبدل‌شده را شنود، دستکاری یا ثبت کند. در استانداردهای بین‌المللی امنیت سایبری و مخابرات، MITM به‌عنوان یک

حکومت جمهوری اسلامی ایران با استفاده از تکنیک‌های پیشرفته نظارتی و توسعه سامانه‌های جاسوسی، سرویس‌های اینترنتی را به بستری برای کنترل و پایش مخفیانه شهروندان تبدیل کرده‌است. برای کنترل و نظارت بر فعالیت‌های شهروندان در فضای مجازی، از سامانه‌های مختلفی استفاده می‌شود که بعضی به‌طور خاص برای جاسوسی و پایش اطلاعات طراحی شده‌اند و بعضی دیگر به ظاهر عملکرد و کاربرد دیگری دارند اما در عین حال انواع دسترسی‌ها و فناوری‌های ثبت و کنترل تمام یا برخی از رفتارهای کاربر حداقل روی دستگاهی که نصب هستند را دارند؛ ابزارهایی مانند ترفند مرد میانی، پوسته‌های حاکمیت‌پذیر و تروجان‌های دسترسی از راه دور (RAT).

نشت اطلاعات از سرورهای ای‌میل «کمپته فیلترینگ» دادستانی کل کشور در نوامبر ۲۰۲۲ نشان داد که نهادهای حکومتی در تلاشند تا با استفاده از تکنیک‌های پیچیده مانند «ترفند مرد میانی» دسترسی شهروندان به اینترنت و خدمات خارجی را کنترل کرده و نظارت کاملی بر فعالیت‌های آنلاین آن‌ها اعمال کنند.^{۴۳} مصوبه ۱۰۴ شورای عالی فضای مجازی در دسامبر ۲۰۲۴ نیز پیاده‌سازی «پوسته‌های حاکمیت‌پذیر» را برای کاربری یوتیوب، تلگرام و سایر پلت‌فرم‌هایی که «مذاکره با آنها شکست بخورد» را توصیه کرده‌است.^{۴۴} در نوامبر ۲۰۲۵، نشت اطلاعات گروه هکری چارمینگ کیتن (APT۳۵) استفاده گسترده این تهدید امنیتی پیشرفته وابسته به سپاه پاسداران انقلاب اسلامی، از تروجان‌های دسترسی از راه دور علیه اهدافی ایرانی و غیرایرانی و جمع‌آوری اطلاعات

۱.۱.۳. نهادهای پیشران شنود مرد میانی در ایران

به‌کارگیری شنود مرد میانی در جمهوری اسلامی ایران حاصل ابتکارهای فنی پراکنده نیست، بلکه نتیجه کنش مجموعه‌ای از نهادهای حکومتی در حوزه‌های قضایی، تنظیم‌گری و امنیتی است. در مرکز این فرآیند، «کارگروه تعیین مصادیق محتوای مجرمانه» یا همان کمیته فیلترینگ قرار دارد که زیر نظر دادستانی کل کشور فعالیت می‌کند و نقش محوری در تعیین اولویت‌های اجرایی برای کنترل محتوا و محدودسازی دسترسی ایفا می‌کند. این نهاد با هماهنگی ارائه‌دهندگان خدمات اینترنتی و اپراتورهای زیرساختی، اهداف سیاستی را به رویه‌های فنی شنود و رهگیری ترجمه کرده‌است.

اسناد به‌دست آمده از نشت اطلاعات این نهاد نشان می‌دهد که شنود مرد میانی نه به‌عنوان اقدامی استثنایی، بلکه به‌مثابه راه‌حلی عملی برای آنچه «خروج کنترل ارتباطات رمزگذاری‌شده و سکوه‌های خارجی از سیطره حکومت» توصیف شده، در نظر گرفته شده‌است؛ به‌ویژه در مواردی که سازوکارهای متعارف فیلترینگ کارایی لازم را نداشته‌اند.^{۴۴}

در کنار نهادهای قضایی، ساختارهای حکمرانی اینترنت نیز در مشروعیت‌بخشی و گسترش این رویه نقش داشته‌اند. شورای عالی فضای مجازی به‌عنوان نهاد بالادستی سیاست‌گذار اینترنت در ایران، بارها بر ضرورت اعمال سازوکارهای موثر برای اعمال حاکمیت بر خدمات آنلاین تأکید کرده است. هرچند این سازوکارها در قالب الزامات تنظیم‌گری معرفی می‌شوند، اما در عمل بر مدل‌های رهگیری و کنترل میانی مبتنی هستند که با منطق شنود مرد میانی هم‌پوشانی مستقیم دارد.

نهادهای امنیتی و نظامی، از جمله وزارت اطلاعات و سازمان اطلاعات سپاه پاسداران انقلاب اسلامی، نیز نقشی موازی در توسعه و به‌کارگیری قابلیت‌های شنود ایفا می‌کنند. این فعالیت‌ها، برخلاف برنامه‌های متمرکزی که زیر نظر وزارت ارتباطات و فناوری اطلاعات اجرا می‌شوند، عموماً طبقه‌بندی‌شده، انعطاف‌پذیر و معطوف به جمع‌آوری اطلاعات هستند. در مجموع، این کنش‌گران قضایی، تنظیم‌گر و امنیتی، اکوسیستمی نهادی شکل داده‌اند که در آن شنود مرد میانی به‌عنوان ابزاری عادی برای حکمرانی، اعمال قانون و نظارت بر شهروندان تثبیت شده است.

فعالیت مخرب یا خصمانه طبقه‌بندی می‌شود و معمولاً با جرایم سایبری، جاسوسی یا نفوذ غیرمجاز به شبکه‌ها مرتبط است. از این رو، این تکنیک به‌عنوان تهدید امنیتی تعریف می‌شود که باید شناسایی و خنثی شود، نه به‌عنوان بخشی از سیاست‌گذاری برای حکمرانی شبکه.

در شکل مجرمانه، حملات مرد میانی معمولاً برای فیشینگ، سرقت نام کاربری و گذرواژه، ربایش نشست‌های ارتباطی و کلاهبرداری مالی به‌کار می‌روند. این حملات از ضعف‌های پیکربندی شبکه، زنجیره اعتماد گواهی‌های امنیتی یا رفتار کاربران سوءاستفاده می‌کنند تا به ارتباطات دسترسی غیرمجاز پیدا کنند. اما زمانی که این تکنیک توسط دولت‌های اقتدارگرا به‌کار گرفته می‌شود، ماهیت آن از یک ترفند غیرقانونی به ابزاری مبتنی بر سیاست‌گذاری تغییر می‌کند. در این حالت، MITM نه در حاشیه شبکه، بلکه در دل زیرساخت‌های ملی، ارائه‌دهندگان خدمات اینترنتی و چارچوب‌های تنظیم‌گری ادغام می‌شود و امکان شنود در مقیاس وسیع و با پشتوانه نهادی را فراهم می‌آورد.

دولت‌های اقتدارگرا عمدتاً به این دلیل به تکنیک‌های مرد میانی متوسل می‌شوند که رمزنگاری سرتاسری (end-to-end encryption) دسترسی مستقیم به محتوای ارتباطات را برای نهادهای نظارتی به‌شدت محدود کرده است. با گسترش پیام‌رسان‌های رمزگذاری‌شده و استفاده فراگیر از HTTPS، شنود سنتی مبتنی بر محتوا کارایی خود را از دست داده است. در چنین شرایطی، رهگیری در نقاط میانی مانند فرآیندهای حل نام دامنه (DNS)، دسته‌دهی TLS یا اعتبارسنجی گواهی‌های امنیتی، به یک گزینه راهبردی برای بازیابی اشراف اطلاعاتی تبدیل می‌شود. از طریق کنترل این لایه‌های میانی، دولت می‌تواند بدون نیاز به همکاری پلت فرم‌های خارجی، به الگوهای رفتاری کاربران، فراداده‌ها و در برخی موارد به خود محتوا دسترسی پیدا کند.

این دگرگونی MITM از یک ترفند فنی به ابزار حکمرانی، نشان‌دهنده تغییری اساسی در شیوه‌های معاصر نظارت است. تغییری که از شنود هدفمند به سمت کنترل زیرساختی حرکت می‌کند؛ جایی که خود معماری شبکه به ابزار پایش، فیلترینگ و تنظیم رفتار شهروندان بدل می‌شود.

۳.۱.۲. جایگاه شنود مرد میانی در معماری شبکه ملی اطلاعات

امکان‌پذیری عملی شنود مرد میانی در ایران به‌طور مستقیم با معماری شبکه ملی اطلاعات گره خورده است. برخلاف رهگیری‌های مقطعی یا موردی، پیاده‌سازی شنود مرد میانی در مقیاس گسترده و پایدار مستلزم کنترل ساختاری بر لایه‌های کلیدی ترافیک شبکه، از جمله مسیریابی، حل نام دامنه و امنیت لایه انتقال است. شبکه ملی اطلاعات با متمرکزسازی جریان‌های ترافیکی، استانداردسازی نقاط دسترسی و ایجاد امکان مداخله هماهنگ در زیرساخت‌های داخلی، چنین سطحی از اشراف متمرکز را فراهم می‌کند.

در سطح فنی، شنود مرد میانی در بستر شبکه ملی اطلاعات از طریق سازوکارهایی مانند دستکاری DNS، رهگیری TLS و تزریق گواهی‌های امنیتی تسهیل می‌شود. با کنترل یا تأثیرگذاری بر فرآیند حل نام دامنه، ترافیک کاربران می‌تواند بدون آگاهی صریح آن‌ها به گره‌های میانی هدایت شود. همچنین رهگیری در مرحله دست‌دهی TLS امکان بازرسی یا دستکاری نشست‌های رمزگذاری‌شده را فراهم می‌کند، به‌ویژه زمانی که با مراجع صدور گواهی مورد اعتماد یا تحت اجبار و سامانه‌های بازرسی عمیق بسته‌ها (DPI) ترکیب شود. این روش‌ها نقطه شنود را به لایه‌های بالادستی شبکه منتقل می‌کنند و آن را در دل عملیات عادی شبکه جای می‌دهند، نه در سطح اپلیکیشن.

ارائه‌دهندگان خدمات اینترنتی و شرکت‌های ارتباطات ثابت (FCP) نقشی کلیدی در امکان‌پذیر ساختن این مدل ایفا می‌کنند. این اپراتورها به‌عنوان دارندگان مجوز، از جایگاهی ساختاری برای اجرای سیاست‌های رهگیری ابلاغ‌شده از سوی نهادهای قضایی یا تنظیم‌گر برخوردارند. اتصال آن‌ها به زیرساخت مسیریابی ملی و الزامات تبعیت از مقررات، امکان پیاده‌سازی یکپارچه و سراسری شنود مرد میانی را فراهم می‌کند. در چنین ساختاری، رهگیری دیگر وابسته به هدف‌گیری کاربران خاص نیست، بلکه بر کل بخش‌هایی از ترافیک اعمال می‌شود و مرز میان شنود قانونی و نظارت فراگیر را مخدوش می‌سازد.

در نتیجه، شبکه ملی اطلاعات به‌عنوان پیش‌نیاز استقرار پایدار شنود مرد میانی عمل می‌کند. با تجمع کنترل بر نقاط تبادل ترافیک و کاهش وابستگی به مسیرهای خارجی، این

شبکه هزینه‌های فنی و عملیاتی رهگیری را کاهش داده و در عین حال دامنه و ماندگاری آن را افزایش می‌دهد. این ادغام، شنود مرد میانی را از یک تاکتیک موقعیتی به قابلیت نظام‌مند و نهادینه‌شده در چارچوب حکمرانی اینترنت در ایران تبدیل می‌کند.

۳.۱.۳. اهداف و کارکردهای مرد میانی

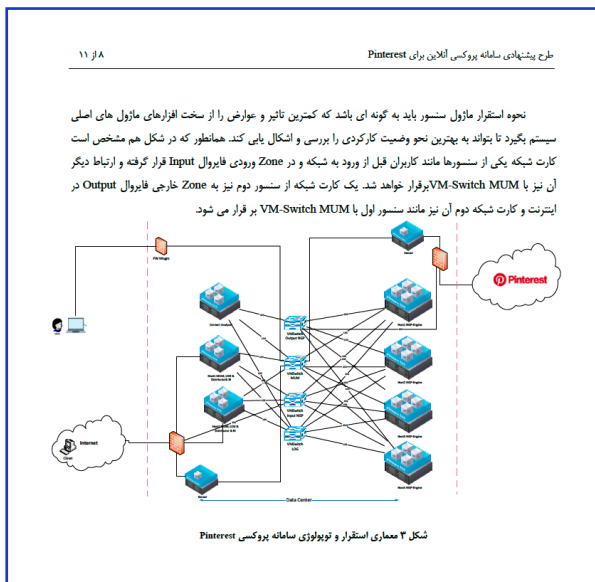
شنود مرد میانی در جمهوری اسلامی ایران چندین هدف هم‌پوشان را دنبال می‌کند که فراتر از فیلترینگ محتوا یا مسدودسازی سکوها است. یکی از کارکردهای اصلی این روش، کنترل دسترسی به خدمات و پلت‌فرم‌های خارجی از طریق تضعیف گزینشی، هدایت مجدد یا اعطای مشروط دسترسی به ترافیک است. برخلاف مسدودسازی‌های صریح و یک‌دست، شنود مرد میانی امکان مداخله‌ای دقیق‌تر را فراهم می‌کند و به نهادهای حکومتی اجازه می‌دهد نحوه، زمان و شرایط دسترسی کاربران به خدمات خارجی را تنظیم کنند.

کارکرد محوری دیگر شنود مرد میانی، دور زدن یا تضعیف رمزنگاری است. هرچند رمزگشایی کامل ارتباطات رمزگذاری‌شده سرتاسری اغلب ممکن نیست، اما رهگیری در لایه‌های میانی شبکه امکان جمع‌آوری فراداده‌ها، شناسه‌های نشست و نشانه‌های رفتاری مرتبط با ارتباطات رمزگذاری‌شده را فراهم می‌کند. این داده‌ها، حتی بدون دسترسی به محتوای پیام‌ها، اطلاعات ارزشمندی درباره شبکه ارتباطی کاربران، الگوهای تماس و سطح فعالیت آن‌ها در اختیار نهادهای نظارتی قرار می‌دهد.

شنود مرد میانی همچنین از شناسایی کاربران و دستگاه‌ها در سطح شبکه پشتیبانی می‌کند. با همبست‌سازی جریان‌های ترافیکی با شناسه‌های فنی مانند نشانی‌های IP، اثرانگشت‌های دستگاه، IMEI و IMSI، امکان پیوند دادن رفتار آنلاین به افراد مشخص و تجهیزات فیزیکی فراهم می‌شود. این قابلیت، رهگیری میان‌سکوپی را تسهیل کرده و داده‌های به‌دست‌آمده را با سایر سامانه‌های نظارتی، از جمله پایگاه‌های هویتی و مخابراتی، یکپارچه می‌سازد.

در سطحی کلان‌تر، شنود مرد میانی به‌عنوان ابزاری برای پایش رفتاری عمل می‌کند. رصد مستمر تلاش‌های اتصال، نوع پروتکل‌های مورد استفاده و ناهنجاری‌های ترافیکی،

تلاش‌های پیشین نیز از همین منطق پیروی می‌کردند. در اوایل دهه ۱۳۹۰، پیام‌رسان وایبر که یکی از محبوب‌ترین سکوها ارتباطی در ایران بود، هدف بهره‌برداری در سطح سکو قرار گرفت. یک پیمانکار خصوصی طرحی را به کارگروه فیلترینگ ارائه کرد که شامل ۱۳ سناریوی فنی از جمله استخراج داده و تزریق محموله از راه دور بود.^{۴۷} همچنین این سناریوها شامل ارسال پیام‌های مخرب، تخلیه اطلاعاتی کاربران، ایجاد جنگ روانی و حتی ایجاد حساب‌های طعمه (هانی پات) برای نفوذ و جمع‌آوری داده‌ها بود.



این اقدامات به‌طور علنی توسط کمال هادیانفر، رئیس وقت پلیس فتا، تأیید شد؛ او اعلام کرد که پیام‌های خصوصی در پیام‌رسان‌هایی مانند وایبر عملاً تحت کنترل نهادهای انتظامی قرار دارند.^{۴۸} این اظهارات در کنار پروژه‌های شرکت‌هایی نظیر کیسان، نشان‌دهنده تلاش سیستماتیک حکومت برای نظارت، جاسوسی و دستکاری اطلاعات کاربران در فضای مجازی است. این اقدامات، به‌ویژه در زمانی که وایبر یکی از محبوب‌ترین پیام‌رسان‌ها در ایران بود، بیانگر نقض گسترده حریم خصوصی و استفاده از فناوری به‌عنوان ابزاری برای کنترل اجتماعی است.

امکان پروفایل‌سازی از رفتار کاربران، شناسایی تلاش‌های دور زدن فیلترینگ و تعیین اهداف برای اقدامات بعدی را فراهم می‌آورد. به این ترتیب، شنود مرد میانی نه‌فقط یک تکنیک نظارتی، بلکه سازوکاری اجرایی است که سیاست‌های فیلترینگ را تقویت کرده، سرکوب‌گرینشی را ممکن می‌سازد و داده‌های لازم را به سامانه‌های گسترده‌تر کنترل تزریق می‌کند.

برای نمونه در سال ۲۰۲۰، شرکتی با نام «یافتار پژوهان پیش‌تاز رایانش» پروژه‌ای موسوم به «پروکسی نسل جدید» را به کارگروه فیلترینگ ارائه داد.^{۴۹} این پروژه شامل ایجاد یک رابط کاربری کاملاً کلون‌شده از پینترست بود که به‌عنوان یک پروکسی واسط عمل می‌کرد و پیش از نمایش محتوا به کاربر، آن را در لحظه شنود، فیلتر و دست‌کاری می‌کرد. این سامانه که به‌عنوان «راهکار دسترسی» معرفی شده بود، امکان ثبت کامل جست‌وجوهای کاربران، ترجیحات محتوایی و امضاهای رفتاری را فراهم می‌ساخت.

طرح «پروکسی نسل جدید» شامل ایجاد نسخه‌ای جعلی از وب‌سایت پینترست بود که به کاربران ایرانی امکان دسترسی به این پلتفرم را از طریق یک واسطه داخلی می‌داد. این واسطه می‌توانست درخواست‌های کاربران را دریافت، بررسی، سانسور و سپس به سرویس اصلی ارسال کند؛ در نهایت پاسخ را نیز پس از دریافت و اعمال سانسور به کاربر ارائه می‌کرد. این روش، که به نوعی فیشینگ در مقیاس گسترده محسوب می‌شود، امکان جاسوسی و نظارت بر فعالیت‌های کاربران را برای نهادهای امنیتی فراهم می‌کند. با ایجاد نسخه‌های جعلی از سرویس‌های محبوب خارجی، اطلاعات حساس کاربران می‌تواند جمع‌آوری و تحلیل شود. این اقدام نه تنها حریم خصوصی کاربران را نقض می‌کند، بلکه امنیت اطلاعات شخصی آن‌ها را نیز به خطر می‌اندازد.

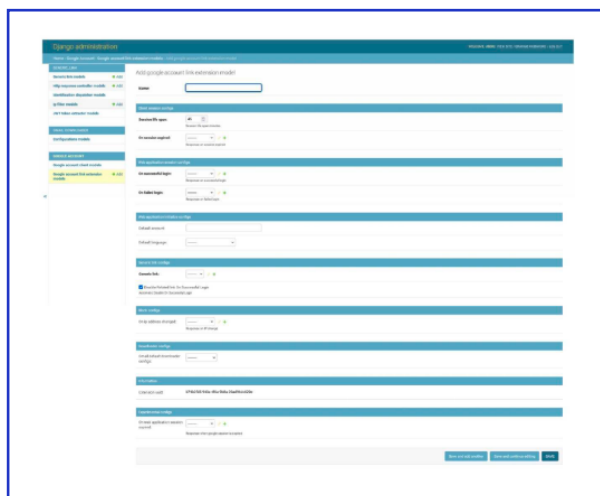
همکاری شرکت یافتارپژوهان پیش‌تاز رایانش با دادستانی تهران در این پروژه نشان‌دهنده تمایل نهادهای حکومتی به کنترل و نظارت بیشتر بر فعالیت‌های آنلاین شهروندان است.^{۴۸} این شرکت از مجموعه‌های اقماری «جمعیت توسعه‌گران فضای مجازی پاک» یا «هلدینگ امنیت نامدار» است. این مجموعه گروهی از سیاست‌گذاران و فعالان فضای ICT ایران هستند که با عنوان سیاست‌گذاران «فیلترینگ هوشمند» شناخته شده و می‌توان از رسول جلیلی استاد دانشگاه صنعتی شریف و عضو شورای عالی فضای مجازی^{۴۹} و عیسی زارع‌پور وزیر سابق ارتباطات به عنوان اعضای شاخص آن یاد کرد.^{۵۰}

۴.۱.۳. رپایش نشست به عنوان ابزار کنترل در سطح پلتفرم

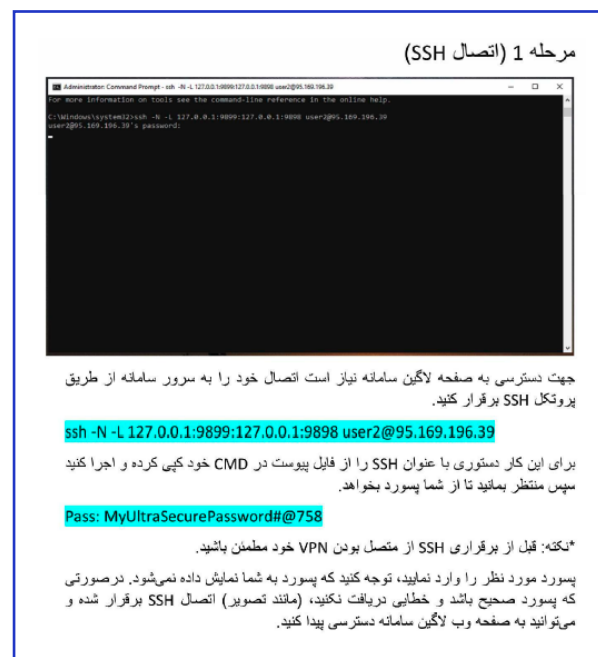
کنند، بی آنکه با محدودیت‌های رمزنگاری سرتاسری مواجه شوند.

اهمیت این تکنیک در زمینه تصاحب پلت فرم در آن است که نظارت را از نفوذ به دستگاه به تسلط بر حساب کاربری منتقل می‌کند. به جای کاشت بدافزار، مهاجم از منظر پلت فرم به خود کاربر تبدیل می‌شود. این منطق با پوسته‌های حاکمیت‌پذیر و خدمات کلون‌شده (دو بخش بعدی) هم‌راستاست: کنترل نه از طریق شکستن رمزنگاری، بلکه با قرار گرفتن در مسیرهای دسترسی مورد اعتماد تحقق می‌یابد. برخلاف جاسوس‌افزارها یا تروجان‌های دسترسی از راه دور، این سامانه برای جمع‌آوری نشست‌های احراز هویت‌شده، کوکی‌ها و داده‌های حساب کاربری طراحی شده و به مهاجمان اجازه می‌دهد بدون نصب بدافزار یا دور زدن سازوکارهای سیستم‌عامل، به حساب‌های Gmail دسترسی پیدا کنند.

اسناد فنی نشان می‌دهد این چارچوب بر یک زیرساخت سمت سرور مبتنی بر پنل کنترلی Django، تولید پویا لینک‌های فیشینگ و مازول‌های مدیریت نشست استوار است. این سامانه امکان استخراج نشست‌های فعال، شناسه‌های کاربر، آدرس‌های IP و اثرانگشت مرورگر را فراهم می‌کند و با استفاده مجدد از کوکی‌های معتبر، عملاً احراز هویت دومرحله‌ای را دور می‌زند. دسترسی به حساب‌های نفوذشده از طریق پراکسی و تونل SSH انجام می‌شود تا الگوی شبکه قربانی حفظ شود.



فراتر از استقرار بدافزارها و برنامه‌های کلون‌شده، یکی از افشاگرانه‌ترین تکنیک‌هایی که جاسوسی پنهان را به تصاحب سکو پیوند می‌دهد، رپایش نشست (Session Hijacking) است. برخلاف جاسوس‌افزارهای سنتی، رپایش نشست نیازی به دسترسی پایدار به دستگاه کاربر ندارد. در عوض، این روش لایه احراز هویت سکوها را هدف می‌گیرد و با سرقت یا بازپخش توکن‌های نشست، کوکی‌ها یا اطلاعات دسترسی فعال، به مهاجم امکان می‌دهد بدون فعال‌سازی هشدارهای امنیتی، کنترل حساب کاربری را در اختیار بگیرد.



یافته‌های افشا شده از عملیات چارمینگ کیتن نشان می‌دهد که رپایش نشست چگونه می‌تواند جایگزینی برای دسترسی در سطح سکو عمل کند. در چندین کارزار مستند، گردانندگان این عملیات داده‌های نشست را از طریق چارچوب‌های فیشینگ و جریان‌های ورود فریبنده جمع‌آوری کرده‌اند و بدین ترتیب به‌طور مستقیم به حساب‌های ایمیل، خدمات ابری و شبکه‌های اجتماعی دسترسی یافته‌اند. پس از به‌دست آوردن یک نشست معتبر، مهاجمان قادر بوده‌اند پیام‌های خصوصی را بخوانند، آرشیوها را دانلود کنند، تنظیمات حساب را تغییر دهند و فعالیت‌های جاری را پایش

از منظر فنی نیز، استفاده از دستکاری DNS، رهگیری TLS و تزریق گواهی‌های امنیتی، مدل‌های اعتماد و حفاظت پیش‌بینی‌شده در استانداردهای بین‌المللی را تضعیف می‌کند. این رویه‌ها مرز میان شنود هدفمند و نظارت فراگیر را از میان برداشته و با ادغام قابلیت‌های رهگیری در زیرساخت ملی و ارائه خدمات اینترنتی، موانع فنی معنادار برای پایش مستمر را حذف می‌کنند.

در جمهوری اسلامی ایران، شنود مرد میانی نه واکنشی استثنایی به تهدیدهای امنیتی، بلکه مؤلفه‌ای ساختاری از حکمرانی اینترنت است که در اسناد سیاسقی، سازوکارهای فیلترینگ و معماری شبکه ملی اطلاعات نهادینه شده است.

۲.۳. ابزارهای فریب و تبدیل تقاضای دسترسی به زیرساخت نظارت

با تشدید محدودیت‌ها بر دسترسی به اینترنت در جمهوری اسلامی ایران، روش‌های دورزدن فیلترینگ، خود به سازوکاری برای نظارت تبدیل شده است. فیلترینگ گسترده، کاهش پهنای باند و مسدودسازی سکوها، تقاضای بالایی برای ابزارهای دور زدن سانسور، به‌ویژه وی‌پی‌ان‌ها و نرم‌افزارهای دسترسی جایگزین ایجاد کرده است. در چنین فضایی، ابزارهای دسترسی فریبنده به یکی از مؤلفه‌های اصلی راهبرد نظارت پنهان حکومت بدل شده‌اند؛ ابزارهایی که تلاش کاربران برای عبور از سانسور را به فرصتی برای پایش و استخراج داده تبدیل می‌کنند.

شواهد فزاینده نشان می‌دهد که بخشی از خدمات وی‌پی‌ان فعال در ایران یا مستقیماً با نهادهای حکومتی همسو هستند یا تحت نظارت و تساهل نهادهای تنظیم‌گر و امنیتی فعالیت می‌کنند. این خدمات نه صرفاً ابزار دور زدن فیلترینگ، بلکه در عمل دروازه‌های کنترل‌شده‌ای هستند که از طریق آن‌ها ترافیک کاربران قابل مشاهده، ثبت یا هدایت مجدد می‌شود. تمرکز تقاضای کاربران بر تعداد محدودی وی‌پی‌ان «کارا»، امکان پیش‌بینی رفتار کاربران را افزایش داده و نقاط گلوگاهی برای نظارت ایجاد می‌کند؛ به‌گونه‌ای که ابزار دسترسی خود به ابزار شنود بدل می‌شود.

جاسوس‌افزارهایی که در این اکوسیستم توزیع می‌شوند، اغلب فشار سانسور را به‌عنوان بردار اصلی انتشار به‌کار

ربایش نشست همچنین امکان استخراج داده در مقیاس‌پذیر را فراهم می‌کند. یک نشست به‌خطر افتاده می‌تواند فهرست مخاطبان، تاریخچه ارتباطات، فراداده‌ها و پیوندهای احراز هویت به سایر خدمات را در اختیار مهاجم قرار دهد. در سطح تجمیعی، چنین دسترسی‌ای از ساخت گراف‌های هویت به رفتار پشتیبانی می‌کند؛ گراف‌هایی مشابه آنچه در پایگاه‌های داده دولتی مانند «سامانه شکار» (بخش‌های بعدی همین فصل) افشا شد، اما بدون نیاز به همکاری مستقیم پلت‌فرم.

از این منظر، ربایش نشست پلی میان عملیات‌های جاسوسی فردمحور و نظارت ساختاری بر پلت‌فرم‌ها ایجاد می‌کند. این تکنیک نشان می‌دهد چگونه روش‌های توسعه‌یافته توسط بازیگران تهدید همسو با دولت می‌توانند همان اهدافی را محقق کنند که در سیاست‌های رسمی تصاحب سکو دنبال می‌شود: دسترسی خاموش، پایش رفتاری و اعمال کنترل پایدار بر هویت‌های دیجیتال.

۵.۱.۳. انحراف‌های حقوقی و فنی از استانداردهای جهانی

چارچوب‌های بین‌المللی شنود قانونی، از جمله استانداردهای تدوین‌شده در ETSI و ۳GPP، بر اصولی مانند ضرورت، تناسب، هدف‌گیری مشخص و پاسخ‌گویی قضایی استوارند. این چارچوب‌ها رویه‌های روشنی برای صدور مجوز، محدودسازی شنود به اهداف مشخص، و سازوکارهای ثبت، حساب‌رسی و نظارت مستقل تعریف می‌کنند. شنود مرد میانی، در سنجش با این معیارها، خارج از دامنه رویه‌های پذیرفته‌شده شنود قانونی قرار می‌گیرد.

در جمهوری اسلامی ایران، به‌کارگیری شنود مرد میانی هم از منظر حقوقی و هم فنی با این استانداردها انحراف اساسی دارد. به‌جای اتکا به مجوزهای فردمحور یا اهداف محدود، رهگیری در سطح زیرساخت اعمال می‌شود و بخش‌های وسیعی از ترافیک شبکه را در بر می‌گیرد. ضمانت‌های حقوقی شفاف نیستند، سازوکارهای مجوزدهی قضایی قابل راستی‌آزمایی نیستند و نشانه‌ای از حساب‌رسی مستقل یا امکان جبران برای شنود غیرقانونی وجود ندارد. در نتیجه، شنود از یک استثنای قاعده‌مند به وضعیتی عمومی و دائمی برای دسترسی به شبکه تبدیل می‌شود.

ناامن سوق دهد، VPN های آلوده به جاسوس افزار هم به سلاحی فنی و هم به تلهای روانی تبدیل می شوند.

این تاکتیک بر الگوی مستند استوار است: با ایجاد وضعیت اضطرار دیجیتال از طریق سانسور گسترده و مسدودسازی سکوها اصلی، حکومت به طور غیرمستقیم کاربران را به استفاده از VPN های بدون ارزیابی و نظارت سوق می دهد. هنگامی که اعتماد کاربران به خدمات داخلی یا سرویس های ناشناس هدایت می شود، این برنامه ها می توانند به ابزارهایی برای پایش فراگیر دیجیتال تبدیل شوند.

213.232.124.157 static.213-232-124-157.client.no vinhost.org Toesegaran Shabakeh Arseh Novin Ltd Iran, Islamic Republic of, Tehran	9.11.4-P2-RedHat-9.11.4-26.P2.e17_9_5 Resolver name: srv.2ndeys.co
94.130.247.148 static.148.247.130.94.clients.you r-server.de Hetzner Online GmbH Germany, Weinheim	9.11.4-P2-RedHat-9.11.4-26.P2.e17_9_9 Resolver name: srv.2ndeys.co

یکی از شاخص ترین نمونه ها در جریان اعتراضات سراسری سال ۲۰۲۲ آشکار شد؛ زمانی که پژوهشگران امنیت سایبری از کارزاری پرده برداشتند که شامل خانواده ای از جاسوس افزار با نام EyeSpy بود. این بدافزار درون یک برنامه VPN پرکاربرد ایرانی به نام ۲۰Speed جاسازی شده بود که به عنوان راهکاری برای دسترسی به اینترنت آزاد تبلیغ می شد. در عمل، این برنامه دریچه ای پنهان به حساس ترین داده های کاربران بود.^{۴۴} پس از نصب، برنامه امکان ثبت کلیدهای فشرده شده، سرقت فایل ها و اسناد، تصویربرداری از صفحه نمایش و حتی استخراج گذرواژه ها و کیف پول های رمزارزی را فراهم می کرد. اوج این کارزار جاسوسی در سپتامبر ۲۰۲۲ ثبت شد و کاربران ایرانی اهداف اصلی آن بودند؛ هرچند خوشه هایی از آلودگی در آلمان و ایالات متحده نیز شناسایی شد.

کارزار EyeSpy و ۲۰Speed از نظر مازولار بودن فنی و پنهان کاری رفتاری اهمیت ویژه ای دارد. بدافزار در کنار یک رابط VPN به ظاهر مشروع بسته بندی شده بود و اغلب از کدهای مبهم یا چندمنظوره استفاده می کرد. پس از نصب، دسترسی پایدار ایجاد می کرد، اجرای دستورات از راه دور را ممکن می ساخت و داده ها را به سرورهای فرماندهی و کنترل مستقر در داخل ایران منتقل می کرد. تحلیل گران زیرساخت این عملیات را به یک گروه تهدید ایرانی با نام SecondEye

می گیرند. اپلیکیشن هایی که با عنوان وی پی ان امن، ابزار حفظ حریم خصوصی یا راهکار اتصال معرفی می شوند، در بسیاری موارد دسترسی های بیش از حد درخواست می کنند، مؤلفه های پایش را در خود جای داده اند یا کانال های پایدار ارتباطی با سرورهای فرماندهی و کنترل برقرار می کنند. در برخی موارد، این ابزارها از طریق کانال های شبه رسمی تبلیغ می شوند یا از عدم اجرای گزینشی مقررات بهره مندند و مرز میان خدمات «تحميل شده» و عملیات پنهان نظارتی را مبهم می سازند.

در سال های اخیر، کارزارهای دسترسی فریبنده به طعمه های مرتبط با استارلینک و ابزارهای اتصال ماهواره ای نیز گسترش یافته اند. این کارزارها با سوءاستفاده از تمایل عمومی به اینترنت ماهواره ای به عنوان جایگزینی برای زیرساخت داخلی، جاسوس افزارهایی را در قالب ابزار پیکربندی، نصب یا فعال سازی توزیع می کنند. هم زمان، کارزارهای جاسوس افزاری روی تلفن همراه و رایانه های شخصی با تمرکز بر کاربران ایرانی تشدید شده اند و از تروجان های دسترسی از راه دور و ابزارهای استخراج داده برای جمع آوری ارتباطات، شناسه های دستگاه و داده های رفتاری استفاده می کنند.

در مجموع، این ابزارهای دسترسی فریبنده نشان دهنده تغییری راهبردی در منطق نظارت هستند: به جای مسدودسازی صرف، کاربران به مسیرهای آلوده هدایت می شوند. در این چارچوب، تلاش برای دور زدن سانسور به طور نظام مند به فرصتی برای نظارت، نفوذ و پایش رفتاری تبدیل می شود.

۱.۲.۳. کارزارهای فریبنده VPN همان زمان با اختلال و قطع اینترنت در هنگامه اعتراضات مردمی علیه حکومت

یکی از نگران کننده ترین تحولات در زرادخانه نظارتی جمهوری اسلامی ایران، به کارگیری جاسوس افزارهای همسو با حکومت از طریق سرویس های VPN ظاهراً محبوب و فریبنده است؛ به ویژه در دوره های تشدید سرکوب دیجیتال، مانند اعتراضات سال های ۲۰۲۲ تا ۲۰۲۳ (جنبش زن، زندگی، آزادی).^{۴۵} در شرایطی که حکومت عمداً دسترسی به اینترنت را محدود می کند تا شهروندان را به سمت ابزارهای دور زدن



گونه‌هایی از DCHpy و ابزارهای دسترسی از راه دور که قادر به دستکاری سامانه فایل، شنود تماس‌ها و پیامک‌ها و برداشت فهرست مخاطبان بودند. در دست‌کم یک مورد، APKهای آلوده‌ای که با عنوان «ابزار فعال‌سازی استارلینک» تبلیغ می‌شدند، در فروشگاه‌های برنامه ایرانی که خارج از نظارت بین‌المللی فعالیت می‌کنند بارگذاری شده بودند.

این عملیات نمونه‌ای از استفاده پیچیده از مهندسی اجتماعی است که هم ناآگاهی فنی و هم استیصال دیجیتال کاربران ایرانی را هدف می‌گیرد. با قاب‌بندی این جاسوس‌افزارها به عنوان ابزار توانمندسازی، مهاجمان خود را همسو با آرزوهای کاربران برای دسترسی بدون سانسور نشان می‌دهند، اما در نهایت همان اهداف را از طریق نظارت و تجسس تضعیف می‌کنند.

۳.۲.۳ جاسوس‌افزاری فریبنده در پوشش یک ابزار بی‌خطر

«عکس یادگاری» یک برنامه نظارتی فریبنده است که در تحقیقات پروژه PRISM به عنوان بخشی از اکوسیستم گسترده‌تری از جاسوس‌افزارهای همسو با حکومت، که کاربران ایرانی را هدف قرار می‌دهند، مستند شده است.^{۵۵} برخلاف تروجان‌های دسترسی از راه دور تمام‌عیار، این ابزار به جای کنترل پایدار در سطح سیستم، بر مهندسی اجتماعی و فریب بصری متکی است. این برنامه به عنوان یک ابزار به ظاهر بی‌ضرر مرتبط با عکس به کاربران عرضه می‌شود، در حالی که به صورت پنهانی داده‌های حساس دستگاه نصب‌شده را جمع‌آوری می‌کند.

تحلیل فنی نشان می‌دهد که این برنامه مجموعه‌ای از دسترسی‌ها را درخواست می‌کند که با کارکرد ادعایی آن تناسبی

نسبت دادند که سابقه‌ای از عملیات‌های نظارتی همسو با اهداف حکومتی دارد.

اگرچه ساختار این کارزار شبیه به توزیع جاسوس‌افزارهای مجرمانه بود، الگوهای هدف‌گیری، زمان‌بندی آن در اوج اعتراضات و زمینه اجتماعی به‌روشنی نشان می‌دهد که این فعالیت‌ها با هماهنگی یا دست‌کم با تحمل نهادهای امنیتی مانند وزارت اطلاعات و سازمان اطلاعات سپاه پاسداران انقلاب اسلامی انجام شده است.

۳.۲.۳ طعمه‌های استارلینک و توزیع جاسوس‌افزار از مسیر ابزارهای اتصال جعلی

آنچه از این روند برمی‌آید، راهبردی مبتنی بر به‌دام‌اندازی دیجیتال است: جمهوری اسلامی کمبود مصنوعی اینترنت آزاد را ایجاد می‌کند و سپس از گرایش کاربران به کانال‌های ناامن برای تحقق اهداف نظارتی بهره می‌برد. تحول تازه‌تر این روش، به سلاح‌سازی از علاقه عمومی به استارلینک مربوط می‌شود. در پی افزایش توجه عمومی به اتصال استارلینک در جریان قطع‌های سراسری اینترنت، کاربران ایرانی به دنبال راه‌هایی برای دسترسی به این شبکه ماهواره‌ای بودند. حکومت و بازیگران وابسته به آن به سرعت از این روند سوءاستفاده کردند و VPN‌ها و برنامه‌های موبایلی جعلی با عنوان استارلینک منتشر کردند که مدعی فراهم کردن دسترسی به این سرویس بودند.

پژوهشگران فایل‌های APK توزیع‌شده‌ای را مستند کردند که به محموله‌های جاسوس‌افزاری آلوده بودند، از جمله

			
Title	Package Name	SHA1	Acquired Date
Earth VPN	com.earth.earth_vpn	556d7ac665fa3cc6e56070641d4f0f5c36670d38	02.07.2025
Comodo VPN	com.comodoapp.comodovpn	7010e2b424eadfa261483ebb8d2cca4aac34670c	25.06.2025
Earth VPN	com.earth.earth_vpn	8f37a3e2017d543f4a788de3b05889e5e0bc4b06	23.06.2025
Earth VPN	com.earth.earth_vpn	9dec46d71289710cd09582d84017718e0547f438	20.06.2025
حضرت عشق (Hazrat Eshq)	hazrateeshgh.apk	6c291b3e90325bea8e64a82742747d6cdce22e5b	2024-04-12
Hide VPN	com.hv.hide_vpn	7267f796581e4786dbc715c6d62747d27d09c61	2023-07-16

```

public String _vvvvvvv0(String str) throws Exception {
    String str2 = "";
    try {
        Regex regex = Common.Regex;
        String[] Split = Regex.Split("\n", str);
        if (Split.length > 0) {
            String trim = Split[0].trim();
            if (trim.startsWith("مشتری گرامی") && trim.endsWith(".")) {
                str2 = trim.replace("مشتری گرامی", "").replace(".", "");
            } else if (trim.startsWith("ایرانسل عزیز به شماره")) {
                str2 = trim.replace("ایرانسل عزیز به شماره", "").trim();
            } else if (trim.startsWith("مشتری گرامی") && trim.contains("در .")) {
                str2 = trim.substring(trim.trim().indexOf("مشتری گرامی"), trim.indexOf("در .")).replace("مشتری گرامی", "").trim();
            } else if (trim.startsWith("همراه گرامی، شماره") && trim.contains("در تاریخ")) {
                String replace = trim.replace("همراه گرامی، شماره", "");
                str2 = replace.substring(0, replace.indexOf("در تاریخ")).trim();
            }
        }
    } catch (Exception e) {
        this.ba.setLastException(e);
        Common.LogImpl("713172754", BA.ObjectToString(Common.LastException(getActivityBA())), 0);
    }
}

```

برای نخستین بار تصویری نظام‌مند از زیرساخت عملیاتی مرتبط با تهدید پیشرفته پایدار بجه گربه ملوس (چارمینگ کیتن یا APT۳۵) ارائه داد.^{۵۷} برخلاف گزارش‌هایی که صرفاً بر رخداد‌های منفرد یا نسبت‌دهی تمرکز داشتند، این افشاگری‌ها دامنه‌های فعال فیشینگ، زنجیره‌های توزیع بدافزار، زیرساخت فرماندهی و کنترل، و مجموعه‌ای از ابزارهای اختصاصی جاسوس‌افزاری مورد استفاده در چندین کارزار را ترسیم کردند. این گذار به مستندسازی در سطح زیرساخت، نقطه عطفی در فهم، تحلیل و زمینه‌مند کردن عملیات‌های چارمینگ کیتن به شمار می‌رود.^{۵۸}

چارمینگ کیتن مدت‌هاست که از سوی پژوهشگران مستقل به‌عنوان یک بازیگر تهدید همسو با حکومت جمهوری اسلامی ایران شناسایی شده که در هماهنگی نزدیک با نهادهای امنیتی ایران فعالیت می‌کند. تحقیقات متعدد، کارزارها، اولویت‌های هدف‌گیری و زمان‌بندی عملیاتی این گروه را با اهداف اطلاعاتی سازمان اطلاعات سپاه پاسداران انقلاب اسلامی، که در ادبیات داخلی از آن با عنوان اداره ۴۰ یاد می‌شود، مرتبط دانسته‌اند.^{۵۹} برخلاف گروه‌های سایبری با انگیزه مالی، عملیات‌های چارمینگ کیتن به‌طور مستمر اهداف راهبردی جمع‌آوری اطلاعات را دنبال می‌کنند؛ از جمله پایش روزنامه‌نگاران، فعالان، پژوهشگران، مخالفان سیاسی و اهداف مرتبط با سیاست خارجی. الگوهای فعالیت این گروه نشان‌دهنده درگیری‌های پایدار و بلندمدت است که بر حفظ دسترسی، تداوم نفوذ و پایش رفتاری تمرکز دارد، نه بهره‌برداری سریع و مقطعی.

اهمیت این نشت اطلاعاتی صرفاً به روابط و ساختار این گروه محدود نمی‌شود، بلکه جزییات بی‌نظیری از تاکتیک‌ها،

```

public Object callSub(String str, Object obj, Object[] objArr) throws Exception {
    BA.senderHolder.set(obj);
    if (BA.fastSubCompare(str, "CHANGEICON")) {
        return _changeicon();
    }
    if (BA.fastSubCompare(str, "HIDEICON")) {
        return _hideicon(((Boolean) objArr[0]).booleanValue());
    }
    return BA.SubDelegator.SubNotFound;
}

```

ندارد. پس از نصب، برنامه می‌تواند به تصاویر ذخیره‌شده، شناسه‌های دستگاه و داده‌های زمینه‌ای دسترسی پیدا کند و هم‌زمان ارتباط‌هایی خروجی با سرورهای تحت کنترل اپراتورها برقرار سازد. فرآیند جمع‌آوری اطلاعات عمدتاً به‌صورت خاموش انجام می‌شود و نیازمند تعامل مستمر کاربر نیست، امری که امکان نظارت بدون جلب توجه فوری را فراهم می‌کند.

آنچه «عکس یادگاری» را از بدافزارهای متعارف متمایز می‌کند، اتکای آن به اعتماد کاربران به‌جای بهره‌برداری از آسیب‌پذیری‌های فنی است. این برنامه به اکسپلویت‌های پیچیده یا نقص‌های نرم‌افزاری وابسته نیست، بلکه از شرایط اجتماعی و سیاسی شکل‌گرفته در نتیجه سانسور، کمبود دسترسی و فضای ترس استفاده می‌کند. کاربران معمولاً از طریق پیام‌های مستقیم یا بهانه‌های موضوعی به نصب برنامه ترغیب می‌شوند و همین تعاملات روزمره دیجیتال به مسیرهای نظارت تبدیل می‌گردد.

۳.۳. چارمینگ کیتن (APT۳۵)؛ دسترسی فریبنده، زنجیره ابزارهای جاسوسی و کنترل دولتی

در پاییز ۲۰۲۵، مجموعه‌ای از افشاگری‌های هماهنگ که توسط پروژه KittenBusters در گیت‌هاب منتشر شد،^{۶۰}

Associated Group Descriptions

Name	Description
TA453	[6][5][7]
COBALT ILLUSION	[4]
Charming Kitten	[8][9][10][2][6][7]
ITG18	[11]
Phosphorus	[12][13][14][3][6][7]
Newscaster	Link analysis of infrastructure and tools revealed a potential relationship between Magic Hound and the older attack campaign called Newscaster (aka Newscasters). ^{[15][1]}
APT35	[1][3][7]
Mint Sandstorm	[16]

در مجموع، این نشت‌ها چارمینگ کیتن را نه صرفاً به‌عنوان یک بازیگر تهدید مستقل، بلکه به‌مثابه یکی از بازوهای عملیاتی کلیدی در معماری گسترده‌تر نظارت دیجیتال آشکار می‌سازند. زنجیره ابزارها، زیرساخت و منطق عملیاتی این گروه، نمونه‌ای عینی از همگرایی دسترسی فریبده، نفوذ از راه دور و پایش رفتاری در قالب یک سیستم پایدار کنترل دیجیتال است. در بخش‌های بعدی، این ابزارها به‌طور تفصیلی بررسی می‌شوند تا نشان داده شود چگونه هر مؤلفه فنی در خدمت اهداف اطلاعاتی و حکمرانی قرار می‌گیرد.

۱.۳.۳. تروجان دسترسی از راه دور ویندوزی ماژولار با سامانه فرماندهی و کنترل مبتنی بر رله

یکی از ابزارهای محوری که در افشاگری‌های داخلی چارمینگ کیتن شناسایی شده، یک تروجان دسترسی از راه دور (RAT) مبتنی بر ویندوز است که بر اساس یک معماری ماژولار طراحی شده است. این بدافزار از چندین مولفه هم‌کنش‌پذیر تشکیل شده که توسط یک ماژول کنترل‌کننده مرکزی، که معمولاً با نام main شناخته می‌شود، هماهنگ می‌شوند. این ماژول اصلی مسئول مدیریت جریان اجرا، برقراری ارتباط با زیرساخت فرماندهی و کنترل (C2) و فعال‌سازی ماژول‌های جانبی است که وظیفه جمع‌آوری داده و تعامل با سیستم را بر عهده دارند.

تکنیک‌ها و رویه‌های عملیاتی (TTPs) چارمینگ کیتن فراهم می‌کند. اسناد افشا شده نشان دادند که این گروه ترجیح عملیاتی مشخصی برای بردارهای دسترسی فریبده دارد: چارچوب‌های فیشینگ برای سرقت اعتبارنامه‌ها و نشست‌ها، بارگذارهای بدافزاری ماژولار، تروجان‌های دسترسی از راه دور، و ابزارهای سمت سرور که امکان تصاحب حساب‌ها و استخراج داده در مقیاس وسیع را فراهم می‌کردند. این ابزارها نه به‌صورت منفرد، بلکه در قالب یک اکوسیستم نظارتی یکپارچه به‌کار گرفته می‌شدند؛ اکوسیستمی که در آن دسترسی، ماندگاری و استخراج داده به‌طور تنگاتنگ به هم پیوند خورده بودند.

نشت‌ها و تحلیل‌های بعدی نیز نشان داده‌اند که ابزارهای چارمینگ کیتن چگونه با راهبردهای کلان نظارت و شنود حکومت جمهوری اسلامی ایران هم‌پوشانی پیدا می‌کنند.^۴ این گروه به‌جای اتکای صرف به بهره‌برداری از آسیب‌پذیری‌های روز صفر، بارها از رفتار کاربران در شرایط فشار سانسور به‌عنوان بردار اصلی سوءاستفاده کرده است؛ از جمله تقاضا برای VPN‌ها، دسترسی ابری و ابزارهای اتصال جایگزین. این رویکرد با سیاست‌های رهگیری داخلی و تلاش‌های تصاحب سکو هم‌راستاست و مرز میان جاسوسی سایبری پنهان و نظارت نهادینه‌شده را کمرنگ می‌کند. موج کنونی افشاگری‌ها، شامل مستندات داخلی و مخازن ابزارها، دیدی کم‌سابقه از نحوه به‌کارگیری قابلیت‌های تهاجمی سایبری در کنار سازوکارهای کنترل اینترنت ملی ارائه می‌دهد.

فایل، و واگذاری وظایف پویا. طراحی ماژولار آن به گردانندگان اجازه می‌دهد بسته به پروفایل هدف، قابلیت‌های خاصی را به صورت گزینشی فعال کنند. ماژول‌های شناسایی شده شامل مؤلفه‌هایی برای استخراج اطلاعات احراز هویت، ثبت کلیدهای فشرده شده، استخراج داده‌های مرورگر و جمع‌آوری هدفمند داده از برنامه‌های مشخص مانند پیام‌رسان‌ها است. شواهد مربوط به سازوکارهای ماندگاری نشان می‌دهد که این بدافزار برای بقا پس از راه‌اندازی مجدد سیستم و حفظ دسترسی بلندمدت به دستگاه‌های آلوده طراحی شده است.

تحلیل فنی نشان می‌دهد که اجرای بدافزار اغلب از طریق ابزارهای مشروع سیستم‌عامل مانند exe.rundll۳۲ انجام می‌شود؛ روشی که معمولاً برای دور زدن کنترل‌های امنیتی پایه به کار می‌رود، زیرا فعالیت مخرب را در قالب رفتار عادی سیستم‌عامل پنهان می‌کند. داده‌های جمع‌آوری شده از قربانیان به صورت محلی در فایل‌های ساختاریافته ذخیره شده و از طریق کانال‌های CP برقرار شده استخراج می‌شوند.

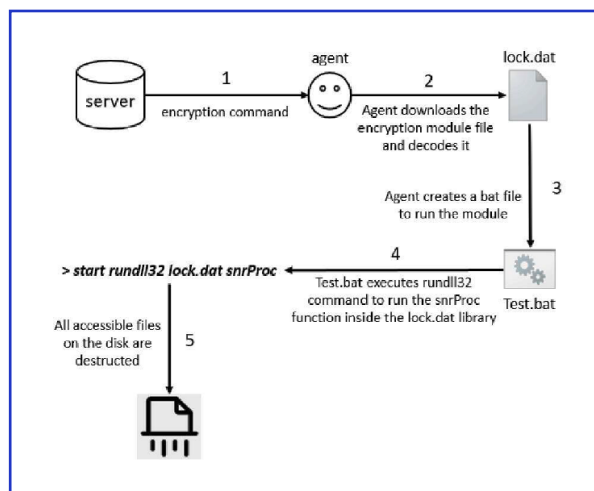
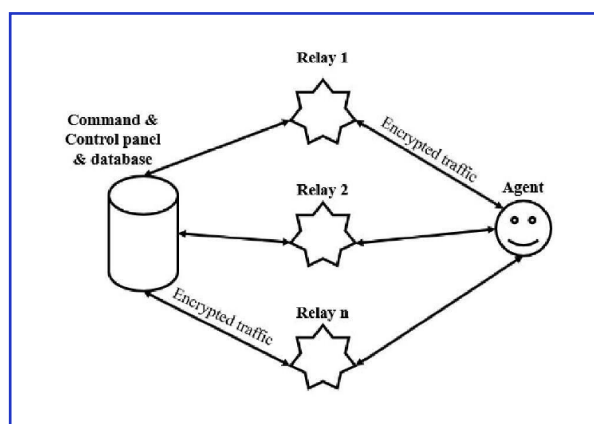
در مجموع، این ابزار نمایانگر یک ایمپلنت نظارتی بالغ و همسو با حکومت است، نه یک ابزار فرصت‌طلبانه مجرمانه. معماری، مجموعه قابلیت‌ها و نظم عملیاتی آن با اهداف جاسوسی بلندمدت هم‌خوانی دارد و ارزیابی‌هایی را تقویت می‌کند که چارمینگ کیتن را به عنوان یک تهدید پیشرفته پایدار درگیر در پایش مستمر کاربران هدف معرفی می‌کنند.

۲.۳.۳. بلا چاو (BellaCiao)؛ بارگذار ماژولار ویندوزی مرکزی در زنجیره عملیات‌های چارمینگ کیتن

بلا چاو یک چارچوب بدافزاری ماژولار مبتنی بر ویندوز است که از طریق پژوهش‌های مستقل امنیت سایبری به تهدید پیشرفته پایدار چارمینگ کیتن (APT۳۵) نسبت داده می‌شد و حالا از طریق نشت پروژه KittenBusters این انتساب تایید شده است.^{۴۱} برخلاف تروجان‌های دسترسی از راه دور با قابلیت‌های کامل، بلا چاو عمدتاً به عنوان یک سکوی بارگذاری و هماهنگ‌سازی عمل می‌کند که برای ایجاد ماندگاری، حفظ دسترسی پنهان و استقرار محموله‌های نظارتی اضافی در صورت نیاز طراحی شده است.

این RAT از هر دو شیوه ارتباط مستقیم و غیرمستقیم با گردانندگان خود پشتیبانی می‌کند. در حالت غیرمستقیم، ترافیک از طریق سرورهای واسط یا رله هدایت می‌شود؛ انتخابی طراحی شده که منشا دستورات را پنهان کرده و تاب‌آوری عملیاتی ابزار را در برابر اختلال یا برچیدن زیرساخت افزایش می‌دهد. این معماری CP مبتنی بر رله، امکان حفظ دسترسی پایدار را حتی در صورت از کار افتادن برخی گره‌ها فراهم می‌کند.

از نظر کارکردی، این بدافزار قابلیت‌های کامل کنترل از راه دور را ارائه می‌دهد، از جمله اجرای دستورات، بارگذاری و دریافت



نام ماژول	عملکرد
central.dat	آخرین نسخه برنامه اصلی است که در صورت به روزرسانی بدافزار دانلود خواهد شد.
creds.dat	ماژول استیلر فایرفاکس
lock.dat	ماژول رمزنگاری فایلها
logging.dat	ماژول کیلاگر
msg.dat	ماژول تلگرام

تفکیک میان ایمپلنت اولیه و محموله‌های بعدی، بازتاب یک راهبرد عملیاتی آگاهانه است: به حداقل رساندن میزان افشا در مرحله نفوذ اولیه، در عین حفظ امکان ارتقای قابلیت‌های نظارتی در صورت لزوم.

به‌کارگیری بلا چاو نشان‌دهنده تحول چارمینگ کیتن از عملیات‌های پراکنده فیشینگ به‌سوی یک چارچوب جاسوسی ساختاریافته و چندلایه است. به‌جای استقرار جاسوس‌افزارهای یکپارچه و حجیم، این گروه بر بارگذاری انعطاف‌پذیری تکیه می‌کند که به‌طور پی‌درپی در سیستم قربانیان ادغام شده و امکان پایش بلندمدت هم‌راستا با اهداف جمع‌آوری اطلاعات را فراهم می‌سازند.

۳.۳.۳. ابزار دسترسی از راه دور مازولار PAC2-RAT

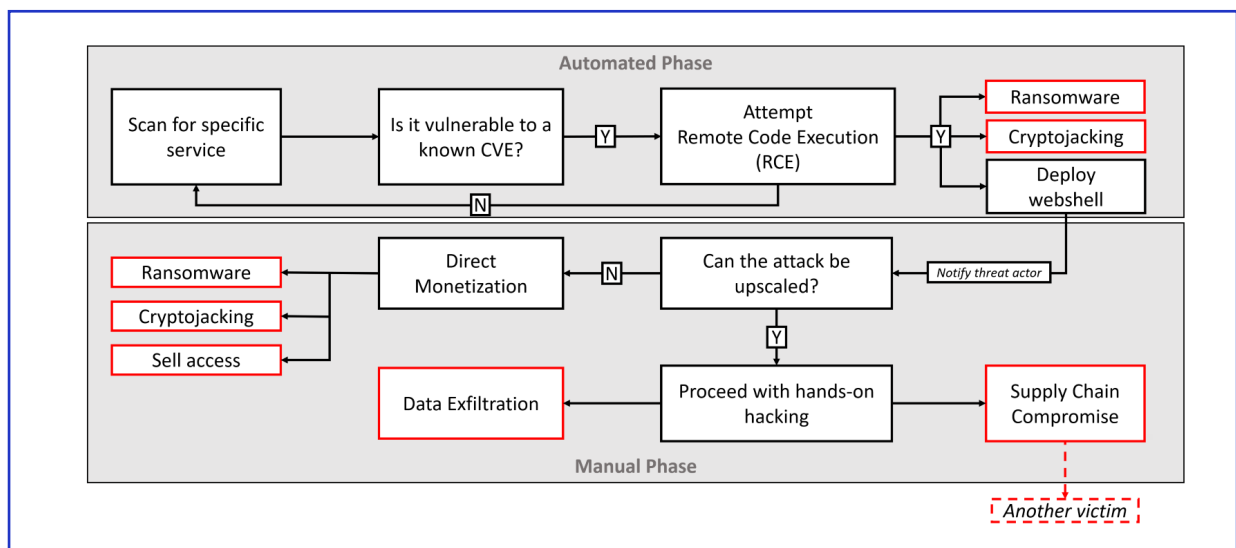
PAC2-RAT در یک «گزارش اولیه» داخلی با تاریخ مارس ۲۰۲۳ مستند شده است؛ گزارشی که یک ابزار دسترسی از راه دور کاملاً عملیاتی را توصیف می‌کند که برای کنترل دستگاه قربانی و جمع‌آوری داده طراحی شده است. این گزارش به‌جای ارائه یک مرور کلی عمومی، جزئیات اجرایی مشخصی را مطرح می‌کند، از جمله معماری سامانه، الزامات استقرار، پنل‌های مخصوص اپراتور، و فهرستی از دستورات و ماژول‌های پشتیبانی‌شده.

در گزارش، یک طراحی کلاینت سرور توصیف شده است که در آن مؤلفه کلاینت با NET و #C پیاده‌سازی شده و یک

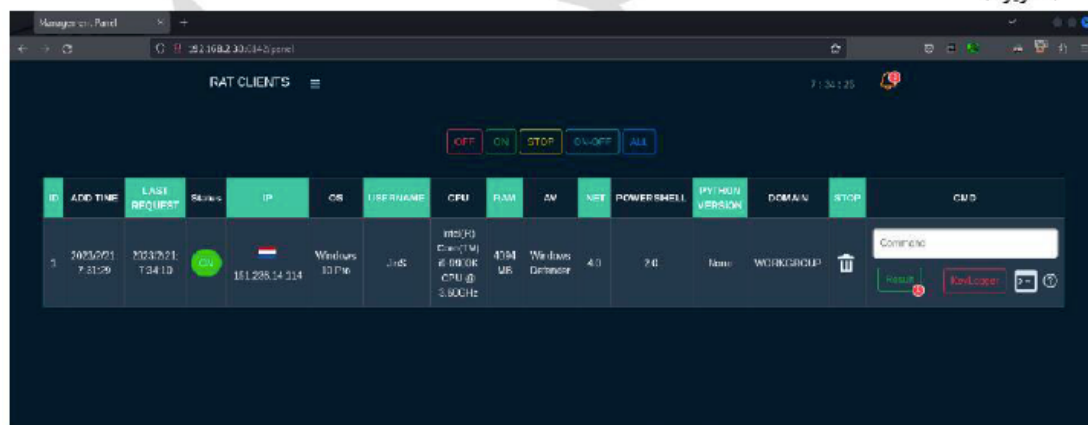
تحلیل فنی نشان می‌دهد که بلا چاو بر پایه یک طراحی به‌شدت مازولار عمل می‌کند و به گردانندگان اجازه می‌دهد مؤلفه‌های ثانویه را به‌صورت پویا و بدون تغییر در ایمپلنت اصلی بارگذاری و اجرا کنند. این رویکرد ریسک شناسایی را کاهش داده و به بدافزار امکان می‌دهد خود را با نیازهای عملیاتی متفاوت تطبیق دهد. این چارچوب از چندین ماژول اجرایی پشتیبانی می‌کند، از جمله مؤلفه‌هایی برای اجرای دستورات، دریافت فایل، شناسایی وضعیت سیستم و تحویل محموله‌های بدافزاری. ارتباط با زیرساخت فرماندهی و کنترل معمولاً رمزگذاری شده است و به‌گونه‌ای طراحی می‌شود که در ترافیک عادی شبکه ادغام شود.

بلا چاو معمولاً از طریق کارزارهای فیشینگ هدفمند توزیع می‌شود و اغلب از اسناد آلوده یا دراپرهایی با ظاهر نصب‌کننده استفاده می‌کند که به‌جای سواستفاده از آسیب‌پذیری‌های نرم‌افزاری، بر اعتماد کاربر تکیه دارند. پس از استقرار، بدافزار با استفاده از تغییرات در رجیستری و سازوکارهای اجرای زمان‌بندی‌شده، ماندگاری خود را برقرار می‌کند و دسترسی مداوم حتی پس از راه‌اندازی مجدد سیستم را تضمین می‌سازد. رفتار کم‌جلب‌توجه آن و اتکا به فرآیندهای مشروع سیستم عامل، به بلا چاو امکان می‌دهد بسیاری از سامانه‌های شناسایی مبتنی بر امضا را دور بزند.

پژوهشگران امنیتی، بلا چاو را به‌عنوان یکی از مؤلفه‌های بنیادین در چندین کارزار چارمینگ کیتن شناسایی کرده‌اند که نقش یک سکوی مرحله‌بندی برای جاسوس‌افزارهای تهاجمی‌تر و ابزارهای استخراج داده را ایفا می‌کند. این

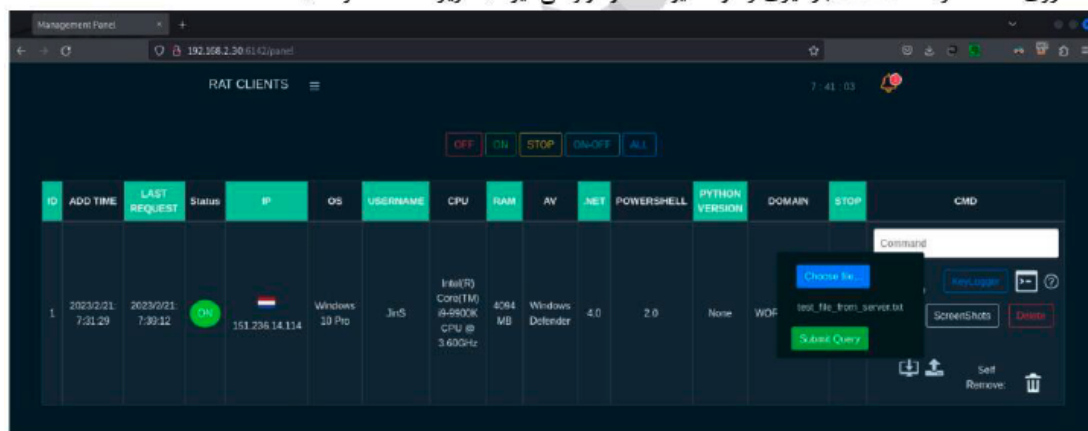


برای اجرا و راه اندازی امکان keylogger می بایست در سامانه دستور keylogger ثبت شود. سپس دکمه keylogger در صفحه به رنگ قرمز در آمده و منتظر دریافت نتایج می شود. کاربر (Client) پس از دریافت این دستور اقدام به ثبت اطلاعات صفحه کلید در یک فایل به صورت مخفی کرده و نتایج را در پاسخ برای سامانه ارسال می کند. پس از دریافت این اطلاعات دکمه keylogger در سامانه به رنگ آبی در می آید و در صورت کلیک بر روی دکمه نتایج دریافتی نمایش داده می شود. (تصویر ۸)



تصویر ۸ - دستور KEYLOGGER پس از ثبت در سامانه و در حالت انتظار برای دریافت نتایج

برای استفاده از قابلیت بارگذاری file بر روی سیستم هدف، ابتدا می بایست در سامانه اقدام به باگذاری file مدنظر و در قسمت ثبت دستورات در panel اقدام به وارد کردن عبارت `UPLOAD=/path/to/file/yourfile.format`، و به جای عبارت `path to file` آدرس و مسیر قرار گیری فایل مدنظر و نام فایل مدنظر قرار می گیرد. پس از ثبت این دستور فایل از روی سامانه توسط client بارگیری و در مسیر مدنظر قرار می گیرد. (تصویر ۱۳، ۱۴ و ۱۵)

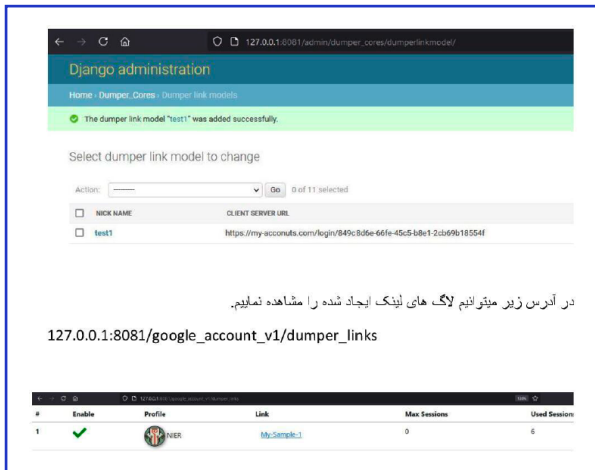


تصویر ۱۳ - بارگذاری file مدنظر بر روی سامانه به منظور بارگیری آن توسط CLIENT

طریق یک رابط پنل متمرکز مدیریت کند.

از نظر کارکردی، PACP-RAT قابلیت های اصلی نظارت و کنترل را که معمولاً با تروجان های دسترسی از راه دور مرتبط است ارائه می دهد. این قابلیت ها شامل اجرای دستورات

اند سرور با Python و با استفاده از چارچوب Flask توسعه یافته است. همچنین گفته می شود ارتباط از طریق HTTPS برقرار می شود و با یک زیرساخت مبتنی بر رله پشتیبانی می گردد، به گونه ای که اپراتور بتواند چندین کلاینت آلوده را از

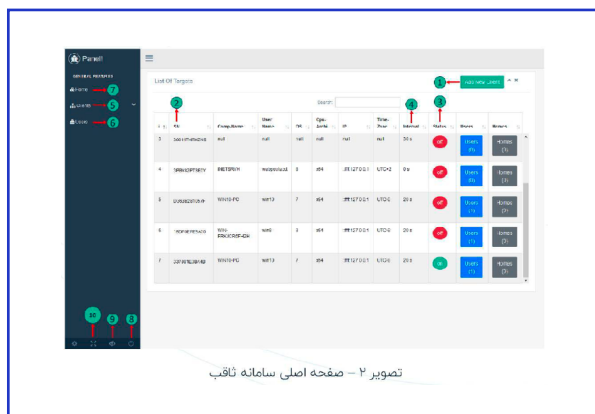


بعدی جاسوس افزارها و ابزارهای دسترسی متصل می‌کنند.

۵.۳.۳. ثاقب؛ تروجان دسترسی از راه دور در معماری نظارت نهادی

«ثاقب» یکی دیگر از تروجان‌های دسترسی از راه دور (RAT) با قابلیت‌های کامل است که در یک گزارش فنی داخلی افشاشده از زیرساخت چارمینگ کیتن مستند شده است. برخلاف بدافزارهای ابتدایی یا جاسوس افزارهای موردی، ثاقب به عنوان یک سکوی نظارتی ساختاریافته معرفی می‌شود که شامل پنل مدیریت متمرکز، معماری کلاینت مازولار و مجموعه‌ای گسترده از قابلیت‌های جاسوسی و کنترلی است. محتوای این مستندات نشان می‌دهد که ثاقب نه صرفاً برای نفوذ اولیه، بلکه برای پایش مداوم، ردیابی رفتاری و کنترل بلندمدت سیستم‌های آلوده طراحی شده است.

در سطح فنی، ثاقب بر پایه یک مدل کلاسیک فرماندهی و کنترل (C2) عمل می‌کند و به اپراتورها اجازه می‌دهد چندین



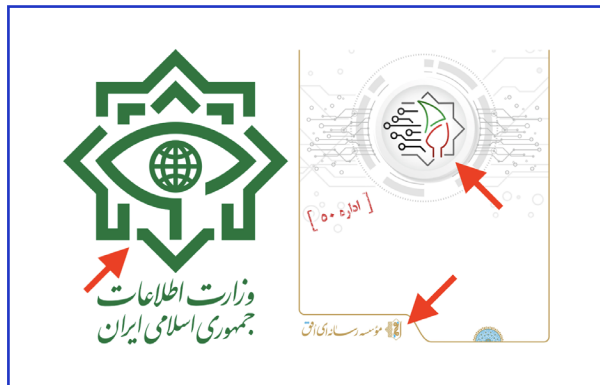
از راه دور از طریق یک رابط شل، بارگذاری و دریافت فایل، کنترل دسکتاپ از راه دور از طریق VNC، و ثبت کلیدهای فشرده شده است. گزارش همچنین ویژگی‌های پروفایل‌سازی سیستم را مستند می‌کند، از جمله جمع‌آوری ویژگی‌های دستگاه و محیط مانند جزئیات سیستم عامل، مشخصات سخت‌افزاری، شناسه‌های شبکه، و محصولات امنیتی نصب شده.

علاوه بر قابلیت‌های اصلی، گزارش به سازوکارهای عملیاتی اشاره می‌کند که برای پشتیبانی از پنهان‌کاری و مدیریت ترافیک در نظر گرفته شده‌اند، از جمله امکان پیکربندی و دستکاری هدرها در درخواست‌های شبکه. درج دستورالعمل‌های راه‌اندازی و مراحل استقرار سرور نشان می‌دهد که RAT-۲AC۲ یک طراحی نظری نیست، بلکه ابزاری است که برای استفاده عملیاتی در دنیای واقعی در نظر گرفته شده است و یک رابط ساختاریافته برای دسترسی پایدار، پایش مداوم، و واگذاری مرحله‌ای وظایف علیه اهداف فراهم می‌کند.

۴.۳.۳. زیرساخت فریب و تحویل مبتنی بر طعمه‌های تصویری

در سندی دیگر از این نشت، زیرساختی فریبنده برای تحویل محتوا را توصیف می‌شود که چارمینگ کیتن برای جذب اهداف و کنترل دسترسی به محتوای مرحله‌بندی شده، پیش از استقرار بدافزار، استفاده می‌کند. این سامانه نه به عنوان یک ایمپلنت نظارتی یا ابزار بهره‌برداری، بلکه به مثابه یک سکوی هدایت و تحویل کنترل شده عمل می‌کند که به اپراتورها امکان می‌دهد لینک‌های معتبرنما تولید کنند، نشست‌های کاربری را مدیریت کنند و فایل‌ها یا محموله‌ها را به صورت گزینشی در اختیار کاربران هدف قرار دهند.

این زیرساخت بر پنل‌های مبتنی بر وب، سرورهای مدیریت شده از طریق SSH، و زنجیره‌های هدایت قابل پیکربندی متکی است؛ سازوکاری که امکان رصد تلاش‌های دسترسی، اعمال محدودیت‌های شرطی، و هدایت کاربر از میان چند مرحله تعامل را فراهم می‌کند. با جاسازی فرآیند تحویل مخرب در قالب لینک‌ها یا اسناد به ظاهر مشروع، این روش سطح سوءظن را کاهش داده و احتمال نفوذ موفق را افزایش می‌دهد. چنین سازوکارهایی نقشی کلیدی در عملیات چارمینگ کیتن دارند، زیرا مهندسی اجتماعی را به استقرار



فراتر از ویژگی‌های فنی، اسناد افشاشده نشان می‌دهد که ثاقب یک ابزار مجرمانه عمومی نیست، بلکه بخشی از یک گردش کار نظارتی سازمان‌یافته است. وجود قابلیت‌های مدیریت کاربر، سامانه ثبت وقایع و رابط‌های تولید کلاینت بیانگر استفاده توسط اپراتورهای آموزش‌دیده است، نه مهاجمان فرصت‌طلب.

از منظر منافع عمومی، ثاقب نشان می‌دهد که نظارت در جمهوری اسلامی ایران بسیار فراتر از فیلترینگ و کنترل سکوها است. ابزارهایی مانند ثاقب امکان نفوذ مستقیم به دستگاه‌های شخصی را فراهم می‌کنند، بدون آنکه به تضمین‌های قانونی پایبند باشند یا تحت نظارت قضایی شفاف عمل کنند. استفاده از چنین جاسوس‌افزارهایی رایانه‌های شخصی را به حسگرهای جمع‌آوری اطلاعات تبدیل می‌کند و حریم خصوصی را نه از طریق سانسور آشکار، بلکه با پایش پنهان و مستمر از میان می‌برد.

در پایان، ذکر یک نشانه بصری معنادار ضروری است: هویت گرافیکی مرتبط با «ثاقب» به‌طور آشکار از لوگوی وزارت اطلاعات الهام گرفته شده است، در حالی که شواهد فنی و زمینه‌ای، مصرف عملیاتی این ابزار را به شبکه‌های همسو با سازمان اطلاعات سپاه پاسداران انقلاب اسلامی نسبت می‌دهند. این ناهمخوانی ظاهری، نه یک خطای طراحی، بلکه بخشی از منطق پوشش و انکارپذیری در اکوسیستم امنیتی جمهوری اسلامی است؛ جایی که مرزهای نهادی عمداً مبهم نگه داشته می‌شوند و نمادها می‌توانند نقش پوششی ایفا کنند.

این الگو با یافته‌های پژوهش‌های مستقل نیز هم‌خوانی دارد. تحقیقات منتشرشده و مطالعات تکمیلی درباره واحدهای

سیستم آلوده را به‌طور هم‌زمان مدیریت کنند. این بدافزار از اجرای دستورات از راه دور، دسترسی به فایل‌های سیستم، ثبت کلیدهای فشرده‌شده، تصویربرداری از صفحه نمایش و استخراج داده پشتیبانی می‌کند. همچنین مازول‌های تخصصی برای برداشت اعتبارنامه‌ها و استخراج اطلاعات از برنامه‌های پرکاربرد، از جمله مرورگرهای وب و پیام‌رسان‌ها، در آن تعبیه شده‌است. این قابلیت‌ها امکان بازسازی تصویری دقیق از زندگی دیجیتال، ارتباطات و الگوهای روزمره هدف را فراهم می‌کند.

یکی از ویژگی‌های برجسته ثاقب تمرکز آن بر ماندگاری و پنهان‌کاری است. این سامانه به‌طور مشخص برای باقی‌ماندن در وضعیت شناسایی‌نشده توسط نرم‌افزارهای امنیتی طراحی شده و از تکنیک‌های ضد دیباگ، منطق اجرای تاخیردار و روش‌های مبهم‌سازی برای دور زدن آنتی‌ویروس‌ها استفاده



تصویر ۳ - پنل راهبری بدافزار ثاقب

می‌کند. ارتباط با زیرساخت فرماندهی و کنترل به‌گونه‌ای سازمان‌دهی شده که کمترین جلب توجه را داشته باشد و در مستندات به استفاده از مسیرهای غیرمستقیم، از جمله لایه‌های ناشناس‌سازی، برای پنهان‌کردن فعالیت اپراتورها اشاره شده است.



تصویر ۴ - صفحه Screen Shot در پنل راهبری بدافزار ثاقب

دیجیتالی روزمره آنان جاسازی می‌کند.

۱.۴.۳. پوسته‌های حاکمیت‌پذیر و برنامه‌های نظارتی ثالث

در راهبرد کنترل دیجیتال جمهوری اسلامی، «پوسته‌های حاکمیت‌پذیر» که نسخه‌های تاییدشده حکومتی از پیام‌رسان‌ها یا برنامه‌های شبکه‌های اجتماعی هستند، به‌عنوان ابزارهای ساختاری برای پایش فعالیت کاربران، شنود ارتباطات خصوصی و اعمال سانسور عمل می‌کنند. این «پوسته‌ها» به‌جای مسدودسازی کامل دسترسی، یک رابط کاربری آشنا مبتنی بر خدمات خارجی ارائه می‌دهند، اما ترافیک را از زیرساخت‌های داخلی عبور می‌دهند؛ مسیری که امکان پالایش محتوا، برداشت فراداده و پروفایل‌سازی رفتاری را فراهم می‌کند.

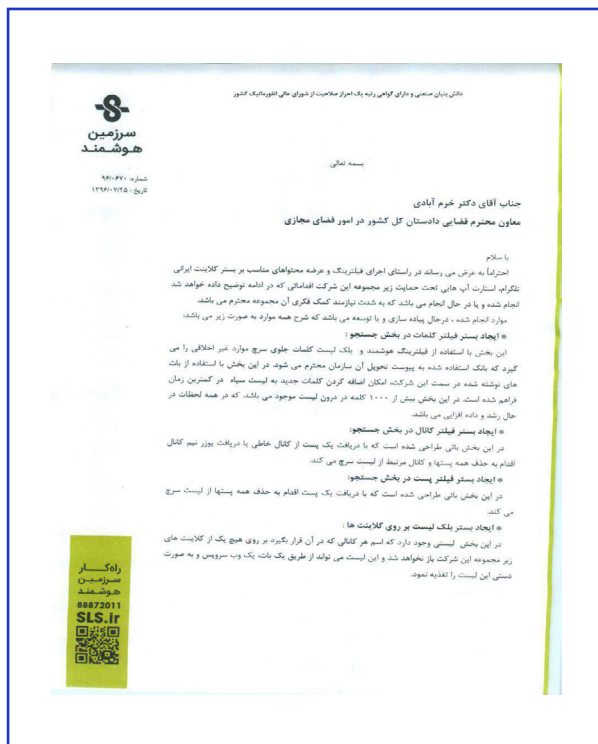
شفاف‌ترین نمونه‌ها «تلگرام طلایی» و «هاتگرام» هستند؛ دو نسخه دست‌کاری‌شده از برنامه تلگرام که توسط شرکت داخلی «راهکار سرزمین هوشمند» توسعه یافتند. این برنامه‌ها پس از مسدودسازی تلگرام به دستور قضایی در سال ۲۰۱۸ به‌سرعت محبوب شدند و در ظاهر دسترسی بدون سانسور ارائه می‌دادند، اما در عمل نظارت عمیق را

سایبری ترکیبی ایران نشان می‌دهد که همکاری، هم‌پوشانی زیرساخت و تقسیم نقش میان وزارت اطلاعات و سازمان اطلاعات سپاه در کارزارهای جاسوسی سایبری امری استثنایی نیست.^{۴۲} در این چارچوب، ثاقب را باید نه به‌عنوان یک ابزار منفرد، بلکه به‌مثابه محصول یک معماری نهادی چندلایه فهم کرد؛ معماری‌ای که توسعه ابزار، عملیات فنی و پوشش سازمانی را در هم ادغام می‌کند.

۴.۳. تسخیر پلتفرم‌ها: شبیه‌سازی، پوسته‌های حاکمیت‌پذیر و کنترل در سطح اپلیکیشن

فراتر از استقرار جاسوس‌افزارها و ابزارهای دسترسی فریبنده، جمهوری اسلامی ایران شکل ساختاری‌تری از نظارت را دنبال کرده است: تصاحب و دست‌کاری خود پلت‌فرم‌های دیجیتال. در این رویکرد، به‌جای نفوذ به دستگاه‌های فردی، لایه کاربرد هدف قرار می‌گیرد و اعتماد کاربران به خدمات پرکاربرد به ابزاری برای پایش، کنترل و تحلیل رفتاری تبدیل می‌شود.

این راهبرد در قالب‌های متعددی بروز یافته است؛ از شنود ترافیک و مهندسی معکوس رفتار برنامه‌ها گرفته تا تجمیع گسترده داده‌ها و دربرخی موارد، کلون‌سازی کامل پلت‌فرم‌های خارجی. در مجموع، این اقدامات یک اکوسیستم پنهان از نظارت در سطح سکو ایجاد می‌کند که برای استخراج هویت، فراداده و الگوهای رفتاری کاربران طراحی شده است، بدون آنکه نشانه‌های آشکار کارزارهای بدافزاری را داشته باشد. این روند نشان‌دهنده یک چارچوب سیاستی منسجم است که در آن پلت‌فرم‌های خارجی به‌عنوان اهداف مشروع برای نفوذ، تکثیر و جایگزینی کارکردی تلقی می‌شوند. برخلاف ایمپلنت‌های جاسوس‌افزاری که کاربران فردی را هدف می‌گیرند، تصاحب سکوها ماهیتی ساختاری و مقیاس‌پذیر دارد. هنگامی که کاربران به نسخه‌های پروکسی یا کلون‌شده تحت کنترل حکومت هدایت می‌شوند، جمع‌آوری جزئیات دقیق داده‌ها به‌صورت بی‌وقفه انجام می‌گیرد؛ از الگوهای جست‌وجو و زمان‌بندی استفاده گرفته تا مواجهه با محتوا و شناسه‌های سطح دستگاه. این رویکرد امکان نظارت پایدار را فراهم می‌کند، در حالی که برای عموم کاربران تا حد زیادی نامرئی باقی می‌ماند و کنترل را مستقیماً در دل محیط‌های



درگاه های متنوع حکمرانی‌پذیر با سرمایه گذاری بخش خصوصی و تنظیم‌گری حاکمیتی

در این چارچوب، اصطلاح «حاکمیت‌پذیر» صرفاً به نظارت حقوقی اشاره ندارد، بلکه به کنترل مهندسی‌شده بر آنچه کاربران می‌توانند به آن دسترسی داشته باشند، ببینند و به اشتراک بگذارند دلالت می‌کند. فراتر از برنامه‌های کلون‌شده، نهادهای حکومتی به بررسی برنامه‌های نظارتی ثالث نیز پرداخته‌اند که در پوشش ابزارهای حقوقی یا مدنی عرضه می‌شوند. در سال ۲۰۲۲، تیمی مستقر در یک شتاب‌دهنده وابسته به دولت، طرحی با عنوان «DATAP: سکوی مستندسازی ادله» را به کارگروه فیلترینگ ارائه داد. این طرح مدعی بود با ایجاد سامانه‌ای برای جمع‌آوری و ارائه ادله الکترونیکی به قوه قضاییه، از دادرسی دیجیتال حمایت می‌کند.^{۴۷}

با این حال، پیاده‌سازی آن بر نفوذ پنهان استوار بود: یک برنامه ثالث که برای دسترسی به گفتگوها، فعالیت شبکه‌های اجتماعی و ایمیل‌های کاربران هدف طراحی شده بود و اغلب از اعلان‌های رضایت فریبده استفاده می‌کرد. در متن طرح آمده است:

«این سامانه مستندسازی با استفاده از مدل ثالث، اعتماد میان کاربران و فضای دیجیتال را تقویت کرده و بررسی پرونده‌ها را از طریق راهکارهای تنظیم‌گری فناورانه تسهیل می‌کند.»

بخش نیازسنجی این طرح به‌صراحت خواستار موارد زیر بود: تصویربرداری از صفحه گفتگوها و پست‌ها، دسترسی به اطلاعات حساب کاربری در سکوهایی مجازی مختلف، و امکان مقابله با «اطلاعات نادرست».

این چارچوب‌بندی، نظارت فراگیر را در قالب گردآوری ادله حقوقی بازنمایی می‌کند و به نیروهای انتظامی اجازه می‌دهد تحت پوشش تنظیم‌گری مدنی، سازوکارهای امنیتی سکوها را دور بزنند. چنین سامانه‌ای مرز میان نظارت قضایی و پایش اطلاعاتی را بیش از پیش مخدوش می‌کند.

ممکن می‌کردند. تحقیقات نشان داد هر دو برنامه داده‌های حساس کاربران، از جمله کدهای احراز هویت، را جمع‌آوری می‌کردند و به‌طور فعال محتوایی را سانسور می‌کردند، از جمله مسدودسازی دسترسی به کانال‌های خبری مستقل مانند بی‌بی‌سی فارسی و سازمان‌های حقوق بشری.^{۴۳} خود تلگرام درباره این برنامه‌ها هشدار داد و در نهایت به دلیل نقض حریم خصوصی از فروشگاه گوگل پلی حذف شدند.^{۴۴}

با وجود تکذیب‌های رسمی، اسناد افشاشده و اظهارات عمومی دخالت دولت در ترویج این پوسته‌ها را تایید می‌کند. ابوالحسن فیروزآبادی، دبیر وقت شورای عالی فضای مجازی، به‌طور علنی اعلام کرد که این کلون‌های تلگرام با حمایت وزارت ارتباطات برای توسعه زیرساختی مستقل از سرورهای تلگرام پشتیبانی شده‌اند. هرچند محمدجواد آذری جهرمی، وزیر وقت ارتباطات، این ادعاها را رد کرد؛ با این حال تلگرام طلایی و هاتگرام پس از مسدودسازی تلگرام به فعالیت خود ادامه دادند و عملاً از تأیید حکومتی برخوردار بودند.^{۴۵}

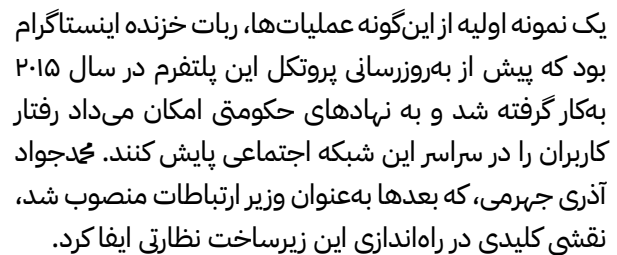
توجیه حقوقی این پوسته‌ها در مصوبات شورای عالی فضای مجازی ریشه دارد. در مصوبه جلسه ۹۶ شورای عالی فضای مجازی سازمان‌های مختلفی موظف شدند «دسترسی کاربران به خدمات مفید خارجی را در قالب‌های حکمرانی‌پذیر» بررسی کنند.^{۴۶} مصداق‌های حکمرانی‌پذیری هم در همین مصوبه معرفی شده‌است:

پنجره دسترسی روی سکوهایی داخلی

مذاکره برای تأسیس نمایندگی داخل کشور



۲.۴.۳. سوءاستفاده از پیام‌رسان‌ها و نظارت در سطح پلت‌فرم



یکی از بدنام‌ترین نمونه‌ها، سامانه «شکار» است؛ [FA](#) پایگاه داده‌ای که در سال ۲۰۲۰ افشا شد و جزئیات خصوصی بیش از ۴۲ میلیون کاربر ایرانی تلگرام را در معرض دید قرار داد. این داده‌ها شامل شناسه‌های کاربری، شماره تلفن‌ها و فراداده‌های مرتبط بود. هرچند تلگرام در سال ۲۰۱۸ به دستور قضایی به طور رسمی مسدود شد، این سکو از طریق ابزارهای دور زدن فیلترینگ همچنان به طور گسترده مورد استفاده قرار می‌گرفت و سال‌ها تحت فشار سیاسی و نظارت پنهان قرار داشت. افشای شکار نشان داد که نهادهای ایرانی به صورت بی‌سروصدا در حال ساخت نقشه‌های جامع پیوند هویت به رفتار بوده‌اند، بدون رضایت کاربران و بدون هیچ‌گونه تأیید یا شفافیت در سطح سکو.

طرح گسترده‌تری با نام «سامانه پایش صافتا» که توسط نهادهای وابسته به بخش دفاعی توسعه یافته و در سال ۲۰۱۷

در مجموع، این تلاش‌ها بازتاب‌دهنده چارچوبی سیاستی هستند که در آن سکوهای خارجی به‌عنوان اهداف مشروع برای نفوذ و تکثیر در نظر گرفته می‌شوند، با هدف نهایی حفظ کنترل اجتماعی از طریق نظارت دیجیتال. برخلاف ایمپلنت‌های جاسوس‌افزاری که کاربران فردی را هدف می‌گیرند، این تکنیک‌ها ماهیتی ساختاری، نظام‌مند و اغلب نامرئی برای عموم دارند.

خطر اصلی در ماهیت مازولار و مقیاس‌پذیر این عملیات نهفته است. سکوهای کلون‌شده و رابط‌های پروکسی می‌توانند با هزینه اندک به‌روزرسانی شوند، در میان خدمات مختلف گسترش یابند یا به برنامه‌های موبایلی منتقل شوند. زمانی که کاربران به نسخه‌های تحت کنترل حکومت از خدمات جهانی مورد اعتماد هدایت می‌شوند، جمع‌آوری جزئیات دقیق داده‌ها به‌صورت بی‌وقفه انجام می‌گیرد؛ از عبارات جست‌وجو و برچسب‌های زمانی گرفته تا چینش محتوا و اثرانگشت‌برداری از دستگاه.



یکی از نمونه‌های شاخص سوءاستفاده از داده‌ها به اپلیکیشن مسیریاب «بلد» بازمی‌گردد که توسط گروه «هزاردستان» توسعه یافته است؛^{۷۱} همان مجموعه‌ای که مالک کافه‌بازار، بزرگ‌ترین فروشگاه اندرویدی ایران، و «دیوار»، سکوی پرکاربرد آگهی‌های آنلاین، نیز هست. در اکتبر ۲۰۲۲، بلد بیانیه‌ای منتشر کرد که به‌طور غیرمستقیم

اسناد افشاشده در اواخر سال ۲۰۲۲ نشان داد که چندین شرکت اینترنتی داخلی، دسترسی‌های مدیریتی ویژه‌ای به داشبوردهای داده کاربران در اختیار دادستانی و کارگروه فیلترینگ قرار داده‌اند.^{۷۰} این دسترسی‌ها به نهادهای حکومتی امکان می‌داد بدون صدور احکام رسمی قضایی، به سوابق هویتی، الگوهای مصرف و فراداده‌های حساس کاربران دست یابند. نام شرکت‌هایی مانند زرین‌پال، ویگول، آپارات، بام و کافه‌بازار در میان ارائه‌دهندگان این دسترسی‌های ممتاز ذکر شده است. اگرچه برخی از این شرکت‌ها بعداً مدعی شدند که چنین اقداماتی برای مقابله با جرایم سایبری انجام شده، نبود رویه‌های حقوقی رسمی تردیدهای جدی درباره این، تجدیدات ایجاد می‌کند.

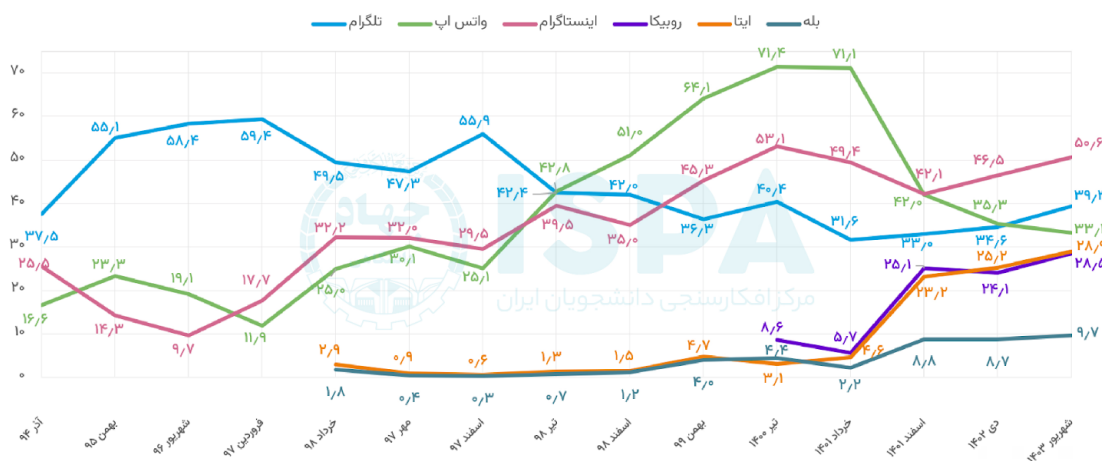
بلد در پنجمین سال فعالیتش با وجود تیمی بالغ‌تر، کم‌نظیر و همدل و متصل‌بسته به پیش از ۱۰ میلیون کارگر فعال روزانه، بناچار پس دهها هزار همکارانش خداحافظ می‌کند. مدهاست که راهای جذب سرمایه در فضای استارت‌آپی و بخش خصوصی هنوز بسته ستانده و امکان دادن کسبوتواریهای بازگشت به زندگی را فراهم نکرده بود و قرار داده بودند و امکان رسیدن به نقطه سر به سر، در کوتاه مدت را ندارند، سخت تر شده است. همچنان هیچ افق روشنی برای خروج سرمایه گذاران از کسبوتواریهای باغری اینترنتی ندارد و این امید را برای آنها که سرمایه های سال تا رسیدن به مرحله خروج فاصله دارند نیز برده است. از طرف دیگر ضمن گزینی بابت محدودیت درآمدها اعمال شده بر اینترنت و امنیتش شدن ضعیف، انداختن اینترنت به کشور چندان قابل پیش بینی نیست و برخی روگردان به خصوص در ماههای اخیر را در درستی رایجی که در پیش گرفته بودیم و موضوعی را در حفاظت از حقوق کاربران به شک انتخاب کرده است. ما بابت شرایط به وجود آمده برای همکارانمان متأسفیم و تمامی تلاش خود را به کار می گیریم که در فضای سخت و نامطمئن فعلی، جابجایی آنرا توانمند و با استعداد در دوره ها سخت‌های کمتر هزینه همراه شود. اما خدمت توسط تقسیم و مسیریابی بلد به گزارشاتی را تا پایان سال جاری تضمین نمی کند. در عین حال هر روز در مورد آینده این محصول و نتایج آن به دلیل میلیون‌ها کاربری که تمام این سال‌ها به آن اعتماد کرده اند اطلاع رسانی دقیقاً تأخیر خواهیم داد.

نگرانی‌های عمومی درباره احتمال دسترسی دولت به داده‌های کاربرانش را تأیید می‌کرد.^{۷۲} پیامدهای این موضوع گسترده بود: اگر چنین دسترسی‌ای در بلد وجود داشته، با توجه به زیرساخت پشتیبان مشترک و مالکیت واحد، خطر مشابهی احتمالاً متوجه دیوار و کافه‌بازار نیز بوده است. این رویداد مسئله کلی‌تری از در معرض بودن داده‌های کاربران در سکوهایی داخلی مسلط را برجسته کرد.

جمهوری اسلامی همچنین سرمایه‌گذاری گسترده‌ای برای شکل‌دهی به یک زیست‌بوم موازی از پیام‌رسان‌های همسو با حکومت انجام داده است؛ از جمله روبیکا، ایتا، بله، آی‌گپ، سروش و گپ که همگی تحت عنوان «حاکمیت دیجیتال» معرفی می‌شوند. این سکوها با پشتیبانی مالی و زیرساختی نهادهای اقتصادی شبه‌دولتی اداره می‌شوند و هدف آنها نه تنها جایگزینی برنامه‌های خارجی، بلکه متمرکزسازی ارتباطات کاربران در محیطی با کنترل مرکزی است. اگرچه این برنامه‌ها به عنوان گزینه‌های «ملی» تبلیغ می‌شوند، در



رند میزان استفاده ایرانیان از شبکه‌ها و پیام‌رسان‌های اجتماعی



میزان استفاده از شبکه‌ها و پیام‌رسان‌های اجتماعی در ایران
 کل کشور (شهر و روستا)
 ۲۲ تا ۲۳ شهریور ۱۳۹۹
 ۳۳ تا ۳۴ شهریور ۱۳۹۹
 ۳۵ تا ۳۶ شهریور ۱۳۹۹
 ۳۷ تا ۳۸ شهریور ۱۳۹۹
 ۳۹ شهریور ۱۳۹۹



گوگل‌پلی حذف شد.^{۷۵} در واکنش، کارگروه فیلترینگ دسترسی به خود گوگل‌پلی را مسدود کرد و عملاً سکوها داخلی را از نظارت بین‌المللی مصون ساخت. این رویداد نشان داد جمهوری اسلامی تا چه اندازه آماده است زیرساخت ملی و سیاست‌های پلتفرمی را در دفاع از نرم‌افزارهای دارای قابلیت نظارتی به سلاح تبدیل کند. مقام‌های حوزه ارتباطات و امنیت ایران بارها به این ماجرا استناد کرده‌اند و اقدام گوگل را به‌عنوان نمونه‌ای از «دخالت خارجی» در امور داخلی معرفی کرده‌اند؛ روایتی که همچنان در گفتمان رسمی تکرار می‌شود.

رویکا توسط هلدینگ‌های اقتصادی شبه‌دولتی تحت کنترل رهبر جمهوری اسلامی توسعه یافت، با این چشم‌انداز که به یک «سوپر اپ» ملی در رقابت با سکوها خارجی تبدیل شود. اما همین ambition زمینه‌ای فراهم کرد تا این سکو به یک واسطه نظارتی بدل شود. با یکپارچه‌سازی دسترسی‌های پشتیبان و اعمال رویه‌های مبهم داده‌ای، رویکا به نمونه‌ای کلاسیک از بهره‌برداری دولت از ظواهر بخش خصوصی برای استخراج انبوه داده‌ها تحت پوشش نوآوری داخلی تبدیل شد.^{۷۶}

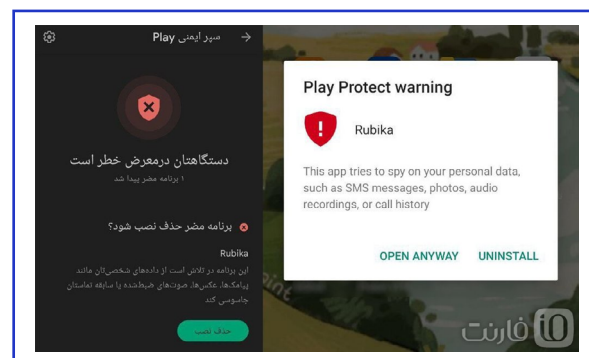
پیام‌رسان بله نیز با نگرانی‌های جدی حریم خصوصی

عمل نقش فعالی در اعطای دسترسی‌های پشتیبان ممتاز به نهادهای حکومتی ایفا کرده‌اند و بدین‌ترتیب نظارت قضایی را دور زده‌اند. بررسی‌های اخیر نشان می‌دهد رویکا، ایتا و بله همواره در میان پرکاربردترین پیام‌رسان‌ها در ایران قرار دارند.^{۷۳}

ممیزی‌های فنی مستقل، از جمله تحقیق مفصل «بنیاد فناوری باز» (OTF)، نگرانی‌های جدی درباره معماری حریم خصوصی رویکا، ایتا و بله مطرح کرده‌اند.^{۷۴} هیچ‌یک از این سکوها به استانداردهای پایه بین‌المللی برای پیام‌رسانی امن پایبند نیستند: داده‌ها به‌صورت ناامن ذخیره می‌شوند، پروتکل‌های رمزنگاری ضعیف یا نادرست پیاده‌سازی شده‌اند و مجوزهای برنامه‌ها بیش‌ازحد گسترده است. یافته‌ها نشان می‌دهد این آسیب‌پذیری‌ها تصادفی نیستند، بلکه به‌طور ساختاری تعبیه شده‌اند تا دسترسی دولت به ارتباطات حساس را تحت پوشش زیرساخت ملی تسهیل کنند.

یکی از افشاگرانه‌ترین لحظات زمانی رخ داد که فروشگاه گوگل‌پلی، رویکا را به‌عنوان تهدید نظارتی علامت‌گذاری کرد. این برنامه که به‌دلیل امکاناتی مانند شرط‌بندی فوتبال و بخش رسانه‌ای محبوب شده بود، به‌سبب نقض حریم خصوصی کاربران و رفتارهای بالقوه جاسوس‌افزاری از

مواجهه بوده است، به‌ویژه پس از یک نشت گسترده که در آن اطلاعات شخصی کاربران، از جمله محتوای گروه‌های خصوصی، افشا شد.^{۷۷} این افشاگری‌ها نشان داد مدیران



بله به پیام‌های خصوصی و فراداده‌های کاربران دسترسی داشته‌اند؛ موضوعی که خشم عمومی و انتقاد گسترده‌ای برانگیخت.

علاوه بر این، مشکلات امنیتی دیگری نیز در برنامه به گزارش شده است؛ از جمله نبود یا ضعف رمزنگاری مناسب و دسترسی غیرمجاز به داده‌های کاربران. این نگرانی‌ها به‌ویژه در دوره‌هایی که فشار حکومت برای پایش فعالیت‌های آنلاین افزایش یافته، تشدید شده و ترس از استفاده به‌عنوان کانالی پنهان برای نظارت دولتی بر ارتباطات حساس را تقویت کرده است.^{۷۸}

پیام‌رسان ای‌تا، یکی دیگر از سکوها مورد حمایت حکومت، نیز با نگرانی‌های جدی در زمینه نقض حریم خصوصی مواجهه بوده است. ممیزی‌های امنیتی و گزارش‌های مستقل، الگوهایی از دسترسی غیرمجاز به داده‌ها، پروتکل‌های انتقال ناامن و سازوکارهای پایش تعبیه‌شده را در این برنامه شناسایی کرده‌اند. مشابه رویکا و بله، ای‌تا تحت مالکیت یا حمایت سرمایه‌گذاران وابسته به حکومت فعالیت می‌کند و از کارزارهای ترویجی دولتی بهره می‌برد. با این حال، معماری آن آسیب‌پذیری‌های ساختاری جدی دارد، از جمله ذخیره‌سازی داده‌های بدون رمزگذاری و دسترسی مدیریتی به محتوای کاربران. این مسائل به‌ویژه در دوره‌های سرکوب سیاسی تشدید شده‌اند؛ زمانی که فراداده و محتوای پیام‌های کاربران، به‌خصوص روزنامه‌نگاران، فعالان و معترضان، می‌تواند جمع‌آوری و تحلیل شود. اگرچه ای‌تا خود را به‌عنوان جایگزینی

امن و بومی معرفی می‌کند، مدل عملیاتی آن بازتاب‌دهنده راهبردی گسترده‌تر از مهار دیجیتال است که ابزارهای ارتباطی را به ابزارهای کنترل دولتی تبدیل می‌کند.

در مجموع، این رویه‌ها نشان می‌دهد جمهوری اسلامی چگونه داده‌های کاربران را، هم از طریق استارت‌آپ‌های بخش خصوصی و هم از طریق پیام‌رسان‌های بومی ترویج‌شده، به سلاحی برای ساخت یک زیرساخت نظارتی چندلایه و گسترده تبدیل کرده است. با سوءاستفاده از دسترسی‌های پشتیبان، شراکت‌های مبهم و فقدان تضمین‌های حقوقی معنادار، نهادهای حکومتی عملاً نظارت قضایی را دور زده و داده‌های رفتاری را استخراج، پایش و به ابزار سرکوب بدل کرده‌اند. این مدل ترکیبی نظارت دولتی و خصوصی نه تنها اعتماد کاربران به خدمات دیجیتال داخلی را تضعیف می‌کند، بلکه نقش شرکت‌های فناوری را به‌عنوان بازوهای عملیاتی دستگاه اطلاعاتی حکومت بازتعریف می‌کند. با گسست فزاینده زیست‌بوم دیجیتال ایران از شبکه‌های جهانی، بهره‌برداری بی‌مهار از داده‌های کاربران به تهدیدی جدی برای آزادی‌های مدنی و خودمختاری دیجیتال بدل شده است.

۶.۳. شبکه کاشف: همجوشی داده‌ها، ترسیم روابط و نظارت عملیاتی

فراتر از عملیات‌های نظارتی منفرد، یکی از پیامدهای بنیادین راهبرد کنترل دیجیتال جمهوری اسلامی، تمرکز بر تجمیع داده است. به‌جای اتکا صرف به شنودهای موردی یا جاسوسی هدفمند، دولت به‌طور فزاینده‌ای جمع‌آوری نظام‌مند، همبسته‌سازی و تحلیل داده‌های کاربران را در میان سکوها، خدمات و شناسه‌های مختلف در اولویت قرار داده است. در این الگو، قدرت نظارتی نه از یک نقطه داده منفرد، بلکه از توانایی ادغام مجموعه‌های ناهمگون داده در قالب پروفایل‌های رفتاری منسجم ناشی می‌شود.

افشاگری‌های مرتبط با عملیات چارمینگ کیتن این منطق را در عمل نشان می‌دهد. زیرساخت این گروه صرفاً به توزیع بدافزار یا تصاحب حساب محدود نبود، بلکه به‌عنوان یک خط لوله داده عمل می‌کرد. اطلاعات گردآوری‌شده شامل اعتبارنامه‌ها، توکن‌های نشست، فراداده‌ها، شبکه‌های ارتباطی و آرشیوهای محتوایی، در طول زمان ذخیره، نمایه‌سازی و با یکدیگر تطبیق داده می‌شدند. این فرآیند

به یکدیگر پیوند دهند: الگوهای ارتباطی، داده‌های مکانی، سوابق ترانکشن و روابط اجتماعی. ترکیب این داده‌ها سطحی از دیدپذیری ایجاد می‌کند که به مراتب فراتر از شنود قانونی متعارف است.

نکته کلیدی آن است که تجمع داده مرز میان نظارت هدفمند و نظارت فراگیر را از میان برمی‌دارد. حق زمانی که دسترسی از منابع گسسته آغاز می‌شود، داده‌های حاصل به صورت افقی گسترش می‌یابند و جمعیت‌ها را، نه صرفاً افراد را، در بر می‌گیرند. این معماری، داده‌های جانبی تولیدشده در فعالیت‌های روزمره دیجیتال را به دارایی اطلاعاتی تبدیل می‌کند و امکان تحلیل پیش‌بینانه، ترسیم گراف‌های اجتماعی و تحقیقات پسینی را بدون نیاز به شنود فعال مداوم فراهم می‌سازد.

در این چارچوب، چارمینگ کیتن را نباید صرفاً یک بازیگر جاسوسی سایبری دانست، بلکه باید آن را نمونه‌ای عملی از نظارت داده‌محور تلقی کرد. روش‌های این گروه نشان می‌دهد چگونه جمع‌آوری غیرمتمرکز می‌تواند به تحلیل متمرکز تغذیه شود و راهبردی دولتی را تقویت کند که داده کاربران را به منبعی راهبردی بدل می‌سازد. همگرایی سکوهایی مورد حمایت دولت، دسترسی‌های پشتیبان ممتاز و برداشت داده از منابع بیرونی، به شکل‌گیری معماری نظارتی یکپارچه‌تری اشاره دارد که در آن خودِ تجمع، به سازوکار اصلی کنترل

بیانیه اپلیکیشن بله دربارهٔ تصویر منتشرشده

قبل از هر چیز همانطور که بارها خاطرنشان کرده‌ایم، امنیت و داده‌های شخصی کاربران، جزو خط قرمزهای بله است و با تمام وجود از آن حفاظت کرده می‌کنیم و خواهیم کرد. این موضوع در این بیش از ۷ سال که از عمر بله می‌گذرد، همواره مورد تأکید بله بوده است.

بله، به عنوان یک پلتفرم، مانند تمام پلتفرم‌های دیگر موظف است تدابیر لازم را برای جلوگیری از کلاهبرداری‌ها و حفظ امنیت، دربارهٔ فعالیت کاربران خود در پلتفرم، اتخاذ کند. از این رو طبق سند قوانین و شرایط استفاده از بله که در آدرس terms.bale.ai منتشر شده «برای کانال‌ها و بازوهای که به صورت عمومی در دسترس هستند، بله از الگوریتم‌های خودکار برای آنالیز پیام‌ها برای جلوگیری از انتشار محتوای مجرمانه استفاده می‌کند. همچنین کاربران می‌توانند در صورت مشاهدهٔ این موارد، گزارش آن را به بازوی پشتیبانی ارسال یا از گزینه «گزارش محتوای نامناسب» استفاده کنند. در این حالت بله این گزارش‌ها را بررسی می‌کند و در صورت تأیید مجرمانه‌بودن آن، طبق قانون، برخورد لازم انجام می‌شود. لازم به ذکر است با گروه‌هایی که بیش از هزار عضو داشته باشند، در حوزهٔ بررسی محتوا، مشابه کانال‌های عمومی رفتار می‌شود.»

آنچه در این تصویر از صفحه مانیتور منتشر شده، مربوط به ابزار اجرایی همین موضوع است. این ابزار صرفاً حاوی محتوای منتشرشده در کانال‌های عمومی و گروه‌های بیش از ۱۰۰۰ عضو است که به صورت سیستمی و حسب نیاز کارشناسی، جهت مقابله با کلاهبرداری از کاربران مورد بررسی قرار می‌گیرد. بدیهی است که اطلاعات خصوصی کاربران، آی‌دی و شمارهٔ فرستندهٔ محتوا و مواردی از این قبیل در جهت حفظ حریم خصوصی کاربران به عنوان خط قرمز بله، در حیطهٔ این ابزار وجود ندارد و تنها محتوا به صورت بی‌نام در آن وجود دارد.

مجدداً تأکید می‌کنیم که حریم خصوصی کاربران خط قرمز ماست و با تمام وجود از آن حفاظت کرده و می‌کنیم و خواهیم کرد. همچنین بله حق قانونی جهت پیگیری و برخورد با منتشرکنندگان این تصویر را برای خود محفوظ می‌دارد.

امکان ساخت نقشه‌های هویت به رفتار را فراهم می‌کرد که فراتر از رویدادهای منفرد بوده و اهداف پایش بلندمدت را پشتیبانی می‌کردند.

این رویکرد مبتنی بر تجمع، شباهت نزدیکی به رویه‌های نظارتی دولت در سکوهایی داخلی دارد. دسترسی پشتیبان به خدمات ایرانی مانند پیام‌رسان‌ها، بازارهای آنلاین، ابزارهای مسیریابی و سامانه‌های پرداخت، به نهادهای حکومتی اجازه می‌دهد سیگنال‌های رفتاری را در حوزه‌های مختلف

تبدیل می‌شود.

بر اساس گزارش‌های موجود، کاشف توسط واحدهای امنیتی و اطلاعاتی برای شناسایی شبکه‌های اجتماعی، ردیابی ارتباطات غیرمستقیم و کشف پیوندهای پنهان میان افراد و مکان‌ها به کار گرفته می‌شود. این سامانه به‌جای شنود لحظه‌ای ارتباطات، الگوهای زندگی را به‌صورت پسینی بازسازی می‌کند و به نهادهای حکومتی امکان می‌دهد روابط اعتماد، هماهنگی‌های لجستیکی و مسیرهای تردد را استنباط کنند. همین ویژگی، کاشف را به ابزاری کلیدی برای پلیس اطلاعات‌محور، سرکوب اعتراضات و حق هدف‌گیری فرامرزی تبدیل کرده‌است.

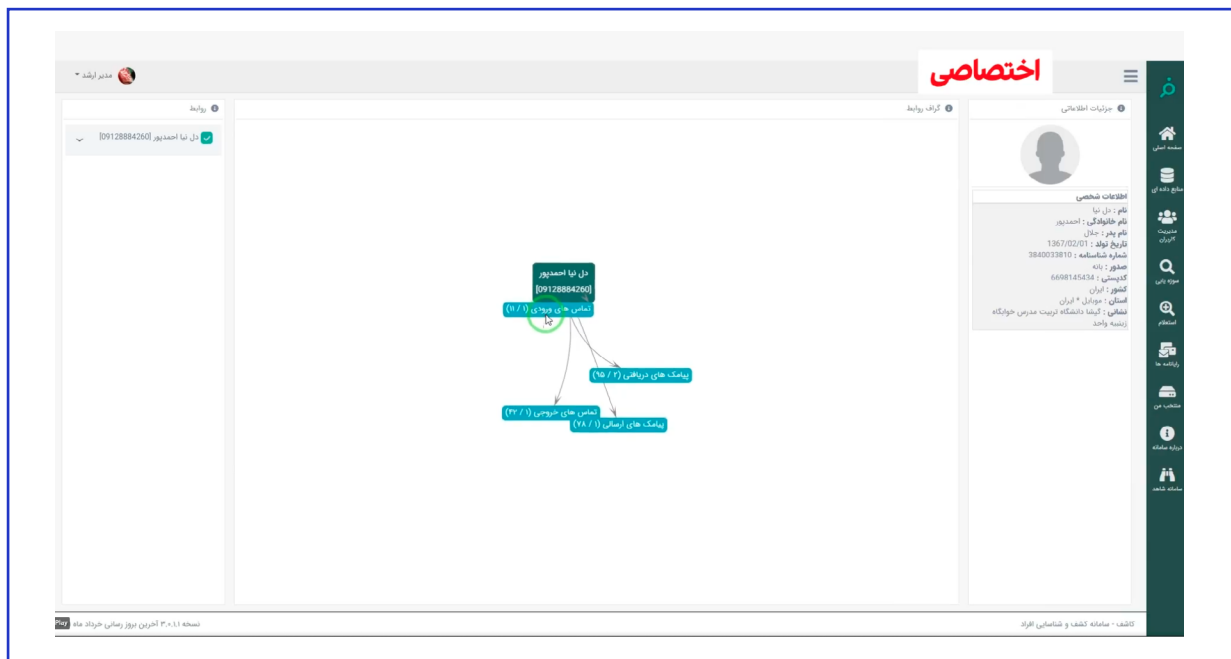
نکته مهم آن است که کاشف ظاهراً به‌عنوان مصرف‌کننده نهایی داده‌هایی عمل می‌کند که از سایر سازوکارهای نظارتی توصیف‌شده در این گزارش به دست آمده‌اند. اطلاعات گردآوری‌شده از طریق جاسوس‌افزارها، دسترسی‌های اداری به سکوها داخلی، سامانه‌های شنود قانونی و نفوذهای سایبری، می‌توانند وارد کاشف شوند و در آن‌جا یکسان‌سازی و تطبیق داده شوند. از این منظر، کاشف نقطه تلاقی پشته نظارتی جمهوری اسلامی است؛ جایی که شنود، دسترسی به داده و پایش رفتاری در یک چارچوب تحلیلی واحد ادغام می‌شوند.

معماری و کارکرد کاشف نشان‌دهنده گذار از نظارت پراکنده به تولید یکپارچه اطلاعات است. جمهوری اسلامی به‌جای

یکی از افشاگرانه‌ترین یافته‌ها درباره اکوسیستم نظارت پنهان جمهوری اسلامی ایران، افشای سامانه‌ای با نام کاشف است؛ یک سیستم اطلاعاتی متمرکز که برای جمع‌آوری همبستگی و عملیاتی‌سازی حجم عظیمی از داده‌های شخصی طراحی شده‌است.^{۷۹} برخلاف ابزارهای نظارتی بررسی‌شده در بخش‌های پیشین، کاشف متکی به نصب بدافزار، شبیه‌سازی پلتفرم‌ها یا تعامل مستقیم با کاربر نیست. این سامانه در عوض به‌عنوان یک موتور همجوشی اطلاعاتی در لایه پشتی عمل می‌کند که داده‌های پراکنده را به نقشه‌های رفتاری و شبکه‌ای قابل استفاده تبدیل می‌کند.

بررسی‌ها نشان می‌دهد کاشف به اپراتورها امکان می‌دهد با وارد کردن هویت یک فرد هدف، شبکه‌ای ساخت‌یافته از ارتباطات او را استخراج کنند؛ از جمله اعضای خانواده، تماس‌های پرتکرار، سابقه سفر و الگوهای حضور مکانی. این سامانه داده‌های فراداده‌ای از منابع مختلف مانند ریز اطلاعات تلفن همراه، داده‌های مکان‌یابی، فهرست‌های پروازی و پایگاه‌های داده افشا یا استخراج‌شده در عملیات‌های سایبری را با یکدیگر همبسته می‌کند. نتیجه این فرآیند، تولید یک گراف پویا از روابط است که می‌توان آن را بر اساس نیازهای اطلاعاتی یا عملیاتی جست‌وجو، گسترش یا پالایش کرد.

The screenshot displays the 'Kashf' (کاشف) software interface. At the top, there's a header with the title 'کاشف' and a search bar. Below the header, a sidebar on the right contains navigation icons and labels in Persian. The main area shows a table of individuals. The table has columns for 'ردیف' (Row), 'نام' (Name), 'تاریخ تولد' (Date of Birth), 'شماره شناسنامه' (National ID), 'نام پدر' (Father's Name), 'شماره' (Number), 'مکان' (Location), 'استان' (Province), 'کشور' (Country), 'کدپستی' (Postal Code), 'نشانی' (Address), and 'فایل' (File). The table lists five individuals, with the first one's name 'عبدالرضا' circled in green. Below the table, there's a footer with some technical information.



اتکا به داده‌های منفرد یا ابزارهای تک‌منظوره، به سمت سامانه‌هایی حرکت کرده که امکان پروفایل‌سازی بلندمدت و استنتاج پیش‌بینانه را فراهم می‌کنند. این الگو مرز میان نظارت داخلی و عملیات اطلاعاتی را محو می‌کند و اجازه می‌دهد داده‌های غیرنظامی بدون شفافیت قضایی یا نظارت معنادار، برای اهداف امنیتی بازاستفاده شوند.

به این ترتیب، کاشف نمونه‌ای روشن از بلوغ حکمرانی نظارتی در جمهوری اسلامی است؛ گذار از پایش ارتباطات به نقشه‌برداری از جامعه. این سامانه با تبدیل ردپاهای دیجیتال به اطلاعات رابطه‌ای، داده‌های شخصی را به ابزار کنترل بدل می‌کند و دامنه نظارت حکومتی را فراتر از پلتفرم‌های منفرد، به ساختار زندگی اجتماعی گسترش می‌دهد.



۴. نظارت خیابانی در جمهوری اسلامی و کشف هویت شهروندان در فضای عمومی

مدل‌های ترکیبی متوسل شود؛ ترکیبی از دوربین تحت کنترل نیروی انسانی، اپلیکیشن موبایل در دست نیروهای میدانی و سامانه‌های دیجیتال. در این الگو، اجرای سیاست‌های کنترل اجتماعی از ابزارهای چهره‌نگاری تا سامانه‌های هشدار پیامکی، شکل شبکه‌ای و موضعی پیدا کرده‌است.

الگوی نظارت جمهوری اسلامی ایران، با وجود محدودیت‌های فناوریانه، در حال حرکت به سمت یک مدل اقتدارگرایی دیجیتال هم‌راستا با مدل چینی است؛ مدلی که نه تنها شهروندان را بر اساس هویت دیجیتال پایش می‌کند، بلکه برای اجرای قوانین ایدئولوژیک، همچون حجاب، به ترکیب پیچیده‌ای از داده، تصویر، رفتار و قانون تکیه می‌کند. این روند، پیامدهای عمیقی برای آینده آزادی‌های مدنی، حقوق دیجیتال و مقاومت اجتماعی در ایران دارد.

۴.۱. اقتدارگرایی و ایدئولوژی دینی در راهبردهای نظارت و احراز هویت

در نظام‌های اقتدارگرایی معاصر، به‌ویژه در دوران پس از گسترش فناوری‌های دیجیتال، احراز هویت شهروندان در فضاهای عمومی صرفاً یک ابزار امنیتی نیست، بلکه به سازوکاری محوری برای اعمال قدرت سیاسی، مهندسی اجتماعی و کنترل بدن و رفتارهای روزمره افراد بدل

جمهوری اسلامی ایران در سال‌های اخیر، به‌ویژه پس از خیزش‌های مدنی گسترده و تغییر رویکرد اجتماعی نسبت به حجاب اجباری، تلاش سازمان‌یافته‌ای را برای بهره‌گیری از فناوری‌های شناسایی هویتی و نظارت دیجیتال آغاز کرده‌است. این تلاش‌ها با هدف بازتعریف کنترل اجتماعی در فضاهای عمومی، در قالب سیاست‌گذاری‌ها و قوانین نظارتی، توسعه زیرساخت‌های اطلاعاتی و بهره‌برداری از سامانه‌های احراز هویت دنبال شده‌اند.

نهادهای امنیتی و اجرایی جمهوری اسلامی ایران این پروژه را از سه مسیر دنبال می‌کنند: واردات تجهیزات نظارتی و دوربین‌های هوشمند از چین، توسعه الگوریتم‌های داخلی در دانشگاه‌ها و شرکت‌های دانش‌بنیان وابسته به نهادهای حکومتی و اتصال سامانه‌های اطلاعاتی خدماتی عمومی موجود مانند شاهکار، همتا، هدا، ثنا و سپتام به شبکه‌ای از دوربین‌ها، شماره موبایل‌ها و کارت‌های ملی. در اغلب موارد، این زیرساخت هنوز در مرحله «پیش‌داد» قرار دارد؛ مرحله‌ای که در آن تصویر، صدا، و مکان افراد گردآوری می‌شود، اما اتصال کامل به تحلیل‌گرهای هوشمند برقرار نیست.

شکاف‌های الگوریتمی در شناسایی دقیق «رفتار» شهروندان، به‌ویژه در حوزه‌هایی مانند تشخیص «حجاب» یا مشارکت در اعتراضات، باعث شده که جمهوری اسلامی ایران به

گرفته تا فناوری‌های نظارت شهری و دیجیتال. حکومت از «حجاب» به‌عنوان نقطه ورودی برای ساخت زیرساخت‌های هویق و کنترلی استفاده می‌کند؛ زیرساخت‌هایی که قابلیت تسری به سایر مصادیق نافرمانی مدنی را نیز دارند.

در چنین چارچوبی، فضای عمومی شهری، از خیابان و مترو گرفته تا پارک‌ها و مراکز تجاری، نه صرفاً محل تردد بلکه عرصه‌ای برای اعمال اقتدار حکومتی تعریف می‌شود. شهروند، دیگر یک فرد ناشناس در میان جمع نیست، بلکه سوژه‌ای قابل‌شناسایی و ردیابی است که باید بر رفتار او نظارت شود. پوشش اجباری و حکومتی «حجاب» که در ظاهر از جنس مذهب یا اخلاق است، عملاً به سکوی برای گسترش سامانه‌های شناسایی هویق، احراز هویت دیجیتال و فناوری‌های نظارت عمومی بدل شده‌است. این فناوری‌ها که در ابتدا با توجیه مقابله با «بی‌حجابی» وارد می‌شوند، به‌سرعت قابلیت تعمیم به سایر گروه‌های نافرمان اجتماعی مانند معترضان، فعالان مدنی، زنان و اقلیت‌ها را پیدا کرده‌اند.

خیزش‌های اجتماعی سال‌های اخیر، از ژانویه ۲۰۱۸ و نوامبر ۲۰۱۹ تا سپتامبر ۲۰۲۲،^{۸۷} نقطه عطفی در راهبردهای کنترلی جمهوری اسلامی پدید آوردند. در این دوره، حکومت به‌تدریج از شیوه‌های سنتی مبتنی بر حضور فیزیکی ماموران مانند گشت‌های «ارشاد» فاصله گرفت و به‌سمت مدل‌های فناورانه و ساختاریافته نظارت حرکت کرد. این چرخش ناشی از دو عامل کلیدی بود: نخست، کاهش مشروعیت و کارایی نیروهای میدانی به‌ویژه پس از قتل مهسا امینی در بازداشت پلیس امنیت اخلاقی و مباحث پیش آمده درباره نقش دوربین‌های مدار بسته؛^{۸۸} و دوم، فراهم‌شدن زیرساخت‌های فنی لازم برای شناسایی هویق شهروندان با استفاده از ابزارهایی چون سامانه‌های تشخیص چهره، ردیابی سیم‌کارت، پایگاه‌های کارت ملی هوشمند، و شماره پلاک خودرو.

۱.۱.۴ تحول راهبردی در کنترل پوشش: از تبلیغ فرهنگی تا رصد امنیتی

تحولات راهبردی حکومت جمهوری اسلامی ایران در زمینه کنترل پوشش شهروندان، از تبلیغ فرهنگی به‌سوی نظارت امنیتی، مسیری روشن و مستند دارد. سه مصوبه مهم شورای عالی انقلاب فرهنگی؛ مصوبه ۴۱۳ (۱۹۹۸)،^{۸۹} مصوبه ۵۶۶ (۲۰۰۵)،^{۹۰} و مصوبه ۸۲۰ (۲۰۱۹)^{۹۱} نشان می‌دهند که

شده‌است. ابزارهایی مانند دوربین‌های نظارتی، سامانه‌های بیومتریک، ردیاب‌های تلفن همراه، و اتصال بین پایگاه‌های داده، در چنین نظام‌هایی نه برای حفظ نظم عمومی، بلکه برای شناسایی، دسته‌بندی و مدیریت کنشگران اجتماعی به‌کار گرفته می‌شوند.

تجربه موسوم به «سیستم امتیاز اجتماعی» (Social Credit System)^{۹۲} در جمهوری خلق چین، یکی از شاخص‌ترین نمونه‌های تلفیق فناوری و حکمرانی کنترلی است؛ مدلی که در آن رفتار شهروندان در حوزه‌های شهری، اقتصادی و دیجیتال، رصد می‌شود.^{۹۳} و براساس معیارهای از پیش تعیین‌شده امتیازدهی می‌شود.^{۹۴} هرچند این سیستم به‌صورت سراسری در چین اجرا نشده و اغلب در قالب پایلوت‌های منطقه‌ای باقی مانده^{۹۵} اما الگوی مفهومی آن یعنی پیوند میان نظارت فناورانه و اعمال پیامدهای اجتماعی، الهام‌بخش حکومت‌هایی مانند جمهوری اسلامی ایران شده‌است.^{۹۶} پیچیدگی‌های فنی و اجتماعی اجرای چنین سامانه‌هایی موجب شده تمرکز عملی در چین بر تخلفات حقوقی و قانونی باشد، نه کنترل فراگیر همه رفتارها؛^{۹۷} اما در ایران، این الگو با جهت‌گیری ایدئولوژیک و امنیتی دنبال می‌شود.

در کنار الگوهای رایج حکمرانی اقتدارگرایانه که تمرکز آن‌ها بر کنترل فناورانه فضای عمومی است، جمهوری اسلامی ایران انگیزه‌های مضاعفی برای توسعه این ساختارها دارد. علاوه بر ملاحظات کلاسیک امنیتی برای مدیریت نافرمانی‌های مدنی، دستگاه حاکم در ایران، از گفتمانی ایدئولوژیک و مذهبی پیروی می‌کند که در آن یک مدل خاص از دستور پوشش اجباری (Mandatory Dressing Code) به‌نام «حجاب»، نه صرفاً به‌مثابه پوشش برای زنان، بلکه به‌عنوان نشانه‌ای از وفاداری به نظم اقتدارگرایی دینی تفسیر می‌شود.

در جمهوری اسلامی «حجاب» تنها یک هنجار فرهنگی یا تکلیف مذهبی نیست بلکه به ابزاری مرکزی برای مدیریت بدن و هویت شهروندان تبدیل شده‌است. برخلاف برخی دیگر از کشورهای مسلمان‌نشین که التزام به حجاب را مسئله‌ای فردی و دینی تلقی می‌کنند، در ایران تخطی از پوشش اجباری، یک تخلف حکومتی محسوب می‌شود که مستوجب مجازات امنیتی است.^{۹۸} در نتیجه، سازوکارهای گسترده‌ای برای شناسایی و برخورد با شهروندانی که از این قاعده تخطی می‌کنند طراحی شده‌است؛ از گشت‌های میدانی پلیس



جانشین او و فرمانده فعلی پلیس ایران، سردار احمدرضا رادان بارها به صراحت اعلام کرد که نظارت دیجیتال، محور برنامه‌های اجرایی فراجا خواهد بود.^{۹۴}

احمد وحیدی وزیر کشور وقت و محمدجعفر منتظری رئیس دیوان عالی کشور نیز تاکید کردند که اجرای قانون عفاف و حجاب باید با استفاده از «فناوری‌های هوشمند» و «ابزارهای دیجیتال» صورت گیرد.

این جهت‌گیری‌ها، نهایتاً در قانون «عفاف و حجاب» تثبیت شد؛ قانونی که ابزارهایی مانند تشخیص چهره، ارتباط با پایگاه‌های اطلاعاتی ثبت‌احوال و جمع‌سپاری در گزارش‌گیری دیجیتال را رسمیت بخشیده و به پلیس و دستگاه قضایی اختیارات قانونی در این حوزه داده است.

۲.۱.۴. قانون عفاف و حجاب؛ چارچوب قانونی برای نظارت دیجیتال در فضاهای عمومی

نقطه عطف سیاست‌های نظارتی جمهوری اسلامی ایران، تصویب قانون «حمایت از خانواده از طریق ترویج فرهنگ عفاف و حجاب» مشهور به قانون «عفاف و حجاب» در اکتبر ۲۰۲۳ است؛^{۹۵} قانونی که با هدف رسمی‌سازی اعمال پوشش اجباری در فضاهای عمومی، جایگاه حقوقی نظارت فناوریانه را تثبیت می‌کند. این قانون ادامه منطقی سه مصوبه پیشین شورای عالی انقلاب فرهنگی است که مسیر گذار از «تبلیغ فرهنگی» به «کنترل هوشمند» را در حوزه پوشش زنان ترسیم کرده‌اند.

مفاد مختلف این قانون، زیرساخت‌های لازم برای شناسایی و مدیریت هویتی شهروندان در فضاهای شهری را پیش‌بینی کرده‌اند. برای نمونه، ماده ۱۴ وزارت کشور را موظف می‌کند به تدوین «شناسنامه اجتماعی منطقه‌ای» اقدام کند؛ اقدامی که بستری برای مهندسی فرهنگی محلی فراهم می‌سازد. ماده ۲۳ از وزارت ارتباطات می‌خواهد روند توسعه «شبکه ملی اطلاعات» را تسریع کند و آن را زیر نظر شورای عالی فضای مجازی به پیش برد. در ماده ۲۵، نقش اطلاعاتی به وزارت اطلاعات و سازمان اطلاعات سپاه سپرده شده تا با بهره‌گیری از ظرفیت‌های دیجیتال، فعالان حوزه «کشف حجاب»، «برهنگی» یا ارسال تصاویر به رسانه‌های خارجی را شناسایی و پیگیری کنند.

سیاست‌های حاکمیتی در زمینه «عفاف و حجاب» از ابزارهای فرهنگی و تبلیغاتی، به‌سوی سازوکارهای اطلاعاتی، میدانی و فناوریانه حرکت کرده‌اند. در مصوبه ۸۲۰، برای نخستین بار بر «استفاده از فناوری‌های نوین»، «رصد آماری» و «گزارش‌گیری امنیتی» تأکید شده و مسئولیت سیاست‌گذاری از وزارت فرهنگ و ارشاد اسلامی به وزارت کشور منتقل شده است؛ تحولی که نشان از تغییر گفتمان از فرهنگ‌سازی به اعمال نظم دارد.^{۹۶}

کشته‌شدن مهسا امینی در سپتامبر ۲۰۲۲ ضمن به چالش کشیدن مشروعیت اجتماعی گشت ارشاد، «حجاب» را به محور مقاومت مدنی در ایران تبدیل کرد.^{۹۷} در واکنش به این بحران، سیاست‌گذاران در جمهوری اسلامی ایران، نه تنها از سیاست‌های قبلی عقب‌نشینی نکردند، بلکه با شتاب بیشتری به‌سوی هوشمندسازی و نامرئی‌سازی ابزارهای نظارتی رفتند. در همین چارچوب، سامانه‌هایی چون ثبت سیم‌کارت، کارت ملی هوشمند، پایگاه‌های داده قضایی و بانکی، دوربین‌های شهری و اپلیکیشن‌هایی برای جمع‌سپاری نظارت مانند «ناظر» وارد میدان شدند. اکنون، فناوری‌های دیجیتال در قالب قانون مشهور به «عفاف و حجاب» به ابزارهای رسمی شناسایی، پایش و سرکوب شهروندان بدل شده‌اند. در همین بازه زمانی، مقامات ارشد جمهوری اسلامی ایران به‌صراحت از به‌کارگیری ابزارهای دیجیتال برای اجرای قانون حجاب سخن گفته‌اند:

مجددالصالح هاشمی گلپایگانی، رئیس وقت ستاد امر به معروف، اعلام کرد که با دوربین‌های شهری و اتصال آن‌ها به سامانه‌های احراز هویت، پیامک هشدار برای زنان «بدحجاب» ارسال می‌شود.^{۹۸}

سردار پاسدار حسین اشتری، فرمانده وقت پلیس ایران (فراجا) از به‌کارگیری دوربین‌های شهری برای مقابله با «ناهنجاری‌های اجتماعی» سخن گفت.

موسی غضنفرآبادی، رئیس کمیسیون حقوقی و قضایی مجلس یازدهم شورای اسلامی (۲۰۲۰-۲۰۲۴) گفت: «برای کسانی که در ملأ عام کارهایی انجام می‌دهند و هنجارشکنی می‌کنند باید رویکردمان از اقدام فیزیکی به سمت چهره نگاری تغییر کند؛ در این صورت به فرد خاطی اعلام و او نیز از برخی از حقوق اجتماعی محروم می‌شود.»^{۹۹}

یکپارچه ملی، نیروهای امنیتی جمهوری اسلامی عمدتاً به سراغ راه‌حل‌های موضعی، ترکیبی و نامتوازن رفته‌اند. این مدل مبتنی بر استفاده از ظرفیت‌های محلی و پراکنده درون سازمان‌ها و شهرهاست؛ به‌گونه‌ای که در برخی فضاهای مشخص مانند ایستگاه‌های مترو یا مراکز تجاری، سامانه‌هایی برای پایش و شناسایی نصب شده‌اند، اما این سیستم‌ها فاقد انسجام ملی‌اند. در عین حال، در بسیاری از موارد، اجزای کلیدی این پروژه به‌جای توسعه بومی، از طریق واردات تامین می‌شوند؛ به‌ویژه در حوزه سخت‌افزارهای نظارتی مانند دوربین‌های شهری، سامانه‌های پلاک‌خوان و تجهیزات ذخیره‌سازی. زیرساخت امنیتی جمهوری اسلامی در این مرحله، که می‌توان آن را «مرحله پیش‌داده» (Pre-data) نامید،^{۹۸} شباهت‌هایی به مدل چینی دارد؛ مدلی که در آن تصویر، صدا، و موقعیت کاربر ذخیره می‌شود، اما هنوز اتصال کامل میان سامانه‌های تحلیلی و پایگاه‌های اطلاعاتی برقرار نشده‌است.

۱.۲.۴. ادعاها درباره استفاده از الگوریتم‌های چهره‌نگاری و میزان تحقق آن در ایران

پوشش رسانه‌ای رسمی و اظهارات مقام‌های ارشد جمهوری اسلامی ایران در سال‌های اخیر، تصویری از یک سامانه نظارتی پیشرفته ترسیم می‌کند که با بهره‌گیری از دوربین‌های مجهز به هوش مصنوعی و اتصال آنها به پایگاه‌های داده ملی، قادر به شناسایی هویت شهروندان در فضای عمومی و صدور خودکار هشدار یا اعمال جریمه است. در این چارچوب، الگوریتم‌های چهره‌نگاری به‌عنوان ابزار اصلی این سازوکار معرفی شده‌اند، به‌ویژه در زمینه کنترل پوشش زنان.^{۹۹}

با این حال، بررسی‌های میدانی و ارزیابی‌های ظاهری نشان می‌دهد این تصویر بیشتر از آنکه بازتاب واقعیت فنی باشد، بازتاب پروژه‌ای تبلیغاتی و بزرگ‌نمایی شده است. نشانه‌ای از اجرای عملیاتی و سراسری چنین الگوریتم‌هایی در سطح شهری وجود ندارد، بلکه در بهترین حالت، برخی پروژه‌های موضعی و در فضاهای محدود ممکن است پیاده‌سازی شده باشند (مانند مراکز تفریحی یا برخی معابر پرتردد).^{۱۰۰}

هرچند در بخش قبل به اصرار و تمایل حکومت جمهوری اسلامی ایران به بهره‌گیری مستقیم از الگوریتم‌های تشخیص چهره برای نظارت بدون واسطه بر شهروندان، براساس

مهم‌ترین بخش فناوریانه این قانون در ماده ۲۹ آمده است؛ جایی که پلیس جمهوری اسلامی ایران (فراجا) موظف شده با اتکا به ابزارهایی چون «دوربین‌های ثابت و سیار»، «هوش مصنوعی»، «گزارش‌های مردمی» و «سامانه‌های هویق»، به شناسایی و برخورد با افراد «بدحجاب» اقدام کند. این ماده نقطه پیوند تکنولوژی نظارتی با سیاست انتظامی جمهوری اسلامی است.

برای جبران شکاف‌های فناوریانه، در ماده ۳۱ سازمان بسیج به‌عنوان نیروی مکمل و انسانی برای «ضابطان قضایی» معرفی شده‌است. تبصره‌های ماده ۳۳ نیز نظارت پوششی را به عرصه‌های اشتغال و خدمات اجتماعی گسترش می‌دهد و رعایت حجاب را شرط لازم برای استخدام، ارتقاء، یا دریافت مجوز فعالیت قرار می‌دهد.

در نهایت، ماده ۶۴ این قانون بعد نهادی نظارت دیجیتال را تثبیت می‌کند؛ تمامی نهادهای دولتی، بانک‌ها، شرکت‌های خصوصی و حتی افراد حقیقی موظفند تصاویر دوربین‌های خود را در اختیار فراجا بگذارند و امکان دسترسی پلیس به اطلاعات هویق شهروندان از جمله شماره ملی، موبایل و مکان‌یابی را فراهم کنند. از این منظر، قانون «عفاف و حجاب» نه تنها یک سیاست فرهنگی یا انتظامی، بلکه چارچوبی حقوقی برای توسعه ساختاریافته حکمرانی دیجیتال در جمهوری اسلامی ایران است.

۲.۴. پیاده‌سازی تشخیص چهره در فضای عمومی: سیاست، فناوری و واقعیت میدانی

جمهوری اسلامی ایران، در چارچوب مصوبات رسمی و سازوکارهای فراقانونی، تلاش دارد با هدف تحمیل پوشش اجباری «حجاب»، نظامی فناوریانه برای شناسایی و احراز هویت شهروندان در فضاهای عمومی طراحی و اجرا کند. اما این پروژه بلندپروازانه در عمل چگونه پیش می‌رود؟ آیا آن‌گونه که تبلیغ می‌شود، سامانه‌های تشخیص چهره و فناوری‌های ردیابی دیجیتال به‌صورت گسترده و عملیاتی در ایران مستقر شده‌اند؟ یا همچنان با محدودیت‌هایی در سطح زیرساخت، توانمندی‌های فنی و توسعه الگوریتمی مواجه‌اند؟

واقعیت میدانی نشان می‌دهد که به جای یک سامانه

متصل شوند. در راس این واردات، تجهیزات نظارت تصویری از جمهوری خلق چین قرار دارد؛ کشوری که در حال حاضر بزرگ‌ترین صادرکننده زیرساخت‌های نظارتی به حکومت‌های اقتدارگراست.^{۱۳}

دوربین‌های هوشمند حتی در پیشرفته‌ترین نسخه‌ها، برای شناسایی هویت یا چهره طراحی شده‌اند و نه تفسیر دقیق رفتارهای اجتماعی. تحلیل اینکه آیا یک کنش خاص (مانند پوشش متفاوت یک زن) ناقض قانون است یا نه، همچنان به قضاوت انسانی یا الگوریتم‌هایی با قواعد بصری خشک وابسته است؛ مسئله‌ای که در ایران، مشابه تجربه چین، مانعی در مسیر اجرای تمام‌خودکار نظارت است.

با وجود این محدودیت‌های الگوریتمی، جمهوری اسلامی ایران همچنان در مسیر تجهیز زیرساخت‌ها حرکت می‌کند. بسیاری از شرکت‌های چینی تأمین‌کننده این فناوری‌ها در فهرست تحریم‌های آمریکا یا اتحادیه اروپا قرار دارند، اما نهادهای امنیتی و شهرداری‌های جمهوری اسلامی، با استفاده از واسطه‌های تجاری یا کانال‌های غیررسمی، فرآیند واردات، نصب و بهره‌برداری را ادامه می‌دهند.^{۱۴} این همکاری‌ها نه تنها زیرساخت فنی سرکوب داخلی را تقویت می‌کند، بلکه نشان‌دهنده همراستایی راهبردی با مدل چینی حکمرانی دیجیتال است؛^{۱۵} الگویی که در آن، اتصال سامانه‌های تصویرمحور با پایگاه‌های داده هویتی، به ابزار اصلی اعمال کنترل اجتماعی بدل می‌شود.^{۱۶}

شرکت‌های چینی و نمایندگی‌های متعدد و موازی آنها در ایران مانند شرکت Tiandy، شرکت Zhejiang Uniview، شرکت Hangzhou Hikvision، شرکت Zhejiang Dahua و ... در تأمین این زیرساخت‌ها برای نهادهای نظامی و امنیتی ایران نقش داشته‌اند و بعضی از آنها نیز در فهرست تحریم‌های آمریکا یا اتحادیه اروپا نیز قرار گرفته‌اند.

در کنار واردات تجهیزات نظارت تصویری، جمهوری اسلامی ایران همکاری‌های راهبردی با شرکت‌های بزرگ مخابراتی چینی همچون Huawei و ZTE در حوزه زیرساخت‌های ارتباطی و نظارتی برقرار کرده است. این همکاری‌ها شامل انتقال فناوری‌هایی است که امکان نظارت گسترده بر ارتباطات تلفنی، اینترنتی و موبایلی را فراهم می‌کند.^{۱۷} برای نمونه، در سال ۲۰۱۰ شرکت ZTE قراردادی به ارزش ۶/۹۸ میلیون یورو با شرکت مخابرات ایران (TCI) امضا کرد که شامل فروش

سیاست‌گذاری‌ها و ادبیات رسمی پرداختیم با این حال، پژوهش‌های مستقل و داده‌های قابل استناد تاکنون نشان نمی‌دهند که این سطح از شناسایی در فضای شهری به صورت فراگیر یا بلادرنگ (Real-time) در حال اجرا باشد. چنین تصاویری بیشتر در سطح نگرانی‌های افکار عمومی و سناریوهای آینده‌پژوهانه مطرحند و از پشتیبانی فنی یا تسهیلات کافی برای اجرا برخوردار نیستند.^{۱۸}

با این حال، تجربه‌های پیشین نشان می‌دهد که جمهوری اسلامی ایران می‌تواند پروژه‌هایی را که در ابتدا غیرواقعی یا تخیلی به نظر می‌رسند، در بازه‌ای بلندمدت و صرف هزینه هنگفت و مدام به مرحله اجرا برساند. نمونه برجسته، «شبکه ملی اطلاعات» است که از یک طرح مفهومی و بیان آرزوهای کلی در دهه ۲۰۰۰، به بستری عملیاتی برای تفکیک ترافیک اینترنت داخلی و خارجی در سال‌های اخیر تبدیل شد. در حوزه نظارت هویتی نیز اگرچه سامانه‌ای ملی برای تشخیص چهره در حال حاضر فعال نیست، اما ابزارهای دیگری مانند سامانه «ناظر»، ردیابی بر اساس پلاک خودرو و فناوری‌های ترکیبی مبتنی بر آنتن‌های پایه شبکه همراه (BTS) و IMSI-Catcher در حال آزمایش و گسترش هستند.^{۱۹}

در نتیجه، آنچه از سوی مقام‌های جمهوری اسلامی تحت عنوان «هوش مصنوعی» و «تشخیص چهره» تبلیغ می‌شود، نه یک سامانه سراسری و عملیاتی، بلکه مجموعه‌ای از پروژه‌های محدود، غیرشفاف و عمدتاً آزمایشی است که در غیاب یک الگوریتم ملی یا توان داخلی مؤثر، به سخری قابل اتکا هستند. با این حال، سرمایه‌گذاری حاکمیت در تصویب قوانین جدید، استفاده از فناوری‌های وارداتی و آماده‌سازی زیرساخت‌های اجرایی، حاکی از آن است که برنامه‌های مربوط به نظارت تصویری و شناسایی هویتی شهروندان در ایران، هرچند به کندی، اما در مسیری بلندمدت قرار گرفته‌اند که هدف نهایی آن، پیاده‌سازی الگویی ترکیبی از کنترل دیجیتال و فیزیکی در فضاهای عمومی است.

۲.۲.۴. واردات تجهیزات از چین با قابلیت اتصال به سامانه‌های چهره‌نگاری

در غیاب الگوریتم‌های بومی کارآمد برای تشخیص چهره در سطح ملی، تمرکز نیروهای امنیتی جمهوری اسلامی بر واردات تجهیزات است که بتوانند در آینده به چنین الگوریتم‌هایی

ارائه کرده که توانایی تحلیل تصاویر در زمان واقعی و تطبیق آن‌ها با پایگاه‌های داده را فراهم می‌کند.^{۱۱۱} همچنین، شرکت CloudWalk به دلیل صادرات فناوری‌های شناسایی چهره به کشورهایی با ریسک نقض حقوق بشر، مورد انتقاد قرار گرفته است. این شرکت به‌ویژه در حوزه تحلیل رفتار چهره و توسعه بانک‌های داده تصویری، نقش مؤثری در الگوی صادراتی چین برای نظارت دیجیتال ایفا کرده است.^{۱۱۲} جذابیت این فناوری‌ها برای جمهوری اسلامی ایران، به‌ویژه در حوزه شناسایی زنان بی‌حجاب یا افراد حاضر در تجمعات اعتراضی، به‌روشنی قابل مشاهده است. هر دو این شرکت‌ها در لیست تحریم‌های وزارت خزانه‌داری آمریکا قرار دارند.

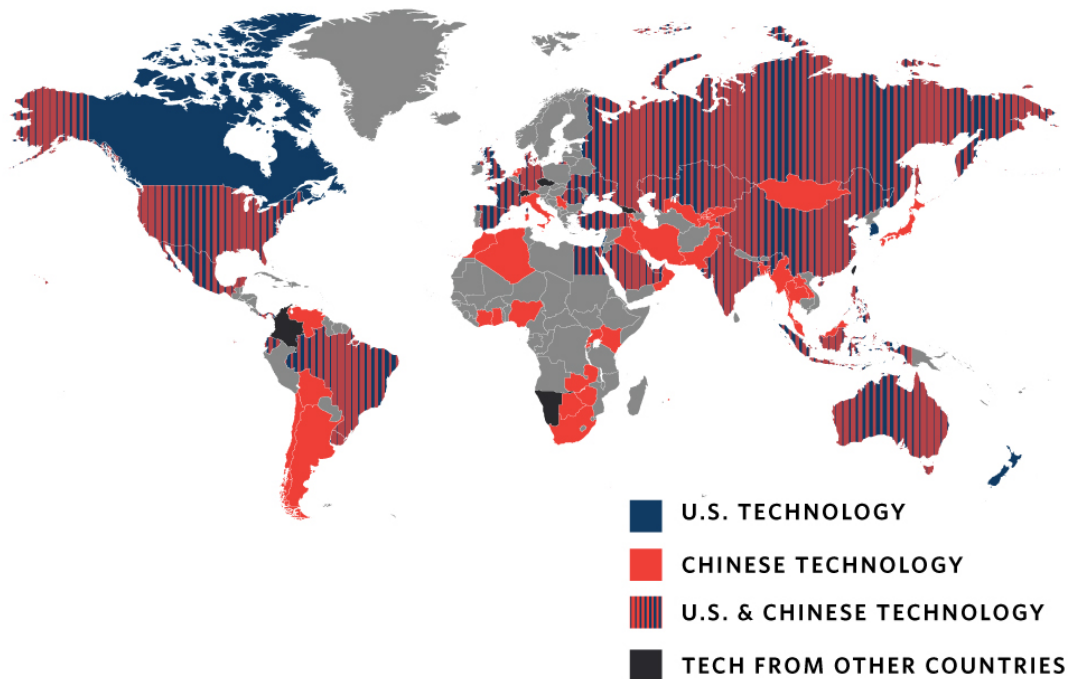
در نهایت، حتی در صورت عدم دسترسی فوری به الگوریتم‌های پیشرفته یا یکپارچه، در اختیار داشتن این سخت‌افزارها به‌معنای در اختیار داشتن مرحله نخست از اجرای سامانه‌های شناسایی چهره است. به بیان دقیق‌تر، ایران وارد مرحله پیش‌داده (pre-data) شده است؛

سیستم‌های نظارتی پیشرفته‌ای با قابلیت پایش مکالمات و اینترنت بود.^{۱۱۳} هرچند این همکاری‌ها با واکنش‌های منفی بین‌المللی روبرو شد، اما فعالیت‌های مشابه با شرکت Huawei نیز ادامه یافت؛ شرکتی که به فروش فناوری‌های نظارتی به ایران متهم شده و احتمالاً نقشی کلیدی در توسعه زیرساخت کنترل ارتباطات دیجیتال ایران دارد.^{۱۱۴}

هم‌زمان، نهادهای امنیتی جمهوری اسلامی ایران از تجربیات نظارتی دولت چین، به‌ویژه پروژه‌های گسترده‌ای مانند Skynet و فناوری‌های شرکت‌های چینی مانند Megvii و CloudWalk، الهام گرفته‌اند. پروژه Skynet که در چین با هدف نظارت تصویری بر فضاهای عمومی به اجرا درآمده، از ترکیب میلیون‌ها دوربین و الگوریتم‌های شناسایی چهره برای ردیابی لحظه‌ای شهروندان استفاده می‌کند و یکی از پیشرفته‌ترین سیستم‌های حکمرانی دیجیتال در جهان محسوب می‌شود.^{۱۱۵} شرکت Megvii با توسعه پلتفرم ++Face، الگوریتم‌هایی با دقت بالا در شناسایی چهره

MAP 1

AI Surveillance Technology Origin





شرکت یافتار پژوهان پیشتاز رایانش (تشخیص چهره در جستجوی اینترنتی و سانسور اینترنت)، شرکت خدمات انفورماتیک نیافام (طراحی و تولید مژول سخت‌افزاری تشخیص چهره در جستجوی اینترنتی)، شرکت داده‌پردازای دوران، شرکت کاوشگران همراه کیش (توسعه نوین همراه کیش در توسعه سامانه احراز هویت عینی غیرحضور و امضای الکترونیکی DIMooZ و توسعه اپلیکیشن ملی ایران پاس)، شرکت طرح و پردازش غدیر (اسکرهای بیومتریکی، احراز هویت پورتابل و نرم افزارهای احراز هویت)، امن‌افزارگستر شریف (سامانه پارس‌پم)، شرکت داتین (داتیس آیرین قشم در توسعه نرم‌افزار ویپاد dopeW)، فن‌آوران اطلاعات پیشخوان ایرانیان (احراز هویت غیرحضور یا الکترونیکی با سامانه سجام و برند آی‌سیگنال)، شرکت پردازش مالی پارت (پلتفرم فراشناسا)، شرکت گیاهوشان آریا (ویدا)، شرکت شاهراه کلید اعتماد (شاکیلید و سامانه آشنامی)، شرکت مهندسی آدان‌نیک افزار (آدانیک) شرکت بینش هوشمند نسل پیشرو (یو آیدی)، شرکت سپید سیستم شریف (سپید آی‌دی، سپید استار و سپید باکس محصولات احراز هویت دیجیتال با اثر انگشت و تشخیص چهره، اسکن عنبیه)، شرکت رادین (از زیرمجموعه حصین)، شرکت به‌پرداز جهان (سامانه مرزن‌نشینی و سامانه تار یا تجارت تک‌پنجره الکترونیک)

اجرای آزمایشی این الگوریتم‌ها عمدتاً در محیط‌های نیمه‌بسته و کنترل‌شده صورت گرفته‌است. برای مثال، برخی پایگاه‌های خبری به استفاده از سامانه‌های هوش مصنوعی تشخیص چهره در مراکز تجاری، ایستگاه‌های مترو و تقاطع‌های شهری اشاره کرده‌اند. اما شواهد میدانی نشان می‌دهد که این سیستم‌ها اغلب به مرحله بهره‌برداری کامل نرسیده‌اند و بیشتر در سطح آزمایش‌های موضعی باقی مانده‌اند. نبود زیرساخت‌های تحلیل داده متمرکز، فقدان الگوریتم‌های بومی پایدار و مشکلات اتصال سامانه‌ها به پایگاه‌های داده هویتی، مانع از اجرای ملی این پروژه‌ها شده‌است.

مرحله‌ای که در آن داده‌های خام مانند تصویر، مکان و صوت ثبت می‌شوند، اما هنوز اتصال یکپارچه آن‌ها به موتورهای تحلیلی و تصمیم‌سازی فراهم نشده است. با این حال، همین زیرساخت می‌تواند به‌زودی مسیر را برای پیاده‌سازی الگوریتم‌های بومی یا وارداتی تسهیل کند و فصل جدیدی در حکمرانی دیجیتال مبتنی بر نظارت تصویری در ایران رقم بزند.

۳.۲.۴. توسعه بومی تشخیص چهره: پروژه‌ها، بازیگران و آزمون‌های میدانی

در نبود دسترسی گسترده به الگوریتم‌های پیشرفته و در شرایط تحریم فناوری، جمهوری اسلامی ایران مسیر بومی‌سازی فناوری تشخیص چهره را از طریق شبکه‌ای از شرکت‌های خصوصی، مراکز تحقیقاتی و نهادهای حکومتی دنبال کرده است. این روند اغلب تحت پوشش پروژه‌های «دانش‌بنیان» و «تحقیقات کاربردی» پیش می‌رود، اما در عمل با نهادهای امنیتی و قضایی در ارتباط مستقیم قرار دارد. تمرکز اصلی این پروژه‌ها، توسعه الگوریتم‌های یادگیری ماشین برای تحلیل چهره، تطبیق تصویر با داده‌های هویتی، و نظارت بر کنش‌های عمومی در فضاهای شهری است.^{۱۱۳}

از جمله شرکت‌های شناخته‌شده در این حوزه می‌توان به یافتار پژوهان پیشتاز رایانش اشاره کرد که سابقه همکاری با دادستانی کل کشور در زمینه فیلترینگ هوشمند را دارد. همچنین، گزارش‌های میدانی نشان می‌دهد که برخی پروژه‌ها از سوی نهادهایی چون سازمان پدافند غیرعامل، وزارت اطلاعات، و پلیس فتا به شرکت‌های خصوصی یا گروه‌های دانشگاهی واگذار شده‌اند. در این میان، پروژه‌هایی با محوریت «تحلیل تصویر»، «نظارت رفتاری» و «تشخیص هویت چهره‌محور» به‌ویژه در بسترهایی نظیر معابر شهری، مراکز خرید، و سیستم حمل‌ونقل عمومی مورد آزمون میدانی قرار گرفته‌اند.^{۱۱۴}

پروژه‌های بومی جمهوری اسلامی ایران اگرچه در مراحل ابتدایی توسعه‌اند، اما از حمایت مالی و قانونی برخوردارند و به‌ویژه در محیط‌هایی با بار امنیتی بالا به‌صورت موضعی پیاده‌سازی شده‌اند. این پروژه‌ها به جمهوری اسلامی امکان می‌دهند تا حتی در غیاب فناوری‌های وارداتی پیشرفته، نوعی سیستم نیمه‌خودکار شناسایی هویت را در سطح محدود فعال کند.^{۱۱۵}

۴.۲.۴. زیرساخت‌های هویتی و نظارت شهری؛ اتصال داده‌ها، دوربین‌ها و پایگاه‌های ملی

در حالی که الگوریتم‌های تشخیص چهره هنوز به‌طور گسترده در فضای عمومی ایران اجرایی نشده‌اند، شبکه زیرساختی نظارت شهری و پایگاه‌های داده ملی به‌عنوان ستون فقرات پروژه کشف هویت شهروندان عمل می‌کنند. در نظام نظارت شهری جمهوری اسلامی ایران، نهادهایی چون شهرداری‌ها، وزارت راه و شهرسازی، بانک‌ها و نیروی انتظامی از طریق دوربین‌های شهری، جاده‌ای و بانکی، شبکه‌ای گسترده از پایش تصویری ایجاد کرده‌اند. هرچند این شبکه در ابتدا با اهدافی چون کنترل ترافیک و امنیت بانکی راه‌اندازی شد، اما اکنون به ابزار کلیدی برای شناسایی شهروندان در فضای عمومی بدل شده است.^{۱۱۶}

یکی از اجزای کلیدی نظام شناسایی در جمهوری اسلامی ایران، شبکه گسترده دوربین‌های نظارتی شهری، جاده‌ای و بانکی است که در سال‌های اخیر با هدف پوشش نقاط پرتردد در سطح معابر عمومی گسترش یافته است. این شبکه که در ابتدا برای کنترل ترافیک و ثبت تخلفات رانندگی ایجاد شده بود، اکنون در خدمت اهداف امنیتی قرار گرفته است.

یکی از اجزای مهم این شبکه، سامانه «سپتام» (سامانه یکپارچه پایش تصویری کشور) است که تصاویر دوربین‌های متعدد از معابر، پاساژها و مراکز دولتی را جمع‌آوری و به نیروی انتظامی متصل می‌کند.^{۱۱۷} طبق ماده ۶۴ قانون عفاف و حجاب، کلیه نهادهای عمومی، فروشگاه‌ها، و بانک‌ها موظف‌اند تصاویر نظارتی خود را در اختیار پلیس جمهوری اسلامی ایران (فراجا) بگذارند.^{۱۱۸} سامانه «سپتام» (سامانه پایش تصویری اماکن عمومی) یک بستر نظارتی است که با همکاری پلیس نظارت بر اماکن عمومی و درگاه ملی مجوزها ایجاد شده است. هدف این سامانه، استانداردسازی، تایید و نظارت بر سیستم‌های نظارت تصویری در واحدهای صنفی و اماکن عمومی اعلام شده است.

سپتام به‌عنوان یک نهاد ناظر، کیفیت سیستم‌های حفاظتی (دوربین) واحدهای صنفی را بررسی و تایید می‌کند. این تاییدیه‌ها بر اساس استانداردهای آزمایشگاهی صادر می‌شوند. بازرسان سپتام بر نحوه اجرای فرایند نصب و جانمایی دوربین‌ها نظارت دارند. با نصب دوربین‌های مذکور، در صورت بروز اتفاق یا جرم در محل واحدهای صنفی و

اماکن عمومی، پلیس اماکن می‌تواند اطلاعات ضبط‌شده را بررسی و موضوع را پیگیری کند. واحدهای صنفی از طریق درگاه ملی مجوزها به سامانه پلیس اماکن لینک داده می‌شوند و با مراجعه به سامانه سپتام از مشخصات فنی دوربین ویژه آن صنف مطلع می‌شوند. پس از تایید سیستم نظارت تصویری، سپتام چند عدد دوربین (بسته به نیاز) در محیط صراف یا واحد صنفی نصب می‌کند که تصاویر این دوربین‌ها در فضای ابری و ارائه‌شده از سوی سپتام ذخیره می‌شوند. سامانه سپتام با این ساختار به پلیس اماکن می‌دهد تا در صورت نیاز، به اطلاعات تصویری مکان‌های خصوصی دسترسی داشته باشد.

زیرساخت داده‌ای پروژه‌های نظارتی در ایران، متکی بر چندین پایگاه ملی است که داده‌های بیومتریک و شناسنامه‌ای شهروندان را در خود جای داده‌اند. کارت ملی هوشمند (سامانه هدا)، پایگاه‌های ثبت احوال، پایگاه‌های اجرای هویت مانند ثنا، گواهینامه رانندگی و پاسپورت و بانک‌ها همگی از جمله منابع داده‌ای هستند که امکان جمع‌آوری داده‌های تصویری لازم را دارند.

۴.۳. شیوه‌های ترکیبی و اجرای میدانی؛ شبکه‌های داده‌ای متصل به هویت دیجیتال

در سال‌های اخیر، سیاست نظارت شهری در جمهوری اسلامی ایران از یک مدل تماماً انسانی و چهره‌به‌چهره، به سمت ساختارهای ترکیبی حرکت کرده است که در آن، فناوری و نیروی انسانی در کنار یکدیگر برای کشف هویت و کنترل اجتماعی به‌کار گرفته می‌شوند. اگرچه روش‌های انسانی مانند گشت ارشاد، گزارش میدانی بسیج، یا مشاهده حضوری نیروهای امنیتی همچنان مورد استفاده‌اند، اما این روش‌ها با چالش جدی «مقیاس‌پذیری» مواجه‌اند. به‌ویژه در مواجهه با نافرمانی‌های مدنی گسترده، حکومت نمی‌تواند در تمام نقاط شهری نیرو مستقر کند یا واکنش لحظه‌ای نشان دهد. به همین دلیل، مدل جدیدی پیاده‌سازی شده است: انسان به‌عنوان نقطه آغاز زنجیره نظارت، گزارش می‌دهد؛ فناوری داده را ثبت و تحلیل می‌کند؛ و سیستم پیامک هشدار یا جریمه، نتیجه را به فرد اعلام می‌کند، بدون نیاز به حضور فیزیکی نیروهای امنیتی.

دیجیتال شهروندان در فضاهای عمومی است. اگر الگوریتم‌های تشخیص چهره را «چشم» و سخت‌افزارهای چینی را «بدن» این پروژه بدانیم، زیرساخت‌های داده‌ای، نقش «مغزو حافظه» آن را ایفا می‌کنند. بدون این زیرساخت، اتصال تصویر به هویت ممکن نیست و با توسعه آن، حتی در غیاب الگوریتم‌ها نیز شناسایی تا حد زیادی عملیاتی می‌شود.

۱.۳.۴. نقش قرارگاه ۱۲ تیر و اقدامات میدانی سپاه و بسیج

در واکنش به اعتراضات شهری و چالش حجاب اجباری، ساختارهای امنیتی جمهوری اسلامی ایران اقدام به راه‌اندازی سازوکارهای میدانی هماهنگ‌تری کرده‌اند. یکی از مهم‌ترین آن‌ها، قرارگاه ۲۱ تیر است که به صورت رسمی زیرمجموعه ستاد امر به معروف تعریف شده و در هماهنگی با سپاه پاسداران و بسیج، وظیفه «سازمان‌دهی نیروهای داوطلب برای مواجهه با بدحجابی» را بر عهده دارد.^{۱۳۰} این قرارگاه، با صدور دستورالعمل‌ها و برگزاری دوره‌های آموزشی، هزاران نیروی بسیجی را برای شناسایی زنان «بدحجاب» در سطح شهرها ساماندهی کرده و از طریق ابزارهایی مانند کارت‌های ضابط، آن‌ها را در اجرای قانون عفاف و حجاب مشارکت می‌دهد. گزارش مرکز پژوهش‌های مجلس نیز صراحتاً به مشارکت «بسیجیان ضابط» در کنار نیروهای انتظامی در اجرای قانون اشاره دارد و ماده ۳۱ قانون عفاف و حجاب، این وظیفه را به بسیج محول کرده است.

۲.۳.۴. اپلیکیشن ناظر؛ جمع سپاری نظارت

یکی از ابزارهای کلیدی برای تبدیل گزارش مردمی به داده عملیاتی، اپلیکیشن ناظر است که توسط نیروی انتظامی جمهوری اسلامی توسعه داده شده است.^{۱۳۱} این اپلیکیشن به کاربران اجازه می‌دهد که تصاویر، ویدیو یا موقعیت افراد «بدحجاب» یا «هنجارشکن» را به طور مستقیم به پلیس ارسال کنند. این داده‌ها سپس در سیستم پلیس تحلیل شده و منجر به صدور پیامک هشدار یا جریمه می‌شود. طبق گزارش‌ها، اپلیکیشن ناظر با سامانه‌های تشخیص هویت و ثبت خودرو نیز تلفیق شده است و پلیس از طریق آن می‌تواند اطلاعات مالک خودرو یا شماره ملی فرد را بازیابی کند.^{۱۳۲}

این تحول نه فقط به معنای کاهش نقش انسان نیست، بلکه نشان‌دهنده تغییر کیفیت این نقش است: انسان از عامل اجرایی به نقطه آغاز یک زنجیره پردازش داده تبدیل شده است. چنین الگوی ترکیبی، به نهادهای امنیتی جمهوری اسلامی این امکان را می‌دهد که بدون نیاز به نظارت دائمی در محل، با تکیه بر ارتباط بین پایگاه‌های داده و ابزارهای ثبت مکان و چهره، به شناسایی، هشدار و مجازات شهروندان بپردازند. در این فصل، اجزای این مدل ترکیبی، سامانه‌های پشتیبان، و شواهد اجرای میدانی آن را مرور می‌کنیم.

هدف از توسعه این زیرساخت‌ها، ایجاد یک نظام یکپارچه برای کشف هویت شهروندان در محیط‌های عمومی است. در این مدل، شناسایی از مسیر تصویر (دوربین شهری)، داده (کارت ملی، سیم‌کارت)، و اتصال تحلیلی (مانند سامانه‌های قضایی یا انتظامی) صورت می‌گیرد. حتی در غیاب الگوریتم‌های هوشمند، اتصال این اجزا با یکدیگر، امکان شناسایی فرد از طریق پلاک خودرو، شماره تماس، یا محل سکونت را فراهم می‌سازد. این سیستم‌ها عملاً به عنوان جایگزین یا مکمل تشخیص چهره در پروژه‌های میدانی عمل می‌کنند، رویکردی که در گزارش‌های بین‌المللی نیز به آن اشاره شده است.^{۱۱۹}

نمونه‌هایی از اتصال این داده‌ها در پروژه‌هایی مانند سامانه سپتام (اداره اماکن نیروی انتظامی) دیده می‌شود که به گزارش‌های مردمی یا تصاویر دوربین‌ها استناد می‌کند و از طریق اتصال به داده‌های ثبت‌شده، افراد را به سیستم‌های بازجویی یا قضایی معرفی می‌کند. همچنین سامانه شاهکار برای تطبیق سیم‌کارت با شماره ملی و سامانه همتا برای ردیابی گوشی‌های موبایل از دیگر اجزای این شبکه در حال توسعه‌اند.

در واقع، این زیرساخت‌ها با یکدیگر یک «نظام داده‌محور شناسایی» را شکل داده‌اند که حتی در غیاب الگوریتم‌های پیچیده تشخیص چهره نیز امکان کشف هویت را فراهم می‌کند. این شبکه، به تعبیر گزارش‌های بین‌المللی، مدل ترکیبی شناسایی در فضای عمومی است که در آن داده‌های پراکنده، از پلاک خودرو گرفته تا تلفن همراه و کارت ملی، در خدمت نظارت حکومتی قرار می‌گیرند.

چنین سیستمی، در کنار پروژه‌های سخت‌افزاری و الگوریتمی، ستون سوم پروژه امنیتی جمهوری اسلامی برای شناسایی

۳.۳.۴. چهره‌نگاری به‌عنوان مکمل سامانه‌های داده‌محور

از این منظر، الگوریتم‌های چهره‌نگاری نه نقطه آغاز، بلکه نقطه تکمیل یک شبکه شناسایی هستند که پیش‌تر از طریق اتصال داده‌های ملی، بانکی، ارتباطی و ویدئویی فعال شده‌است. جمهوری اسلامی ایران در مرحله‌ای قرار دارد که شناسایی نیمه‌خودکار در فضاهای عمومی را از طریق تلفیق داده و نظارت تصویری عملیاتی کرده‌است حتی اگر ادعای بهره‌گیری از الگوریتم‌های هوش مصنوعی هنوز اغراق‌آمیز باشد.

در فرآیند شناسایی ترکیبی، ابزارهایی مانند IMSI-catcher صرفاً نقطه آغاز هستند. این ابزارها با شبیه‌سازی دکل‌های مخابراتی، شماره موبایل یا شناسه IMSI شهروندان را جمع‌آوری می‌کنند، اما بدون اتصال به پایگاه‌های اطلاعاتی دولتی، این داده‌ها به‌تنهایی فاقد ارزش هویقی هستند.^{۱۳۴} برای تبدیل داده‌های خام ارتباطی به پروفایل‌های شناسایی‌شده، جمهوری اسلامی از سامانه‌های واسطی استفاده می‌کند که قابلیت تطبیق شماره موبایل یا سایر شناسه‌های ارتباطی با اطلاعات شناسنامه‌ای، خانوادگی، قضایی یا مالی شهروندان را دارند.

سامانه‌هایی مانند همتا (برای رجیستری گوشی و سیم‌کارت)، شاهکار (برای تطبیق کد ملی و سیم‌کارت)، سیام (برای احراز بانکی)، هُدا (برای خدمات دولتی)، ثنا (برای اطلاعات قضایی)، و اشراف (به‌عنوان سیستم نظارت اطلاعاتی) در واقع نقش لایه تحلیلی را در این ترکیب ایفا می‌کنند. اتصال این سامانه‌ها به ابزارهای میدانی مانند دوربین یا IMSI-catcher، امکان کشف سریع هویت، موقعیت مکانی، سوابق قضایی و حتی مشخصات خانواده فرد را برای نهادهای امنیتی فراهم می‌کند.

پس از اصفهان، گزارش‌های پراکنده‌ای از اجرای مدل‌های مشابه در شهرهای دیگر نیز منتشر شده‌است. به‌عنوان مثال، در استان گیلان و شهر رشت، گزارش‌هایی از استقرار دوربین‌های جدید و ارسال پیامک به رانندگان منتشر شد. در شیراز و تهران نیز فعالان محلی اشاره کرده‌اند که به‌ویژه در مناطق پرتردد یا تجاری، رفتار نیروهای امنیتی مشابه الگویی است که در اصفهان دیده شده‌است: مشاهده، ثبت تصویر، استخراج شماره پلاک یا موبایل، و سپس هشدار یا اقدام قضایی. این شواهد نشان می‌دهد که جمهوری اسلامی، به‌جای ساخت یک سیستم ملی واحد، در حال توسعه «پایگاه‌های نظارت محلی» است که به ابزارهای داده‌ای

در کنار پروژه‌های الگوریتمی و واردات سخت‌افزار، یکی از استراتژی‌های محوری جمهوری اسلامی ایران، اتصال داده‌های هویقی به زیرساخت‌های نظارت تصویری و مخابراتی است. برخلاف تصور رایج، کشف هویت شهروندان لزوماً نیازمند سامانه‌های پیچیده تشخیص چهره نیست، بلکه اتصال میان اجزای مختلف داده‌محور، از کارت ملی هوشمند و ثبت‌نام سیم‌کارت گرفته تا سامانه شاهکار و سامانه همتا می‌تواند در نبود الگوریتم تشخیص چهره نیز کار شناسایی را انجام دهد.^{۱۳۵}

برای نمونه، در سیستم ارسال پیامک هشدار حجاب که طی سال ۲۰۲۵ در شهرهایی مانند مشهد، تهران، شیراز و اصفهان اجرا شد، شناسایی افراد نه از طریق چهره‌نگاری، بلکه با تحلیل پلاک خودرو، مالکیت آن، شماره تماس و تطبیق آن با سوابق ثبت‌احوال انجام شد. این مکانیزم نشان می‌دهد که دوربین‌های شهری وقتی به پایگاه‌های داده ملی متصل شوند، نقش مکمل الگوریتم‌های تشخیص چهره را بازی می‌کنند.

سامانه‌هایی مانند شاهکار (برای تطبیق شماره ملی با سیم‌کارت)، همتا (برای ردیابی دستگاه‌های موبایل)، سیم‌کارت‌های احراز شده با کارت ملی هوشمند، و دوربین‌های شهری متصل به سیستم‌های ثبت تخلف راهنمایی و رانندگی، همگی زیرساخت‌هایی هستند که در کنار هم، امکان کشف هویت را بدون استفاده از الگوریتم‌های پیشرفته فراهم می‌کنند.

به‌ویژه در اجرای قانون جدید «عفاف و حجاب»، مقررات جدید الزام‌آور دستگاه‌های مختلف برای اتصال داده‌های هویقی به دوربین‌های شهری و سامانه‌های مخابراتی، بر این الگوی ترکیبی تأکید دارد. ماده ۶۴ این قانون، همه سازمان‌ها و شرکت‌های خدمات‌رسان عمومی را مکلف می‌کند تصاویر دوربین‌های خود را در اختیار پلیس قرار دهند و امکان دسترسی به شماره ملی، مکان‌یابی، شماره تماس و سایر داده‌ها را نیز فراهم سازند. این سیاست در واقع تأکید می‌کند که حتی بدون یک الگوریتم تشخیص چهره دقیق، داده‌های پراکنده اما مرتبط با هویت شهروندان برای دستگاه امنیتی کفایت می‌کند.

۴.۴. تحلیل پیامدها و سطح بلوغ این مدل‌ها برای شناسایی معترضان در آینده

در تحلیل نهایی، استفاده جمهوری اسلامی ایران از شیوه‌های ترکیبی نظارت برای شناسایی هویت شهروندان در فضاهای عمومی، نشانگر گذار از نظارت سنتی به یک مدل نیمه‌دیجیتال و چندلایه است. اما آیا این سیستم‌ها برای اجرای فراگیر، مستمر و در سطح ملی آماده‌اند؟

واقعیت این است که مدل فعلی هنوز در سطحی پیش‌ابلوغ قرار دارد؛ زیرساخت‌های پراکنده، نبود یکپارچگی نرم‌افزاری، و محدودیت‌های فنی و حقوقی، مانع از تحقق نظارت هوشمند در سطحی مشابه مدل چینی شده‌اند. استفاده از ابزارهایی نظیر IMSI-catcher، الگوریتم‌های ساده چهره‌نگاری، یا داده‌های موبایل، اغلب در مقیاس‌های موضعی و با اهداف تاکتیکی (مانند سرکوب معترضان زن یا رهگیری فعالان مشخص) صورت می‌گیرد و هنوز از یک مدل کلان و کاملاً هماهنگ فاصله دارد.

با این‌حال، جهت‌گیری کلی حکومت جمهوری اسلامی به سمت توسعه چنین سیستم‌هایی کاملاً روشن است. تجربه پروژه‌هایی مانند شبکه ملی اطلاعات و نهادهای نظارت بی‌وقفه در حوزه عفاف و حجاب نشان داده‌اند که عدم کارآمدی کوتاه‌مدت، مانع سرمایه‌گذاری بلندمدت نیست. تمرکز تدریجی بر توسعه APIهای داخلی بین سامانه‌ها، خرید زیرساخت از چین، و حمایت قانونی از اتصال‌پذیری داده‌ها، همه نشانگر تلاش حکومت برای گذر از مرحله آزمایشی به مرحله عملیاتی پایدار در آینده است.

۵. اشاعه جهانی فناوری‌های نظارت، تجسس، سانسور و سرکوب اینترنت

آورده است. این همکاری‌ها ابعاد مختلفی از جمله اقتصادی، نظامی، امنیتی و فناوری را در بر می‌گیرد و بستر مناسبی برای تبادل دانش و تجهیزات، از جمله در حوزه کنترل و نظارت بر فضای سایبری، فراهم می‌کند.

۱.۵. بستر راهبردی و انگیزه‌های صدور

توافق‌نامه‌های راهبردی و امنیتی بلندمدت با قدرت‌هایی مانند چین و روسیه، بستر مناسبی را برای تبادل فناوری، در حوزه‌های مختلف از نظارت و امنیت سایبری تا توانایی‌های سایبری تهدیدآمیز و آفندی فراهم کرده‌اند. توافق ۲۵ ساله با چین^{۱۲۸} که شامل همکاری‌های اقتصادی، نظامی و امنیت سایبری است، به طور مشخص به انتقال فناوری‌هایی اشاره دارد که برای نظارت و کنترل داخلی به کار گرفته می‌شوند.^{۱۲۹}

برای نمونه، در ضمیمه شماره (۱) اهداف اصلی؛ به توسعه همکاری‌ها در زمینه فناوری‌های ارتباطی و اطلاعاتی اشاره کرده و به خصوص به «حوزه‌های مختلف فضای مجازی. تجهیزات کاربر نهایی» اشاره دارد. همچنین در ضمیمه شماره (۲) عناوین اصلی برای همکاری‌های جامع ۲۵ ساله؛ بند د - همکاری در زمینه فناوری ارتباطات از راه دور، توسعه ارتباطات نسل پنجم، خدمات اساسی (موتورهای جستجو، پست الکترونیک و پیام‌رسان‌های اجتماعی)، تجهیزات ارتباط از راه دور (مسیریاب جی‌پی‌اس، سوئیچ، سرور و ذخیره اطلاعات)، تجهیزات کاربر نهایی (موبایل، تبلت و لپ‌تاپ)، سیستم عامل

جمهوری اسلامی ایران سابقه‌ای طولانی در به‌کارگیری فناوری برای کنترل فضای اطلاعاتی داخلی و سرکوب مخالفت‌ها دارد. این رویکرد که با توسعه زیرساخت‌های ملی مانند شبکه ملی اطلاعات (NIN) و اعمال سانسور گسترده اینترنت همراه بوده، در سال‌های اخیر با پیچیدگی و ابعاد بیشتری دنبال شده است.^{۱۲۶} همزمان، جمهوری اسلامی ایران در عرصه بین‌المللی نیز به دنبال تقویت جایگاه خود از طریق ایجاد شراکت‌های راهبردی و حضور در مجامع تصمیم‌گیر بوده است. این موضوع نیز از همان ابتدای ورود اینترنت به ایران در سال ۱۹۹۸ به دستور علی خامنه‌ای در فرمان هفت ماده‌ای با نام «سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه‌ای گنجانده شده بود»^{۱۲۷}

بند ۷: اقدام مناسب برای دستیابی به میثاق‌ها و مقررات بین‌المللی و ایجاد اتحادیه‌های اطلاع‌رسانی با سایر کشورها به‌ویژه کشورهای اسلامی به‌منظور ایجاد توازن در عرصه اطلاع‌رسانی بین‌المللی و حفظ و صیانت از هویت و فرهنگ ملی و مقابله با سلطه جهانی.

این دو روند یعنی کنترل داخلی و نفوذ خارجی، می‌توانند در نقطه «صدور فناوری‌های کنترل و نظارت اینترنتی» به هم برسند. جمهوری اسلامی ایران در راستای مقابله با فشارهای بین‌المللی و پیشبرد اهداف منطقه‌ای و جهانی خود، به تقویت همکاری با کشورهای همسو، به ویژه چین و روسیه، روی

کامپیوتر و موبایل، آنتی‌ویروس، هوش مصنوعی و ... از موارد این توافق‌نامه ذکر شده‌است.

گزارش‌ها حاکی از آن است که چین به ایران در استقرار سانسور اینترنتی بیشتر کمک کرده و شرکت‌های چینی مانند ZTE و هواوی در فروش سیستم‌های نظارتی پایش ارتباطات خطوط ثابت، موبایل و اینترنت و توسعه زیرساخت‌های ارتباطی ایران نقش داشته‌اند.^{۱۳۲} این همکاری‌ها، که در چارچوب ابتکار «کمربند و جاده» چین نیز قرار می‌گیرند، نگرانی‌ها را در مورد الگوبرداری ایران از مدل کنترل اینترنت چین (دیوار آتش بزرگ) و استفاده از فناوری‌های مشابه برای سرکوب افزایش داده‌است.^{۱۳۱}

به طور مشابه، توافق‌نامه جامع راهبری (امنیتی - ۲۰۲۵)^{۱۳۲} و توافق‌نامه امنیت اطلاعات (سایبری - ۲۰۲۱)^{۱۳۳} با روسیه بر همکاری در زمینه امنیت اطلاعات، مقابله با جرایم سایبری و تبادل تخصص در مدیریت اینترنت ملی تأکید دارند.^{۱۳۴}

در توافق‌نامه امنیتی، در ماده ۴ به ارتقا سطح همکاری نهادهای اطلاعاتی و امنیتی ایران و روسیه برای تبادل اطلاعات و تجربیات و اشاره کرده و می‌گوید: «نهادهای اطلاعاتی و امنیتی طرف‌های متعاقد در چارچوب موافقت‌نامه‌های جداگانه همکاری خواهند کرد.»

در همین توافق‌نامه، ماده ۱۱ بند ۱ به اقدام طرفین در چارچوب «توافق‌نامه همکاری در امنیت اطلاعات» رسمیت می‌بخشد. متن لایحه این توافق‌نامه همکاری در ژانویه ۲۰۲۱ افشا شد. اما پس از تصویب در کابینه در جولای ۲۰۲۲، به مجلس ایران رفت و در ژوئن ۲۰۲۴ تصویب و منتشر شد.

در ماده ۱۱ به توسعه مشترک و تبادل فناوری‌هایی تأکید شده که منجر به پیاده‌سازی و تقویت شبکه‌های داخلی محدود و در کنترل حکومت (در هر دو کشور ایران و روسیه) می‌شود. «تقویت حاکمیت ملی در فضای اطلاعاتی بین‌المللی»، مقابله با «تلاش برای محدود کردن حق حاکمیتی برای تنظیم و تضمین ایمنی بخش‌های ملی شبکه جهانی» و «تبادل تجربیات در مدیریت بخش‌های ملی شبکه اینترنت و توسعه زیرساخت‌ها» در مفاد این ماده آمده که همگی ناظر به توسعه سیستم‌هایی هستند که مشابه آنها برای نظارت و تجسس بر شهروندان ایرانی توسعه پیدا کرده‌است.

در توافق‌نامه سایبری، جزئیات این همکاری مشخص شده‌است. در ماده ۲ این توافق‌نامه شش تهدید امنیت اطلاعات برای دو طرف ذکر شده از جمله انتشار محتوای تبلیغاتی که برای «نظام‌های اجتماعی، سیاسی، اقتصادی و محیط معنوی و اخلاقی» دولت‌ها زیان‌بار است.

در ماده ۳ این توافق‌نامه امکان تبادل فناوری‌های لازم، کمک‌های فنی و همکاری بین‌المللی برای «غلبه بر تهدیدات ماده ۲» فراهم شده که متضمن به اشتراک‌گذاری تجربیات، سیستم‌ها، فناوری‌ها و روش‌هایی طرفین در «نظارت و تجسس» در زندگی شهروندان است. این توافق‌نامه همکاری، امکان صادرات فناوری‌های سرکوب و تجسس از زندگی شهروندان را برای طرفین ایجاد می‌کند.

هر دو کشور، منافع مشترکی در ترویج مدل‌های کنترل دولتی بر اینترنت و مقابله با آنچه «نفوذ غربی» می‌خوانند، دارند. روسیه به امنیت سایبری جمهوری اسلامی ایران کمک می‌کند و شرکت‌های فناوری روسی، از جمله شرکت‌های تحریم‌شده مانند Positive Technologies، با وزارت ارتباطات ایران برای صادرات فناوری روسی و همکاری در زمینه امنیت سایبری و مخابرات دیدار و گفتگو کرده‌اند.^{۱۳۵} تلاش روسیه برای ایجاد «اینترنت مستقل» و تلاش ایران برای تکمیل «شبکه ملی اطلاعات» اهداف مشابهی را در جهت افزایش کنترل حکومتی اینترنت دنبال می‌کنند.

حضور ایران در مجامع بین‌المللی مانند اتحادیه بین‌المللی مخابرات (ITU) نیز فرصتی برای ترویج دیدگاه‌های خود در زمینه حاکمیت اینترنت و به چالش کشیدن مدل‌های بازتر فراهم می‌کند.^{۱۳۶} شکایت ایران از استارلینک به ITU و تلاش برای الزام این شرکت به رعایت قوانین داخلی ایران، نمونه‌ای از این تلاش‌ها برای گسترش کنترل دولتی بر فضای سایبری، حتی فراتر از مرزهای فیزیکی است.^{۱۳۷}

این مجموعه از توافق‌ها، همکاری‌ها و سازوکارهای نهادی، بستری را ایجاد می‌کند که در آن جمهوری اسلامی نه تنها توانایی‌های داخلی خود را در زمینه کنترل و نظارت اینترنتی توسعه می‌دهد، بلکه انگیزه و امکان بالقوه صدور این فناوری‌ها و دانش فنی مرتبط با آن را به کشورهای متحد یا مشتریان دیگر پیدا می‌کند.

۲.۵. شرکت‌ها و پیمانکاران ایرانی صادرکننده فناوری‌های سرکوب اینترنت

در کنار همکاری‌های سطح بالای حکومتی، سازوکارهای تجاری نیز برای بازاریابی و صدور فناوری‌های بالقوه دوگانه یا مرتبط با کنترل، وجود دارد. توسعه و نگهداری زیرساخت پیچیده سانسور و نظارت در ایران، نیازمند همکاری نزدیک میان نهادهای دولتی و امنیتی با شرکت‌های فناوری خصوصی و نیمه‌خصوصی است. این شرکت‌ها نقش کلیدی در بومی‌سازی، تولید و پیاده‌سازی ابزارهای کنترل اینترنت ایفا می‌کنند.



در پاریس، کاتالوگ‌هایی را برای بازاریابی شرکت‌های ایرانی در دسته‌بندی‌های مختلف ارائه کرده‌است^{۱۳۹} که در میان آنها نام ده‌ها شرکت تحت تحریم یا عضو هلدینگ‌های تحت تحریم ایالات متحده و اتحادیه اروپا دیده می‌شود.

یک نمونه آن شرکت تحت تحریم «دوران» پیمانکار دادستانی تهران، در پیاده‌سازی سیستم‌های فیلترینگ است.^{۱۴۰} این شرکت در بخش «فناوری اطلاعات» به مخاطبان معرفی شده و نام اصلی آن، در این کاتالوگ به درستی و دقت ذکر نشده‌است.^{۱۴۱} چند شرکت دیگر اینترنتی ایران، مانند «ابر آروان» هم دیده می‌شوند.^{۱۴۲} این شرکت‌ها با همکاری نزدیک با نهادهای امنیتی، فناوری‌هایی را توسعه داده‌اند که امکان کنترل و نظارت گسترده بر فعالیت‌های اینترنتی شهروندان را فراهم می‌کند.

این کاتالوگ را «معاونت دیپلماسی اقتصادی وزارت امور خارجه جمهوری اسلامی ایران» تهیه کرده و باید انتظار داشت در همه سفارت‌خانه‌های جمهوری اسلامی ایران به‌خصوص در کشورهای اقتدارگرا، به دست مشتریان رسیده‌باشد.^{۱۴۳}

شرکت‌های ذکر شده در این لیست، در گروهی با نام «باشگاه شرکت‌های صادراتی دانش‌بنیان» عضو هستند و عنوان این «باشگاه» در این کاتالوگ‌ها دیده می‌شود.^{۱۴۴} این «باشگاه» بخشی از فعالیت‌های معاونت علمی و فناوری ریاست جمهوری اسلامی ایران با وزارت امور خارجه جمهوری اسلامی ایران است.

ده‌ها شرکت ایرانی تحت تحریم با فناوری‌های دوگانه در وب‌سیات وزارت امور خارجه جمهوری اسلامی ایران معرفی شده‌اند که یکی از نمونه‌های آن شرکت تحت تحریم «امن افزار شریف» است که قابلیت‌های آن در وب‌سایت وزارت امور خارجه جمهوری اسلامی ایران، برای مشتریان خارجی فهرست شده‌است (تصویر پایین).^{۱۴۵}



در دهه گذشته، چندین شرکت ایرانی به‌طور فعال در توسعه و عرضه فناوری‌های مرتبط با سانسور و کنترل اینترنت مشارکت داشته‌اند. این فناوری‌ها شامل سیستم‌های بازرسی عمیق بسته‌ها (DPI)، فایروال‌های پیشرفته و سامانه‌های پایش محتوا هستند که عمدتاً توسط نهادهای امنیتی جمهوری اسلامی برای اعمال محدودیت در اینترنت استفاده می‌شوند.^{۱۴۶}

بررسی سوابق این شرکت‌ها و محصولاتشان، شواهدی از توانمندی‌های فنی ایران در این حوزه و پتانسیل صدور آن‌ها به دست می‌دهد. اما یکی از عوامل محدودکننده عمل این شرکت‌ها، تحریم‌های بین‌المللی است که در پاسخ به گسترش سانسور اینترنتی و نقض حقوق بشر در ایران، ایالات متحده و اتحادیه اروپا، علیه این شرکت‌ها و نهادهای حکومتی مرتبط با آنها اعمال کرده‌اند.

با این حال می‌بینیم که حق تحریم‌ها نیز مانعی برای دستگاه دیپلماسی خارجی جمهوری اسلامی ایران، برای بازاریابی این شرکت‌ها نیست. برای مثال سفارت جمهوری اسلامی ایران

یکی از این برنامه‌های تاسیس و تقویت نهادی به نام «خانه نوآوری و فناوری ایران» (IHIT) بود. مجموعه IHIT ابتکاری دولتی تحت نظر معاونت علمی و فناوری ریاست جمهوری (سازمان توسعه همکاری‌های علمی و فناوریانه بین‌المللی) است و شبکه‌ای جهانی برای کمک به شرکت‌های ایرانی در صادرات فناوری‌های «دانش‌بنیان» ایجاد کرده است.^{۱۴۷} این شبکه که در کشورهای روسیه، چین، ازبکستان، ترکیه، عراق، سوریه، اوگاندا و کنیا شعبه دارد و از طریق بازاریابی آنلاین و کارگزاری صادراتی فعالیت می‌کند، می‌تواند به عنوان مجرای برای صدور فناوری‌های حساس، از جمله تجهیزات الکترونیکی، مخابراتی و بالقوه نظارتی، عمل کند.

اگرچه هدف ظاهری IHIT تقویت اقتصاد دانش‌بنیان و دور زدن تحریم‌هاست، اما خطر استفاده از این شبکه برای صادرات یا واردات اقلام دوگانه با کاربردهای نظامی یا سرویگرانه وجود دارد. در فهرست این نهاد که به دست نهادی دیگر در معاونت علمی به نام «صندوق توسعه صادرات و تبادل فناوری» تهیه شده نیز تعداد زیادی از این شرکت‌های پیمانکار و توسعه‌دهنده فیلترینگ، سانسور و سیستم‌های سرکوب اینترنتی دیده می‌شوند.^{۱۴۸}

مجموعه IHIT همچنین با کارگزاران صادراتی خصوصی و شرکت‌های مدیریت صادرات (EMC) همکاری می‌کند. نمونه‌هایی از این شرکت‌ها عبارتند از «امین توسعه صادرات و تبادل فناوری» که نماینده انحصاری IHIT در روسیه است، شرکت آلمانی Rhyton Solutions که مالک آن مدیر شعبه استانبول IHIT است و با شرکت ایرانی Ritone Iran (فعال در صادرات فناوری به روسیه) و شرکت «هیراد تجارت هوشمند» که مدیرعامل آن مدیر بازرگانی IHIT روسیه است، مرتبط است.^{۱۴۹}

نقش بالقوه سفارتخانه‌های ایران در تسهیل این فعالیت‌ها و بازاریابی مستقیم یا غیرمستقیم این فناوری‌ها نیز، هرچند در اسناد بررسی‌شده به صراحت ذکر نشده، اما با توجه به رویکرد کلی جمهوری اسلامی ایران در استفاده از تمام ظرفیت‌های دیپلماتیک برای پیشبرد اهداف راهبردی، قابل بررسی است.

دفتر کنترل دارایی‌های خارجی وزارت خزانه‌داری ایالات متحده (OFAC) در سال ۲۰۲۴ مقررات جدیدی را تصویب کرد که ارائه خدمات فناوری به نهادهای دولتی ایران را محدود

در میان اسناد به‌دست آمده از نفوذ به سرور ای‌میل «کمیته فیلترینگ» (کارگروه تعیین مصادیق محتوای مجرمانه در معاونت پیگیری امور فضای مجازی دادستانی کل کشور) نیز نامه ای دیده می‌شود که نشان می‌دهد دادستانی کل کشور، تعداد نه شرکت را برای مشارکت در جلسات «گروه کاری باز امنیت بین‌الملل و ارتباطات» به اداره «صلح و امنیت بین‌المللی وزارت امور خارجه» معرفی کرده است. اکثر این شرکت‌ها و نهادهای، یا خود مستقیماً تحت تحریم‌های بین‌المللی هستند یا بخشی از هلدینگ هستند که آن تحریم است.




تاریخ: ۱۴۰۱/۰۲/۲۱
شماره: ۹۰۰۰/۳۴۴۷/۴۰
پیوست: ۱ د فای د

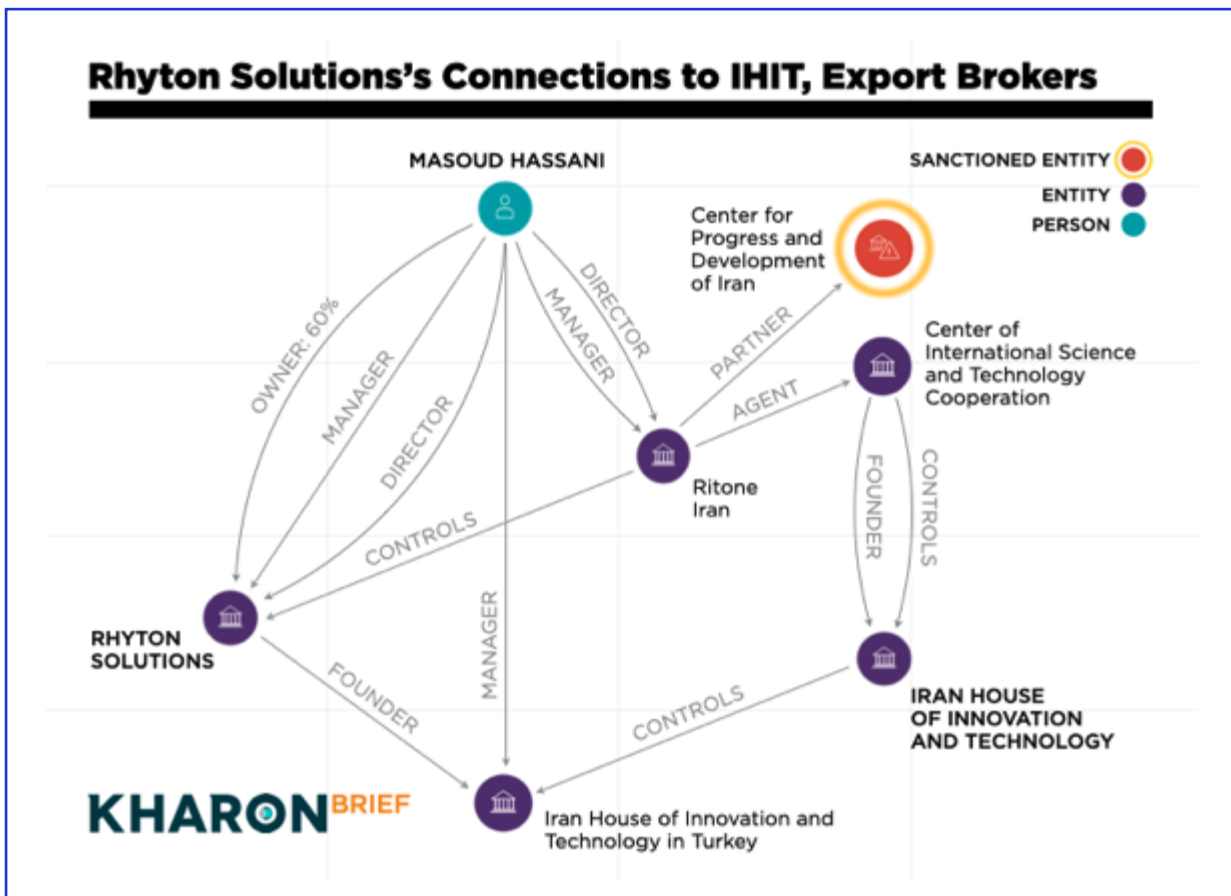
جناب آقای شرف‌بری
میرزا محرم معتمدی، رئیس هیئت مدیره و مدیر عامل
مدیر کل

احتراماً بازگشت به نامه شماره ۶۱۵/۱۱۶۹۹۲۵ در تاریخ ۱۴۰۱/۰۲/۲۰، برخی سازمان‌ها و مؤسسات غیردولتی داخلی که در حوزه امنیت سایبری فعالیت دارند و در این حوزه صاحب تجربه و تخصص می‌باشند به شرح ذیل جهت مشارکت در جلسات گروه کاری باز امنیت بین‌الملل اطلاعات و ارتباطات، معرفی می‌گردند:

ردیف	نام و عنوان مؤسسه غیردولتی	حوزه فعالیت	پایگاه اینترنتی
۱	شرکت نرم افزاری امن پرداز (پادویش)	امنیت سایبری و مقابله با بدافزار	www.amnpardaz.com
۲	پژوهشگاه امنیت رایسانامانه های شریف	پژوهش در حوزه امنیت سایبری	www.parsasharif.ir
۳	شرکت امن افزار گسترش شریف	امنیت سایبری	www.amnafzar.ir
۴	شرکت اطلاعات و ارتباطات امن مهین	امنیت سایبری	www.mohaymen.ir
۵	دانشگاه صنعتی شریف	امنیت سایبری	www.sharif.edu
۶	شرکت توسعه فناوریاتیکه فراز پژوهان	امنیت سایبری	www.farazpajohan.com
۷	مرکز تحقیقات صنایع انفورماتیک	امنیت شبکه و فناوری اطلاعات	www.rcii.ir
۸	آزمایشگاه فناوریاتیکه توسعه امن ناجی	فازنیکه و امنیت سایبری	www.cybersec.ir
۹	شرکت پایش ابراز سیرغ	امنیت سایبری	

رونوشت:
جناب آقای دکتر سجادی، معاون محترم تنظیم مقررات مرکز ملی فضای مجازی جهت اطلاع.

رهبری جمهوری اسلامی ایران، علی‌خامنه‌ای، در ابتدای هر سال در تقویم خورشیدی رسمی ایران، نامی را برای آن سال انتخاب می‌کند و این نام و مفهوم پشت آن، همواره یکی از سوبه‌های تبلیغات حکومتی در طول آن سال توسط نهادهای و سازمان‌های حکومتی است. این سنت بیش از دو دهه است که در ایران ادامه دارد. پس از اینکه او سال ۱۴۰۱ (مارس ۲۰۲۲ تا مارس ۲۰۲۳) را سال «تولید؛ دانش بنیان، اشتغال آفرین» نامید،^{۱۴۴} بخشی از برنامه‌های دستگاه‌های حکومتی در آن سال به موضوع «شرکت‌های دانش‌بنیان» تخصیص پیدا کرد.



شرکت‌ها متهم به انتقال فناوری‌های حساس آمریکایی به بانک مرکزی ایران هستند.^{۱۵۱} یکی از این شرکت‌ها، «شرکت خدمات انفورماتیک» است که شرکت مادر تخصصی فناوری‌های بانکی ایران است و مسئول تهیه زیرساخت پروژه رمزارز ملی است.

نکته حائز اهمیت در این مقررات، تعریف و کنترل «اقدام نظارت سایبری» (Cyber-surveillance items) است. این اقدام به عنوان کالاهای دوگانه‌ای تعریف شده‌اند که «به طور خاص برای فعال کردن نظارت پنهانی بر اشخاص حقیقی از طریق پایش، استخراج، جمع‌آوری یا تحلیل داده‌ها از سیستم‌های اطلاعاتی و مخابراتی طراحی شده‌اند». در مجموع، هرچند تحریم‌ها و کنترل‌های صادراتی، به ویژه از سوی آمریکا، موانعی جدی بر سر راه توسعه و صدور فناوری‌های کنترل اینترنتی جمهوری اسلامی ایران ایجاد می‌کنند و هزینه‌هایی را به شرکت‌های دخیل تحمیل می‌کند اما پیچیدگی‌های اجرایی، امکان دور زدن تحریم‌ها از طریق شبکه‌های واسطه‌ای و ناهماهنگی‌های احتمالی میان

می‌کند. این مقررات استانداردهایی را برای سخت‌افزارهای مجاز برای صادرات به ایران تعیین کرده‌اند.^{۱۵۲} اتحادیه اروپا از سال ۲۰۱۱ تحریم‌هایی را علیه ایران به دلیل نقض حقوق بشر اعمال کرده است. این تحریم‌ها شامل ممنوعیت ارائه خدمات فنی، دلالتی یا مالی مرتبط با تجهیزاتی است که ممکن است برای سرکوب داخلی استفاده شوند، از جمله تجهیزات نظارت بر اینترنت و ارتباطات.

تحقیقات نشان می‌دهد که جمهوری اسلامی ایران از شبکه‌ای پیچیده از شرکت‌های واسطه در کشورهای مختلف برای دور زدن تحریم‌ها و واردات فناوری‌های دوگانه استفاده می‌کند. این شبکه‌ها شامل شرکت‌هایی در امارات متحده عربی، ترکیه، مالزی، چین و ... هستند که با استفاده از شرکت‌های صوری و اسناد جعلی، تجهیزات حساس را به ایران منتقل می‌کنند. تعدادی از گره‌های این شبکه واسطه‌گری تاکنون افشا شده‌اند.

برای مثال در فوریه ۲۰۲۴، OFAC تحریم‌هایی را علیه چهار شرکت و سه فرد در ایران، امارات و ترکیه اعمال کرد. این

کشورها، اثربخشی کامل این محدودیت‌ها را به چالش می‌کشد.

با این حال همکاری‌های راهبردی و سازوکارهای نهادی نشان‌دهنده تلاش سیستماتیک ایران برای ادغام در شبکه‌های قدرت غیرغربی و استفاده از این روابط برای تقویت توانمندی‌های داخلی (از جمله در حوزه کنترل سایبری) و همچنین ایجاد فرصت‌هایی برای صدور فناوری و نفوذ است. شراکت با چین و روسیه نه تنها دسترسی به فناوری‌های پیشرفته را تسهیل می‌کند، بلکه یک جبهه ایدئولوژیک مشترک در برابر مدل اینترنت باز و ترویج «حاکمیت سایبری» دولتی ایجاد می‌کند.

۳.۵. ارزیابی تشدید خطر روند چندپارگی اینترنت

شواهد به روشنی نشان می‌دهند که ایران توانمندی‌های فنی قابل توجه و بومی‌شده‌ای در زمینه کنترل و نظارت بر فضای دیجیتال توسعه داده است. این شامل زیرساخت‌هایی مانند شبکه ملی اطلاعات (NIN)، سیستم‌های پیشرفته‌ای چون سیام (SIAM) برای کنترل ارتباطات موبایلی، استفاده گسترده از بازرسی عمیق بسته (DPI) برای فیلترینگ و مسدودسازی VPN‌ها، و ابزارهای نوین نظارت اجتماعی مانند اپلیکیشن ناظر و فناوری تشخیص چهره می‌شود. این قابلیت‌ها در داخل کشور به طور گسترده برای سرکوب مخالفان و کنترل جریان اطلاعات به کار گرفته شده‌اند و احتمالاً از طریق همکاری با کشورهایی مانند چین و روسیه تقویت نیز شده‌اند. در عرصه خارجی، ایجاد سازوکارهای دولتی مانند خانه نوآوری و فناوری ایران (IHIT) نشان‌دهنده نیت آشکار برای صدور فناوری (از جمله فناوری‌های دوگانه) و دور زدن تحریم‌هاست. اتحادیه‌های راهبردی با چین و روسیه نیز بر منافع مشترک در ترویج مدل‌های جایگزین حاکمیت اینترنت و مقابله با نفوذ غرب تأکید دارد.

با وجود قابلیت‌های فنی و نیت احتمالی، بر اساس شواهد موجود در این مجموعه اسناد، مدارک مستقیم و قابل تأییدی مبنی بر صادرات سیستماتیک سیستم‌های اصلی سانسور و نظارت اینترنتی ایران (مانند اجزای NIN یا سیام) به متحدان مشخصی چون سوریه و ونزوئلا، محدود و عمدتاً غیرمستقیم یا مبتنی بر شواهد جانی است. این وضعیت در

تضاد آشکار با صادرات گسترده و مستند فناوری‌های نظامی (پهپادها و موشک‌ها) توسط ایران به روسیه و گروه‌های نیابتی‌اش قرار دارد که نشان می‌دهد اقدامات جمهوری اسلامی ایران در صادرات فناوری‌های نظارت، تجسس، سانسور و سرکوب کاربران اینترنت با حساسیت کمتری از سوی دنیای آزاد دنبال می‌شود. با این حال اقدامات جمهوری اسلامی (توسعه NIN، به چالش کشیدن استارلینک در ITU، اتحاد با چین و روسیه) به تشدید روند چندپارگی اینترنت (fragmentation) و ترویج مدل‌های «حاکمیت سایبری» تحت کنترل دولت کمک می‌کند و پارادایم اینترنت باز و جهانی را به چالش می‌کشد.

خطر چنین صادراتی با توجه به توانمندی فنی، نیت احتمالی و زیرساخت‌های صادراتی موجود، معتبر و جدی است. این امر مستلزم نظارت مستمر، تحقیقات عمیق‌تر و هوشیاری جامعه بین‌المللی برای ردیابی، مستندسازی و مقابله با گسترش بالقوه ابزارهای سرکوب دیجیتال ایرانی در سطح جهانی است. عدم وجود شواهد قطعی در حال حاضر، نباید به معنای نادیده گرفتن این خطر تلقی شود، بلکه باید انگیزه‌ای برای افزایش تلاش‌ها جهت شفاف‌سازی این فعالیت‌ها باشد.

تقارن زمانی میان شکل‌گیری نهادهای عالی حکمرانی دیجیتال در چین و ایران معنادار است. اداره فضای مجازی چین (Cyberspace Administration of China) در سال ۲۰۱۱ تأسیس شد و تنها چند ماه بعد، در اسفند ۱۳۹۰، مرکز ملی فضای مجازی در ایران ایجاد شد. هر دو نهاد با هدف متمرکزسازی کنترل دولت بر زیرساخت‌های دیجیتال، مقررات‌گذاری فراگیر و ایجاد مرجع واحد برای سیاست‌گذاری اینترنت شکل گرفتند. نکته مهم‌تر این است که هر دو حکومت، به جای استفاده از واژه «اینترنت»، از اصطلاحی با بار معنایی خاص یعنی «فضای مجازی» بهره می‌برند؛ اصطلاحی که به حکومت‌ها اجازه می‌دهد عرصه ارتباطات دیجیتال را نه به عنوان یک شبکه جهانی باز، بلکه به مثابه «قلمرو» قابل حکمرانی، تنظیم، تصرف و کنترل بازنمایی کنند.

۳.۵.۱. نظام هویت معتبر در «فضای مجازی»

«احراز هویت» در کنار «مجوز» و «مدیریت حساب» (AAA;) (Authentication, Authorization, Accounting) اجزای اصلی هر چارچوب امنیتی برای دسترسی به منابع و

۲.۳.۵. برنامه هفتم پیشرفت جمهوری اسلامی

«برنامه هفتم پیشرفت جمهوری اسلامی ایران» که نقشه راه توسعه کشور برای پنج سال است و در سال ۲۰۲۴ تصویب شده است، تأکید ویژه‌ای بر توسعه زیرساخت‌های دیجیتال، دولت الکترونیک و هوشمندسازی خدمات عمومی در سال‌های پیش رو دارد. این برنامه نقش کلیدی در تسریع روند گسترش سامانه‌های احراز هویت در ایران دارد. عدم قوانین شفاف، نظارت مستقل و رعایت حقوق شهروندی در جمهوری اسلامی ایران احتمال اینکه این سامانه‌ها را به ابزارهای نقض حریم خصوصی و کنترل اجتماعی تبدیل کند بسیار بالا می‌برد. این ابزارها هنوز در مرحله طراحی هستند. مشهورترین سامانه که در زمان تصویب این برنامه توجه افکار عمومی را به خود جلب کرد «سامانه رصد و سنجش سبک زندگی مردم» بود.

در بخش بعدی به بررسی جزئی‌تر سیستم‌ها و سازوکارهای سامانه‌های «اشراف بر فضای مجازی» خواهیم پرداخت. هر سیستم، معمولاً یک نهاد سفارش‌دهنده در حکومت از نهادهای انتصابی و غیرانتخابی دارد و یک اپراتور یا توسعه‌دهنده دارد که بخشی از دولت، یا شرکت‌های وابسته به سرمایه‌گذاران حکومتی یا حتی بخش خصوصی است.

خدمات در یک شبکه است. اما این مساله آنجا تبدیل به پتانسیلی برای «نظارت و تجسس» شهروندان می‌شود که همه این خدمات از درگاه‌های واحد مرکزی (SSO; Single Sign-on)، یکپارچه و فراگیر «احراز هویت» که تحت کنترل حکومت است در دسترس قرار بگیرند. «احراز هویت» در مرکز و هسته اصلی هر سامانه «نظارت و تجسس» قرار دارد.

در سپتامبر ۲۰۱۹ در شورای عالی فضای مجازی مصوبه «نظام هویت معتبر در فضای مجازی کشور» تصویب شد که در توضیح آن آمده که هدفش «ایجاد زیرساخت‌های لازم برای تعاملات امن و قابل اطمینان در فضای مجازی» است. این مصوبه «تمامی تعاملات فنی، اقتصادی، فرهنگی، اجتماعی، سیاسی و اداری» را ملزم به استفاده از شناسه‌های معتبر می‌کند.

بر اساس این مصوبه، تمامی موجودیت‌ها در شبکه ملی اطلاعات و شبکه‌های مرتبط با آن باید هویت احراز شده داشته باشند و ارائه‌دهندگان خدمات موظفند از پذیرش تعاملات فاقد هویت معتبر خودداری کنند. ماده ۳ تأکید می‌کند که، تمام تعاملات کاربران با شبکه ملی اطلاعات یا سامانه‌های داخلی مثل پنجره دولت هوشمند باید از کانال احراز هویت بگذرند. براساس این ماده (بند۴) این شناسه برای «هر شخص» منحصر به فرد است و «هر تعامل» [در شبکه ملی اطلاعات] باید به شخصی منحصر به فرد منتهی شود. براساس ماده ۴، وزارت ارتباطات، زیرساخت تأمین شناسه را توسعه می‌دهد. سایر دستگاه‌های اجرایی در لایه‌های کاربردی شبکه ملی اطلاعات، تحت نظر مرکز ملی فضای مجازی از این سیستم برای توسعه سیستم تأمین شناسه‌های لایه کاربرد خود استفاده می‌کنند.

در ماده ۴ این مصوبه برای توسعه «درگاه واحد» برای تأمین‌کنندگان شناسه، دوره گذار ۳ ساله در نظر گرفته شده است. با وجود گذشتن این زمان هنوز «نظام هویت معتبر در فضای مجازی» به‌طور کامل و فراگیر پیاده‌سازی نشده است. جمهوری اسلامی ایران با تکمیل «نظام هویت معتبر در فضای مجازی» زیرساخت‌های جامع برای مدیریت هویت کاربران در فضای دیجیتال را به‌دست می‌آورد. هدف اصلی این طرح در ظاهر «تضمین شناسایی کامل کاربران و تعاملات آنان در فضای مجازی» است اما در نهایت به «تسهیل در رهگیری، کنترل محتوا و اقتدار لازم برای اعمال سیاست‌های حاکمیتی» منجر می‌شود.

منابع

۹. در بخش پنجم، «امنیت»، بخش «حفاظت و مدیریت تعاملات در شبکه ملی» زیباییاتی از جنبه‌های مختلف نظارت و تجسس در فعالیت‌های کاربران و فیلتر کردن محتوا (که در زبان رسمی به آن «پالایش محتوا» گفته می‌شود) شرح داده شده‌است.

۱۰.

Stanford University, Digichina; Jamie P. Horsley; "Behind the Facade of China's Cyber Super-Regulator"; Aug 8, 2022; [Link](#), [Archive](#)

۱۱. «حکم تشکیل و انتصاب اعضای شورای عالی فضای مجازی»؛ ۱۷ اسفند ۱۳۹۰؛ [لینک](#)، [یابگانی](#)

۱۲. شورای عالی فضای مجازی؛ «نظام هویت معتبر در فضای مجازی کشور»؛ شهریور ۱۳۹۸؛ [دانلود](#)

۱۳. «قانون برنامه پنجساله هفتم پیشرفت جمهوری اسلامی ایران (۱۴۰۳-۱۴۰۷)»؛ ۱۸ تیر ۱۴۰۳؛ [لینک](#)، [یابگانی](#)

۱۴. شورای عالی فضای مجازی؛ «شرح وظایف، اختیارات و ترکیب اعضای کمیسیون عالی تنظیم مقررات فضای مجازی کشور»؛ ۵ شهریور ۱۴۰۱؛ [دانلود](#)

۱۵. شورای عالی فضای مجازی؛ «دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی»؛ دی ۱۴۰۲؛ [لینک](#)، [دانلود](#)

۱۶. «قانون آیین دادرسی کیفری»، الحاقیه مصوبه ۱۳۹۲ (شامل قانون جرایم رایانه‌ای)؛ ۱ تیر ۱۳۹۴؛ [لینک](#)

۱۷.

Gary Miller, Noura Aljizawi, Ksenia Ermoshina, Marcus Michaelsen, Zoe Panday, Genny Plumptre, Adam Senft, and Ron Deibert; The Citizen Lab; "You Move, They Follow; Uncovering Iran's Mobile Legal Intercept System"; Jan. 16, 2023; [Link](#), [Archive](#)

۱۸.

3GPP; "Lawful Interception in mobile networks", Aug. 08, 2022; [Link](#), [Archive](#)

۱۹.

ETSI; "Lawful Intercept"; [Link](#), [Archive](#)

۲۰. شورای عالی فضای مجازی؛ «طرح کلان و معماری شبکه ملی اطلاعات»؛ دی ۱۳۹۹؛ [دانلود](#)

۲۱. ایران وایر؛ «گروه انانیموس سرورهای «کارگروه فیلترینگ» را هک کرد»؛ ۱۴ آبان ۱۴۰۱؛ [لینک](#)، [یابگانی](#)

۲۲. مواد ۲ تا ۵ اساسنامه سپاه پاسداران انقلاب اسلامی ([یابگانی](#)):

ASL19; Citizen Lab; "Iran's National Information Network"; Nov. 9, 2012; [Link](#), [Archive](#)

Center for Human Rights in Iran; "Guards at the Gate: The Expanding State Control Over the Internet in Iran"; Jan. 2018; [Download](#)

Article19; "Iran: Tightening the Net"; Sep. 2020; [Link](#), [Download](#) (Persian Version)

۲. «طرح ساماندهی پیام‌رسان‌های داخلی»؛ ۲۷ آبان ۱۳۹۷؛ [دانلود](#)

«طرح صیانت از حقوق کاربران در فضای مجازی و ساماندهی پیام‌رسان‌های اجتماعی»؛ ۱۳۹۹؛ [دانلود](#)

«طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی»؛ ۱۳۹۹؛ [دانلود](#)

«طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی»؛ ۲۶ تیر ۱۴۰۰؛ [دانلود](#)

«طرح نظام تنظیم مقررات خدمات فضای مجازی»؛ ۵ دی ۱۴۰۰؛ [دانلود](#)

«طرح نظام تنظیم مقررات خدمات فضای مجازی»؛ ۹ بهمن ۱۴۰۰؛ [دانلود](#)

۳. رادیو فردا؛ «گزارشگران بدون مرز: طرح صیانت از فضای مجازی برگرفته از روش «سانسور در چین» است»؛ ۶ مرداد ۱۴۰۰؛ [لینک](#)

۴.

Washington Post; "Iran just showed it has no intention of improving ties with the West"; Dec. 15, 2020, [Link](#)

۵. پی‌پی‌سی فارسی؛ «تلگرام پس از عدم همکاری با دولت ایران موقتاً مسدود شد»؛ ۲۸ مهر ۱۳۹۴؛ [لینک](#)، [یابگانی](#)

۶.

Pavel Durov post on X (formerly Twitter); Oct. 20, 2015; [Link](#), [Archive](#)

۷. شورای عالی انقلاب فرهنگی؛ «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای»؛ ۱۲ آذر ۱۳۸۰؛ [لینک](#)، [یابگانی](#)

۸. شورای عالی فضای مجازی؛ «سند تعیین الزامات شبکه ملی اطلاعات»؛ ۳۰ آذر ۱۳۹۵؛ [دانلود](#)

۳۴. تسنیم؛ «تحول در احراز هویت الکترونیکی با "سامانه هدا"»؛ ۴ مهر ۱۴۰۳؛ [یابگانی](#)

۳۵. تابناک؛ «ثبت نام در سامانه ثنا»؛ ۱۸ شهریور ۱۴۰۳؛ [یابگانی](#)

۳۶.

Gary Miller, Noura Aljizawi, Ksenia Ermoshina, Marcus Michaelson, Zoe Panday, Genny Plumptre, Adam Senft, and Ron Deibert; The Citizen Lab; "You Move, They Follow; Uncovering Iran's Mobile Legal Intercept System"; Jan. 16, 2023; [Link](#)

۳۷. دیجی کالا؛ «آموزش رجیستری گوشی»؛ ۳۰ مهر ۱۴۰۳؛ [یابگانی](#)

۳۸. آسان ثبت؛ «سامانه ام‌تا چیست»؛ [یابگانی](#)

۳۹. تسنیم؛ «مزیت استفاده از ام‌تا برای کسب و کارها چیست؟»؛ ۱۵ مهر ۱۳۹۹؛ [یابگانی](#)

۴۰. تابناک؛ «سامانه سخا چیست، راهنمای تصویری ثبت نام در سخا»؛ ۲۰ آذر ۱۴۰۳؛ [یابگانی](#)

۴۱. تابناک؛ «نحوه احراز آدرس در سامانه سخا»؛ ۱۵ مهر ۱۴۰۳؛ [یابگانی](#)

۴۲. دیجی کالا؛ «راهنمای سامانه میخک؛ از ورود تا ثبت نام و نوبت دهی»؛ ۳۰ شهریور ۱۴۰۴؛ [یابگانی](#)

۴۳. ایران وایر؛ «گروه انانیموس سرورهای «کارگروه فیلترینگ» را هک کرد»؛ ۱۴ آبان ۱۴۰۱؛ [لینک](#)، [یابگانی](#)

۴۴. مهر؛ «طرح مرحله‌ای رفع فیلترینگ؛ از بازگشایی واتساپ تا شرط دسترسی به یوتیوب و تلگرام»؛ ۴ دی ۱۴۰۳؛ [یابگانی](#)

۴۵.

KittenBusters; "CharmingKitten"; September 2025; [Link](#)

۴۶. عبدالصمد خرم‌آبادی (معاون وقت فضای مجازی دادستان کل کشور)؛ «گزارش معاونت فضای مجازی دادستانی کل کشور در خصوص برخی از امور مربوط به فضای مجازی»؛ گزارش فعالیت شش ماهه پانزدهم کمیته فیلترینگ، نیمه نخست ۱۳۹۶؛

در بخشی از این گزارش آمده:

استفاده از روش مرد میانی (Man in the middle)

با توجه به اینکه برخی از سایت‌ها و ارائه‌دهندگان خدمات خارجی از یک سو محتوای عمومی پایگاه‌های اینترنتی خود را به صورت رمز شده منتشر می‌کنند که قابلیت اعمال نظارت و پالایش را از حاکمیت سلب می‌کند و از سوی دیگر از قوانین و مقررات کشور تبعیت نمی‌کنند لذا یک راهکار فنی قابل اجرا در کوتاه مدت برای پالایش مصادیق مجرمانه در این‌گونه سایت‌ها استفاده از شیوه موسوم به مرد میانی است.

ماده ۲ - مبارزه قانونی با عوامل و جریان‌هایی که در صدد خرابکاری، براندازی نظام جمهوری اسلامی، و یا اقدام علیه انقلاب اسلامی ایران می‌باشند.

ماده ۳ - مبارزه قانونی با عواملی که با توسل به قوه قهریه در صدد نفی حاکمیت قوانین جمهوری اسلامی باشند.

ماده ۴ - اقدام همانند دیگر نیروهای انتظامی در جهت خلع سلاح کسانی که بدون مجوز قانونی اسلحه و مهمات حمل و نگهداری می‌نمایند.

ماده ۵ - همکاری با نیروهای انتظامی در مواقع لزوم، در جهت برقراری نظم و امنیت و حاکمیت قانون در کشور.

تبصره - سپاه پاسداران انقلاب اسلامی در زمینه مأموریت‌های مذکور در مواد فوق به عنوان ضابط قوه قضائیه عمل می‌کند.

۲۳.

Gary Miller, Noura Aljizawi, Ksenia Ermoshina, Marcus Michaelson, Zoe Panday, Genny Plumptre, Adam Senft, and Ron Deibert; The Citizen Lab; "You Move, They Follow; Uncovering Iran's Mobile Legal Intercept System"; Jan. 16, 2023; [Link](#)

۲۴. تابناک؛ «آشنایی با سامانه شاهکار و نحوه کار با آن»؛ ۲ آبان ۱۴۰۳؛ [یابگانی](#)

۲۵.

Sam Biddle, Murtaza Hussain; The Intercept; "Hacked Documents: How Iran Can Track and Control Protesters' Phones"; Oct. 28, 2022; [Link](#), [Archive](#)

۲۶.

"Iran's SIAM Manual in Persian for Tracking and Controlling Mobile Phones", Page 35-44, [Link](#), [Archive](#)

۲۷. ایران وایر؛ «نهادهای امنیتی در ایران چگونه تلفن همراه را ردگیری می‌کنند؟»؛ ۱۸ بهمن ۱۳۹۹؛ [لینک](#)، [یابگانی](#)

۲۸. قیام تا سرنوشت؛ «اقدامات حراست قوه مقننه در خصوص اغتشاشات، نامه حسین عرفانیان رئیس مرکز حراست قوه قضائیه به محمدباقر قالیباف، رئیس مجلس شورای اسلامی در ۴ مهر ۱۴۰۱»؛ [لینک](#) ([یابگانی](#)) صفحه اول و [لینک](#) ([یابگانی](#)) صفحه دوم

۲۹. سینا قنبرپور؛ پی‌پی‌سی فارسی؛ «سامانه رصد و سنجش سبک زندگی مردم» چیست و چگونه کار می‌کند؟؛ ۱۴ مرداد ۱۴۰۲؛ [لینک](#)، [یابگانی](#)

۳۰. فیلترین؛ «سامانه «سنجش سبک زندگی» ابزار جدید جاسوسی از مردم»؛ ۳۰ اکتبر ۲۰۲۳؛ [لینک](#)، [یابگانی](#)

۳۱. ایرنا؛ «احراز هویت معتبر در فضای مجازی برای تمام کاربران»؛ ۲۵ اردیبهشت ۱۴۰۰؛ [یابگانی](#)

۳۲. تابناک؛ «سامانه هدا چیست و چگونه می‌توان در آن ثبت نام کرد؟»؛ ۲۸ مرداد ۱۴۰۳؛ [یابگانی](#)

۳۳. ایرنا؛ «سامانه هدا جایگزین ارائه‌کپی شناسنامه و کارت ملی شد»؛ ۱۰ مرداد ۱۴۰۳؛ [یابگانی](#)

۴۷. فیلترینگ؛ «فیلترینگ «نسل جدید»؛ فیشینگ با قالب‌های حکمرانی‌پذیر»؛ ۵ آوریل ۲۰۲۴؛ [لینک](#)
۴۸. نریمان غریب؛ «قسمت چهارم: نگاهی به عملیات مالی و شبکه زیرساخت چارمینگ کیتن»؛ ۶ آبان ۱۴۰۴؛ [لینک](#)، [یابگانی](#)
۴۹. امیرهادی انواری؛ ایران اینترنشنال؛ «افشای هویت مدیران «اداره ۴۰» اطلاعات سپاه؛ بزرگترین بانک اطلاعاتی جاسوسی تهران»؛ آبان ۱۴۰۴؛ [لینک](#)، [یابگانی](#)
۵۰. نریمان غریب؛ «اداره ۴۰: هک‌هایی که آدم می‌کشند»؛ ۲ آذر ۱۴۰۴؛ [لینک](#)، [یابگانی](#)
۵۱. نریمان غریب؛ «ادامه اسناد افشا شده چارمینگ کیتن: فیش‌های حقوق و یک سند سرقت شده از آژانس بین‌المللی انرژی اتمی»؛ ۱۸ آذر ۱۴۰۴؛ [لینک](#)، [یابگانی](#)
۵۲. Martin Zugec; Bitdefender; “Unpacking BellaCiao: A Closer Look at Iran’s Latest Malware”; Apr 26, 2023; [Link](#), [Archive](#)
۵۳. Ravie Lakshmanan; The Hacker News; “Charming Kitten's New BellaCiao Malware Discovered in Multi-Country Attacks”; Apr 26, 2023; [Link](#), [Archive](#)
۵۴. Jai Vijayan; Dark Reading; “‘BellaCiao’ Showcases How Iran's Threat Groups Are Modernizing Their Malware”; Apr 28, 2023; [Link](#), [Archive](#)
۵۵. Jonathan Greig; The Record; “Iran APT using ‘BellaCiao’ malware against targets in US, Europe and Asia”; Apr 30, 2023; [Link](#), [Archive](#)
۵۶. Ravie Lakshmanan; The Hacker News; “Iran's Charming Kitten Deploys BellaCPP: A New C++ Variant of BellaCiao Malware”; Dec 24, 2024; [Link](#), [Archive](#)
۵۷. Saher Naumaan; Proof Point; “Crossed wires: a case study of Iranian espionage and attribution”; Nov 5, 2025; [Link](#), [Archive](#)
۵۸. ۶۳. کمپین حقوق بشر ایران؛ «انکار دولت، سیاست غیرشفاف قوه قضاییه: تمديد فعاليت تلگرام طلای و هات‌گرام تا پایان آذر ماه»؛ ۲۰ شهریور ۱۳۹۷؛ [لینک](#)، [یابگانی](#)
۵۹. کمپین حقوق بشر ایران؛ «ادامه نقض حریم خصوصی کاربران تلگرام طلای و سکوت شرکت تلگرام»؛ ۲۸ آبان ۱۳۹۷؛ [لینک](#)، [یابگانی](#)
۶۰. کمپین حقوق بشر ایران؛ «شواهد جدید درباره امکان جاسوسی از کاربران و سانسور محتوا توسط تلگرام طلای و هات‌گرام»؛ ۲۱ آبان ۱۳۹۷؛ [لینک](#)، [یابگانی](#)
۶۱. Vitor Ventura; Cisco TALOS; “Persian Stalker pillages Iranian users of Instagram and Telegram”; Nov. 5, 2018; [Link](#), [Archive](#)
۴۷. فیلترینگ «نسل جدید»؛ فیشینگ با قالب‌های حکمرانی‌پذیر»؛ ۵ آوریل ۲۰۲۴؛ [لینک](#)
۴۸. US Department of the Treasury; “Treasury Sanctions Iranian Officials and Companies Connected to Repression in Advance of the Anniversary of Mahsa “Zhina” Amini’s Death”; Sep 15, 2023; [Link](#)
۴۹. Open Sanctions; “Rasoul Jalili”; [Link](#)
۵۰. Open Sanctions; “Issa Zarepour”; [Link](#)
۵۱. فیلترینگ؛ «سرکوبگران اینترنت؛ نگاهی به عملکرد دادستانی و پیمانکاران سرکوب»؛ تیر ۱۴۰۴؛ [دانلود](#)
۵۲. ایستنا؛ رئیس پلیس فتا: بدانید پیام‌های خصوصی در وایبر و واتساپ توسط پلیس فتا قابل کنترل است»؛ ۲۱ شهریور ۱۳۹۳؛ [یابگانی](#)
۵۳. Netblocks; “Internet disrupted in Iran amid protests over death of Mahsa Amini”; Sep 19, 2022; [Link](#)
۵۴. Janos Gergo SZELES; Bitdefender; “EyeSpy - Iranian Spyware Delivered in VPN Installers”; Jan. 11, 2023; [Archive](#)
۵۵. Blackpoint Cyber; “Tech Tuesday: Eye Spy – The Dangers of Legal Malware”; Aug. 30, 2022; [Archive](#)
۵۶. رازنت؛ «جاسوس‌افزار اندرویدی با نام «عکس یادگاری» در تلگرام منتشر شده که هدفش صرافی‌های رمزارز ایرانی است»؛ ۱۷ آبان ۱۴۰۴؛ [لینک](#)
۵۷. KittenBusters; “CharmingKitten”; September 2025; [Link](#)
۵۸. MITRE; “Magic Hound”; [Link](#)
۵۹. نریمان غریب؛ «نشت تاریخی اسناد گروه هکری بچه‌گره جذاب وابسته به سپاه»؛ ۸ مهر ۱۴۰۴؛ [لینک](#)، [یابگانی](#)
۶۰. نریمان غریب؛ «قسمت دو و سه از فایل‌های لو رفته چارمینگ کیتن در پنج قاره را افشا می‌کند»؛ ۲۴ مهر ۱۴۰۴؛ [لینک](#)، [یابگانی](#)

روزنامه خراسان؛ «انحصار توسکا پشت ماسک همراه اول»؛ ۴ فروردین ۱۳۹۹؛

[یابگانی](#)

۷۷. فکت‌نامه؛ «ابهام‌های بی‌پایه پیام‌رسان بله درباره نمایش اطلاعات

کاربران»؛ ۱ مرداد ۱۴۰۲؛ [لینک](#)، [یابگانی](#)

۷۸. فیلترین؛ «آزمایشگاه امنیتی صندوق فناوری باز (OTF) دریافت که سه

اپلیکیشن پیام‌رسان ایرانی ایمن نیستند»؛ ۱۷ دسامبر ۲۰۲۴؛ [لینک](#)، [یابگانی](#)

۷۹. نریمان غریب؛ «اداره ۴۰: هک‌هایی که آدم می‌کشند»؛ ۲ آذر ۱۴۰۴؛ [لینک](#)،

[یابگانی](#)

امیرهادی انواری؛ ایران اینترنشنال؛ «افشای هویت مدیران «اداره ۴۰» اطلاعات

سپاه، بزرگترین بانک اطلاعاتی جاسوسی تهران»؛ آبان ۱۴۰۴؛ [لینک](#)، [یابگانی](#)

۸۰.

Drew Donnelly; Horizons; "China Social Credit System Explained – What is it & How Does it Work?"; Feb. 11, 2024;

[Link](#), [Archive](#)

Zeyi Yangarchive; MIT Tech. Rev.; "China just announced a new

social credit law; Here's what it means"; Nov. 22, 2022; [Link](#),

[Archive](#)

۸۱.

Ms. Smith; CSO; "Skynet in China: Real-life 'Person of Interest' spying in real time"; Sep 26, 2017; [Link](#), [Archive](#)

Raymond Zhong; NY Times; "China Snares Tourists' Phones in Surveillance Dragnet by Adding Secret App"; Jul. 2, 2019; [Link](#),

[Archive](#)

۸۲.

Paul Mozur; NY Times; "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras"; Jul. 8, 2018; [Link](#), [Archive](#)

۸۳.

Vincent Brussee; MERICS; "China's social credit score – untangling myth from reality"; Feb 11, 2022; [Link](#), [Archive](#)

Jessica Reilly, Muyao Lyu, Megan Robertson; The Diplomat; "China's Social Credit System: Speculation vs. Reality"; Mar. 30, 2021; [Link](#), [Archive](#)

۸۴.

Paul Mozur, Aaron Krolik; NY Times; "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers"; Dec. 17,

2019; [Link](#), [Archive](#)

۶۵.

Durov Post Pavel Durov post on X (formerly Twitter); Oct. 29, 2017; [Link](#), [Archive](#)

ایرنا؛ «وزیر ارتباطات و فناوری اطلاعات: امنیت تلگرام‌های ایرانی را تایید نمی‌کنیم»؛ ۲۱ مرداد ۱۳۹۷؛ [یابگانی](#)

۶۶. شورای عالی فضای مجازی؛ «بررسی راهکارهای افزایش میزان سهم

ترافیک داخلی و مقابله با پالایش‌شکن‌ها»؛ ۲۳ آبان ۱۴۰۳؛ [یابگانی](#)

۶۷. شرکت فناوری‌های تنظیم بار شریف؛ «پروپوزال فی سامانه مستندساز

ادله الکترونیکی»؛ ۱۴ تیر ۱۴۰۱؛ [دانلود](#)

فکت‌نامه؛ «پیمانکاران فیلترینگ در ایران»؛ ۸ بهمن ۱۴۰۲؛ [لینک](#)، [یابگانی](#)

۶۸. ایران‌وایر؛ «سامانه شکار که اطلاعات ۴۲ میلیون کاربر تلگرام را منتشر کرد،

متعلق به کجا است؟»؛ ۱۵ فروردین ۱۳۹۹؛ [یابگانی](#)

وب‌آموز؛ «مسئول افشا اطلاعات ۴۲ میلیون ایرانی بر روی سامانه شکار

کیست؟»؛ ۳۱ خرداد ۱۳۹۹؛ [یابگانی](#)

۶۹. دادستانی کل کشور؛ «سامانه رصد و پایش اخبار و تلگرام»؛ فروردین

۱۳۹۶؛

۷۰.

Anonymous OpIran; Post on Telegram; Nov. 3 2022; [Archive](#)

۷۱.

Crunchbase; Ava Hamrah Hooshmand Hezardastan; [Link](#), [Archive](#)

۷۲. پیوست؛ «هزاردستان خبر داد: احتمال تعطیلی بلد بعد از پایان سال/

تعدیل ده‌ها نیرو»؛ ۳ آبان ۱۴۰۱؛ [یابگانی](#)

۷۳. ایسپا؛ «میزان استفاده ایرانیان از پیام‌رسان‌ها و شبکه‌های اجتماعی»؛ ۷ مهر ۱۴۰۳؛ [یابگانی](#)

۷۴.

Open Technology Fund; "Iranian Messaging Apps - Security Audit"; [Archive](#)

۷۵.

PC Jow; "Why did Rubica get a warning from Google's security shield?"; Oct. 3 2022; [Archive](#)

۷۶. جماران؛ «نام چه کسانی در «توسکا» دیده می‌شود؟»؛ ۲۶ اسفند ۱۳۹۷؛ [یابگانی](#)

- ۷ شهریور ۱۴۰۱؛ [لینک](#)، [بایگانی](#)، [یوتیوب](#)
۹۵. ایسنا؛ «پیشنهاد رئیس کمیسیون حقوق و قضایی مجلس برای تغییر رویکرد پلیس در موضوع حجاب»؛ ۲۳ مهر ۱۴۰۱؛ [لینک](#)، [بایگانی](#)
۹۶. مهر؛ «شناسایی و برخورد جدی پلیس با کشف حجاب از ۲۶ فروردین»؛ ۱۹ فروردین ۱۴۰۲؛ [لینک](#)، [بایگانی](#)
- ایسنا؛ «رادان: طرح عفاف و حجاب از فردا آغاز می‌شود، دوربین‌های طرح هیچ خطایی نخواهد داشت»؛ ۲۵ فروردین ۱۴۰۲؛ [لینک](#)، [بایگانی](#)
- فارس؛ «آغاز طرح برخورد با کشف حجاب از امروز/ معابر، اصناف و خودروها در رصد دوربین‌های پلیس»؛ ۲۶ فروردین ۱۴۰۲؛ [لینک](#)، [بایگانی](#)
۹۷. «قانون حمایت از خانواده از طریق ترویج فرهنگ عفاف و حجاب»؛ مهر ۱۴۲۰؛
۹۸. «پیشا-داده» (Pre-data) به مرحله‌ای اطلاق می‌شود که در آن زیرساخت‌های جمع‌آوری اطلاعات (مانند دوربین‌ها، میکروفون‌ها یا ابزارهای ردیابی) فعال شده‌اند، اما هنوز داده‌ها به صورت تحلیلی پردازش، طبقه‌بندی یا به سامانه‌های هوش مصنوعی متصل نشده‌اند. این مرحله، پیش‌نیاز توسعه سامانه‌های تحلیلی در نظام‌های نظارتی و تصمیم‌گیری دیجیتال محسوب می‌شود.
- Sandra Wachter, Brent Mittelstadt; Columbia Business Law Review; "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI."; vol. 2019, no. 2, Oct. 5, 2018; [Link](#), [Archive](#)
- ۹۹.
- Sanam Mahoozi; Thomson Reuters Foundation; "Mahsa Amini death: facial recognition to hunt hijab rebels in Iran"; Sep. 21, 2022; [Link](#), [Archive](#)
۱۰۰. فلیتریان؛ «نظارت و پنهان کاری: بررسی ادعاهای ایران در مورد استفاده از فناوری تشخیص چهره برای کنترل اجتماع»؛ ۱۲ اردیبهشت ۱۴۰۲؛ [لینک](#)، [بایگانی](#)
۱۰۱. فکت‌نامه؛ «بررسی ادعای اغراق‌آمیز نقش هوش مصنوعی در طرح عفاف و حجاب»؛ ۲۸ فروردین ۱۴۰۲؛ [لینک](#)، [بایگانی](#)
- ۱۰۲.
- Access Now; "Weapons of control, shields of impunity: Internet shutdowns in 2022"; Feb. 28, 2023; [Link](#), [Archive](#), [Download](#)
- ۱۰۳.
- Steven Feldstein; Carnegie Endowment for International Peace; "The Global Expansion of AI Surveillance"; Sep. 17, 2019; [Link](#), [Archive](#), [Download](#), [AI Global Surveillance \(AIGS\) Index](#)
- Jeremy Daum; The Jamestown Foundation, China Brief; "Far From a Panopticon, Social Credit Focuses on Legal Violations"; Volume: 21, Issue: 19, Oct. 8, 2021; [Link](#), [Archive](#)
- ۸۵.
- Nectar Gan; The China Morning Post; "The complex reality of China's social credit system: hi-tech dystopian plot or low-key incentive scheme?"; Feb. 7, 2019; [Link](#), [Archive](#)
- BBC; "In Your Face: China's all-seeing state"; Dec. 10, 2017; [Link](#), [Archive](#)
- Lily Kuo; The Guardian; "China bans 23m from buying travel tickets as part of 'social credit' system"; Mar. 1, 2019; [Link](#), [Archive](#)
۸۶. سیدعلی خامنه‌ای؛ «دیدار رضائی مسئولان نظام با رهبر انقلاب»؛ ۱۵ فروردین ۱۴۰۲؛ [لینک](#)، [بایگانی](#)
- ۸۷.
- Erwin van Veen, Hamidreza Azizi; Clingendael, The Netherlands Institute of International Relations; "Protests in Iran in comparative perspective"; Mar. 8, 2023; [Link](#), [Archive](#), [Download](#)
- ۸۸.
- Amnesty International; "What happened to Mahsa/Zhina Amini?"; Sep. 15, 2023; [Link](#),
۸۹. شورای عالی انقلاب فرهنگی؛ «اصول و مبانی و روشهای اجرایی گسترش فرهنگ عفاف»؛ ۱۴ بهمن ۱۳۷۶؛
۹۰. شورای عالی انقلاب فرهنگی؛ «راهنمای گسترش فرهنگ عفاف»؛ ۴ مرداد ۱۳۸۴؛
۹۱. شورای عالی انقلاب فرهنگی؛ «مجموعه تکمیلی اقدامات اجرایی گسترش فرهنگ عفاف و حجاب»؛ ۱۲ شهریور ۱۳۹۸؛
- ۹۲.
- Khari Johnson; Wired; "Iran Says Face Recognition Will ID Women Breaking Hijab Laws"; Jan. 10, 2023; [Link](#), [Archive](#)
- ۹۳.
- Tirana Hassan; Human Rights Watch; "Iran Events of 2023"; [Link](#), [Archive](#)
- ۹۴.
- خبر فوری؛ «دیر ستاد امر به معروف، با فناوری، کدملی بی حجاب را پیدا کنیم»؛

۱۰۴. Bulelani Jili; EPIC; "The Rise of Chinese Surveillance Technology in Africa"; May 31, 2022; [Link](#), [Archive](#)
۱۰۵. Amy Hawkins; Foreign Policy; "Beijing's Big Brother Tech Needs African Faces"; Jul. 24, 2018; [Link](#), [Archive](#)
۱۱۳. لویی شکپی؛ فیلترین؛ «احراز هویت و شناسایی صورت؛ از حقیقت تا تبلیغات سیاسی»؛ ۲۸ سپتامبر ۲۰۲۳؛ [لینک](#)، [بایگانی](#)
۱۱۴. Tehran Times; "Senior MP: Iran-China cooperation plan is a win-win game"; Apr. 12, 2021; [Link](#), [Archive](#)
۱۰۶. SCSP, Foreign Policy Panel; "Defending Digital Freedom and the Competition for the Future of the Global Order"; Dec. 2022; [Download](#)
۱۰۷. CIRA; "Iranian Companies Provide Facial Recognition Services to Government and Security Services"; May 22, 2023; [Link](#), [Archive](#)
۱۱۵. فیلترین؛ «احراز هویت و شناسایی صورت؛ از حقیقت تا تبلیغات سیاسی»؛ ۶ مهر ۱۴۰۲؛ [لینک](#)
۱۱۶. Iran Watch; "Investigative Report on the U.S. National Security Issues Posed by the Chinese Telecommunications Companies Huawei and ZTE"; Oct. 8, 2012; [Link](#), [Archive](#)
۱۰۸. تسنیم؛ «دوربین‌های سطح شهر تهران به صورت زنده تمام معابر را پوشش می‌دهد/ رد هرگونه سرقت اطلاعات از دوربین‌های شهری»؛ ۱۸ خرداد ۱۴۰۱؛ [بایگانی](#)
۱۰۹. Light Reading; "ZTE Defends Iran Position"; Mar. 28, 2012; [Link](#), [Archive](#)
۱۱۷. پیوست؛ «سپتام؛ سامانه پایش تصویری اماکن چیست و چرا برای کسب‌وکارها الزامی است»؛ ۱۴ آذر ۱۴۰۳؛ [بایگانی](#)
۱۱۸. رادیو زمانه؛ «سامانه «سپتام»، دسترسی بی‌واسطه و اجباری نیروی انتظامی به دوربین‌های اصناف»؛ ۱۵ مهر ۱۴۰۳؛ [بایگانی](#)
۱۱۹. ایران وایر؛ «سامانه سپتام؛ راه تازه اعمال حجاب اجباری و شروع اجرای مصوبه عفاف»؛ ۱۵ مهر ۱۴۰۳؛ [بایگانی](#)
۱۱۰. Charles Custer; Tech in Asia; "How Huawei Helped Iran Spy on Citizens and Why Brand China is Poison"; Dec. 6, 2012; [Link](#), [Archive](#)
۱۲۰. Freedom House; "Freedom Net 2024"; Jun 2024; [Link](#), [Archive](#)
۱۲۱. فکت‌نامه؛ «بررسی ادعای اغراق‌آمیز نقش هوش مصنوعی در طرح عفاف و حجاب»؛ ۲۹ فروردین ۱۴۰۲؛ [لینک](#)
۱۲۲. بی‌بی‌سی فارسی؛ نیما اکبرپور؛ «اپلیکیشن ناظر یک، ابزاری در دست حجاب‌بانان مجوزدار»؛ ۲۰ آذر ۱۴۰۲؛ [لینک](#)
۱۱۱. FilterWatch; Azin Mohajerin, Amir Rashidi; "Nazer App: How Iran is Using Technology to Suppress Women's Rights"; Jan 5, 2024; [Link](#)
۱۲۳. Masha Borak; SCMP; "Why one of China's largest facial recognition companies faces a US ban"; Sep. 20, 2019; [Link](#), [Archive](#)
۱۲۴. Bernard Marr; Forbes; "The Amazing Ways Chinese Face Recognition Company Megvii (Face++) Uses AI And Machine Vision"; May 24, 2019; [Link](#), [Archive](#)
۱۲۵. Filter Watch; Solmaz Eikder; "A Battlefield Named Isfahan: Targeted Use of IMSI-Catchers and Surveillance Cameras to the Enforce Chastity and Hijab Law"; Apr 17, 2025; [Link](#)

- Emilio Lasiello; Strike Source; What Does Iran-Russia Cyber Partnership Mean for US National Security?"; Feb. 2, 2021; [Link](#), [Archive](#). ۱۲۴
- EFF; "Cell-Site Silulators, IMSI Catchers"; [Link](#). ۱۲۵
- Darya Lavrova; Positive Technologies; "Iran's cybersecurity threatscape for 2021-H1 2024"; Oct 25, 2024; [Link](#), [Archive](#). ۱۳۵
- Jazeh Miller; Iran News Update; "Iran's Regime Tightens Grip on Internet Access through Cyber Partnership with Russia"; Jan. 23, 2025; [Link](#), [Archive](#). ۱۳۶
- Farzaneh Badii; Digital Medusa; "Islamic Republic V. Starlink: Will The ITU Fragment Satellite Internet?"; Jan. 29. 2024; [Link](#), [Archive](#). ۱۳۷
- Miaan Group; "ITU Must Press Iran on Internet Shutdowns, Not Enable Them"; Aug. 21. 2024; [Link](#), [Archive](#). ۱۳۸
- «فکت‌نامه؛ «پیمانکاران فیلترینگ ایران»؛ ۸ بهمن ۱۴۰۲؛ [لینک](#)، [بایگانی](#)». ۱۳۹
- سفارت جمهوری اسلامی ایران، پاریس؛ «معرفی شرکت‌های دانش‌بنیان صادراتی ایران»؛ ۴ شهریور ۱۴۰۱؛ [بایگانی](#). ۱۴۰
- اینترنت‌آباد؛ «شرکت داده پردازان دوران»؛ [لینک](#)، [بایگانی](#). ۱۴۱
- IHTECC; "Iran Hi-Tech Export Companies Club, Information technology"; Aug 2022; [Link](#), [Archive](#). ۱۴۲
- اینترنت‌آباد؛ «شرکت نویان ابر آروان»؛ [لینک](#)، [بایگانی](#). ۱۴۳
- معاونت دیپلماسی اقتصادی وزارت امور خارجه جمهوری اسلامی ایران؛ «شرکت‌های نمونه صادراتی»؛ [لینک](#)، [لینک ۲](#). ۱۴۴
- باشگاه شرکت‌های صادراتی دانش‌بنیان؛ [لینک](#). ۱۴۵
- اینترنت‌آباد؛ «شرکت امن‌افزار گستر شریف»؛ [لینک](#)، [بایگانی](#). ۱۴۶
- سید علی خامنه‌ای، رهبری جمهوری اسلامی ایران؛ «پیام نوروزی به مناسبت آغاز سال ۱۴۰۱»؛ ۲۹ اسفند ۱۴۰۰؛ [لینک](#)، [بایگانی](#). ۱۴۷
- خانه نوآوری و فناوری؛ [لینک](#)، [لینک ۲](#). ۱۴۸
- سازمان توسعه همکاری‌های علمی و فناوریانه بین‌المللی، معاونت علمی و فناوری ریاست جمهوری اسلامی ایران؛ [لینک](#). ۱۴۹
- Access Now; Weapon of Control, Shields of Impunity"; Feb 2023; [Download](#). ۱۲۶
- Freedom House; "Freedom Net 2024"; Jun 2024; [Link](#), [Archive](#). ۱۲۷
- «سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای»؛ ۱۱ مهر ۱۳۷۷؛ [لینک](#)، [بایگانی](#). ۱۲۸
- «برنامه همکاری‌های جامع (۲۵ ساله) ایران و چین» - متن تایید نشده؛ خرداد ۱۳۹۹؛ ۱۲۹
- Ghazal Vaisi; Middle East Institute; "The 25-year Iran-China agreement, endangering 2,500 years of heritage"; Mar. 1, 2022; [Link](#), [Archive](#). ۱۳۰
- Tehran Bureau; "The Chinese Companies Building Iran's Surveillance State"; Sep. 30, 2022; [Link](#), [Archive](#). ۱۳۱
- A Conversation with Nader Habibi and Hadi Kahalzadeh; Crown Center for Middle East Studies, Brandeis University; "The Iranian-Chinese Strategic Partnership: Why Now and What it Means"; Apr 28, 2021; [Link](#), [Archive](#). ۱۳۲
- «توافقنامه جامع راهبردی ایران و روسیه»؛ ۲۸ دی ۱۴۰۳. ۱۳۳
- «موافقتنامه همکاری در حوزه امنیت اطلاعات بین دولت جمهوری اسلامی ایران و دولت فدراسیون روسیه»؛ ۶ تیر ۱۴۰۳؛ [لینک](#)، [بایگانی](#). ۱۳۴
- SC Media; "Increased cybersecurity cooperation forged by Russia, Iran"; Jan. 23, 2025; [Link](#), [Archive](#). ۱۳۵
- Council on Foreign Relations; "The Iran-Russia Cyber Agreement and U.S. Strategy in the Middle East"; Mar. 15, 2021; [Link](#), ۱۳۶

۱۴۸. صندوق توسعه صادرات و تبادل فناوری، سازمان توسعه همکاری‌های علمی و فناوریانه بین‌المللی؛ [لینک](#)

۱۴۹.

Kharon; “A Sprawling Iranian Network Is Facilitating Its Tech Exports, Sidestepping Sanctions”; Feb 11. 2025; [Link](#), [Archive](#)

۱۵۰.

OFAC; “31 CFR Parts 501 and 515”; Mar. 21, 2025; [Link](#), [Archive](#)

۱۵۱.

Fatima Hussein; AP; “U.S. sanctions Iran Central Bank subsidiary for U.S. tech procurement and violating export rules”; Feb. 14, 2024; [Link](#), [Archive](#)