استفاده موثر و امن از ابزارهای دیجیتال

ویژه وکلا و مدافعان حقوق بشر

درس‌نامه

توانا
TAVAANA

استفاده موثر و امن از ابزارهای دیجیتال

ویژه وکلا و مدافعان حقوق بشر

درس‌نامه

توانا TAVAANA
آموزشکده آنلاین برای جامعه مدنی ایران
e-collaborative for civic education

www.tavaana.org

پروژهٔ

e-collaborative
for civic education

www.eciviced.org

استفاده موثر و امن از ابزارهای دیجیتال
ویژه وکلا و مدافعان حقوق بشر
درس‌نامه

ناشر: E-Collaborative for Civic Education

زمستان ۱۴۰۳

---

e-collaborative
for civic education

ECCE (E-Collaborative Civic Education) یک سازمان غیرانتفاعی در ایالات متحده آمریکا تحت 501c3 است که از فناوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیان‌گذاران و مدیران این سازمان اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از جامعه سیاسی دموکراتیک پایه و اساس کار است؛ همان‌طور که حقوق عام بشر که هر شهروندی باید از آن‌ها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک‌تک شهروندان و امنیت، برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار است که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند.

ما پروژه اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعه مدنی ایران» را در سال ۲۰۱۰ تاسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس‌ماندن دانشجویان، به یک جامعه آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وب‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زنده دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با کنشگران و روشنفکران، دستورالعمل‌های خودآموز، کتابخانه مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاوره آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعه توانایی‌های آموزشکده توانا متوجه گردآوردن بهترین متفکران ایران و صداهای حذف‌شده است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان در جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فناوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هم‌وطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما!

فهرست

پیش‌گفتار

دوره «استفاده موثر و امن از ابزارهای دیجیتال؛ ویژه وکلا و کنشگران مدافع حقوق بشر» با هدف افزایش آگاهی وکلا و فعالان حوزه حقوقی در سال ۱۴۰۳ خورشیدی برگزار شد. در این دوره طی هشت جلسه به مواردی از این دست پرداخته شد: استفاده از تکنولوژی در دنیای حقوق، امنیت دیجیتال در پروسه حقوقی، امنیت تلفن همراه و تبلت برای فعالان حقوقی و وکلا، استفاده از هوش مصنوعی (AI) و یادگیری ماشین (ML) و کلان‌داده (BIG DATA)، آرشیو و ثبت مستندات، امنیت آرشیو و داده‌ها، تهدیدهای دیجیتال و تاریخچه و دورنمای سوءاستفاده حکومت‌های سرکوبگر از تکنولوژی دیجیتال.

اکنون درس‌نامه این دوره، شامل متن آموزشی آن، در قالب یک کتابچه در دسترس شما قرار می‌گیرد. امیدواریم با راهکارهای ارائه‌شده در این مجموعه، بتوانیم قدمی در مسیر افزایش آگاهی وکلا و فعالان حوزه حقوقی در حفظ امنیت دیجیتال و حریم خصوصی‌شان برداشته باشیم.

درس نخست
تکنولوژی در دنیای حقوق و قضا: فرصت یا تهدید؟

بیش از سه دهه از همه‌گیرشدن استفاده از ابزارهای دیجیتال می‌گذرد. نخست شهروندان کشورهای پساصنعتی و پس از آن، مردم کشورهای صنعتی و درحال‌رشد، به صورتی روزافزون استفاده از وسایلی چون کامپیوترهای‌شخصی، تلفن‌های همراه، تبلت و ابزارهای مشابه را آغاز کردند. کشور ما، ایران، هم با وقفه‌ای بسیار کوتاه، به کاروان جهانی استفاده از ابزارها و سرویس‌های دیجیتال پیوست و علی‌رغم بیش از سی سال فیلترینگ و اعمال محدودیت، امروز در میان کشورهایی قرار دارد که با بیش‌ترین ضریب نفوذ تلفن‌های همراه و استفاده کاربران از پیام‌رسان‌های دیجیتال هستند.

گسترش انفجارگونه استفاده از ابزارهای دیجیتال، بی‌تردید به دگرگونی غیرقابل‌بازگشتی در حیات فرهنگی، اجتماعی، اقتصادی و سیاسی جوامع مختلف انجامیده است. روابط حقوقی، میان شهروندان و همچنین سازوکارهای قانونی حاکم بر جوامع هم، مصون از تغییرات شگرف برآمده از انقلاب دیجیتال نبوده‌اند.

از سال‌های نخستین هزاره‌ی دوم میلادی، استفاده از ابزارهای دیجیتال در میان نهادهای قانون‌گذار، اجرایی و قضایی کشورهای مختلف، به‌تدریج، اما با روندی رو به رشد، رسما آغاز شد. امکان ارتباط مستقیم شهروندان و ارسال شکوائیه و درخواست‌هایشان به پارلمان یا نخست‌وزیر در اسکاتلند و بریتانیا، مثال روشنی از ظهور نخستین سرویس‌های

قانونی دیجیتال است. سرویس‌های دولتی الکترونیک اما، تنها بخش بسیار کوچکی از تغییرات برآمده از گذار دیجیتال‌اند.

از همان روزهای نخست استفاده از اینترنت و حتی قبل از رواج وب جهانی (www) کاربران اینترنت، بولتن‌های عمومی موسوم به BBS سرویس‌های نظیر تل.نت (TelNet) یا چت‌روم‌های IRC را برای گزارش مواردی چون نقض حقوق بشر یا درخواست‌های دسته‌جمعی به‌کار گرفتند. پس از ظهور و محبوبیت استفاده از ایمیل و همه‌گیرشدن ایمیل‌های عرضه‌شده توسط شرکت‌هایی چون AOL و Yahoo، صندوق الکترونیک کاربران، روزانه مقصد نامه‌های زنجیره‌ای با هدف خبررسانی و درخواست برای امضای نامه‌های سرگشاده اینترنتی (e-petition) شد. موضوع بسیاری از این نامه‌های سرگشاده یا زنجیره‌ای - که تا همین امروز نیز ادامه یافته - آزادی زندانیان سیاسی، تقاضای محکومیت نقض حقوق بشر، تحریم کشور و بنگاه اقتصادی ناقض قوانین و ناقض حقوق بشر بود.

در میانه دهه نخستین سال‌های ۲۰۰۰، وب دو (Web ۲,۰) با ظهور بلاگ‌ها و سرویس‌های اشتراک محتوایی مثل YouTube و بعد از آن شبکه‌های اجتماعی مثل فیس‌بوک و توییتر به انقلابی در تولید محتوا برای کاربران از سراسر جهان منجر شدند.

حضور مستقیم کاربران و استفاده نسبتا ساده از ابزارهای دیجیتال، برای ثبت و گزارش موارد نقض حقوق بشر، فساد و بی‌عدالتی و دریافت و بازنشر همزمان آن موارد، توسط میلیون‌ها کاربر از سراسر گیتی، تحولی عمیق در عرصه حقوق و قضا بود که تاثیرات روزافزون آن تا همین امروز ادامه دارد.

برای مقایسه این تاثیرات، می‌توان از مثال‌های بی‌شماری استفاده کرد. مقایسه بازتاب رویدادهای منجر به اعتراضات ۱۸ تیرماه ۱۳۷۸ و حمله به کوی دانشگاه تهران با سرکوب خونین خرداد ۱۳۸۸ و تظاهرات گسترده متعاقب آن در فاصله‌ای کم‌تر از ۱۰ سال، دگرگونی عمیق فضای ارتباطی کشور را به نمایش می‌گذارد. اگر چه سال ۱۳۸۸ دوران آغاز عضویت ایرانیان در شبکه‌های اجتماعی مثل فیس‌بوک و توییتر است، اما در همین مدت کوتاه میلیون‌ها شهروند ایرانی از این رسانه‌ها و همچنین تلفن‌های هوشمند دارای دوربین، برای ثبت وقایعی تاریخ‌ساز مانند «صحنه قتل ندا آقاسلطان» توسط نیروهای دولتی استفاده می‌کنند.

هزاران ساعت، مدرک تصویری و صوتی از سرکوب معترضان توسط شهروندان به اشتراک گذاشته می‌شود و نام و وضعیت معترضان بلافاصله پس از بازداشت - مثلا در مواردی چون افشای بازداشتگاه کهریزک و قتل معترضانی چون محسن روح‌الامینی و امیر جوادی‌فر - حتی عالی‌ترین سطوح حکومت را به عقب‌نشینی و صدور دستور بازخواست از مسئولان کهریزک وادار می‌کند.

ده سال مابین سال‌های ۱۳۷۸ تا ۱۳۸۸، دوران جوانه‌زدن استفاده از شبکه‌های اجتماعی و تکنولوژی دیجیتال و پیامدهای حقوقی و قضایی آن در ایران است. در این دوران حکومت جمهوری اسلامی در شکلی تدافعی، با پایین نگاه‌داشتن سرعت اینترنت و تلاش‌های عمدتا ناموفق برای فیلتر اینترنتِ آزاد و پاره‌ای اقدامات دیگر در صدد مهار موج استفاده عمومی از اینترنت توسط منتقدان و کنشگران هوادار حاکمیت قانون و گشایش است.

استفاده روزافزون از اینترنت توسط معترضان و پیامدهای حقوقی و قضایی آن، منحصر به ایران ما نیست. در سراسر جهان فعالان و کنشگران، قدرت ابزارها و سرویس‌های دیجیتال برای مبارزه مدنی و حقوقی را درمی‌یابند. یک سال پس از استفاده گسترده از ابزارهای دیجیتال توسط معترضان ایرانی، موج اعتراضات گسترده موسوم به «بهار عربی» سراسر دنیای عرب را درمی‌نوردد و به سقوط چندین نظام اقتدارگرا یا دیکتاتوری دیرپا در مصر، تونس و لیبی می‌انجامد.

اگرچه اعتراضات بهار عربی به شکلی تمام‌عیار، قابلیت‌های بی‌نظیر شبکه‌های اجتماعی در ساماندهی اعتراضات مردمی و بسیج عمومی در برابر قدرت‌های سرکوبگر را به نمایش می‌گذارند، اما همان‌گونه که در ادامه این دوره خواهیم دید، زنگ‌های خطر را برای قدرت‌های اقتدارگرا و مستبد بین‌المللی مانند «چین»، «روسیه» و «جمهوری‌اسلامی» به صدا درمی‌آورند.

آنچه در ده سال پس از اعتراضات ماه‌های ابتدایی سال ۲۰۱۱ شاهد هستیم، بسیج تمامی امکانات از سوی کشورهایی چون چین، روسیه و ایران برای ازمیان‌برداشتن خطر استفاده فعالان از اینترنت و تبدیل تکنولوژی دیجیتال به ابزاری موثر برای سرکوب و کنترل است.

با گسترش اعتراضات به سوریه در بهار و آغاز تابستان ۲۰۱۱ و سرکوب خونین

معترضان توسط دولت اسد با استفاده از ادوات سنگین نظامی مثل تانک، شهروندان معترض تصاویری تکان‌دهنده و غیرقابل باور از خشونت علیه غیرنظامیان را از طریق شبکه‌های اجتماعی و پیام‌رسان‌ها منتشر می‌کنند، تصاویری که در مدت‌زمانی کوتاه، توسط تلویزیون‌های ماهواره‌ای و کابلی در سراسر جهان پخش می‌شوند.

معترضان و گروه‌های حقوق بشری در سوریه همچنین، از دیگر قابلیت‌های شبکه‌های اجتماعی برای ردیابی قربانیان، بازداشت‌شدگان و همین‌طور افشای هویت سرکوبگران استفاده می‌کنند. در درس‌های بعدی دوره، به چند نمونه از کاربرد شبکه‌های اجتماعی در شناسایی قربانیان از یک سو و ناقضان حقوق بشر از سوی دیگر، اشاره خواهیم کرد و از تلاش‌های حکومت‌های ایران، سوریه و روسیه برای فریب و هک فعالان حقوقی و توقف انتشار تصاویر و اطلاعات مربوط به سرکوب معترضان در سوریه خواهیم گفت.

به فاصله کوتاهی از رویدادهای خون‌بار سوریه، این‌بار کی‌یف - پایتخت اوکراین - شاهد استفاده گسترده معترضان از اینترنت بود. یک فراخوان فیس‌بوکی از شهروندان اوکراینی خواسته بود برای اعتراض به فشار روسیه بر اوکراین، برای توقف گسترش روابط با اتحادیه اروپا به خیابان بیایند. اجتماع مصمم و طولانی شهروندان در میدان استقلال کی‌یف و سرکوب آنان توسط نیروهای ویژه هوادار روسیه، جنبه‌های دیگری از استفاده وکلا و فعالان حقوق بشر از شبکه‌های اجتماعی، پیام‌رسان‌ها و سرویس‌های آنلاین اطلاع‌رسانی را به نمایش گذاشت.

Euromaidan SOS، ابتکاری از سوی چند دانشجوی حقوق و فعال حقوق بشر است که با کمک حقوقی و اطلاع‌رسانی از وضعیت ناپدیدشدگان و زندانیان‌سیاسی آغاز شده و به یکی از موفق‌ترین نمونه‌های حمایت حقوقی از قربانیان نقض‌حقوق‌بشر تبدیل شده است. در درس‌های بعد، این ابتکار و همچنین تدابیر دستگاه سرکوب برای مقابله با آن را مفصل مورد بحث قرار می‌دهیم.

واکنش گسترده و تمام‌عیار نظامی، رسانه‌ای و اطلاعاتی، به پیروزی شهروندان خواستار گشایش و شکست رئیس‌جمهور دست‌نشانده روسیه در اوکراین را می‌توان آغاز عصر جدیدی از تلاش همه‌جانبه قدرت‌های اقتدارگرای جهانی برای توقف و به عقب‌بازگرداندن مطالبات دمکراتیک شهروندان دانست.

اشغال بخشی از اوکراین و آغاز عملیات نظامی علیه دولت منتخب این کشور، با

گسترده‌ترین حجم از عملیات رسانه‌ای و ارتباطی علیه اوکراین و متحدان این کشور همراه بود. بخش بزرگی از این عملیات را می‌توان در به‌روزرسانی و به‌کارگیری ابزارهای اطلاعاتی دوران جنگ سرد علیه کنشگران مدنی و فعالان سیاسی خواستار تغییر در جای‌جای جهان، به‌خوبی رصد و مشاهده کرد.

به طور مثال شباهت تکنیک‌ها و عملیات دیجیتال علیه مستندسازان نقض حقوق بشر در اوکراین از ۲۰۱۴ و سوریه از ۲۰۱۵، انکارناپذیر است و مطالعه این ابزارها، می‌تواند ما را در شناسایی و ردیابی این موراد و همین‌طور مقابله با کپی‌برداری توسط جمهوری‌اسلامی، یاری کند.

از سال‌های نیمه دوم ۲۰۱۰، قدرت‌های اقتدارگرا، به‌روشنی، بخش قابل توجهی از امکانات و منابع خود را برای تسلط بر عرصه تکنولوژی دیجیتال، بسیج کردند. تخصیص منابعی عظیم و پیشرفت تکنولوژی سرکوب از یک سو و به‌روزرسانی ابزارهای قانونی، قضایی و امنیتی برای کنترل فضای دیجیتال، از سوی دیگر، بازی را این بار به نفع اقتدارگرایی تغییر داد. از دخالت گسترده در انتخابات کشورهای آزاد گرفته، تا ده‌ها و صدها هک و آزار بین‌المللی چهره‌های سیاسی و فعالان دموکراسی‌خواه، از ایجاد مجموعه‌هایی عظیم و اهریمنی چون IRA در روسیه یا ده‌ها و صدها گردان سایبری در چین و ایران گرفته تا اختلاف‌افکنی، جعل، نشر اطلاعات نادرست (Disinformation) و جعلی اخبار، همه و همه از پیامدهای موج تهاجمی اقتدارگرایان پس از سال ۲۰۱۴ بودند - هجمه‌ای که تا امروز ادامه دارد.

شبکه‌های اجتماعی و سایت‌های اشتراک محتوا، مثل YouTube - که روزگاری امید اصلی کنشگران مدنی برای انتشار پیام، تماس با شهروندان و نظارت بر نهادهای قدرت و پاسخگویی بودند - با توسعه ابزارهای پیچیده اطلاعاتی-روانی از سوی قدرت‌های اقتدارگرا برای انتشار بخش بزرگی از تبلیغات مسموم، اختلاف‌افکنی و ایجاد نفرت در سراسر جهان مورد استفاده قرار می‌گیرند.

سرمایه‌گذاری کلان روی تحقیقات گسترده و پیشرفت تکنولوژی در جمهوری خلق چین، از یک سو و به‌روزرسانی ابزارهای اطلاعاتی کا.گ.ب (KGB) از دوران جنگ سرد توسط روسیه، از سوی دیگر، دورنمای تیره‌وتاری را مقابل فعالان حقوق بشر و وکلای خواستار حاکمیت قانون و عدالت، ترسیم می‌کند. در فصل‌های آینده به مطالعه موردی

استفاده از این پیشرفت‌ها در کنترل دیجیتال شهروندان اشاره خواهیم کرد.

سال‌های پایانی ۲۰۱۰ اما، یکسره عرصه پیروزی قدرت‌های اقتدارگرا نبود. با تلاش فعالان خواهان شفافیت و مقابله با فساد و همکاری میان وکلا و روزنامه‌نگاران، مجموعه عظیمی از اسناد سرّی، بیانگر فساد گسترده بسیاری از رهبران کشورهای عموما اقتدارگرا، منتشر شد و در دسترس عموم قرار گرفت. مجموعه اسنادی چون اسناد پاناما (panama)، اسناد پاندورا (pandora)، اسناد بهشت و چندین افشاگری دیگر، تصویری تکاندهنده از شبکه‌ها پیچیده فساد، رشوه، پول‌شویی و سوءاستفاده از مناصب سیاسی در سراسر جهان را به نمایش گذاشتند.

امروز، یعنی در تابستان ۱۴۰۱، جهان، عرصه جنگ تمام‌عیار میان اقتدارگرایان و دنیای آزاد است. برای نخستین‌بار، بخش بسیار بزرگی از این جنگ در دنیای مجازی و با بسیج همه‌جانبه منابع و استفاده از آخرین پیشرفت‌های تکنولوژیک صورت می‌پذیرد. از جعل اخبار و تصاویر و تولید محتوای صوتی-تصویری بسیار پیشرفته فِیک-دیپ (Deep Fake) گرفته تا به‌کارگیری هوش‌مصنوعی (AI) در تولید وسیع محتوای مسموم، نفرت‌افکنی و ایجاد تفرقه میان کنشگران مدنی و منتقدان.

از راه‌اندازی بات‌های (Bot) چندصدهزارشناسه‌ای برای تولید کامنت، لایک، گزارش تخلف و مواردی از این دست گرفته تا فراگیری عمیق (Deep Learning) و پردازش کلان‌داده‌ها (Big Data) و پیشرفته‌ترین روش‌های رصد و کنترل شهروندان در فضای فیزیکی و مجازی، همه و همه، بخشی از جنگ گسترده قدرت‌های اقتدارگرا علیه مطالبات شهروندان خواهان قانون، شفافیت و گشایش‌اند.

دیوار دیجیتال موسوم به «دیوار بزرگ آتش» در چین، طرح صیانت و مجموعه روبه‌رشدِ فیلترینگ و احراز هویت در ایران و همین‌طور سوءاستفاده گسترده از قوانین مربوط به بنگاه‌های خارجی و تروریسم در روسیه نمونه‌ای هستند از رویکرد این حکومت‌های دیکتاتوری برای ارعاب شهروندان کنشگر خود.

بازداشت و فشار قضایی بر وکلا در این کشورها، در کنار هک و جلوگیری از ارائه سرویس‌های دیجیتال به فعالان حقوقی منتقد، حضور نگران‌کننده جمهوری‌خلق چین در زیرساخت‌های ارتباطی دیجیتال سراسر جهان و امکان سوءاستفاده آتی از این موقعیت علیه منتقدان، طراحی و ایجاد ابزارهای هوش مصنوعی برای حذف محتوای منتقد، در

کنار تبلیغ برای اخبار جعلی و مواضع دولتی، همه و همه بخش کوچکی از مجموعه تدابیر اقتدارگرایان برای تبدیل تکنولوژی دیجیتال به ابزار سرکوب و کنترل‌اند. درباره این موارد در درس‌های بعدی دوره به طور مفصل بحث و گفت‌گو خواهد شد.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدامیک، از نخستین مثالهای کاربرد ابزارهای دیجیتال در عرصه حقوق و قضا است؟

الف) استفاده از شبکه‌های اجتماعی در انتشار ویدیوهای نقض‌حقوق بشر
ب) استفاده شهروند خبرنگاران از لایواستریم یا مخابره ویدیوی زنده
ج) امکان ارسال شکوائیه‌های آنلاین
د) استفاده از نقشه‌های گوگل‌مپس برای گزارش نقض حقوق بشر

۲- مهم‌ترین ریسک استفاده از وسایل دیجیتال توسط کنشگران در جوامع استبدادی چیست؟

الف) هزینه نسبتا بالا در مقایسه با شیوه‌های سنتی‌تر
ب) مشکلاتی نظیر فیلترینگ و در مواردی سرعت پایین اینترنت
ج) شنود و رصد حکومتی، هک و مراقبت از راه‌دور
د) احتمال سرقت و ضرر هنگفت مالی مثلا در مورد تلفن‌های هوشمند

۳- اهمیت تلفن‌های هوشمند در اعتراضات پس از سال ۱۳۸۸ در ایران چه بود؟

الف) استفاده از امکاناتی نظیر موقعیت‌یاب و بلوتوث برای تماس تظاهرکنندگان
ب) رمزگذاری داده‌ها و امنیت بالاتر تلفن‌های همراه
ج) افزایش قابل ملاحظه حافظه تلفن‌های همراه و امکان ذخیره حجم بالای فایل
د) ضبط و پخش تصاویر نقض‌حقوق بشر و خشونت دولتی علیه معترضان

درس دوم
امنیت دیجیتال در پروسه حقوقی

این درس، مهم‌ترین زیربنا برای ادامه مباحث این مجموعه است و در پایان آن شما به عنوان یک وکیل، دانشجوی حقوقی، فعال در یک سازمان مردم‌نهاد مدافع حقوق شهروندان قادر به ارزیابی، تخمین و ارتقای پروسیه امنیت دیجیتال محیط شخصی و کاری پیرامون خود در سطح زیربنایی و مفهومی خواهید بود.

ما از یک خانه، محل سکونت خانواده‌ای بزرگ واقع در یکی از پررفت‌وآمدترین، شلوغ‌ترین و ناامن‌ترین محله‌های یک شهر فرضی به عنوان مثالی برای تشریح ابعاد متفاوت طراحی پروسه امنیت دیجیتال استفاده خواهیم کرد. هدف از شبیه‌سازی امنیت سازمان، نهاد، دفتر وکالت یا حتی لپ‌تاپ یا تلفن‌همراه شما به یک منزل مسکونی، ترسیم اشکال مختلف تهدیدات امنیتی در دنیای واقع و جستجو برای راهکارهای مشابه پیشگیری در هر دو نمونه است.

خانواده پرجمعیت ما در یک خانه بزرگ زندگی می‌کنند. این خانه یک آدرس مشخص دارد و راه‌های ارتباطی این خانه با دنیای خارج عبارتند از درب‌های متعدد ورود و خروج مثلا درب‌اصلی، درب پارکینگ و درب پشت ساختمان، همچنین پنجره‌های طبقه همکف نیز می‌توانند در صورت بازبودن برای ورود به خانه مورد استفاده قرار گیرند. خانواده مرکب از پدر، مادر، پدربزرگ و مادربزرگ و چهار فرزند است.

قفل و کلید منحصر به فرد

امنیت ورود به خانه از طریق قفل و کلید تامین می‌شود. قفل و کلید خانه برای هر ۸ ساکن خانه یکسان است. یعنی هر عضو خانواده کپی چند کلید را در اختیار دارد که با آن می‌توان وارد خانه شد، درها را قفل و باز کرد. طبیعی است که این کلید و قفل‌ها مختص به ساکنان خانه هستند یعنی بقیه همسایگان و دوستان و افراد دیگر نمی‌توانند از کلیدهای خودشان برای ورود به این خانه استفاده کنند.

دیوار

دیوار مانعی فیزیکی و سخت است که خانه را از دنیای بیرونی جدا می‌کند. بدون وجود دیوار، درب و قفل بی‌معنی است. به صورت تئوریک هر نوع عبور از دیوار ناممکن است، چه برای اعضای خانواده و چه برای افراد ناشناس دنیای بیرون. استفاده از قفل، کلید و درب تنها راه ورود یا خروج از خانه‌اند. به این معنا که اگر یکی از اعضای خانه کلید خود را گم کند، طبعا نمی‌بایست راهی برای ورود و خروج از خانه داشته باشد. در دنیای واقعی و دیجیتال، مثال‌های بسیار استثنایی عبور از ورای دیوار وجود دارند که موضوع بحث این مرحله ما نیستند.

پنجره، بالکن و تراس

پنجره و بالکن اساسا برای ورود و خروج به خانه طراحی نمی‌شوند. پنجره و بالکن از راه‌های ورود هوای تازه و نور به داخل ساختمان‌اند. در مورد پنجره‌ها و بالکن چند تفاوت عمده با دیوار و درب منزل وجود دارد. تفاوت عمده پنجره و بالکن با دیوار، امنیت فیزیکی عموما کمتر است. دیوار ساخت معمولا محکمی است که بر خلاف پنجره یا درب بالکن باز و بسته نمی‌شود و از امنیت بالاتری برای جلوگیری از ورود افراد غیرمجاز به ساختمان برخوردار است. تفاوت دیگر پنجره و بالکن با درب ورودی یا پارکینگ یک‌طرفه‌بودن آن‌ها ست. پنجره از داخل ساختمان و به خواست ساکنان درون منزل به صورتی یک‌طرفه باز می‌شود، درحالی که درب از هر دو طرف امکان بازوبسته‌شدن دارد.

اشیاء و دارایی‌های حساس و قیمتی

تصور کنید باران شدیدی باریده است. شهر در معرض جاری‌شدن سیل قرار دارد. مقامات

محلی با بلندگو از ساکنان خانه می‌خواهند فورا شهر را ترک کنند. هر خانواده برای لباس‌پوشیدن، آماده‌شدن و خروج از خانه ۱۰ دقیقه فرصت دارد. ساکنان خانه هر یک فقط برای پرکردن یک ساک کوچک از ضروری‌ترین دارایی‌های خود وقت دارند و نه بیش‌تر. در شکلی مرسوم مدارک شناسایی، مدارک طبی و داروهای ضروری پدربزرگ و مادربزرگ، پول نقد یا اشیاء فوق‌العاده قیمتی و دارای ارزش احساسی و همچنین کیت کمک‌های اولیه، چراغ‌قوه و ...انتخاب عموم خانواده‌ها ست.

نکته مهم ایجاد نقشه و طبقه‌بندی هر کدام از هزاران شی موجود در خانه به «فوق‌العاده حساس»، «حساس و ضروری»، «ضروری برای زندگی روزمره»، «کارآمد ولی غیرحساس» و «ضروری» و سرانجام «غیرحساس» است. مثلا تلفن همراه، شناسنامه و لپ‌تاپ فوق‌العاده حساس ولی مبلمان خانه و پلوپز معمولا از حساسیت کمتری برخوردارند. همان‌طور که مشاهده می‌کنید، اولویت اول در تامین امنیت یک منزل مسکونی، حفاظت از جان و امنیت ساکنان و سپس دارایی‌های فوق حساس نظیر مدارک شناسایی، پول نقد، کارت‌های بانکی و همچنین اشیاء دارای بار احساسی است و در وهله بعد دارایی‌هایی چون تلویزیون، یخچال یا مبلمان.

زنگ هشدار، دزدگیر، زیرساخت‌ها و ابزارهای ایمنی

هر خانه مسکونی از شمار بسیاری از زیرساخت‌ها و امکانات ایمنی برخوردار است که این خانه را در برابر دسترسی خارجی مانند ورود غیرمجاز و سرقت و خطرات طبیعی نظیر باد، باران، رعدوبرق یا حشرات و آلودگی محافظت می‌کنند. همچنین شمار بسیاری از ادوات تشخیص دود و آتش، سنسورهای مربوط به گاز و مونوکسیدکربن و غیره در صورت خطر، بعضا به صورتی خودکار از سیستم اطفای حریق یا تماس با پلیس استفاده و در ساده‌ترین شکل پخش آلارم و هشدار به ساکنان را بر عهده دارند. طبیعی است که همه این ادوات می‌بایستی به صورتی دائم مورد ارزیابی و بررسی شوند.

پیش‌طراحی، نظارت بر ساخت و ارزیابی دائمی امنیت خانه

مرحله اول: پیش‌طراحی

پیش از ساخت خانه و خرید مصالح، همه ابعاد ایجاد و حفظ امنیت روی کاغذ طراحی و

میان معمار، طراح و سازندگان خانه مورد بحث و بررسی قرار گرفته است مثلا برای ساخت دیوار کدام یک از مصالح ساختمانی بهتر است؟ چه شکلی از درب و قفل استحکام و دوام بیش‌تری دارد و کدام پنجره در برابر بازشدن با زور از خارج خانه، بیش‌تر مقاومت می‌کند؟ آخرین تکنولوژی تشخیص دود و آتش چیست و مزیت‌ها و معایب دزدگیرهای مختلف کدام‌اند؟ این مرحله پیش‌طراحی پروسه امنیت است.

مرحله دوم: نظارت بر نصب

مرحله بعدی، نصب درست و اصولی و اطمینان از کارایی، دیوار، درب، قفل، پنجره، دزدگیر، سنسور و موارد مشابه آن است. این مرحله در واقع تطبیق و آزمایش کارآیی حفاظ‌های امنیتی قبل از ورود به منزل است.

پس از پایان این مرحله - یعنی نصب حفاظ‌ها، کلیدها برای درب ورود و پارکینگ تکثیر و کدهای مربوط به زنگ هشدار در اختیار ساکنان قرار می‌گیرد. ساکنان برای استفاده از این وسایل مثلا تجهیزات ورود و خروج، اطفای حریق و ... آموزش می‌بینند و با پایان این مرحله، پروژه به عنوان محصول در اختیار ساکنان قرار گرفته و استفاده از آن آغاز می‌شود.

مرحله سوم: نظارت و ارزیابی دائمی

با شروع استفاده از خانه، مرحله سوم - یعنی ارزیابی دائمی امنیت - آغاز می‌شود. بستن پنجره‌ها به هنگام خروج از خانه، قفل‌کردن درب و اطمینان از کارایی قفل، بررسی دوره‌ای و دائمی دزدگیر، دوربین و سنسورهای گاز، اطمینان از کارآمدی درب پارکینگ که ممکن است به خاطر طوفان و باد شدید درست بسته نشود. همان‌طور که مشاهده‌می‌کنید ساکنان از روی یک لیست نوشته‌شده و اجباری، تک‌تک اقدامات امنیتی را هر شب و قبل از خروج از خانه و مخصوصا ترک خانه برای مسافرت انجام می‌دهند. امنیت تعطیل‌بردار نیست و برای همیشه و به صورتی متناوب تکرار، ارزیابی و بازتکرار می‌شود.

از بررسی مثال محل سکونت خانواده مورد بحث، ۱۰ اصل زیر به‌خوبی می‌توانند زیربنای همه هشت درس این درس‌نامه و ارتقای امنیت دیجیتال و حتی غیردیجیتال دفتر، محل‌کار، NGO، خانه، لپ‌تاپ و تلفن شما باشند.

امنیتِ تماما فردی، ناممکن است

رعایت امنیت کامل فردی، فقط زمانی ممکن است که فرد مزبور در دل جنگل یا عمق اقیانوس و بدون هر نوع تماس و ارتباطی با دیگران زندگی کند. ما در امنیت دیجیتال همانند امنیت شخصی متکی به همکاری دیگران هستیم. در مثال خانه مسکونی، همه باید درب را قفل و زنگ هشدار را فعال کنند و حتی اگر یک نفر در رعایت موارد امنیتی سهل‌انگاری کند، تلاش همه ساکنان دیگر بی‌اثر خواهد شد. در دفتر حقوقی هم کافی ست یکی از همکاران فلش‌دیسک ناشناس و آلوده‌ای را به کامپیوتر خود وصل کند، در این صورت حتی با رعایت تمام موارد ایمنی، خطر آلودگی دیگر دستگاه‌های وصل به شبکه وجود دارد. در این باره در دس‌ها بعدی بیش‌تر خواهیم گفت.

امنیت پروسه است، نه پروژه

خطرناک‌ترین تفسیر از امنیت به صورت عام و امنیت دیجیتال به شکل خاص، تلقی محصول و پروژه از امنیت است. مثلا با خرید آنتی‌ویروس، تلفن ساخت شرکت اپل و نصب فایروال و رمز عبور، امنیت ما کامل است و از این پس نیاز به کار خاصی نیست.

امنیت پروسه‌ای است مانند مثال خانه مسکونی که حتی پیش از طراحی و خرید مصالح آن آغاز، نیازمند فراگیری، مطالعه روزانه، به روزرسانی و آزمون متناوب است و هرگز پایان نمی‌پذیرد. در شکل بسیار ساده می‌توان گفت که درست مثل تخصیص زمان و هزینه برای بخش‌های مختلف دفتر حقوقی، همان‌گونه که مثلا برای اجاره و نظافت دفتر و همین‌طور آرشیو اسناد، وقت و هزینه صرف می‌شود، حفظ امنیت کار حقوقی شما نیز نیازمند صرف وقت و هزینه دائمی است.

امنیت بیشتر فرهنگ است تا محصول برتر

خرید قفل ضدسرقت و آخرین تکنولوژی زنگ‌های هشدار، هرگز امنیت خانه را بالا نخواهد برد مگر اینکه ساکنان منزل مورد بحث، فرهنگ رعایت موارد امنیتی را داشته باشند. در دفتر حقوقی شما اگر حتی یکی از همکاران‌تان از اعدادی مانند ۱، ۲، ۳، ۴ به عنوان رمز عبور استفاده کند، خرید و نصب آخرین سخت‌افزارِ امن کمکی به حفظ امنیت دفتر نخواهد کرد. بنابراین درست مانند فرهنگ بهداشت فردی، فرهنگ زیست جمعی و

خانواده، ایجاد و انتقال فرهنگ رعایت موارد امنیتی دیجیتال و غیر دیجیتال نقطه کانونی همه موارد دیگر است.

امنیت دلخواه و داوطلبانه نیست

در مثال منزل مسکونی همه ساکنان متعهد و ملزم به قفل‌کردن درب و بستن پنجره به هنگام ترک منزل‌اند. در دفتر حقوقی یا سازمان مردم‌نهاد شما و حتی در ارتباط شما با موکل هم نباید از کسی سوال شود که «آیا مایلید کامپیوترِ شما پسورد داشته باشد؟»، «آیا مایلید مدارک پرونده و مستندات فقط با سرویس‌های امن دیجیتال مورد تبادل و مکاتبه قرار گیرند؟» و «آیا مایلید از داده‌های حساس نسخه پشتیبان تهیه شود؟». تمام موارد بالا ضروریات کار جمعی و امن حقوقی است که تنها در صورت توافق عمومی همه افراد درگیر قابل ادامه و اجرا است.

زیربنای امنیت: مطالعه و رصد محیط پیرامونی

چه خطراتی منزل مسکونی ما را تهدید می‌کند؟ آیا ما در مجاورت دریا و رودخانه با خطر سیل مواجه‌ایم؟ آیا خانه همسایگان و اهل محل بارها مورد سرقت از طریق شکستن پنجره قرار گرفته است؟ مطالعه و رصد محیط پیرامونی، سنگ زیربنای همه تدابیر امنیتی شما ست. یک دفتر حقوقی در ایالات متحده آمریکا به احتمال قریب به یقین، بدون هیچ واهمه‌ای می‌تواند جلسه مطبوعاتی برگزار کرده و اسناد کشف‌شده از نقض حقوق بشر توسط پلیس یا خشونت احتمالی علیه اقلیت‌ها را در اختیار روزنامه‌نگاران و عموم قراردهد. به دلیل محیط و بستر کاملا متفاوت حقوقی، سیاسی و ساختاری ایران، همین عمل از سوی یک وکیل یا دفتر وکالت در ایران، با مخاطرات غیرقابل تصوری روبرو ست.

انتشار اسناد نقض حقوق بشر در کشور ما، تدابیری به‌شدت متفاوت از ایالات متحده آمریکا را می‌طلبد. در اینجا با مثالی بسیار روشن تاثیر تفاوت‌های محیطی در ایران و ایالات متحده برای شما روشن می‌کنیم:

متخصصان امنیت‌دیجیتال در ایالات‌متحده به وکلا هشدار می‌دهند که برای حفظ امنیت اسناد مربوط به پرونده‌های بسیار حساس برای دولت یا دستگاه قضایی آمریکا از سرویس‌های ایمیل عمومی مثل گوگل، پیام‌رسان‌ها و دیگر ابزارهای شبکه‌های اجتماعی

مانند یوتیوب یا فیس‌بوک استفاده نکنند چرا که مقامات دولتی به صورتی قانونی قادر به دست‌یابی برخی از این اسناداند. آیا همین توصیه در مورد عدم استفاده از Gmail به یک وکیل یا فعال حقوقی ایرانی صحیح است؟ البته که خیر. جی‌میل و دیگر محصولات شرکت گوگل در صورت رعایت دیگر موارد ایمنی، بهترین دوست و پشتیبان شهروندان دیجیتال کشورهای فاقد اینترنت آزاد نظیر ایران‌اند.

پیش‌طراحی امنیت دیجیتال روی کاغذ

درست مانند طراحی نقشه منزل، امنیت دیجیتال محل کار شما نیازمند طراحی روی کاغذ است. درها و پارکینگ، راه‌های ارتباطی شما با موکلان، دادگاه‌ها و وکلای دیگر، کلا مجاری ارتباطی شما با دنیای خارج هستند. این ارتباطات می‌توانند به صورت شنیداری، شنیداری-دیداری، ایمیل، ارسال و دریافت فایل و اشکالی دیگر باشند. با ترسیم همه این مجاری ارتباطی درست مانند طراحی حفاظت از خانه، نیازمند تدابیری برای حفظ و محرمانه‌ماندن این ارتباطات‌ایم.

آرشیو اسناد و مدارک موکلان، آرشیو مستنداتی که به صورت ناشناس برای شما ارسال می‌شود و آرشیو یادداشت‌های وکلا و همکاران شما در دفتر، بخش دیگری از اجزای پیش‌طراحی امنیت برای دفتر کار روی کاغذاند. الزام به طراحی روی کاغذ با هدف به‌اشتراک‌گذاشتن و ایجاد تعهد میان همکاران از یک‌سو و همچنین فکر و تدبیر جوانب مختلف آن از سوی دیگر است. نسخه کاغذی پیش‌طراحی امنیت البته می‌تواند به صورت دیجیتال انجام شده و همان‌گونه که بعدا خواهیم دید، دائما به‌روزرسانی و تکمیل شود.

طبقه‌بندی و اولویت‌گذاری، مهم‌ترین اجزای پیش‌طراحی امنیت

پیش‌از این به ارزیابی محیطی محل کار شما اشاره کردیم. کدام بخش از داده‌ها و اسناد شما حساس‌ترند؟ ازبین‌رفتن کدام بخش از یافته‌ها می‌تواند شما و دیگران را دچار مشکل بزرگ‌تری کند؟ آیا با از بین‌رفتن یک برگ سند، فرد بی‌گناهی روانه زندان خواهد شد؟ آیا مستندات پرونده سوءاستفاده یک مقام دولتی از اموال عمومی تنها در یک نسخه و به صورت کاغذی در کشوی میز دفتر یا آرشیو جی‌میل شخصی یکی از همکاران نگهداری می‌شود؟

درست مانند طلا، جواهرات، کارت‌های‌اعتباری و مدارک بانکی یا شناسنامه و پاسپورت، برخی از اسناد الکترونیکی، برخی از آرشیوها، برخی از فایل‌ها از دیگر فایل‌های معمولی و روزمره حساس و حیاتی‌تراند. در جلسات بعدی ایجاد چندین آرشیو مختلف، دسته‌بندی، طبقه‌بندی، رمزگذاری و ایجاد گاوصندوق‌های فیزیکی و دیجیتال متعدد هم برای حفاظت از اسناد و هم برای ارتباطات حساس مورد بحث و بررسی قرار خواهند گرفت.

ارزیابی و نظارت دائمی: نقشه، قانون، انضباط و تعهد

همان‌طور که در مثال خانه مسکونی بحث شد، تضمین امنیت خانه در ۳ مرحله نقشه (طراحی)، قانون و انضباط (مقیدکردن ساکنان به رعایت و تعهد)، برای الزام ساکنان به تکرار تدابیر امنیتی و عدم توقف آن است. در شکل روشن و مرسوم، نقشه و پروتکل استفاده از ایمیل، اپلیکیشن‌های ارتباطی مثل اسکایپ یا تلگرام، خرید و نصب مودم، کامپیوتر یا تبلت محل‌کار، استفاده از تلفن و اینترنت همراه در محل‌کار، استفاده از فلش‌دیسک و ... پیش از آغاز کار دفتر، به صورتی مکتوب در اختیار همکاران قرار می‌گیرد و پس از بحث و استدلال همه و همه به رعایت تمام و کمال این موارد ملزم می‌شوند.

در بسیاری از کشورهای جهان حتی قانون مصوب برای تغییر پسورد وکلا و مقامات قضایی مثلا هر ماه یا هر ۶ ماه وجود دارد. بدون ورود به محدوده تخصصی مثلا در زمینه نظارت الکترونیک بر ایمیل قضات فدرال در ایالات متحده، در آینده بیش‌تر از التزام به رعایت موارد توافق‌شده و اجباری امنیت دیجیتال در محیط کار قضایی خواهیم گفت.

انتخاب صحیح، نصب و کاربرد صحیح و نظارت دائمی

قبل از خرید و نصب سخت‌افزار، چه در مثال خانه و چه در مثال دفتر حقوقی، پس از بررسی خطرات محیط خاص آن خانه یا دفتر وکالت، سخت‌افزار، اپلیکیشن و سرویسی انتخاب خواهد شد که بیش‌ترین محافظت را از خطرات خاص آن محیط تضمین کند. مثلا در محیطی که موارد بسیاری از سرقت از طریق شکستن پنجره و درب‌های غیرمحافظت‌شده وجود دارند، نصب پنجره و درب ضدسرقت امنیت خانه را بالا خواهد برد. در کشور یا محیطی که ۹۹ درصد همه ویروس‌ها روی سیستم‌های عامل ویندوز یا اندروید منتشر می‌شوند، طبعا خرید و استفاده صحیح از محصولات شرکت اپل، شما را بیش‌تر در

برابر ویروس‌ها محافظت خواهد کرد. مثال ساده بالا البته به معنی تضمین امنیت شما برای همیشه نیست، حتی بهترین سخت‌افزار، بهترین فایروال، بهترین دزدگیر، بهترین نرم‌افزار یا سرویس ضدبدافزار یا جاسوس‌افزار نیز نیازمند آموزش، نصب صحیح و کاربرد و نظارت دائمی است. شما دائما می‌بایستی اطمینان حاصل کنید که شما و همکارانتان آخرین نسخه از این ابزارهای را در همه دستگاه‌های دفتر فعال و به‌روزرسانی کرده‌اند و آیا اگر سرویس و نرم‌افزاری که پنج‌سال پیش بهترین انتخاب بوده، امروز همچنان همان کارایی امنیتی را دارد یا سرویس‌هایی نوین و کارآمدتری جایگزین بهتری برای آن شده است؟

ضرورت به‌روزرسانی دائمی

بهترین سخت‌افزار، بهترین نرم‌افزار، بهترین و گران‌ترین سرویس‌های دیجیتال همگی نیازمند به‌روزرسانی‌اند. در حقیقت استفاده از سخت‌افزار یا نرم‌افزار قدیمی درست مثل قفل و درب و پنجره قدیمی، بازشدن درب خانه‌ی مجهز به زنگ هشدار روی همه افراد ناشناسی است که به دلیل قدیمی‌بودن و در عرض نیم‌دقیقه می‌توانند کد جایگزین برای سیستم هشدارِ خارج‌ازرده شما تولید کنند. شرکت‌های بزرگ ارائه‌دهنده خدمات کامپیوتری مثلا مایکروسافت، اپل و گوگل دائما محصولات خود را با هدف رفع حفره‌ها و مشکلات امنیتی به‌روزرسانی می‌کنند. توجه داشته باشید که تقریبا همیشه فعال‌کردن گزینه به‌روزرسانی خودکار بهترین انتخاب است اما در عین حال بسیاری از محصولات بسیار قدیمی مثلا نسخه ۱۵ سال پیش مایکروسافت ویندوز یا آیفون ۱.۰۰، دیگر از پشتیبانی و به‌روزرسانی شرکت‌های خالق‌شان خارج شده‌اند و برای استفاده امن مناسب نیستند.

بسیاری از کاربران این‌گونه ابزارها مثلا تبلت‌های قدیمی را به عنوان پخش‌کننده موسیقی یا قاب عکس استفاده می‌کنند و دور نمی‌اندازند، این عمل مخصوصا اگر با ادامه اتصال این وسایل به مودم و شبکه اینترنت خانگی یا دفتر شما همراه باشد، خطرناک است چرا که هکرها می‌توانند با استفاده از قدیمی‌بودن این دستگاه‌ها وارد شبکه خانگی یا کاری شما شده و به بقیه ابزارها نفوذ کنند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدامیک از موارد زیر بخشی از پروسه امنیت دیجیتال در دفتر کار شما نیست؟

الف) اتکای صرف به آنتی‌ویروس قوی و قابل اعتماد
ب) طراحی و بازبینی دائم پروتکل‌های امنیت دیجیتال
ج) حفاظت فیزیکی از ابزارهای دیجیتال مثلا هارددیسک اکسترنال
د) کدگذاری داده‌های حساس

۲- در اولین روزِ کاری در دفترِ جدید کدامیک از موارد زیر برای امنیت شما مهم‌تر است؟

الف) خرید و نصب یک مودم وایرلس امن
ب) خرید و نصب آنتی‌ویروس، برنامه‌های ضدِ جاسوس‌افزار و ایمیل مطمئن
ج) کدگذاری و ایجاد نسخه پشتیبان از اطلاعات دفترِ قبلی
د) طراحی پروسه امنیت دیجیتال برای یک دفتر حقوقی

۳: کدامیک از موارد زیر برای ارتقای امنیت ارتباط و تبادل داده‌ها با موکلین ضروری‌تر است؟

الف) شفافیت کامل در استفاده از شبکه‌های اجتماعی
ب) کدگذاری تمام ارتباطات، استفاده از پیام‌رسان‌ها و ایمیل‌های صددرصد امن
ج) مکاتبه فقط با نام و نشان واقعی و استفاده از فایل‌های فشرده یا zip
د) مکاتبه و ارسال فایل تنها با نرم‌افزارهایی نظیر PDF و Word

درس سوم
کاربرد و امنیت تلفن همراه و تبلت برای فعالان حقوقی و وکلا

در این درس به بحث پیرامون حفظ و ارتقای امنیت تلفن همراه شما می‌پردازیم. به صورت خلاصه مراد از تلفن همراه یا هوشمند در این درس فقط تلفن مثلا آیفون یا اندروید شما نیست. بلکه انواع تجهیزات ارتباطی مثلا تبلت و دیگر دستگاه‌های هوشمند با قابلیت اتصال به اینترنت و تماس متنی، شنیداری یا دیداری نیز به صورت اجمالی با عنوان تلفن همراه مورد بحث و بررسی قرار می‌گیرند.

تلاش ما در این مبحث ترسیم تصویری ساده و رسا از تهدیدات مختلفی است که در کمین تلفن همراه شما نشسته‌اند. در حالی که از دفتر کار شما با انواع و اقسام حفاظ‌های فیزیکی از دنیای بیرونی محافظت می‌شود، رمز عبور تنها مانع دسترسی دیگران به داده‌های تلفن همراه شما ست با این تفاوت که مثلا یک سارق برای ورود به دفتر و دزدیدن همه دارایی‌ها و اسناد شما به زمان و امکانات زیادی نیاز دارد اما با ورود از راه دور یک هکر به تلفن همراه شما، در کسری از دقیقه، میلیون‌ها تصویر، سند، صوت و دیگر داده‌های حساس قابل سرقت، تکثیر و پخش در سراسر جهان‌اند.

تلفن‌همراه تنها به شکل بایگانی یا مخزنی از اسناد تهدید نمی‌شود. یعنی تنها مشکل

نفوذ به تلفن همراه سرقت داده‌های حساس شما نیست. فرض کنید یک دستگاه امنیتی با استفاده از نرم‌افزارهای پیچیده نفوذ کنترل تلفن همراه شما را از راه دور در اختیار گرفته باشد. این دستگاه می‌تواند تلفن شما را به‌راحتی تبدیل به وسیله شنود، ضبط مکالمات و تصویربرداری کرده و حتی از راه دور از محیط اطراف شما ویدیو ضبط کند.

ما در اینجا با ذکر مثال‌هایی برای هر کدام از انواع مختلف تهدیدات، راهکارهایی را برای مقابله با هر یک ذکر خواهیم کرد.

تهدید فیزیکی تلفن همراه نیاز به توضیح مفصل ندارد. متاسفانه بسیاری از ما سرقت، جاگذاشتن و گم‌شدن، آسیب در شکل ضربه‌خوردن و شکستن تلفن‌های همراه خود را تجربه کرده‌ایم.

۴ تهدید امنیتی پس از ازدست‌رفتن تلفن همراه

۱- تقریبا همیشه انبوهی از اطلاعات شما، اعم از ایمیل، یادداشت‌ها، شماره‌های تلفن و دیگر اشکال فهرست مخاطبان، تقویم، پسوردهای ذخیره‌شده، فایل‌های صوتی و ویدیوهای دستگاه‌تان از بین می‌روند.

۲- ارتباط ما با بسیاری از سیستم‌های احراز هویت از طریق موبایل قطع یا دچار اختلال می‌شود. مثلا بسیاری از بانک‌های الکترونیک، سیستم‌های پرداخت و انواع دیگری از سرویس‌های حساس دولتی و خصوصی هویت شما را با ارسال پیامک یا کد به تلفن همراه شما احراز می‌کنند و شرکت‌های گوگل و اپل از دستگاه‌های اندروید و آیفون برای تایید رمز و ورود به سرویس‌هایی نظیر پست‌الکترونیکی بهره می‌گیرند. طبیعی است که در صورت ازبین‌رفتن تلفن شما این امر دیگر مسیر نخواهد بود و در مواردی دسترسی شما مثلا به جی‌میل برای همیشه از بین خواهد رفت. احتمال بدتر اما سرقت موبایل شما ست که نه تنها دسترسی شما به داده‌ها و این سرویس‌ها را قطع خواهد کرد بلکه این احتمال وجود دارد که سارق یا افراد ناشناس به جای شما به سرویس‌هایی نظیر بانک الکترونیکی و دیگر سرویس‌های حساس متصل و اسناد و مدارک و حتی دارایی‌های شما را سرقت و مورد سوءاستفاده قرار دهند.

۳- تهدید فیزیکی علیه تلفن می‌تواند در پی چند دقیقه سهل‌انگاری صورت پذیرد. مثلا شما در دادگاه یا دادسرا برای چند لحظه تلفن خود را در بایگانی جا می‌گذارید و از آنجا که بسیاری از مکان‌های دولتی به هنگام ورود تلفن همراه افراد را به طور موقت از آنان تحویل می‌گیرند، موارد بسیاری پیش آمده که در این محدوده زمانی نرم‌افزارهای جاسوسی و شنود روی این تلفن‌ها نصب شده است که تهدیدی بزرگ برای امنیت شما خواهد بود.

۴- بخش دیگری از تهدیدات فیزیکی علیه تلفن همراه مجددا ناشی از سهل‌انگاری است؛ فرض کنید شما تلفن قدیمی خود را دور انداخته، هدیه داده یا می‌فروشید. اگر فهرستی از اقدامات امنیتی برای پاک‌کردن حافظه تلفن و برگرداندن آن به تنظیمات کارخانه را انجام نداده باشید، افراد غیرمجاز می‌توانند همچنان با استفاده از همان تلفن قدیمی به سرویس‌هایی نظیر بانک یا ایمیل شما متصل شوند.

۱۲ تدبیر امنیتی برای کاهش خسارت بر امنیت

۱- داده‌های غیرضروری را به صورت روزانه پاک کنید

هر روز، هر هفته یا به صورتی متناوب، وارد قسمت فایل‌های تلفن خود شوید و تا حد امکان همه موارد زیر را پاک کنید:

- فایل‌های قدیمی و غیرضروری در همه زیرشاخه‌ها، خصوصا قسمت دانلود
- تصاویر غیرضروری و قدیمی خصوصا تصاویر حساس
- پیام‌های شنیداری و دیداری آرشیوشده در مسنجرهایی مثل تلگرام، واتساپ و سیگنال
- حافظه اپلیکیشن‌ها (Cache) که بعضا با گذشت زمان چند گیگابایت می‌شود، خصوصا حافظه مرورگرها

البته پاک‌کردن فایل‌ها به‌تنهایی اطلاعات را به کلی از بین نمی‌برد و با نرم‌افزارها و متدهای بازیافت اطلاعات می‌توان حتی اطلاعات پاک‌شده را بازیافت کرد. بسیاری از کارشناسان در این زمینه، استفاده از نرم‌افزارها و اپلیکیشن‌های تمیزکاری حافظه،

پاک‌کردن فایل‌های زائد و غیرقابل بازیافت‌کردن فایل‌های پاک‌شده را توصیه می‌کنند.

اگر فایل‌های مشکل‌ساز غیر ضروری به‌درستی از حافظه موبایل شما پاک شده باشند، ضرر سرقت یا نفوذ به تلفن شما کم‌تر از وضعیتی است که هزاران صفحه اسناد، مدارک و تصاویر غیرضروری در پی سرقت یا گم‌شدن تلفن شما به دست افراد ناشناس بیفتد.

۲- پسورد، قفل اثر انگشت، تایید هویت بیومتریک

در سال‌های گذشته امنیت قفل ورود به تلفن‌های همراه به مراتب ارتقاء یافته است. در حالی که در ابتدای ظهور تلفن‌های موبایل از یک کد عددی (PIN) برای ورود به تلفن استفاده می‌شد. امروزه علاوه بر PIN مربوط به سیم‌کارت، PIN ورود به تلفن، امکان تعریف پسورد برای اپلیکیشن‌ها، قابلیت تایید هویت با اثر انگشت و دیگر نشانه‌های بیومتریک مثلا احراز هویت از طریق صورت کاربران نیز وجود دارد. امنیت این شیوها البته همچنان ۱۰۰ درصد نیست مثلا بسیاری از افراد برای شوخی قفل تلفن را با انگشت دوست در حال خواب یا صورت او باز می‌کنند. در مواردی از آینه یا دوربین‌های مداربسته از بالا، برای ضبط و بعدا کشف پسورد وکیلی استفاده شده که مثلا در یک اتاق انتظار دادگاه وارد تلفن همراه خود می‌شود. با این همه، تلفن همراه شما حتما و حتما می‌بایستی با مجموعه مستحکمی از پسوردهای متنی، شکلی، PIN، اثر انگشت و دیگر نشانه‌های بیومتریکی محافظت شده باشد.

۳- رمزگذاری (Encryption)

تمام داده‌های حساس شما اعم از پرونده‌ها، شواهد، فیلم، صدا، تصویر و موارد دیگری که برای فعالیت حقوقی شما مهم است و افشاء آن‌ها می‌تواند مشکل‌ساز باشد، بدون استثنا می‌بایستی رمزگذاری شوند. فرق حافظه یک تلفن رمزگذاری‌شده با تلفن معمولی در این است که در حالت دوم هر فردی می‌تواند با اندکی اطلاع فنی تمام داده‌های ذخیره‌شده روی آن تلفن را کپی و مشاهده کند اما برای مشاهده فایل‌های روی تلفن رمزگذاری‌شده، دیگران نیازمند پسورد اصلی رمزگذاری شما خواهند بود. توجه داشته باشید که در اغلب موارد اگر پسورد رمزگذاری تلفن و انواع دیگر حافظه خود را فراموش کنید با خطر از بین‌رفتن فایل‌های رمزگذاری‌شده برای همیشه مواجه خواهید بود.

۴- ایجاد نسخه پشتیبان (Backup)

بسته به نوع تلفن شما و تنظیمات آن، سیستم‌های عامل اندروید و IOS قادرند از تلفن و همه محتویات آن نسخه پشتیبان تهیه کنند. با این قابلیت اگر تلفن شما به هر دلیل از بین برود، بخش بزرگی از داده‌های نسخه پشتیبان، به‌سادگی قابل انتقال به تلفن جدید شما هستند. در عین حال بی‌توجهی در ایجاد نسخه‌های پشتیبان نیز می‌تواند امنیت داده‌های شما را تهدید کند.

اگر اکانت اصلی گوگل یا Icloud شما پسورد قوی، سیستم تایید هویت دومرحله‌ای نداشته باشد و به پیکربندی و تنظیمات امنیتی دیگر توجه نشده باشد، افراد غیرمجاز می‌توانند با استفاده از نسخه پشتیبان تلفن شما، همه داده‌های ریز و کوچک تلفن شما را روی دستگاه غیرمجاز و ناشناسی بازیافت کنند.

۵- جستجوی فیزیکی (Find My Phone)

با فعال‌کردن این قابلیت روی اکانت گوگل یا آی‌کلاود خود می‌توانید آخرین موقعیت تلفن اندروید یا آیفون و تبلت‌های خود را مشاهده کنید. این قابلیت خصوصا برای زمانی که تلفن‌تان را جا گذاشته باشید، به شما برای یافتن آن کمک می‌کند. مثل همه تنظیمات امنیتی دیگر این قابلیت نیز مانند شمشیری دولبه مزایا و معایب خود را دارد. مثلا اگر دسترسی غیرمجاز به اکانت اصلی گوگل شما ممکن باشد، فرد مهاجم می‌تواند از این طریق تمام مسیرهای رفت‌وآمد شما را با دقت خیابان و کوچه کنترل کند.

۶- تلفن من را پاک کن (Wipe my Phone)

هر دو سیستم عامل اصلی برای تلفن‌های هوشمند یعنی IOS و اندروید این توانایی را به شما می‌دهند که تلفن سرقت‌شده خود را از راه دور قفل یا پاک کنید. برای استفاده از این قابلیت تلفن شما می‌بایست روشن و متصل به اینترنت باشد. گرچه در مواردی می‌توان از این قابلیت حتی زمانی که تلفن به اینترنت وصل نیست هم استفاده کرد.

۷- مسدودکردن سیم‌کارت از طریق شرکت تلفن

پس از سرقت یا گم‌شدن تلفن همراه، خصوصا اگر از این تلفن برای ورود به ایمیل، بانک

و دیگر موارد حساس استفاده می‌کنید.
با تماس با شرکت ارائه‌دهنده خدمات تلفن موبایل می‌توانید سیم‌کارت خود را برای همیشه از بین ببرید و بعدا با ارائه مدارک و اثبات مالکیت سیم‌کارت دیگری دریافت کنید. این قابلیت مانع از استفاده از سیم‌کارت سابق شما توسط تبهکاران می‌شود. لازم به ذکر است که متاسفانه در شرایط امروز ایران و با کمک شرکت‌های تلفن همراه، دولت قابلیت دسترسی به سیم‌کارت همه مشترکان، خواندن پیامک‌ها و حتی ارسال پیامک به نام آنان را دارد.

۸- غیرفعال‌کردن Siri و Google Assistant

استفاده از فرمان صوتی برای تلفن‌هایی که از آن‌ها برای کارهای حساس استفاده می‌شود، خطرآفرین است به هر دو شکل اولا افراد می‌توانند بدون تایید شما و با تقلید صدا شماری از فرمان‌ها را روی تلفن‌تان حتی بدون حضور شما اجرا کنند و ثانیا با فراموش‌کردن خروجی صوتی مثلا پیامک‌ها یا پیام‌های واتس‌آپ در اتومبیل یا در میان جلسه برای شما با صدای بلند خوانده خواهد شد.

۹- قابلیت اعلان اپ‌ها را خاموش کنید

هنگام ورود به دادسرا، زندان یا مواردی که ناچار به تحویل موبایل خود هستید، اگر فراموش کرده باشید که اعلان‌ها یا نوتیفکیشن‌های متنی تلفن خود را خاموش کنید حتی با برخورداربودن از قفل و رمز مناسب افراد غیرمجاز قادر به خواندن بخشی از پیام‌های متنی شما خواهند بود که روی صفحه اصلی به شکل اعلان ظاهر می‌شود. پس با خاموش‌کردن هر نوع اعلانی روی صفحه اصلی، جلوی دسترسی افراد غیرمجاز به اطلاعات را بگیرید.

۱۰- خطرات نصب اینستاگرام، فیس‌بوک، تلگرام و واتساپ روی تلفن کاری

بخش عمده عملیات هک تلفنهای همراه، از طریق ارسال لینک‌های فریبنده در شبکه‌های اجتماعی صورت می‌پذیرد. ما به تفصیل در بخشی با عنوان «مهندسی اجتماعی»، نمونه‌هایی از این عملیات فریب را شرح خواهیم داد.

۱۱- به‌روزرسانی سیستم عامل تلفن همراه

هر دو سیستم عامل اندروید و IOS به صورت مرتب درخواست به‌روزرسانی یا آپدیت برای شما می‌فرستند. گوگل، اپل و شرکت‌های سازنده تلفن همراه همواره آخرین تهدیدات، حفره‌های امنیتی و همچنین برنامه‌های مخرب را رصد می‌کنند و برای رفع اشکالات احتمالی تولیدات خود، بسته‌های به‌روزرسانی را مرتبا برای کاربران ارسال می‌کنند. اهمال و تاخیر در به‌روزرسانی سیستم عامل، گشودن راه هکرها برای نفوذ به تلفن شما ست. در کنار سیستم عامل اندروید و اپل، firmware یا سفت‌افزار تلفن شما مثلا از شرکت سامسونگ یا سونی و دیگر سازندگان نیز همواره می‌بایستی آپدیت و به‌روزرسانی شود.

۶ ملاحظه امنیتی هنگام استفاده از تلفن‌های همراه

۱- اطمینان داشته باشید که شرکت‌های تلفن و دستگاه‌های امنیتی نزدیک‌ترین سطح همکاری را با هم دارند. فرض را بر این بگذارید که تمام مکالمات، پیامک‌ها، فهرست مخاطبان و شماره‌های مختص تلفن همراه یا IMEI، به صورتی نسبتا ساده در ایران قابل احراز هویت‌اند. دولت ایران از سال‌ها پیش کاربران را مجبور به ثبت هویت (Register) همه تلفن‌های همراهشان کرده است. با گذشت زمان، توان دولت‌ها برای مکان‌یابی، ذخیره مسیر حرکت و شنود مکالمات صوتی و متنی تلفن‌های همراه شهروندان، افزایش یافته است بنابراین فقط و فقط مطالبی را در تماس‌های تلفنی و پیامک منتقل کنید که مطمئنید منجر به ایجاد مشکل برای شما و مو کلانتان نخواهند شد.

۲- تجهیزات رهگیری میانی تلفن‌های همراه به‌سادگی در دسترس دولت‌ها قرار دارد و بر این اساس می‌توان تلفن‌های همراه را حتی خارج از مرزهای ایران با شیوه رهگیری میانی کنترل کرد. در ایران نهادهای مختلف قادرند حتی بدون کمک شرکت مخابرات این کار را انجام دهند مثلا در اطراف یک زندان یا در میانه یک تظاهرات یا در دفتر شما می‌تواند تجهیزاتی نصب شود که تمام تلفن‌های همراه مجاور به جای اتصال به دکل مخابرات محل، به آنتن یک دستگاه شنود میانی متصل شوند. استفاده از تجهیزات مشابه حتی در کشورهای آزاد نیز به بحث و جدل بسیار انجامیده است.

۳- تلفن کاری و حساس‌تان را از چشم‌ها دور نکنید، هرگز آن را در اختیار فرد دیگری حتی برای یک لحظه قرار ندهید چرا که با مراجعه به یک وبسایت یا اتصال چیزی شبیه کابل شارژر می‌توان در کسری از دقیقه تلفن همراه را آلوده کرد و بعدا وارد آن شد. ممکن است در زندان یا اتاق‌های دادگاه و دادسرا به شما پیشنهاد استفاده از یک پلاگ مثل شارژ داده شود. این امکان وجود دارد که سیم ظاهرا بی‌خطر شارژر در حقیقت وسیله‌ای برای کپی همه محتویات دستگاه موبایل شما باشد.

۴- هرگز و هرگز به هیچ شبکه یا مودم وایرلسی بیرون از دفتر کار یا خانه‌تان وصل نشوید و اگر مجبور به این کار هستید حتما تلفن خود را مجهز به وی.پی.ان با رمزگذاری قوی کنید. اتصال به وای‌فای ناشناس و بدون رمز مثلا در رستوران‌ها و هتل‌ها دعوت هکرها به سرقت اطلاعات تلفن شما ست.

۵- تلفن کاری شما باید حتی‌الامکان فاقد هر نوع اپلیکیشن غیرضروری باشد. اپلیکیشن‌های بازی و سرگرمی جایشان روی تلفن کاری نیست. هر یک از این اپلیکیشن‌ها قادرند راه نفوذ را برای تبهکاران باز کنند. حتی اپلیکیشن‌های نصب‌شده روی تلفن خود را در صورتی که هرگز از آن‌ها استفاده نکرده‌اید، یکی یکی پاک کنید. نصب هر اپلیکیشن APK یا از جایی غیر از فروشگاه Google Play و App Store، مثلا استفاده از «کافه‌بازار» تقریبا به صورت قطع و یقین احتمال هک‌شدن تلفن شما را افزایش می‌دهد.

۶- قابلیت‌های اتصالی غیرضروری مثلا NFC و Airdrop و بلوتوث را همواره در حالت خاموش نگه دارید و مراقب باشید که گزینه قابل کشف و رویت تلفن همراه حساس شما، توسط تلفن‌های مجاور خاموش باشد. هر یک از این شیوه‌های ارتباط خطرات خاص خود را ایجاد می‌کنند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام مورد می‌تواند خطرناک‌ترین تهدید استفاده از تلفن هوشمند شما باشد؟

الف) استفاده از تلفنی بدون قابلیت‌هایی نظیر موقعیت‌یاب

ب) استفاده از تلفن با سیستم‌عاملی به‌روز نشده

ج) استفاده از تلفن بدون امکاناتی نظیر NFC و اتصال ۵G

د) استفاده از تلفن با حافظه کم‌تر از ۱۶ مگابایت

۲- کدامیک از موارد زیر به یافتن تلفنِ گمشده شما کمک می‌کند؟

الف) Find my Phone

ب) تایید هویت دو مرحله‌ای ۲FA

ج) کدگذاری داده‌های تلفن

د) استفاده از PIN

۳- عدم توجه به کدام مورد زیر می‌تواند به ایجاد مشکل برای شما و موکلان‌تان بینجامد؟

الف) استفاده‌نکردن از تلفن‌های گران‌قیمت و سریع

ب) عدم اتصال از طریق وایرلس منزل و دفتر، به جای ۵G

ج) پاک‌کردن دائم داده‌های مشکل‌زا، حساس و غیرضروری

د) عدم استفاده از هندزفری و گوشی‌های بدون‌سیم برای مکالمه

درس چهارم
هوش مصنوعی (AI)، یادگیری ماشینی (ML) و کلان‌داده (BIG DATA)

انقلابی تمام‌عیار در دنیای دیجیتال در جریان است. هوش مصنوعی، کلان‌داده و یادگیری‌ماشین (Machine Learning) به واژه‌هایی روزمره بدل شده‌اند. فضای حقوق و قضا به عنوان یکی از اولین عرصه‌های کاربرد این دسته از تکنولوژی‌های نوظهور حتی همین امروز دچار دگرگونی غیرقابل تصوری است.

ما در این مبحث به ارائه دورنمایی از امکانات سودمند و همچنین خطرات بالقوه این ابزارها برای وکلا و فعالان حقوق و قضا می‌پردازیم. تمرکز ما در تهدیدات بیش‌تر روی نمونه‌های عینی استفاده حکومت‌های تمامیت‌خواه و سرکوبگر از تکنولوژی‌های نسبتا نوظهور یاد شده است.

با این همه آیا سربرآوردن تکنولوژی‌های نو و سوءاستفاده دولت‌های اقتدارگرا و تمامیت‌خواه از آنان به پایان هر نوع کنشگری، دادخواهی و فعالیت حقوقی و مدنی با هدف حفاظت از حقوق شهروندان خواهد انجامید؟ البته که خیر، چرا که همین امکانات - مثل استفاده از هوش مصنوعی - هم‌زمان به توانمندسازی بی‌مانند شهروندان نیز خواهد انجامید و رقابت بزرگ میان جامعه مدنی و فعالان از یک سو و اقتدارگرایان خواستار انسداد حوزه

عمومی از سوی دیگر، باز هم ادامه خواهد یافت. ما در درس سوم از این گفتارها به اختصار به یکی از کاربردهای هوش مصنوعی و کلان‌داده‌ها، در رصد تلفن‌های همراه شهروندان اشاره کردیم. شرکت‌های تلفن، انبوهی از داده‌ها - مثل موقعیت‌یاب GPS تلفن همراه شهروندان - را در اختیار دارند. با بهره‌گیری از یادگیری ماشین و هوش مصنوعی می‌توان این حجم عظیم داده را در پی‌کشف الگوهایی کلی یا حتی جزئی، کاوید. مثل هویت شهروندانی که در چند ماه گذشته در محلی خاص حاضر بوده‌اند یا از مسیری مشابه رفت‌وآمد کرده‌اند یا حتی احتمالا با یکدیگر ملاقات کرده‌اند. مثلا این امکان وجود دارد که هویت همه شهروندانی را که در تظاهرات‌های اعتراضی در نقاط متفاوت شهر حضور داشته‌اند را به‌سادگی و از طریق کاوش و پردازش داده‌های انبوه دکل‌های تلفن همراه احراز کرد.

۸ نمونه استفاده قانونمند از هوش مصنوعی و کلان‌داده‌ها

۱- مقابله با جرم و قانون‌گریزی

در سطح ملی و به شکل فزاینده‌ای در سطح بین‌المللی، هوش مصنوعی و کلانداده‌ها برای مقابله با گریز تبهکاران از قوانین مختلف، خصوصا قوانین مربوط به پول‌شویی، تحریم و تامین مالی تروریسم استفاده می‌شود. این فن‌آوری قادر است آخرین شیوه‌های تحریم‌گریزی گروه‌های تروریستی، تبهکاران و دولت‌های یاغی را با تجزیه و تحلیل میلیون‌ها تراکنش مالی، کشف کند.

۲- کشف و پیشگیری از کلاهبرداری

ارائه‌دهندگان سرویس‌های خرید و فروش آنلاین، ارائه‌دهندگان کارت‌های اعتباری، بان‌کها و دیگر مراکزی که همواره و به صورتی گسترده با پدیده کلاهبرداری اینترنتی روبرو بوده‌اند، امروزه از فن‌آوری هوش مصنوعی، یادگیری ماشین و کلان‌داده‌ها برای تشخیص و پیش‌بینی وقوع موارد بسیار متنوع کلاهبرداری استفاده می‌کنند. با تجزیه و تحلیل الگوهای رفتار آنلاین تبهکاران در فضای مجازی، تکرار و مشابهت با آن الگوها در انبوهی از داده‌های مربوط به تراکنش‌های آنلاین، به توقف و بررسی بیش‌تر برخی از این تراکنش‌ها می‌انجامد. البته باید توجه داشت که کارآمدی و دقت این تکنولوژی هرگز ۱۰۰ درصد

نیست یعنی هم مواردی از کلاهبرداری بدون تشخیص از سوی الگوریتم و هم مواردی از تشخیص اشتباه یک تراکنش مالی سالم به عنوان کلاهبرداری اتفاق می‌افتد.

۳- پیش‌بینی جرم و جنایت

در سال‌های گذشته توجه دستگاه‌های حافظ امنیت شهری، بیش از پیش به پیشگیری از وقوع جرم از طریق پیش‌بینی جرم و جنایت قبل از وقوع معطوف شده است. مثلا از روی تحلیل داده‌های مربوط به سرقت مانند مکان، طول و زمان وقوع سرقت می‌توان وقوع موارد مشابه و حتی آدرس احتمالی آن را با شباهت مناسبی پیش‌بینی کرد و از آن جلوگیری کرد. همچنین در مواردی باز از طریق داده‌های دکل‌های تلفن‌همراه و افزایش فعالیت شبکه‌ای از شماره‌های تلفن در ساعاتی خاص از روز و شب نیز می‌توان وقوع انواعی از جرایم سازمان‌یافته را قبل از وقوع پیش‌بینی کرد.

۴- احراز هویت از راه شناسایی چهره

بسیاری از فرودگاه‌های جهان امروزه بدون دخالت ماموران کنترل پاسپورت از دوربین‌های شناسایی چهره برای تطبیق هویت افراد با داده‌های بیومتریک پاسپورت آنان استفاده می‌کنند. این فن‌آوری و گسترش آن به سایر عرصه‌ها ارائه بسیاری از خدمات شهری را تسهیل کرده و همچنین به آسان‌کردن تردد شهروندان به اماکن مختلف انجامیده است.

۵- بررسی شواهد و مستندات پرونده‌های قضایی توسط ماشین

در جریان دادرسی و بررسی شواهد و مستندات، هوش مصنوعی قادر است با پردازش حجم انبوهی از داده‌های مرتبط با موضوع پرونده، مثلا داده‌های بیولوژیک، ژنتیک نظیر DNA و همچنین مدل‌سازی از موضوع قضایی پرونده و مقایسه آن با ده‌هاهزار مورد مشابه، به وکلا و قضات کمک کند تا با دقتی بیش‌تر و صرف وقت و هزینه کم‌تر جوانب مختلف پرونده و مستندات آن را بررسی‌کنند.

۶- کشف فساد قضایی و نظارت بر عملکرد قضات و دادستان‌ها

در برخی کشورهای جهان، حتی همین امروز نوعی نظارت برآمده از تکنولوژی اطلاعات

از آغاز تا پایان روند دادرسی اعمال می‌شود مثلا قضات از نوعی فن‌آوری نظارتی دیجیتال استفاده می‌کنند. با جمع‌آوری و تحلیل انبوه داده‌های مربوط به محاکمات توسط الگوریتم، مواردی غیرطبیعی از صدور یا عدم صدور احکام در شعبات مختلف کشف می‌شود و کار را برای متخلفان احتمالی مثلا قضات فاسد سخت‌تر و سخت‌تر می‌کند.

۷- راستی‌آزمایی اسناد، شواهد و قراردادها

بر خلاف دوران سابق که تایید صحت یک برگ سند، گواهی تولد، ازدواج یا قرارداد نیازمند کار کارشناسی و استعلام و ارجاع به بایگانی‌ها کاغذی بود، فن‌آوری هوش مصنوعی امروز قادر به تشخیص اعتبار بسیاری از اسناد مثلا قراردادها ست، همان‌طور که در بخش تشخیص کلاهبرداری عنوان شد با پردازش الگوها و شیوه‌ها از خلال کلان‌داده‌ها می‌توان الگوریتم‌هایی را برای تشخیص صحت اسناد و مدارک توسعه داد؛ الگوریتم‌هایی که به ظهور نسل نوینی از سیستم‌های پردازش اسناد الکترونیکی انجامیده‌اند.

۸- تشخیص و مقابله با هک، حملات سایبری

هم‌زمان با افزایش استفاده و همچنین پیچیدگی حملات هکری توسط مجموعه متکثری از دولت‌های اقتدارگرا تا گروه‌های تبهکار و تروریستی، هوش مصنوعی با فراتررفتن از محدودیت‌های تشخیص و مقابله با حملات سایبری به خط محکمی از دفاع در برابر جاسوسی الکترونیک دولت‌هایی نظیر چین و همچنین حملات خرابکارانه و سایبری حکومت‌های سرکوبگری چون ایران، کره شمالی و روسیه بدل شده است.

پیش از ظهور تکنولوژی حفاظت سایبری از داده‌های حساس، به دلیل نیاز به منابع عظیم تکنولوژی و نیروی انسانی در انحصار دولت‌ها و سازمان‌های نظامی بود. حال آنکه با بهره‌گیری از هوش مصنوعی حتی کاربران عادی و فعالان و کنشگران نیز می‌توانند خود را در برابر حملات نسبتا پیچیده دولتی محافظت کنند.

دورنمای سوءاستفاده دولت‌های سرکوبگر از هوش‌مصنوعی و کلان‌داده‌ها

ناظران، همه دهه گذشته را شاهد ظهور و افزایش موارد سوءاستفاده حکومت‌های سرکوبگر از تکنولوژی‌های نوظهور ذکرشده بوده‌اند. جمهوری خلق چین با اختلاف بسیار از دیگر

حکومت‌های اقتدارگرا مشغول توسعه، آزمایش و راه‌اندازی سازوکارهای کنترل و سرکوب متکی به هوش‌مصنوعی است.

در درس‌های بعدی در بخشی مجزا به ذکر مواردی از استفاده اقتدارگرایانه از تکنولوژی‌های نوظهور اختصاص داده‌ایم چرا که اطمینان داریم این نوع تکنولوژی به‌زودی توسط دیگر قدرت‌های اقتدارگرا و از جمله جمهوری اسلامی ایران علیه فعالان حقوق بشر، کنشگران و شهروندان عادی، آزمایش و به کار گرفته خواهد شد.

۱۱ نمونه از سوءاستفاده دولت‌های سرکوبگر از هوش‌مصنوعی و کلان‌داده‌ها

۱- فن‌آوری تشخیص چهره و صدا

هم‌اینک در جمهوری خلق چین با نصب میلیون‌ها دوربین مداربسته و همچنین شبکه پیچیده و متکثری از اپلیکیشن‌های موبایل گرفته تا دوربین اماکن خصوصی و دولتی از چهره و دیگر مشخصات بیومتریک شهروندان برای کنترل نامحسوس استفاده می‌شود.

تصور کنید توسعه این تکنولوژی و استفاده از آن در راهروهای مترو، محل عابربانک‌ها و دوربین‌های مداربسته متعدد می‌تواند عرصه عمومی را کاملا زیر چتر کنترل دولتی قرار دهد تا جایی که کوچک‌ترین حرکت شهروندان نیز از دید الگوریتم‌های حساس، مثل تجمع و ملاقات چند شهروند در گوشه‌ای از پارک، مخفی نماند. همین تکنولوژی را می‌توان برای تشخیص صدای مکالمه یک یا چندصد فرد خاص از هر جای کره زمین و از خلال میلیون‌ها تماس تلفنی، مکالمه صوتی یا پیام‌رسان‌ها به کار گرفت.

۲- دست‌کاری شبکه‌های اجتماعی و افکار عمومی

ظهور وبلاگ‌ها و سپس شبکه‌های اجتماعی و سایت‌های تولید محتوا توسط شهروندان مانند YouTube، توییتر و فیس‌بوک، در میانه دهه ۲۰۰۰ میلادی، به چالشی بزرگ برای نظام‌های اقتدارگرا که برای کنترل کامل فضای رسانه‌ای تبدیل شد. شهروندان با انتشار انتقادات و گزارش ابعاد وسیع نقض حقوق بشر، احکام قضایی ناعادلانه و بدون محاکمه، به صورت مستند از ظلم و بی‌عدالتی پرده برداشتند. فعالان از این شبکه‌ها برای تشکل، سازماندهی و اعتراض مدنی بهره گرفتند. حکومت‌های سرکوبگر در مدت‌زمانی نسبتا کوتاه

تلاش‌های خود را متوجه توسعه و استفاده از تکنولوژی دیجیتال برای سرکوب کردند. شما همه واژه‌هایی مانند بات و ربات را شنیده‌اید، لشکری انبوه از کاربران غیر واقعی که با هدف نمایندگی غیرواقعی، جهت‌دهی، دستکاری و بعضا انحراف افکار عمومی سازماندهی می‌شوند. در مواردی بسیار وظیفه ایجاد اختلاف و چنددستگی میان منتقدان را بر عهده دارند یا به صورت دروغین حمایت کامل افکار عمومی از سیاست‌های نظام مستبد حاکم را برای دنیای بیرون روایت می‌کنند. با ظهور تکنولوژی‌های نوظهور نظیر هوش مصنوعی و کلان‌داده‌ها ایجاد و راهبری مجموعه‌های بزرگ و چندصدهزارنفری از پروفای‌لهای دروغین در فضای مجازی ساده‌تر شده است.

۳- آزار و اذیت، جعل و ترور شخصیت

بسیاری از شما موارد خلق و انتشار تصاویر یا صدای جعلی سیاستمداران را که با بهره‌گیری از هوش مصنوعی خلق شده‌اند و به ویدئو یا صدای واقعی ایشان شباهت بسیار دارند حتما دیده‌اید. محتوایی که از آن با نام Deep Fake از آن یاد می‌شود.

امروزه با دست‌کاری شبکه‌های اجتماعی، از تکنولوژی برای زیرسوال‌بردن گروهیِ روایت قربانیان نقض حقوق بشر یا گزارشگران طرفدار عدالت استفاده می‌شود. به این ترتیب که انبوهی از حساب‌های کاربری در شبکه‌های اجتماعی که توسط نرم‌افزارهای پیچیده هدایت می‌شوند، دست به ترور شخصیت مخالفان، منتقدان و فعالان حقوق بشر می‌زنند، آن‌ها با بهره‌گیری از الگوریتم جذب مخاطب در این پلتفرم‌ها و سایت‌های اشتراک محتوا و همچنین شیوه‌های پیشرفته داده‌کاوی از کاربران - بر اساس ویژگی‌ها و تعلقات این افراد - حتی بدون نیاز به ارعاب، بازداشت و آزار فیزیکی، به صورت دیجیتالی و آنلاین، فعالان را مورد اذیت و آزار قرار می‌دهند.

۴- دسته‌بندی و ایجاد پروفایل برای گروه‌های اجتماعی

در سال‌های گذشته اطلاعات و شواهدی مفصل از آزار گرفته تا تعقیب دسته‌جمعی، بازداشت و بازآموزی در اردوگاه‌های کار اجباری علیه اقلیت اویغور مسلمان در چین منتشر شده است. بر اساس این اطلاعات بخشی از شناسایی و کنترل فعالیت‌های شهروندان اویغور در چین، با استفاده از شیوه‌های پیچیده دیجیتال انجام می‌پذیرد. سوءاستفاده

از هوش مصنوعی برای طبقه‌بندی، شناسایی و داده‌کاوی (Data mining) شهروندان توسط الگوریتم‌های هوش مصنوعی - مثلا بر اساس رنگ پوست، مشخصات نژادی یا شیوه پوشش آنان - می‌تواند به سطحی بی‌سابقه از تبعیض مثلا در فرودگاه‌ها، اماکن عمومی یا توسط پلیس بیانجامد.

۵- فیلترینگ، محدودیت دسترسی به محتوا

شما هم حتما واژه فیلترینگ هوشمند را بسیار شنیده‌اید. فیلترینگ هوشمند رویای حکومت‌های سرکوبگر برای فیلتر گزینشی بخشی از محتواهایی است که به زعم آن‌ها مشکل‌ساز است. اگر انسداد و قطع کامل اینترنت به نارضایتی گسترده عمومی می‌انجامد تلاش این دسته از نظام‌ها بر بهره‌گیری از فن‌آوری نظیر هوش مصنوعی برای انسداد گزینشی محتوا متمرکز می‌شود. مثلا بر خلاف شیوه‌های سابق، مثل انسداد نام دامنه، که می‌توانست با استفاده از شیوه‌هایی چون پروکسی از سوی شهروندان، دورزده شود این بار محتوی متنی یا تصویری با بهره‌گیری از هوش مصنوعی به دنبال تصاویر یک اعتراض یا نشان سمبل یک گروه منتقد واکاوی و فیلتر می‌شود.

۶- داده‌کاوی و شناسایی مخالفان

داده‌کاوی (Data Mining)، استفاده از یادگیری ماشین، کار با مجموعه‌های انبوه کلان‌داده و کشف الگوها و نتایج جستجو از خلال واکاوی و فهم اطلاعات انبوه است. فرض کنید مجموعه‌ای چندصدمیلیونی از فعالیت میلیون‌ها کاربر توییتر فارسی در ماه‌های اخیر را در اختیار دارید. با واکاوی این داده‌ها مثلا به دنبال الگوهای متنی مشخص، نگارش توسط یک کاربر خاص احتمالا می‌توان هویت او را حتی در حالت فعالیت با نام مستعار در توییتر با سطحی از تقریب جستجو کرد.

۷- کنترل اجتماعی از طریق امتیازبندی

در جمهوری خلق چین، نظام حاکم حتی امروز از نوعی فن‌آوری پیچیده امتیازبندی اجتماعی برای کنترل شهروندان استفاده می‌کند. در حالی که وابستگی به حزب حاکم کمونیست و شرکت در کمپین‌های مختلف آن برای شهروند امتیاز مثبت به ارمغان

می‌آورد و برعکس انتقاد از این حزب در شبکه‌های اجتماعی و سیاه‌نمایی آن، از امتیاز او خواهد کاست. شهروندان با از دست‌دادن امتیازات اجتماعی خود مثلا دیگر قادر به اخذ وام و تسهیلات بانکی نخواهند بود و می‌بایست راهی برای جبران و کسب امتیاز مثبت بیابند.

۸- تعقیب و مراقبت و شنود

حتما در گذشته نه‌چندان دور، تصاویر فیلم‌های سینمایی از شنود تلفن تبهکاران یا تعقیب آنان با خودرو توسط ماموران پلیس را دیده‌اید. این روشی بود که در گذشته از آن استفاده می‌شد، اما امروز نظام‌های تمامیت‌خواه با جدیت به دنبال توسعه شیوه‌های دیجیتال تشخیص مخالفت و انتقاد و سپس شنود خودکار، تعقیب رفت‌وآمدهای فرد منتقد مثلا با استفاده از تلفن همراه خود او یا ضبط خودکار مکالمات یا تصاویر افراد مرتبط با آن فرد منتقد هستند.

۹- دستکاری نتایج انتخابات

همان‌گونه که در جریان کشف شبکه IRA از تلاش گسترده با منشاء روسیه و با هدف تاثیر بر انتخابات در کشورهای آزاد، پرده‌برداشته شد، می‌توان انواع و اقسام عملیات انحراف و تاثیرگذاری بر نتایج انتخابات توسط دولت‌های اقتدارگرا را رصد کرد. از ایجاد شبهه و تردید نسبت به سلامت انتخابات، تا رادیکالیزه‌کردن فضای انتخاباتی و ایجاد درگیری و همچین ترور شخصیتی و تخریب نامزدهای مختلف، همه و همه امروز با بهره‌گیری از آخرین امکانات پیشرفته تکنولوژی دیجیتال نظیر هوش مصنوعی توسط این نظامها دنبال می‌شوند.

۱۰- دستکاری پرونده‌های قضایی و فساد

اگر با تلاش فعالان حقوقی مستقل و کنشگران جامعه مدنی مواردی از فساد و سوءاستفاده افشا شود، باز با استفاده از هوش مصنوعی مثلا با جعل اسناد و دستکاری پایگاه‌های بزرگ داده، مثل پایگاه‌های ملی ثبت سند، روایت فاش‌کنندگان فساد زیر سوال می‌رود. همان‌گونه که در مبحث Deep Fake اشاره شد خلق یک تماس تلفنی جعلی، اسناد

جعلی و حتی ویدئوی تقطیع‌شده و بازسازی‌شده توسط هوش مصنوعی می‌تواند فرجام دیگری را برای یک پرونده قضایی پرسروصدا رقم زند.

۱۱- حملات هکری و سرقت داده‌ها

در سال‌های گذشته حملات سایبری با پیچیدگی بیش از پیش با بهره‌گیری از یادگیری ماشین در ابعادی بسیار فراتر از حملات با منشا یک یا چند هکر، دولت‌ها، موسسات، گروه‌ها و اشخاص مختلف در سراسر جهان را هدف قرار داده‌اند. با بهره‌گیری از تکنولوژی مشابه، ایرادات و حفره‌های امنیتی سیستم‌های کامپیوتری و تلفن‌های همراه قربانیان کشف و با انگیزه‌های مختلف داده‌های ایشان به سرقت می‌رود. البته همان‌طور که پیش‌تر ذکر شد از همین نوآوری‌ها می‌توان برای مقابله و حفاظت از شهروندان در برابر این‌گونه حملات نیز استفاده کرد.

استفاده گسترده و به نوعی شیفتگی و علاقه نظام‌های تمامیت‌خواه به استفاده از آخرین یافته‌های مبتنی بر تکنولوژی اطلاعات نظیر هوش مصنوعی، آینده‌ای مبهم را پیش روی فعالان حقوق و قضا در این کشورها قرار داده است. این تکنولوژی‌ها مانند شمشیر دولبه قادرند شیوه‌های کنونی دفاع از حقوق اساسی شهروندان و اثبات ظلم و تعدی دولتی را با مشکل مواجه کنند، هر چند همان‌گونه که پیش‌تر عنوان شد، ممکن است به شهروندان عادی، فعالان جامعه مدنی و دیگر کنشگران نیز برای ایستادگی در برابر اقتدار نظام حاکم کمک کنند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- از هوش مصنوعی چگونه برای شناسایی و توقف تبهکاری مالی استفاده می‌شود؟

الف) با بهبود سرعت تراکنش‌های مالی خصوصا با استفاده از بلاک‌چین
ب) با کنترل میلیون‌ها ایمیل و کاوش در فایل های ضمیمه ایمیل‌ها
ج) با رصد و کاوش، میلیون‌ها تراکنش مالی و کشف الگوهای پول‌شویی
د) با کدگذاری پایگاه‌های بزرگِ داده از همه تراکنش‌های مالی ماه‌ها و سال‌های اخیر

۲- مهم‌ترین دغدغه در استفاده روزافزون هوش مصنوعی توسط دولت‌های مستبد چیست؟

الف) تضعیف نظام آموزشی خصوصا برای کودکان و نوجوانان
ب) صرف وقت شهروندان در شبکه‌های اجتماعی و نه دنیای واقعی
ج) بالارفتن سرعت تمام ارتباطات دیجیتال و انبوهی از فایل‌ها و داده‌ها
د) شناسایی و کنترل مخالفان، سرکوب انتقاد و شکل‌دادن به افکار عمومی

۳- کدام مورد، از فواید استفاده از هوش مصنوعی و یادگیری ماشین در عرصه حقوق نیست؟

الف) کاوشِ سریع انبوهی از داده‌های دیجیتال در پی الگوهای وقوع جرم
ب) کاوش کلان‌داده‌ها، آرشیو محاکمات و اثبات فسادِ قضایی
ج) جایگزینی کامل دادخواهی، قضاوت، وکالت و صدور و حقوق شهروندان با هوش مصنوعی
د) تحلیل عمیق مستندات با کاوش بانک‌های داده در پی مواردی مثل DNA و دیگر مستندات

درس پنجم
آرشیو و ثبت مستندات، امنیت آرشیو و داده‌ها

جستجو، آرشیو و ثبت مستندات

در درس پنجم از مجموعه مباحث امنیت دیجیتال برای وکلا و فعالان حقوق و قضا، به صورتی مختصر تاثیر انقلاب ارتباطات و ظهور دنیای دیجیتال در عرصه حقوق و قضا را بررسی خواهیم کرد. تمرکز ما در این مبحث کاربرد ابزارها و استفاده از امکانات پلتفرم‌های دیجیتال برای ارتقای کارآمدی فعالیت حقوقی توسط وکلا و دیگر فعالان عرصه حقوق و قضا است. وکالت دیجیتال در دنیای امروز و در کشور ما ایران دیگر امری چندان غریب و نوظهور نیست. جستجویی ساده در پیام‌رسان‌ها و شبکه‌های اجتماعی، ما را با تعداد قابل توجهی سرویس حقوقی دیجیتال آشنا خواهد کرد. وکلایی که بعضا خدمات خود را به صورت رایگان و داوطلبانه برای کمک به شهروندان مثلا بازداشت‌شدگان تظاهرات و جنبش‌های اعتراضی ارائه می‌کنند. وکلا امروز قادرند با استفاده از امکانات رمزگذاری‌شده پیام‌رسان‌هایی چون تلگرام با موکلان خود یا افراد نیازمند مشاوره و کمک حقوقی به صورتی بعضا ناشناس تماس متنی، شنیداری و دیداری داشته باشند. مستندات پرونده را به صورت دیجیتال دریافت و مطالعه کنند و چنان‌که در مبحث این درس اشاره خواهیم کرد با بهره‌گیری از انبوهی از داده‌ها و ابزارهای موثر دنیای دیجیتال وظایف حقوقی خود

را به بهترین نحو به انجام رسانند.

۱۲ روش موثر از امکانات دیجیتال دنیای اینترنت برای پیشبرد کارهای قضایی

۱- جستجوی موارد نقض حقوق شهروندان از خلال وب جهانی

حدود ۳ دهه از حضور موثر وب جهانی در عرصه عمومی می‌گذرد. با افزایش حضور و فعالیت شهروندان در فضای دیجیتال حالا بخش مهمی از کنش‌های اجتماعی در سراسر جهان روی وب جهانی و به صورت مجازی صورت می‌گیرد. شهروندان در ابعادی غیرقابل‌باور زندگی بعضا خصوصی خود را روی شبکه‌های اجتماعی با دیگران به اشتراک می‌گذارند. همه ما در سال‌های گذشته نمونه‌هایی از انتشار تصاویر و ویدئوهای مربوط به خشونت پلیس و گروه‌های تندرو مثلا علیه رنگین‌پوستان یا دیگر اقلیت‌ها را مشاهده کرده‌ایم. محتوایی که نشر آن بعضا به چندین هفته یا چندین ماه اعتراض گسترده انجامیده است. امروزه بخش بزرگی از فعالیت کوشندگان حقوق بشر و وکلا از طریق تحقیق و جستجو برای مواردی از این دست در شبکه‌های اجتماعی است و تحلیل آن با هدف کمک به پروسه حقوقی و وکالت صورت می‌گیرد.

هجوم پلیس به یک تجمع، استفاده نیروهای لباس‌شخصی از اسلحه برای سرکوب، ورود و بازرسی منازل و دفاتر اشخاص و گروه‌ها بدون ارائه حکم، همه و همه از مواردی هستند که انتشار محتوا توسط حاضران یا حتی عابران و افراد تماشاچی پیرامون حادثه بعدا به افشای ابعاد پنهان و بعضا زیرسوال‌بردن روایت ارائه‌شده توسط نهادهای سرکوبگر کمک می‌کند. خصوصا در سال‌های گذشته نوع نسبتا جدیدی از کمپین‌های انحراف افکار عمومی از بلاروس گرفته تا ایران و از روسیه تا ونزوئلا، خشونت علیه شهروندان را از اساس انکار می‌کند، جستجو، تحقیق و انتشار داده‌های موجود بیش از پیش ضرورت پیدا کرده است.

۲- تماس با شهود و قربانیان

همان‌گونه که در مورد قبل اشاره شد، مثلا پس از هجوم گروه‌های نیمه‌نظامی و لباس‌شخصی به دفتر یک نشریه، گردهم‌آیی زنان یا ضرب‌وشتم دانشجویان در خوابگاه، می‌توان با همه افرادی که ماجرا را روی شبکه‌های اجتماعی خود روایت کرده‌اند، تماس

گرفته یا با جستجوی معکوس تصاویر منتشرشده، شهود و قربانیان را شناسایی و پس از تماس، روایت ایشان را ثبت و ضبط کرد.

لازم به ذکر است که معمولا در موارد مشابه مخصوصا زمانی که یک طرف ماجرا دولت و نیروهای امنیتی قرار دارند تلاش‌هایی به موازات وکلا توسط نهادهای سرکوبگر و با هدف سکوت و ارعاب شهود و خانواده قربانیان با استفاده از داده‌های موجود در فضای مجازی در جریان است. در این‌گونه موارد، افشای همین تلاش‌ها در فضای عمومی به روشن‌شدن حقیقت و برخورد با ناقضان حقوق قربانیان کمک خواهد کرد.

۳- راستی‌آزمایی و ثبت شواهد دیجیتال

با رشدانفجارگونه انتشار اطلاعات در فضای مجازی، تبادل ده‌ها و صدها میلیون پیام به صورتی روزانه و انتشار میلیون‌ها تصویر و ویدئو از رویدادهای متفاوت، خصوصا در موارد دارای ارزش خبری و قابل پیگیری حقوقی انبوهی از داده‌های راست و غلط با انگیزه‌های متفاوت منتشر می‌شوند. برای مثال وقوع یک حادثه دلخراش نظیر فروریختن یک برج را در نظر آورید. شما به عنوان وکیل قربانیان به دنبال بررسی ابعاد مختلف و اثبات قصور و تقصیر مثلا در زمینه صدور مجوزید. به همین دلیل همه ویدیوها و تصاویر شهروندان از واقعه مزبور را جمع‌آوری می‌کنید. اما آیا همه این ویدیوها و تصاویر واقعا مربوط به مورد خاص فروریختن برج‌اند؟

پاسخ به این سوال معمولا منفی است. افراد و کاربران بسیاری با انگیزه‌های مختلف اقدام به انتشار اطلاعات اشتباه، نادقیق یا اساسا جعلی از این حادثه می‌کنند.

انتشار برخی از این ویدئوها مثلا با هدف کسب درآمد روی سایت‌هایی مانند یوتیوب انجام می‌شود و با استفاده از حساسیت موضوع و کلیک بسیار، ویدیوهای قدیمی و غیرمرتبط با عنوانی غیرواقعی به حادثه فوق ربط داده شده و منتشر می‌شود.

سیلی از اخبار و تصاویر راست و دروغ با هدف لایک و بازنشر توسط کاربران شبکه‌های اجتماعی پس از هر واقعه پرسروصدا منتشر می‌شوند. همچنین در بسیاری از موارد حکومت‌های خودکامه، پس از سرکوب گسترده شهروندان خود، اخبار و تصاویر دروغین را برای فریب و انحراف افکار عمومی و زیرسوال‌بردن روایت قربانیان منتشر می‌کنند.

در سال‌های اخیر نیز همان‌گونه که پیش‌تر گفته شد، ظهور تکنولوژی هوش مصنوعی

امکان بازسازی نسبتا واقعی تصاویر غیر واقعی را فراهم کرده است مثلا با استفاده از چند دقیقه ویدئوی یک فرد سرشناس و تحلیل صدا و تصویر او توسط کامپیوتر می‌توان ویدئوی او را در حال ادای واقعی هر سخنی که شما بخواهید بازتولید کرد.

۴- تحلیل داده‌های متا از تصاویر و ویدئوها

در بسیاری از موارد، فایل‌های عکس یا ویدئو حاوی اطلاعاتی چون موقعیت جغرافیایی، تاریخ و حتی دوربین به‌کاررفته در ثبت تصویر و ویدئو است در این‌گونه موارد می‌توان با استفاده از سرویس‌های در دسترس تحلیل داده‌های متا صحت تصاویر یا ویدئوها را مورد بررسی قرار داد.

۵- جستجوی معکوس تصاویر و انواع دیگر داده‌ها

در بسیاری از موارد می‌توان از جستجوی معکوس برای تشخیص تصاویر جعلی یا قدیمی بهره جست، مثلا در گوگل با آپلود تصاویر یا استفاده از لنز گوگل می‌توانید تحقیق کنید که آیا این تصاویر در جای دیگری یا زمانی پیش از زمان موردِ ادعا، استفاده شده‌اند یا خیر؟

۶- استفاده از نقشه برای واکاوی و استخراج موقعیت جغرافیایی

فعالان دیجیتال هر روز بیش از پیش از امکاناتی چون نقشه‌های گوگل‌مپ و گوگل‌ارث (Google Earth) برای راستی‌آزمایی شواهد و همچنین بررسی و تحقیق ابعاد وقایعی چون نقض حقوق بشر استفاده می‌کنند.

مثلا در استفاده از نیروهای نظامی علیه یک اقلیت قومی و یا شهروندان بی‌دفاع، با تحلیل ویژگی‌های منحصر به فرد تصاویر و ویدئوها و استخراج موقعیت دقیق جغرافیایی آن محل روی گوگل‌مپ و سپس استخراج اطلاعات دیگر عکس مثلا تاریخ و زمان ثبت تصویر با بررسی مواردی نظیر سایه یا وضعیت جوی و مقایسه آن با تصاویر و ویدیوهای دیگر در مدت‌زمان مشابه، به اصلی‌ترین ابزارهای فعالان دیجیتال بدل شده است.

با جستجوی واژه‌هایی چون Geo located روی شبکه‌های اجتماعی می‌توان در مدت‌زمانی نسبتا کوتاهی محل وقوع و ثبت محتوای تصویر یا فریمی از ویدئوی مورد بحث

را که توسط کاربران شبکه‌های اجتماعی، کشف و بازنشر شده است را یافت.

۷- واکاوی تاریخچه، کشف و ثبت الگوها

در موتورهای جستجو و شبکه‌های اجتماعی می‌توان تاریخ را به عقب برگرداند و مثلا از ابتدا تا انتهای سال ۲۰۰۲ - یعنی ۲۱ سال پیش - به دنبال یک رشته متنی یا عکس گشت. در گوگل و یوتیوب می‌توان زمان خاصی را برای جستجوی محتوی تعیین کرد. این موضوع امری فوق‌العاده مهم و ذی‌قیمت برای وکلا و فعالان حقوقی است، چرا که با بررسی تاریخچه یک موضوع مثلا نقض حقوق شهروندان یا فساد یک دستگاه دولتی خاص و نحوه گسترش و الگوهای آن در طول زمان می‌توان از جوانب مختلف این روند پرده برداشت. در نظر بگیرید که دو افسر پلیس متهم به خشونت بیش‌ازاندازه با شهروندان‌اند، بررسی تاریخچه موارد ضرب‌وشتم افراد آن محل، از طریق شبکه‌های اجتماعی، ویدئوهای یوتیوب و همچنین نتایج گوگل می‌تواند الگویی از مرتبط‌بودن موارد بالای خشونت با حضور آن دو افسر خاص در منطقه مورد بحث را در همه سال‌های گذشته تایید کند. همین مورد می‌تواند در مورد خشونت علیه زندانیان یک زندان خاص و تاریخچه آن و همه موارد مشابه مورد استفاده قرار گیرد.

۸- به‌کارگیری شیوه‌های کارآمد تحقیق (تحلیل بازار)

در دنیای تجارت و روابط عمومی از شیوه‌های پیچیده‌ای برای تحقیق در مورد بازار استفاده می‌شود. مثلا برای شناسایی مشتریان احتمالی یک محصول خاص انواع و اقسام ابزارهای تحقیق از بازار (Market Research) و همچنین دسته‌بندی افراد علاقه‌مند احتمالی، تحلیل ویژگی‌های مشترک ایشان و همچنین هدف‌قراردادن آنان با پیام‌هایی جهت‌دار با هدف فروش استفاده می‌شود. این ابزارها را برای فعالیت حقوقی نیز می‌توان به کار برد. اینجا به جای جستجو برای مشتریان یک محصول خاص، مجموعه‌ای بزرگ از شهروندان، به شکلی دسته‌بندی می‌شود که بتوان با گروهی خاص از قربانیان فساد یا خشونت دولتی ارتباط برقرار کرد و آنان را در کمپین‌های اطلاع‌رسانی و مشاوره حقوقی هدف قرار داد.

۹- استفاده از داده‌های تحلیلی شبکه‌های اجتماعی و موتورهای جستجو

در ادامه مورد بالا یعنی تحلیل و استخراج داده‌ها با هدف دسته‌بندی و ارتباط با گروه‌های

خاص و مورد نظر، می‌توان از داده‌های شبکه‌های اجتماعی مثلا موضوعات ترندشده در توییتر و انواع و اقسام هشتگ‌ها استفاده کرد. به طور مثال همه پست‌های اینستاگرامی با یک هشتگ یا دارابودن مشخصات یک مکان جغرافیایی خاص را می‌توان برای بررسی رویدادی در حوالی آن منطقه به کار گرفت. سرویس جستجوی گوگل نیز اطلاعات نسبتا مفصلی از رشته‌های جستجو در خلال یک بازه زمانی خاص و از یک موقعیت جغرافیایی مشخص ارائه می‌کند. مثلا می‌توان از خلال داده‌های گوگل‌ترند فهمید که کدام منطقه جغرافیایی در ایران در هفته یا ماه گذشته بیش از جاهای دیگر واژه «شکنجه» و «خشونت» و «بازداشت» را جستجو کرده است. این داده‌ها می‌تواند ما را برای ردیابی و تحقیق یاری رسانند.

۱۰- تحقیق بر پایه اطلاعات موجود در فضای عمومی

در سال‌های گذشته اطلاعات استخراج‌شده از منابع عمومی (OSINT) به عنوان یکی از اصلی‌ترین بازوهای بررسی و تحلیل وقایع در دسترس همگان قرار گرفته است. از دولت‌ها، پلیس و دستگاه‌های امنیتی گرفته تا روزنامه‌نگاران، وکلا و بسیاری از اقشار و

گروه‌های دیگر به‌سادگی انبوهی از اطلاعات را در پی موارد مورد نیاز خود برای رصد و کشف جرم یا نقض حقوق بشر و موارد دیگر می‌کاوند. در وب جهانی شمار غیر قابل باوری از داده عمومی، از شماره تلفن و محل‌سکونت افراد، تصاویر و ویدئوهای آن‌ها و همچنین ابزارهایی که می‌توانند با آپلود یک عکس هویت صاحب آن را حدس بزنند و با پیمایش ده‌ها و صدها هزار تصویر - مثلا در تصاویر گوگل با کمک گوگل‌لنز - تصاویر مشابه را در کسری از دقیقه بیابند. این ابزارها و رواج استفاده از آنان به پیدایش گروهی از فعالان دیجیتال متخصص در گردآوری داده‌های با منشاء عرصه عمومی انجامیده است. مثلا ده‌ها و صدها کاربر در جریان تجاوز روسیه به اوکراین میلیون‌ها تصویر و داده مشابه را تجزیه و تحلیل و اطلاعاتی بسیار دقیق و قابل اتکاء از تلفات، موقعیت جغرافیایی و حتی فنی‌ترین ویژگی‌های جنگ را به رایگان منتشر و دردسترس همه کاربران شبکه‌های اجتماعی خصوصا توییتر و یوتیوب قرار می‌دهند؛ اطلاعاتی که تا پیش از این در انحصار سرویس‌های نظامی و اطلاعاتی پیچیده و دولتی بوده است.

۱۱- جستجو و تحلیل از خلال انجمن‌ها و شبکه‌های اجتماعی

امروزه حجمی بی‌مانند از داده‌ها و اطلاعات صاحب ارزش در اختیار هر فعال حقوقی و وکیلی قرار دارد. حتی بدون پرداخت هزینه می‌توان از خلال گفت‌وگوهای شهروندان در فوروم‌ها، انجمن‌ها، وبلاگ‌ها و شبکه‌های اجتماعی، اطلاعاتی را به دست آورد که تا پیش از این نیازمند ماه‌های تحقیق، مصاحبه و گفت‌وگو و سفرهای دور و دراز بودند. گروهی از کارگران یک معدن سال‌هاست مورد تضییع حقوق، فشارهای غیرقانونی و نقض حقوق کار قرار دارند. این کارگران یک کانال تلگرامی برای انتشار اخبار این موارد ایجاد کرده‌اند. برخی از آنان پست‌های این کانال تلگرامی را در کانال دیگری مثلا در واتس‌اپ بازنشر کرده و مورد بحث و بررسی قرار می‌دهند. فقط بررسی این دو کانال و تماس با حاضران آن‌ها ذی‌قیمت‌ترین ارتباطات و اطلاعات را در اختیار فعال حقوقی و وکیل قرار می‌دهد. همچنین با ارتباط مستقیم با کارگران یا نمایندگان ایشان می‌توان از آنان درخواست اطلاعات بیش‌تر یا راستی‌آزمایی اطلاعات موجود در کانال‌های عمومی کرد.

۱۲- داده‌کاوی و کلان‌داده‌ها

داده‌کاوی و کلانداده‌ها همان‌طور که پیش‌تر اشاره شد به ابزارهای مرسوم در پروسه‌های حقوقی و محاکمات بدل شده‌اند. در سال‌های گذشته مثلا تعدادی از شرکت‌های تولیدکننده دارو و دیگر ابزارهای پزشکی، پس از بررسی ده‌ها و صدها هزار مورد استفاده این محصولات توسط شهروندان از خلال کلانداده‌ها و بروز عوارض جانبی در شمار قابل توجهی از ایشان باز توسط داده‌کاوی دیجیتال به سهل‌انگاری یا اشتباه در تولید دارو و محصول پزشکی متهم شدند. باز بر خلاف دوران گذشته که مطالعات پس از درمان با روش‌هایی چون مصاحبه و نمونه‌برداری تصادفی انجام می‌پذیرفت، امروزه به دلیل توسعه و تکامل کلان‌داده‌های مثلا مربوط به درمان و سلامتی می‌توان روند بهبود میلیون‌ها بیمار پس از درمان و عوارض احتمالی را با استفاده از هوش مصنوعی و ابزارهای مشابه رصد کرد. حال پروسه مشابهی را در مورد نقض حقوق زندانیان یا یک گروه اقلیت نژادی و قومی در نظر آورید، با کنکاش داده‌های بعضا موجود در عرصه عمومی می‌توان مواردی از این دست را با یافت ادله و شواهد کافی تبدیل به بخشی از پروسه دادخواهی و فعالیت حقوقی کرد

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- بهترین روش دسترسی به اسناد از راه دور چیست؟

الف) ذخیره‌سازی روی ایمیل شخصی

ب) ذخیره‌سازی روی هارد دیسک اکسترنال با قابلیت اتصال به اینترنت NAS drive

ج) کدگذاری اسناد، ذخیره آن در کلاود (فضای ابری) امن و اتصال با VPN امن

د) ذخیره‌سازی روی فلش دیسک و هارد اکسترنال

۲- چرا باید از اسناد حساس نسخه پشتیبان تهیه کرد؟

الف) این اسناد می‌توانند به دلایلی چون سرقت، آسیب فیزیکی یا سهل‌انگاری از بین بروند.

ب) این روشی ساده و کم‌هزینه در مقایسه با فتوکپی و آرشیو کاغذی است

ج) برای جست‌وجوی سریع داده‌ها و دسترسی ساده و بدون مشکل به اطلاعات مورد نیاز

د) امکان راحت کپی‌کردن آن در کسری از ثانیه برای ارسال به ایمیل

۳- کدامیک از موارد زیر برای حفظ امنیت کنشگران مهم و ضروری‌تر است؟

الف) عدم استفاده از فلش‌دیسک و هارددیسک اکسترنال تحت هیچ عنوانی

ب) استفاده از تلفن‌های هوشمند در مقایسه با دیگر ابزارهای دیجیتال

ج) استفاده از ابزارهای سریع و کارآمد دیجیتال

د) پاک‌کردن دائم داده‌های خصوصا حساسِ قدیمی، زائد و فاقدِ مصرف

جلسه ششم
۱۵ سناریو برای تهدیدات دیجیتال

۱- خطر اینترنت اشیاء

فرض کنید در دفتر وکالت فردی به نام فرید، ۹ دستگاه متصل به اینترنت وجود دارد. دو تلفن هوشمند؛ یکی برای امور شخصی و دیگری برای موکلین. یک تبلت و یک کامپیوتر شخصی با سیستم عامل ویندوز، یک بلندگوی دیجیتال دارای قابلیت اتصال از طریق بلوتوث و اینترنت، یک تلویزیون هوشمند، یک دوربین برای مانیتورکردن دفتر و در نهایت یک پرینتر. همه این ۸ دستگاه از طریق یک مودم وایرلس به اینترنت متصل است، علاوه بر آن هر ۲ تلفن هوشمند از طریق سیم‌کارت هم می‌توانند به اینترنت 4G موبایل وصل شوند.

در حالت کلی هر چه دستگاه‌های کم‌تری به یک شبکه وصل باشند، ارتقای امنیت آن آسان‌تر است. مثلا اگر تلفن هوشمند اداری دفتر، اینترنت موبایل 4G مخصوص به خود را دارد، بهتر است که هرگز به وای‌فای دفتر وصل نشود. برای این که این اتصال، داده‌های حساس را در معرض تهدید بیش‌تری قرار می‌دهد. همه این دستگاه‌ها به مودم متصل‌اند، پس به یکدیگر هم وصل‌اند و این یعنی در مرحله بعدی به شبکه اینترنت و تمام جهان متصل‌اند. حالا اگر همه این ۹ دستگاه، تلفن همراه، کامپیوتر و همه و همه غیر از مثلا مودم، پسورد قوی داشته باشند، آیا از اطلاعات دفتر فرید به‌خوبی محافظت شده است؟ البته که

نه. چرا که افرادی می‌توانند از طریق شبکه اینترنت وارد مودم بدون پسورد دفتر شوند و از آنجا با شناسایی‌حفره‌های دیگر، احتمالا راه نفوذ به دستگاه‌های دیگر را بیابند. مثلا کپی فایل‌هایی را که برای پرینتر وایرلس ارسال می‌شود را دریافت کنند.

در حالت کلی هر دستگاه و وسیله متصل به اینترنت، به شرط اینکه از منابع معتبر و شناخته‌شده و موفق از تست‌های امنیتی خریداری شده باشد، می‌بایست دارای پسورد قوی و غیرقابل حدس‌زدن باشد و صد البته به طور مرتب به‌روزرسانی هم شده باشد.

پس اگر نرم‌افزار چاپگر، تلویزیون، وب‌کم یا بلندگوی دفتر را با استفاده از آخرین آپدیت‌های ارائه‌شده توسط سازندگان به‌روزرسانی نکنید، این خطر وجود دارد که مهاجمان از عیوب نسخه‌های قدیمی‌تر برای ورود به شبکه و دستگاه‌های حاوی اطلاعات حساس شما استفاده کنند.

۲- خطر داده‌های کدگذاری نشده

NGO یا سازمان مردم‌نهادی به نام «حامی» به شهروندان این امکان را می‌دهد که با ارسال اسناد و مدارک خشونت دولتی، انواع مختلفی از حمایت حقوقی را دریافت کنند. این اسناد از آن جهت اهمیت دارند که با گذشت زمان اثبات مواردی مانند سوءاستفاده و ضرب‌وشتم یا شکایاتی که نیازمند ارائه تاریخچه تعدد وقوع جرم یک مامور دولتی‌اند، کم و کم‌تر می‌شود. طبیعی است این‌گونه فایل‌ها که صورت متنی، صوتی یا تصویری هستند، اهمیت بسیاری برای فعالیت سازمان این مردم‌نهاد دارند، مثلا شماره تلفن و آدرس تماس همه کسانی که از نیروهای امنیتی شکایت کرده‌اند در یک فایل پی‌دی‌اف خاص ذخیره شده است. اگر این فایل به صورت عمومی منتشر شود، بیم آن می‌رود که مرتکبان جرائم، آثار جرم را محو کنند یا به دنبال ارعاب شاکیان و شهود باشند. چگونه فایل‌های فوق را در برابر هک و افشاء و حتی سرقت فیزیکی محافظت کنیم؟

یکی از ساده‌ترین راه‌حل‌ها استفاده از کدگذاری (Encryption) است. هر دو سیستم اندروید و ISO به شما امکان کدگذاری همه داده‌های تلفن همراه‌تان را می‌دهند. این قابلیت برای سیستم‌های ویندوز و Mac OS هم وجود دارد. مثلا در ویندوز می‌توان یک فایل یا یک سند یا یک فلش‌دیسک و انواع دیگر کارت‌های حافظه یا هارددیسک‌های اکسترنال را کدگذاری کرد چرا که ممکن است داده‌های حساس و ارزشمند شما نه در

حافظه داخلی خود تلفن هوشمند و کامپیوتر، بلکه مثلا در کارت حافظه خارجی آن باشند.

۳- خطر فلش‌دیسک ناشناس

جلوی دفتر کار، داخل آسانسور و حتی داخل دفتر یک فلش‌دیسک ناشناس پیدا کرده‌ام، چه کار کنم؟

هرگز آن را به کامپیوتر و دیگر دستگاه‌های خود وصل نکنید، به این دلیل که معمولا از فلش‌دیسک‌های ناشناس به عنوان طعمه استفاده می‌شود. افراد نادانسته آن‌ها را به دستگاه‌های حساس خود وصل می‌کنند و بلافاصله بعد از اتصال بدافزارها و کدهای جاسوسی به صورت اتوماتیک روی کامپیوتر یا موبایل‌شان منتقل می‌شود. بنابراین فلش‌دیسک ناشناس هرگز نمی‌بایست به کامپیوتر متصل شود.

۴- خطر باج‌افزارها

در سال‌های گذشته باج‌افزارها به یکی از عمده‌ترین تهدیدات علیه موسسات و نهادها تبدیل شده‌اند. با ارسال فایل یا لینکی آلوده توسط ایمیل یا از طریق پیام‌رسان‌هایی نظیر تلگرام یا واتس‌اپ، کدی آلوده وارد دستگاه‌های شما مثل کامپیوتر یا تلفن همراه می‌شود و با رمزگذاری، همه داده‌های آن را از دسترس‌تان خارج می‌کند. تبهکاران با تماس تلفنی از شما می‌خواهند که مبلغی به عنوان باج را مثلا با استفاده از بیت‌کوین برایشان ارسال کنید تا دسترسی شما به داده‌هایتان دوباره برقرار شود.

برای جلوگیری از حملات باج‌افزاری، هرگز روی لینک‌های ناشناس کلیک نکنید، هرگز فایل‌های ناشناسی را که روی پیام‌رسان‌ها و شبکه‌های اجتماعی دریافت کرده‌اید باز نکنید.

برای به‌حداقل‌رساندن زیان‌های ناشی از باج‌افزارها می‌توانید همیشه از همه داده‌های تلفن و کامپیوترتان یک نسخه پشتیبان در یک فضای ابری مثل گوگل یا icloud تهیه کنید و بلافاصله پس از وقوع حمله باج‌افزاری تلفن و کامپیوتر خود را پس از راه‌اندازی دوباره، به تنظیمات کارخانه برگردانید، تمام داده‌ها و اطلاعات روی آن (از جمله کد آلوده هکرها) را یکپارچه پاک کنید و مجددا از روی فضای ابری، داده‌های ذخیره‌شده قبلی خود را باز گردانید.

۵- خطر وای‌فای، اتصال میهمان

در حالت کلی، وای‌فای دفتر شما فقط مختص شما و همکاران ۱۰۰٪ مورد اطمینان است. همان‌طور که شما تمام موارد ایمنی مثل انتخاب رمز عبور قوی و به‌روزرسانی دستگاه‌های خود را به صورت روزانه بازبینی می‌کنید، همه همکاران نیز می‌بایستی به بررسی و کنترل دائم امنیت دستگاه‌های خود توجه نشان دهند چرا که فقط یک تلفن هوشمند یا لپ‌تاپ غیر ایمن، بدون پسورد یا با سیستم عامل قدیمی و آپدیت‌نشده می‌تواند دروازه‌های امنیتی دفتر شما را روی تبهکاران بگشاید. در چنین مواقعی فقط یک حفره برای نفوذ و آلوده‌کردن همه چیز کافی ست.

برخی از دفاتر رمز عبور اینترنت خود را در اختیار مراجعین قرار می‌دهند. این کار تقریبا فراهم‌کردن زمینه نفوذ مراجع بعضا ناشناس به همه دستگاه‌های دفتر شما ست. هرگز به مراجعین و بازدیدکنندگان اجازه وصل‌شدن به وای‌فای و شبکه اصلی دفتر را ندهید. اگر این کار حتما ضرورت داشت، از مودم و اتصال جداگانه‌ای برای مراجعان استفاده کنید یا اگر به هیچ شکل امکان این کار نیست روی مودم اصلی دفتر گزینه اتصال به صورت مهمان را فعال کنید.

۶- خطر فیشینگ

مهرداد از بانک آنلاین خود ایمیلی دریافت کرده است. این ایمیل به او اطلاع می‌دهد که می‌بایست مشخصات خود در بانک را به صورت آنلاین به‌روزرسانی کند و اگر نه، حساب او طی ۲۴ ساعت آینده مسدود خواهد شد او با کلیک روی لینک داخل ایمیل در حقیقت وارد سایتی می‌شود که فقط و فقط با ظاهری مشابه بانک او و با هدف سرقت، نام کاربری و رمز عبور او طراحی شده است. بلافاصله پس از واردکردن رمز عبور، او پیامکی از بانک دریافت می‌کند که برای ورود به حساب بانکی‌اش لازم است. بنابراین با واردکردن آن پیامک در سایت جعلی و به اصطلاح فیشینگ، حساب آنلاین او تماما در اختیار تبهکاران قرار می‌گیرد.

حملات فیشینگ از طریق طراحی سایت‌هایی با ظاهر کاملا شبیه به جی‌میل، مایکروسافت، بانک، شرکت تلفن و ... طراحی می‌شوند و با فریب کاربران رمزعبور و دیگر مشخصات امنیتی آنان را به سرقت می‌برند.

فعالان حقوقی با انواع پیچیده‌تری از حملات فیشینگ روبرو هستند مثلا ممکن است پیام‌های فریبنده‌ای تحت عنوان ارسال یا دریافت مدارک، ثبت شکایت یا سایت‌های اسناد رسمی برای ایشان ارسال شود.

۷- خطر هک از طریق ارسال لینک آلوده در تلگرام

سارا عضو گروهی تلگرامی است که در آن قربانیان نقض حقوق بشر از وکلا درخواست کمک می‌کنند. کاربری به نام مهدی برای سارا پیام خصوصی ارسال کرده و خواستار کمک شده است. پس از ردوبدل‌شدن چند پیام شماری فایل و تصویر و همچنین یک لینک برای سارا ارسال شده است. سارا با کلیک روی آن لینک به صفحه‌ای هدایت می‌شود که به صورت اتوماتیک برنامه‌ای را روی دستگاه او دانلود کرده و در ادامه خواستار اجرای فایل دانلودشده می‌شود.

در بررسی‌های انجام‌شده پیرامون شیوه‌های فریب و هک در ایران بیش‌ترین شمار عملیات هک از طریق ارسال لینک یا فایل آلوده، پس از فریب قربانیان در شبکه‌های اجتماعی نظیر اینستاگرام و پیام‌رسان‌هایی نظیر تلگرام است. تبهکاران معمولا برای تماس از شیوه‌های مهندسی اجتماعی استفاده می‌کنند مثلا با سوءاستفاده از هیجان یا ترس یک کاربر او را وادار به اقدامی سریع و نسنجیده مثل بازکردن لینک می‌کنند. مثلا یک کاربر در شبکه ایکس پیامی دریافت می‌کند به همراه یک لینک با این مضمون که در این لینک تصاویر خصوصی تو منتشر شده است! بسیاری از ما بدون فکرکردن به خطرات احتمالی لینک بلافاصله هول شده و روی لینک کلیک می‌کنیم.

۸- خطر تنها راهاکردن تلفن همراه

مهناز وکالت شماری از زندانیان را بر عهده دارد. او از چندین تلفن همراه استفاده می‌کند که یکی از آن‌ها حاوی اطلاعاتی حساس و مهم است. او هنگام ورود به محل ملاقات با زندانیان، کیف حاوی تلفن‌های همراه خود را تحویل می‌دهد. در ساعتی که مهناز از تلفن‌های به‌امانت‌گذاشته‌اش دور است، افراد یا نهادهایِ خواستار دسترسی به اطلاعات تلفن او، می‌توانند به‌سادگی و با اتصال یک لینک به تلفن او ، حتی اگر خاموش باشد، برای هک و دستیابی به اطلاعات حساس او تلاش کنند. مهناز می‌توانست با به‌همراه‌نیاوردن

تلفن حساس خود جلوی این تهدید احتمالی را بگیرد.

۹- خطر استفاده از شارژرهای عمومی

مهناز وکالت شماری از زندانیان را بر عهده‌دارد. این بار او تلفن حساس خود را به اتاق ملاقات آورده است، باتری تلفن، رو به اتمام است و او تلفن را به شارژری که در اتاق ملاقات تعبیه شده است، متصل می‌کند. افراد و مقامات می‌توانند شارژرهای مثلا USB را با نصب تجهیزات هکری تبدیل به وسیله‌ای برای نفوذ و هک تلفن قربانیان کنند. پس تلفن‌های حساس خود را هرگز به شارژر یا هیچ وسیله جانبی جز ابزار شناخته‌شده خود، متصل نکنید.

۱۰- خطر مودم‌های جاسوس و دوربین‌هایی برای هک

مهناز مجددا تلفن حساس خود را در زندان همراه دارد. به دلیل عدم وجود سیگنال و در جستجوی مورد خاص آنلاین، به وای‌فای عمومی زندان وصل می‌شود. افرادی که وای‌فای زندان را پیکربندی کرده‌اند، به‌سادگی می‌توانند از طریق مودم عمومی زندان وارد تلفن مهناز شوند. حتی اگر تلفن کدگذاری شده باشد. همچنین هنگام اعمال رمز عبور دستگاه توسط مهناز، دوربین‌های مداربسته‌ای که همه جای زندان یا دادسرا وجود دارند، می‌توانند واردکردن رمز عبور توسط مهناز را مانیتور و ضبط کنند.

۱۱- Google Authenticator بهتر است یا تایید هویت با پیامک؟

فرید از یک حساب کاربری امن گوگل برای ذخیره‌سازی اطلاعاتی استفاده می‌کند که به هیچ وجه نباید فاش شوند. او بارها با این پیام از گوگل مواجه شده که گروهی در صدد هک این اکانت هستند. فرید رمز عبوری قوی و مطمئن برای حساب طراحی کرده است اما می‌خواهد بداند که قابلیت تایید هویت دومرحله‌ای از طریق دریافت پیامک بهتر است یا توسط دستگاه تلفن اندروید یا اپلیکیشن Authenticator؟ پاسخ به این سوال بستگی به ارزیابی خطر از سوی فرید دارد. اگر او احتمال می‌دهد این مقامات دولتی هستند که برای هک ایمیل او تلاش می‌کنند، استفاده از پیامک که کاملا در حیطه کنترل دولت است، به صلاح نیست، چرا که دستگاه‌های مخابراتی به‌راحتی این پیامک را حتی پیش از فرید

دریافت می‌کنند. اما اگر گروهی که قصد نفوذ به تلفن همراه او را دارد، غیردولتی و فاقد امکانات حکومتی مثل دسترسی به زیرساخت‌های مخابرات و سرویس ارسال و دریافت متن‌اند، آن‌گاه استفاده از قابلیت تایید هویت دومرحله‌ای با پیامک قابل قبول خواهند بود.

۱۲- خطر تلگرام‌طلایی، وی.پی.ان مجانی و اپلیکیشن‌های محیرالعقول

بازار اپلیکیشن‌های آلوده و جاسوس در ایران داغ است. فقط در یک مورد، دولت ایران هم‌زمان با تلاش برای انسداد نرم‌افزار محبوب تلگرام، چندین اپلیکیشن با قابلیت جاسوسی از کاربران ایرانی را روانه فروشگاه‌های غیررسمی مثل «کافه‌بازار» کرد. یک جستجوی ساده نشان می‌دهد که انواع و اقسام اپلیکیشن‌ها از فارسی‌ساز واتس‌اپ گرفته تا ده‌ها و صدها فیلترشکن و وی.پی.ان ناشناس، مجانی و مدعی سرعت بالا در حال جذب و ذخیره داده‌های کاربران ایرانی‌اند. اساسا هیچ اپلیکیشنی غیر از اپلیکیشن‌های صددرصد ضروری روی ۲ فروشگاه رسمی اپل یا گوگل را نمی‌بایست روی هیچ یک از تلفن‌های هوشمند متصل به شبکه محل کار نصب کرد. نصب اپلیکیشن قدیمی، ناشناس، غیرضروری یا برآمده از جایی غیر از فروشگاه‌های اپل و گوگل، تقریبا با اطمینان می‌توان گفت که تلفن شما را آلوده می‌کند.

۱۳- خطر ایمیل، پیام و تماس‌های تلفنی افراد ناشناس

حرفه وکالت و تماس با افرادی بعضا ناشناس، دو امر جدایی‌ناپذیر هستند. افراد مثلا می‌توانند با یک جستجوی ساده گوگل یا به صورت تصادفی با یک وکیل تماس بگیرن و کمک او را جویا شوند. از این رو تشخیص موکل و فرد نیازمند به کمک واقعی، از فریبکاران در لباس موکل بسیار مشکل است. رعایت اصولی که در ادامه می‌آید، می‌تواند تا اندازه‌ای امنیت دیجیتال شما را علی‌رغم تماس با افراد ناشناس تضمین کند.

کسب اطلاعات از افراد و تماس‌های ناشناس باید یک‌طرفه باشد و شما به هیچ‌وجه نمی‌بایستی اطلاعاتی را در اختیار آن فرد ناشناس قرار دهید چه با تلفن، چه با پیامک، چه پیام‌رسانی نظیر تلگرام یا مثلا در دایرکت ایکس و اینستاگرام. این اطلاعات می‌تواند ناخواسته و بسیار ساده باشد. فرید پیام کوتاهی در اینستاگرام با این مضمون دریافت کرده است که «قربان کی می‌توانم مزاحم شوم دفتر؟» فرید پاسخ این پیام را به شکل

زیر می‌دهد که «من فعلا در سفر هستم. تا هفته آینده و می‌توانید هفته دیگه تشریف بیاورید». این پاسخ مشکل‌ساز است چرا که فرید به‌نوعی خالی‌بودن دفتر و عدم حضور خود در هفته را تایید کرده است در حالی که به سادگی می‌توانست چنین پاسخ دهد که «این هفته امکان ملاقات شما را ندارم تا هفته بعد». همین سطح از پیشگیری و دقت در عدم پذیرش لینک، فایل، فلش‌دیسک، سی‌دی و... از افراد ناشناس و از طریق پست یا ایمیل و پیام‌رسان هم لازم است.

۱۴- خطر حافظه مرورگر، حافظه موقعیت‌یاب و داده‌های غیرضروری

به هنگام استفاده از تلفن‌های هوشمند اگر تلفن شما به شکلی مناسب تنظیم و پیکربندی نشده باشد، ممکن است حافظه مرورگر مثلا کروم همه رشته‌های جستجوی شما را برای سالیان سال حفظ و ذخیره کند. مرور این رشته‌ها همه عملکرد شما در این سال‌ها را در اختیار فردی که به تلفن دسترسی پیدا کرده، قرار می‌دهد. همین مسئله در مورد موقعیت‌یاب (GPS) تلفن هم وجود دارد. مثلا در Google Maps با گزینه Time-line می‌توان هر قدم جابه‌جاشدن و سفر صاحب حساب در ماه‌های گذشته را موبه‌مو مشاهده و تحلیل کرد. با ظهور ابزارهایی مثل ساعت اپل حالا حتی ضربان قلب و میزان اکسیژن خون افراد برای سال‌ها نیز آرشیو می‌شود. برای مقابله با تهدیدات ناشی از این حجم غیرقابل باور داده، بهتر است اولا این آرشیوها را از روی تلفن‌های کاری و حساس خود پاک کنید و ثانیا مثلا با تنظیم حساب کاربری خود از گوگل بخواهید رفت‌وآمدها یا جستجوهای شما در گوگل و یوتیوب را اساسا آرشیو نکند.

۱۵- خطر DeepFake

در سال‌ها و ماه‌های گذشته، تکنولوژی تقلید صدا و شبیه‌سازی چهره نزدیک به واقعی توسط هوش مصنوعی به صورتی انفجارگونه پیشرفت کرده است. الهه یکی از دوستان قدیمی فرید است. با تکنولوژی نسبتا ساده و در دسترس همگان می‌توان با دانلود چند کلیپ یوتیوب از الهه و تحلیل عمیق صدای او توسط نرم‌افزارهای تقلید صدا، نرم‌افزار یا اپلیکیشن واسطی را فعال کرد که صدای میکروفن را به صدایی بسیار شبیه صدای الهه تبدیل کند. این امکان حتی برای تماس تصویری و شبیه‌سازی هم‌زمان صدا و تصویر الهه

نیز وجود دارد. این خطر وجود دارد که در سال‌های آینده و با سوءاستفاده از این تکنولوژی، وکلا نیز مانند بسیاری مشاغل دیگر هدف قرار گیرند. ابتدایی‌ترین شیوه مبارزه با این نوع تهدیدات عدم انتقال اطلاعات حساس و مشکل‌زا در خلال تماس‌های دیداری یا شنیداری است، همچنین راه‌حل‌های فنی نسبتا کارآمدی برای تشخیص صدا و ویدئوی غیرواقعی نیز به تدریج در اختیار کاربران قرار می‌گیرند.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- مهم‌ترین تهدید علیه امنیت دیجیتال دفاتر حقوقی چیست؟

الف) فریب، مهندسی اجتماعی، فیشینگ و سرقت داده‌ها

ب) استفاده از سیستم‌عامل اندروید برای تلفن‌های هوشمند

ج) استفاده از وب‌کم و مصاحبه تصویری در مکالمات

د) استفاده از سخت‌افزار ارزان‌قیمت و با حافظه پایین

۲- مشکل استفاده از وای‌فای عمومی مثلا در کافی‌شاپ یا هتل چیست؟

الف) معمولا سرعت و کیفیت کم‌تری نسبت به اینترنت 5G دارند

ب) مهاجمان با روش‌های نسبتا ساده می‌توانند ارتباطات شما را هک کنند

ج) با برخی تلفن‌های هوشمندِ خاص مشکل اتصال و پسورد دارند

د) اساسا استفاده از وای‌فای چه عمومی و چه خصوصی صلاح نیست

۳- فیشینگ چیست؟

الف) استفاده از روش‌های تکنیکی برای ورود به کامپیوتر قربانی از طریق مودم وایرلس

ب) استفاده از روش‌های تکنیکی برای ورود به کامپیوتر قربانی از طریق کارت و درگاهِ شبکه

ج) انتشارِ کرم‌های کامپیوتری Worms از طریق اتصال شبکه یا وای‌فای با هدف آلودگی بیش‌تر

د) فریب از طریق طراحی سایت‌هایی با ظاهر مشابه ایمیل، بانک برای سرقت رمزعبور و دیگر داده‌ها

جلسه هفتم
۴ مطالعه موردی درباره کنشگری حقوق و قضا

در این درس، ۴ مطالعه موردی از کنشگری دیجیتال با هدف دفاع از حقوق بشر، کشف حقیقت، پاسخگویی و مقابله با فساد را مرور خواهیم کرد. هدف این مطالعات به‌نمایش‌گذاشتن ظرفیت ابزارهای دیجیتال در مقابله با ظلم و تعدی دولت‌های تمامیت‌خواه در عرصه‌های ملی و بین‌المللی است.

۱- اوکراین، Euromaidan SOS

در میانه تلاش دیرپای مردم اوکراین برای مقاومت در برابر سالیان دراز دخالت و اعمال فشار از سوی حاکمان روسیه، در آخرین روزهای نوامبر ۲۰۱۳، گروهی از شهروندان عمدتا جوان و طرفدار گسترش روابط با اتحادیه اروپا، حرکت اعتراضی یورومیدان (Euro-maidan SOS) را در مرکز «کیف»، پایتخت اوکراین، آغاز کردند. این تجمع در آخرین روز نوامبر و با یورش پلیس ضدشورش نیروهای دولت وفادار به مسکو با خشونت پاسخ داده شد. خشونتی که خود به آغاز یکی از بزرگ‌ترین جنبش‌های اعتراضی علیه نفوذ و دخالت مسکو انجامید.

برای فهم شرایط تولد جنبش موسوم به Euromaidan SOS می‌بایست قدری به عقب بازگشت. بر خلاف گذشته، تظاهرات طرفداران دموکراسی در سال‌های ۲۰۰۴ و

۲۰۰۵ که بعدها به «انقلاب نارنجی» مشهور شد، این‌بار در پایان سال ۲۰۱۳ بخش قابل توجهی از شهروندان اوکراینی خصوصا جوانان به اینترنت موبایل، با سرعتی قابل قبول دسترسی داشتند. میلیون‌ها شهروند از فیس‌بوک، اینستاگرام و دیگر شبکه‌های اجتماعی استفاده می‌کردند و تلویزیون آنلاینی به نام «تلویزیون شهروندان» بدون محدودیت‌های معمول دیگر رسانه‌ها، مستقیم و به صورت آنلاین رویدادهای میدان را مخابره می‌کرد.

پس از موفقیت دعوت‌کنندگان به تظاهرات و با حضور جمعیت بسیار قابل توجهی در میدان استقلال کیف و پس از مخابره و پخش آنلاین تصاویر خشونت پلیس، چند وکیل و دانشجوی وکالت صفحه فیس‌بوکی Euromaidan SOS یا EvromaidanSOS@ را تاسیس کردند. این صفحه، وکلا، دانشجویان حقوق و سازمان‌ها و نهادهای مردم‌نهاد مدافع حقوق بشر را مستقیما با تظاهرکنندگان مرتبط می‌کرد. دوستانِ افراد بازداشت‌شده می‌توانستند به‌سرعت برای دوستانشان وکیل داوطلب پیدا کنند. اسامی و تصاویر افراد ربوده‌شده توسط پلیس بلافاصله هم برای اطلاع رسانه‌ها و هم برای پاسخگویی مراجع قانونی و قضایی منتشر می‌شد.

متن زیر نمونه‌ای از اعلانات، Euromaidan SOS است که در اوج سرکوب تظاهرات در شهرهای مختلف اوکراین در آغاز فوریه ۲۰۱۴ است:

«تا تاریخ دوم فوریه ۲۰۱۴، اطلاعات مربوط به ۳۶ شهروند مفقودشده در خلال تظاهرات در شهرهای مختلف اوکراین منتشر می‌شود. از ۱۶ ژانویه تاکنون ما ۱۲۹ درخواست جستجو برای شهروندان معترض دریافت کرده‌ایم.»

ریز اطلاعات مربوط به شهروندان مفقود (احتمالا بازداشت یا ربوده‌شده) در شکل تصویر، در اختیار رسانه‌ها قرار می‌گرفت. علاوه بر این در تابلوهایی به شکل تصویر زیر نام و تصویر افراد مفقودشده در مکان‌هایی نظیر دانشگاه‌ها و میادین اصلی نزدیک به محل تجمعات نصب می‌شد تا دیگر معترضان در صورت اطلاع از چند و چون بازداشت یا ربایش احتمالی تظاهرکنندگان مفقودشده و از طریق فیس‌بوک یا تلفن با وکلای داوطلب و دیگر فعالان مدنی تماس برقرار کنند.

Euromaidan SOS الهام‌بخش حرکت‌های مشابهی توسط دیگر شهروندان و کنشگران شد. در مدت کوتاهی گروهی دیگر از پزشکان و کادر درمانی در تشکلی مشابه، مداوای مجروحان و آسیب‌دیدگان سرکوب را بر عهده گرفت یا گروهی دیگر از شهروندان از شبکه‌های اجتماعی برای جمع‌آوری کمک و پرداخت هزینه غذا و اسکان موقت تظاهرکنندگان در هوای بسیار سرد فوریه اوکراین استفاده کردند.

در بهار ۲۰۱۴ و با ادامه اعتراضات و پیروزی انقلاب مردمی و آزادی‌خواهانه اوکراین، دولت روسیه با اشغال «کریمه» و آتش‌افروزی و جنگ در شرق اوکراین به صورتی بی‌پرده به اشغال و خونریزی روی آورد. از این پس بازداشت فعالان مدنی، ربایش روزنامه‌نگاران و کنشگران دموکراسی‌خواه در مناطق تحت اشغال روسیه و فشار بر اقلیت‌های قومی خصوصا تاتارهای کریمه به امری روزمره بدل شد.

Euromaidan SOS از آن پس فعالیت خود را بر گزارش جنایات روسیه در مناطق تحت اشغال و انتشار گزارش از پیگیری وضعیت فعالان ربوده‌شده، زندانی و تحت شکنجه و آزار متمرکز کرد. وکلا و کنشگران نقشه‌ای آنلاین از قتل، بازداشت و ربایش و همچنین تبعید اجباری فعالان در مناطق تحت اشغال روسیه ایجاد کردند. بسیاری از

موارد از بازداشت و حبس فعالان دموکراسی‌خواه در مناطق تحت اشغال روسیه به کمپینی بین‌المللی و با استفاده از همه امکانات دادگاه‌ها و سازمان‌های بین‌المللی نظیر شورای اروپا، سازمان OSCE و سازمال ملل متحد انجامیدند.

فعالیت Euromaidan SOS پس از تجاوز همه‌جانبه روسیه به اوکراین در فوریه ۲۰۲۲ همچنان ادامه دارد. در این میان ده‌ها هزار مورد قتل، تجاوز، ربایش کودکان و بزرگسالان و دیگر جنایات جنگی روسیه مستند و برای پیگیری به دادگاه‌ها و مراجع بین‌المللی ارسال شده‌است.

موسسه آزادی‌های مدنی (The Center for Civil Liberties) که Euro-maidan SOS یکی از پروژه‌های آن است، یکی از دریافت‌کنندگان جایزه صلح نوبل در سال ۲۰۲۳ بود.

۲- سوریه، اسناد سزار، تصاویر شکنجه و قتل زندانیان

اسناد موسوم به سزار، اسنادی مربوط به شکنجه، قتل و اعدام بیش از ۱۱ هزار زندانی در زندان‌های بشار الاسد، دیکتاتور خونریز سوریه، در مدتی بیش از ۲ سال از ۲۰۱۱ تا ۲۱۰۳ است. سازمان دیده‌بان حقوق بشر پس از هفته‌ها کار کارشناسی و بررسی این اسناد صحت و دامنه فاجعه‌بار نقض حقوق بشر در این اسناد را مورد تایید قرارداد.

این اسناد با ورود جمع قابل توجهی از روزنامه‌نگاران، مدافعان حقوق بشر و همچنین سازمان‌های بین‌المللی مدافع حقوق بشر به روشن‌شدن هویت بسیاری از جان‌باختگان و آسیب‌دیدگان سرکوب اعتراضات سوریه در سراسر جهان انجامید و دست‌مایه محاکماتی نظیر محاکمه یکی از عاملین این جنایات در آلمان شد. پس از افشای این اسناد، روزنامه‌نگاران، وکلا و فعالان حقوق بشر با استفاده از اطلاعات در دسترس عموم، از طریق شبکه‌های اجتماعی و همچنین مصاحبه و گفت‌وگو با افراد درگیر در وقایع خون‌بار سوریه از فجایعی چون قتل‌عام ۴۴ زندانی در «تدمن»، در اطراف دمشق، از خلال بررسی ۶ دقیقه فیلم ویدئوی قتل این افراد و با ماه‌های پیگیری و کار مستمر و حتی ایجاد دوستی مجازی با عاملان این جنایات در شبکه‌های مجازی هویت شماری از آنان را برملا کردند.

انتشار این اسناد به محکومیت و انزجار بین‌المللی بیش‌تر علیه رژیم خون‌ریز بشار اسد انجامید و ایالات متحده با توسل به قوانین فراگیر موسوم به مگنیتسکی (Magnitsky)

و همچنین قوانین محافظت از غیرنظامیان موسوم به سزار (Caesar) در سال ۲۰۲۰ بر تحریم‌های خود علیه رژیم بشار اسد افزود.

وقایع خون‌بار سوریه و مرگ صدها هزار انسان و آوارگی میلیون‌ها نفر دیگر، هم‌زمان با رشد و استفاده هم‌زمان از شبکه‌های اجتماعی، محققان قضایی، فعالان حقوق بشر و شهروندان کنشگر را با حجم غیرقابل باور از اسناد، مدارک، شواهد، هویت قربانیان و همچنین جنایتکاران ناقضان حقوق بشر، مواجه کرده است. بررسی و تحلیل این اسناد با شیوه‌های سنتی ده‌ها سال به طول خواهد انجامید حال آنکه امید می‌رود با پیشرفت‌های اخیر در تکنولوژی ارتباطات فناوری‌های نو و هوش مصنوعی بتوانند با تحلیل این حجم انبوه داده‌ها به شنیده‌شدن صدای قربانیان و نوعی تسلی بازماندگان و خانواده‌ها کمک کنند.

۳- پروژه شهروندخبرنگاری به نام Bellingcat

به فاصله کوتاهی پس از آغاز اعتراضات موسوم به بهار عربی که به‌سرعت به درگیری و جنگ مسلحانه در لیبی و سوریه انجامید. جوانی که تحصیلات خود را قبل از به پایان‌رساندن ترک کرده بود، با اسم مستعار Brown Moses مشغول بلاگ‌نویسی بود. او بدون تحصیلات و هر نوع مطالعه خاص درباره سیستم‌های تسلیحاتی، تنها به دلیل علاقه به بازی‌های کامپیوتری، تسلیحات مورد استفاده طرفین درگیر در لیبی و سوریه را از خلال ویدئوهای اینترنتی منتشرشده توسط گروه‌های مختلف پیگیری می‌کرد. او از انگلستان و فقط و فقط به اتکای ویدیوهای در دسترس عموم، توجه بسیاری را به استفاده مکرر از تسلیحات ممنوعه نظیر بمب‌های خوشه‌ای توسط بشار الاسد جلب کرد. کم کم طیف وسیعی از روزنامه‌نگاران، وکلای حقوق بشر و حتی کارشناسان نهادهای بین‌المللی مخاطب پروپاقرص یافته‌های این بلاگر شدند.

اطلاعات ذی‌قیمت Brown Moses که حال خود را با نام واقعی‌اش الیوت وارد هیگینز (Eliot Ward Higgins) معرفی می‌کرد، سنگ بنای هزاران گزارش رسانه‌ای و حقوقی از نقض حقوق بشر در خلال درگیری‌های خصوصا سوریه شد.

هیگینز مدتی بعد و در سال ۲۰۱۴، سایت و پروژه جدیدی را برای پیگیری کاوشگری بر پایه اطلاعات دیجیتال توسط شهروندان خبرنگاران آغاز کرد. Bellingcat یکی از

موفق‌ترین پروژه‌های شهروندخبرنگاری است که در بسیاری از موارد با جمع‌آوری اطلاعات از عرصه عمومی حتی عملکرد بهتری از سازمان‌های عریض و طویل چندصدمیلیون‌دلاری تحقیقی یا دولتی داشته است.

با شروع اشغال نظامی اوکراین در سال ۲۰۱۴ توسط روسیه، آتش تجاوز مستقیما مورد حمایت روسیه بخش‌های شرقی اوکراین و خصوصا منطقه «دنباس» را فرا گرفت. روز ۱۷ جولای سال ۲۰۱۴، هواپیمای MH۱۷ خطوط هوایی مالزی از هلند به مقصد کوالالامپور بر فراز اوکراین مورد اصابت موشکی روسی (Buk) قرار گرفت و همه ۲۹۸ سرنشین آن کشته شدند. بلافاصله پس از این جنایت دستگاه‌های دولتی و رسانه‌ای روسیه یکی از بزرگ‌ترین عملیات فریب و گمراه‌سازی افکار عمومی را آغاز کردند. سیلی از نقشه‌های ماهواره‌ای، تصاویر، پست‌های شبکه‌های اجتماعی و گزارشات جعلی و دست‌کاری‌شده همه و همه با هدف سلب مسئولیت از رهبری و ارتش و شورشیان مورد حمایت روسیه تولید و در فضای رسانه‌ای منتشر شدند.

Bellingcat به اتکای اطلاعاتی که شهروندخبرنگاران و فعالان و کنشگران کاوش اطلاعات عمومی فراهم آورده بودند از بسیاری جوانب این کمپین‌های انحراف افکار عمومی پرده برداشت. با بررسی هزاران ساعت ویدئو - بعضا پس‌زمینه ویدئوهای شهروندان مناطق ساکن دنباس - Bellingcat با موفقیت سامانه پرتاب موشک Buk روسی، که از شهر «کورسک» در روسیه رهسپار دونباس اوکراین بود را شناسایی کرد. همچنین با استفاده از ابزارهای ساده موجود و در دسترس همگان جعلی‌بودن نقشه‌های ماهواره‌ای منتشرشده توسط وزارت خارجه روسیه نیز اثبات شد. حجم اطلاعات بررسی‌شده و شواهد یافته‌شده از خلال شبکه‌های اجتماعی چنان انبوه بود که از این پس Bellingcat به یکی از حاضران و شاهدان همیشگی جلسات رسیدگی به جنایت شلیک به هواپیمای بی‌دفاع مسافربری توسط روسیه و شورشیان تحت حمایت این کشور تبدیل شد.

داده‌های Bellingcat از تماس‌های تلفنی یا بیسیم شورشیان، هویت واقعی شبکه‌ای بسیار پیچیده از فرماندهان تحت حمایت مستقیم و همچنین نیروهای روسیه در مناطق اشغال‌شده شرق اوکراین را که در شلیک به هواپیمای مسافربری نقش داشتند را به‌روشنی هویدا کرد و در اختیار جهانیان قرار داد.

با آغاز درگیری‌ها و اشغال کریمه از سال ۲۰۱۴، چندین شهروند در مناطق مختلفی از

اروپا، مثلا در پارکی نزدیک به قلب نهادهای دولتی در برلین به قتل رسیدند. از همان ابتدا شواهدی حکایت از دخالت نهادهای اطلاعاتی و رهبران روسیه داشت. حاکمان کرملین اما، این همه را حاصل توطئه نهادهای غربی برای بدنام‌کردن روسیه وانمود کردند. در یکی از پرسروصداترین این عملیات‌ها در سال ۲۰۱۸، سرگئی‌اسکریپال (Sergei Viktorovich Skripal)، از افسران سابق اطلاعاتی-نظامی روسیه، به همراه دخترش در انگلستان و با استفاده از یکی از خطرناک‌ترین سلاح‌های شیمیایی جهان یا نووی‌چوک (Novichok) مورد سوءقصد قرار گرفتند. دولت انگلستان بلافاصله اسنادی از دخالت مستقیم روسیه در این عملیات ترور و حتی تصاویر ورود ۲ تروریست روس به فرودگاهی در انگلستان را برای اطلاع عموم منتشر کرد. از اینجا به بعد Bellingcat و چند سازمان غیردولتی و کنشگران شهروند با کنار هم گذاشتن اطلاعات عرصه عمومی از شبکه‌ای بزرگ از قاتلین و افسران اطلاعاتی تعلیم‌دیده از سوی نهادهای امنیتی مسکو پرده‌برداشتند که در دهها عملیات مشابه وظیفه تعقیب، ترور و اطمینان از قتل مخالفان را بر عهده داشتند.

کارهای تحقیقاتی Bellingcat تنها به پرده‌برداشتن از عملیات اطلاعاتی روسیه خلاصه نمی‌شود، از قتل یک صحرانشین در اسرائیل، کاربرد سلاح‌های انگلیسی یا پهپادهای ساخت ایران در یمن یا اتیوپی، قتل یک مهاجری در یونان و انواع و اقسام کمپین‌های گمراه‌سازی افکار عمومی در سراسر جهان، از دیگر نمونه‌های موفقیت Bellingcat در استفاده از تلاش شهروندان و امکانات عرصه دیجیتال برای پرده‌برداری از سیاه‌ترین موارد نقض حقوق بشر توسط جنایتکاران بزرگ و کوچک‌اند.

۴- اسناد پاناما و اسناد بهشت

«اسناد پاناما» مجموعه‌ای حاوی بیش از ۱۱.۵ میلیون سند محرمانه شرکتی حقوقی در پاناما بود که توسط فردی ناشناس در اختیار یک روزنامه‌نگار آلمانی قرار گرفت. ماه‌ها بررسی این اسناد از هزاران شبکه فساد بسیار بزرگ در سراسر جهان پرده برداشت که در آن صدها چهره سرشناس، از جمله ۱۴۰ سیاستمدار از ۵۰ کشور مختلف با کلاهبرداری، رشوه و فرار مالیاتی، میلیاردها دلار سوءاستفاده کرده بودند. لیست این سیاستمداران که حتی تا بالاترین رده‌های سیاسی کشورهای مختلف را در بر می‌گرفت، به استعفا و بعضا محاکمه برخی از این چهره‌ها انجامید.

اسناد پاناما نمونه بسیار موفقی از همکاری شهروندان ناشناس با روزنامه‌نگاران، خبرنگاران کاوشگر، وکلا و محققان است. بررسی اسنادی در این حجم طبعا نیازمند حجم بزرگی از همکاری بین‌المللی با زبان‌های مختلف و با بهره‌گیری از اطلاعات حقوقی و همچنین تماس با خبرنگاران محلی برای دنبال‌کردن رد سوءاستفاده، فساد و قانون‌شکنی از سوی افراد بانفوذ و صاحب‌قدرت است. در نمونه‌ای دیگر موسوم به «اسناد بهشت»، مجموعه بسیار بزرگ دیگری از اسناد مخفی شرکتی دیگر که با عملیات همزمان در چند بهشت مالیاتی به رهبران دنیای کسب‌وکار بین‌المللی و همچنین شرکت‌ها و موسسات مالی صاحب نام برای فرار مالیاتی کمک می‌کرد، در اختیار روزنامه‌نگاران قرار گرفت و با شروع تحقیقات گسترده توسط کارشناسان حقوقی و همچنین روزنامه‌نگاران کاوشگر، پرده از شیوه‌های بسیار پیچیده انتقال منابع مالی در شبکه‌هایی پنهان از نهادهای نظارتی برداشته شد.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- کدام دسته از ابزارهای زیر به کنشگران برای فعالیتِ امن بیش‌تر کمک می‌کنند؟

الف) تلفن‌های هوشمند و تبلت‌های دارای امکان e-sim به جای سیم‌کارت فیزیکی
ب) استفاده هم‌زمان از وای‌فای و سیم‌کارت‌های ۵G
ج) پیام‌رسان‌های ایمن از شنودِ دولتی و ابزارهای کدگذاری و ذخیره امن داده‌ها
د) شبکه داخلی دفتر با قابلیت اتصال به پرینتر و هارد دیسک قابل اتصال به اینترنت NAS

۲- اطلاعات منبع‌باز یا OSINT چیست؟

الف) اطلاعات منتشرشده توسط اتاق‌های‌فکر و مراکز دولتی و نیمه‌دولتی
ب) اطلاعات محرمانه نهادهای دولتی و نظامی
ج) اطلاعات منتشرشده توسط دانشگاه‌ها، مراکز تحقیقاتی و آکادمیک
د) جمع‌آوری، کاوش و تحلیلِ بضعا عمیق داده‌های در دسترس همگان

۳- در مثال اسنادِ پاناما و اسنادِ بهشت کدامیک از موارد زیر نقشی آغازکننده داشت؟

الف) افشاگران یا whistle-blowers
ب) تلویزیون‌ها و رسانه‌های بین‌المللی
ج) دفاتر و فعالان اقتصادی و حقوقی
د) فعالان دیجیتالِ آزادی اینترنت و امنیت دیجیتال

درس هشتم
تاریخچه و دورنمای سوءاستفاده حکومت‌های سرکوبگر از تکنولوژی دیجیتال

موضوع این درس سوءاستفاده حکومت‌های سرکوبگر از تکنولوژی دیجیتال و دورنمای آن با ظهور پیشرفت‌های تکنیکی نظیر کلان‌داده‌ها و هوش مصنوعی است. ما از خلال دو مطالعه موردی، هر یک با تمرکز بر شماری از تکنولوژی‌های نوظهور و سوءاستفاده از آن توسط دولت‌های سرکوبگر تلاش خواهیم کرد که زمینه بحث بر سر واکنش مناسب بین‌المللی را ایجاد کنیم، مثلا از واکنش غول‌های تکنولوژی نظیر گوگل، آمازون و همچنین آمادگی فعالان، کنشگران و وکلا در جوامع بسته بگوییم.

۱- مطالعه موردی: آژانس تحقیقاتی اینترنت (IRA)

آژانس تحقیقاتی اینترنت (Internet Research Agency)، شهرت موسسه‌ای است در شهر سن‌پطرزبورگ روسیه و دارای ارتباطات بسیار قوی با چندین نهاد اطلاعاتی روس از جمله FSB دستگاه اطلاعاتی جایگزین KGB و GRU یا دستگاه اطلاعاتی ارتش روسیه.

این نهاد با حمایت مالی و تدارکاتی یوگنی‌پریگوژین (Yevgeny Prigozhin)، الیگارش بدنام روس تاسیس‌شده است و شهرت بین‌المللی آن به انتخابات سال ۲۰۱۶ در

ایالات‌متحده و افشای ابعاد تکان‌دهنده دخالت روسیه در فرآیند انتخاباتی ایالات متحده و چند کشور دیگر برمی‌گردد. ما در اینجا قصد ورود به مبحث جزئیات تلاش IRA برای ایجاد بی‌اعتمادی، ناآرامی و اغتشاش در ایالات متحده را نداریم و بیش‌تر روی روش‌ها و شیوه‌های شناخته‌شده دستگاه‌های امنیتی روسیه برای کنترل و تاثیر بر افکار عمومی از طریق فضای مجازی تمرکز می‌کنیم چرا که شیوه‌های مشابهی توسط روسیه و هم‌پیمانانش نظیر جمهوری اسلامی ایران همین امروز در دنیای دیجیتال در حال اجرا و قابل رصد است.

به طور خلاصه شالوده صدها کمپین مختلف IRA با هدف قراردادن گروه‌هایی با گرایشات بعضا متضاد از اسلامگرایان افراطی گرفته تا گروه‌های نژادپرست سفید و گروه‌های رادیکال بزرگ و کوچک دیگر به مفهوم Emotional Manipulation یا دست‌کاری و فریب احساسی برمی‌گردد. در تعریفی خلاصه می‌توان نابودکردن استدلال و منطق، آمار، مطالبات شهروندان، پاسخگویی و مسئولیت‌پذیری و جایگزین‌کردن آن با خشم، هیجان و احساسات آنی را نقطه تمرکز همه کمپین‌های IRA دانست.

این کمپین‌ها در اشکال متفاوت و با به‌کارگیری قالب‌هایی مختلف و با مطالعه بسیار دقیق تکنیک‌های انحراف روانی و همچنین مشکلات درونی شبکه‌های اجتماعی نظیر فیس‌بوک و ایکس و سایت‌های انتشار محتوا، نظیر یوتیوب، طراحی شده بودند. ما چند قالب متفاوت از این کمپین‌ها را در ادامه معرفی خواهیم کرد.

۳ قالب عمده کمپین‌های انحراف افکار عمومی در روسیه

قالب اول: ایجاد تفرقه، چندقطبی‌سازی و خشونت

کاربر A به لحاظ سیاسی، بیکاری دوستان و نزدیکان خود و ورشکستگی واحدهای تولیدی سابقا پررونق را حاصل سیاست‌های مهاجرتی حزب حاکم می‌داند. IRA با صرف هزینه‌ای نسبتا پایین، چند وبسایت خبری با لوگو و نام مشابه رسانه‌های معتبر را طراحی می‌کند، اخباری کاملا دروغ (Fake News) دال بر سوءاستفاده، قتل و تجاوز مهاجران و آینده سیاه کشور در این سایت‌ها منتشر می‌شود. IRA سپس با پرداخت هزینه این اخبار را در شبکه‌اجتماعی فیس‌بوک منتشر می‌کند. کاربر A به دلیل پیشینه ذهنی خود جذب این اخبار شده و در گروه فیس‌بوکی این اخبار عضو می‌شود. افسران اطلاعاتی روس در این

گروه با شیوه‌های روانی-تکنیکی بسیار پیچیده اعضای گروه را روز به روز بیش‌تر در دام تئوری‌های توطئه گرفتار آورده و به اخبار کذب و افراط‌گرایانه معتاد می‌کنند. در نهایت، از هزاران عضو گروه، فردی بسیار افراطی و فاقد تعادل روانی شناسایی و برای حمله خشونت‌بار به تجمع طرفداران حزب حامی دموکراسی آماده و تشویق می‌شود.

قالب دوم: هک و افشا، ایجاد بی‌اعتمادی و نظریه توطئه

کاربر B یک سیاستمدار حامی دموکراسی و منتقد سیاست‌های دولت روسیه است. با استفاده از آخرین شیوه‌های و ابزارهای چندصدمیلیون‌دلاری هک دولتی، مهندسی اجتماعی و فریب، ایمیل او هک می‌شود و محتوای ده‌ها هزار ایمیل به دست IRA می‌افتد، بلافاصله انتشار برخی از ایمیل‌ها از طریق وب‌سایتی نظیر ویکی‌لیکس (wikileaks) آغاز می‌شود. در ادامه انتشار گزینشی ایمیل‌ها، پاره‌ای اطلاعات دروغ و گمراه‌کننده به برخی از ایمیل‌های اصل اضافه می‌شود. ایمیل‌هایی برای افشای انتخاب می‌شوند که حداکثر تخریب و ایجاد سوءظن عمومی و بدگمانی به فضای عمومی انتخابات و سیاست را موجب شوند. شماری از سیاستمداران با انتشار اخبار دروغ از طریق ایمیل‌ها به سوءاستفاده جنسی یا فساد متهم می‌شوند. این دروغ‌ها به صورتی عجیب با استفاده از چندین بات که از ده‌ها هزار شناسه جعلی و غیرواقعی تشکیل شده‌اند در تازه‌های شبکه‌های اجتماعیِ میلیون‌ها کاربر واقعی منتشر می‌شوند و فضای اطلاعاتی کشور را به شکلی آلوده می‌کنند که در نهایت یکی از کاربران خشمگین تصمیم می‌گیرد با اسلحه سراغ سیاستمداران حزب مخالف روسیه رود.

قالب سوم: رهبران و سخنگویان ناشناس Sock Puppet

شما هم حتما حساب‌های کاربری بسیار ناشناس و با نام مستعاری را دیده‌اید که در شبکه‌های اجتماعی چون ایکس ده‌ها و صدها برابر افراد شناخته‌شده و افرادی که در رسانه‌های با مخاطب چندمیلیونی مثل تلویزیون ظاهر می‌شوند، لایک می‌گیرند و دنبال‌کننده دارند. همه این حساب‌های ناشناس توسط دستگاه‌های امنیتی یا دیگر نهادهای در تلاش برای کنترل افکار عمومی، هدایت نمی‌شوند، اما مثلا IRA مجموعه بسیار پیچیده‌ای از ده‌ها و صدها حساب مثلا در لباس دفاع از حقوق اقلیت‌های نژادی یا دیگر اقلیت‌ها در ایالات

متحده راه‌اندازی کرد. این احساب‌های کاربری جعلی سپس با بهره‌گیری از بات‌ها مزین به ده‌ها، صدها و بعضا هزاران لایک، دنبال‌کننده و بازنشر در فیس‌بوک، ایکس و شبکه‌های اجتماعی دیگر شدند. IRA با بهره‌گیری از تکنیک‌های هنری و صرف هزینه، محتوایی را تولید می‌کرد که از خلال انتشار توسط این حساب‌ها (Sock Puppet) ده‌ها و صدها هزار دنبال‌کننده و این بار واقعی را به دنبال آورد. در مواردی افسران اطلاعاتی روس از خلال این حساب‌های Sock Puppet با کاربران واقعی تماس برقرار کرده و آنان را ترغیب به حضور در اعتراضات و اقدام به خشونت کرده‌اند.

۲ - مطالعه موردی: چین کمونیست، دورنمای تاریک زندان دیجیتال

یک دهه پس از رویدادهای خون‌بار میدان تیان‌من (Tiananmen Incident)، رهبران چین کمونیست مانند دیگر حکومت‌های تمامیت‌خواه توجه ویژه خود را معطوف به پیشرفت‌های دیجیتال و دورنمای استفاده شهروندان از این ابزارها برای ایجاد فضای گفت‌وگو، انتقاد و گسترش مطالباتی نظیر حقوق بشر، احترام و آزادی بیان و اندیشه کردند. دیوار آتش یا دیوار دیجیتال چین برای توقف هر نوع تبادل‌نظر و تجربه شهروندان با دنیای آزاد و با هدف کنترل صددرصدی و محدودکردن فعالیت‌های آنلاین شهروندان، روزبه‌روز مستحکم‌تر شد.

تقریبا همه رسانه‌های اصلی دنیای آزاد فیلتر شدند. موتورهای جستجو، پیام‌رسان‌های مورد استفاده در سراسر جهان و همچنین شبکه‌های اجتماعی و سایت‌های به‌اشتراک‌گذاری محتوی نظیر ایکس نیز به روی کاربران چینی مسدود شدند. حزب‌کمونیست چین همه سال‌های دهه ۲۰۱۰ را به تحقیق و آزمایش درباره استفاده از تکنولوژی چون هوش مصنوعی و کلان‌داده مثلا برای شناسایی چهره و تحت‌کنترل گرفتن رفت‌وآمد شهروندان کرد. در این میان گزارش‌هایی تکاندهنده از جمع‌آوری DNA و دیگر داده‌های بیومتریک برخی اقلیت‌ها، خصوصا اقلیت اویغور ، منتشر شده است.

همه این گزارش‌ها دورنمایی بسیار سیاه از نوعی سیاه‌چال و زندان دیجیتال را به نمایش می‌گذارد که تمام افکار و حرکات افراد به صورت ۲۴ساعته توسط ماشین و الگوریتم‌های خودکامل‌کننده هوش مصنوعی کنترل می‌شود تا معترضان یا اقلیت‌های تحت ستم، حتی قبل از انجام هر نوع حرکت اعتراضی بازداشت و سرکوب شوند. موارد

زیر همه قالب‌هایی از تلاش دولت چین برای کنترل دیجیتال اعتراضات را نشان می‌دهند

۴ قالب عمده تلاش چین برای کنترل دیجیتال اعتراضات

۱- تکنولوژی تشخیص و دسته‌بندی چهره با هوش مصنوعی

گزارش‌هایی مبنی بر توسعه الگوریتم‌هایی توسط دولت چین و نهادهای وابسته به حزب کمونیست منتشر شده که در آن شکل صورت و خصوصیات بیولوژیک نظیر فاصله چشم، پیشانی و دیگر مشخصات صورت برای پروفایل‌کردن شهروندان اقلیت «اویغور» و «تبت» در اماکن عمومی مورد استفاده قرار گرفته است به این معنا که در میان هزاران عابر در یک خیابان یا میدان، تکنولوژی هوش مصنوعی از طریق دوربین‌های مداربسته همه افرادی که چهره و دیگر مشخصات بیولوژیک شبیه اویغورها یا تبتی‌ها دارند را شناسایی و در اختیار پلیس قرار می‌دهد. همچنین دولت چین با سرعت مشغول کار روی شاخه دیگری از این تکنولوژی است که با تحلیل حجم عظیم داده‌های دوربین‌های مداربسته حال روحی و روانی و احساسات افراد را اندازه‌گیری می‌کند و الگوریتم افراد به‌شدت خشمگین و تحت استرس بیش‌تر را به صورت زنده شناسایی می‌کند.

۲- جمع‌آوری DNA و دیگر داده‌های بیومتریک از اقلیت‌ها

علاوه بر جمع‌آوری و ثبت DNA و دیگر داده‌های بیومتریک از اقلیت‌ها و ناراضیان، دولت چین با جدیت مشغول تکمیل کلان‌داده‌هایی است که در آن حجم عظیمی از داده از رنگ چشم و مشخصات فیزیکی گرفته تا نمونه منحصربه‌فرد صدا، نحوه راه‌رفتن و فهرست بلند بالایی از مشخصات فیزیکی او در آن ثبت شوند. هم‌زمانی این پروژه‌های بسیار پردامنه جمع‌آوری داده با انتشار گزارش‌هایی از کمپ‌های بازداشت، فشار و شستشوی مغزی جوانان و حتی نوجوانان اقلیت‌هایی چون ایغورها بسیار نگران‌کننده است.

۳- سیستم رتبه‌بندی اعتبار اجتماعی (Social Credit System)

چین در ده سال گذشته به‌سرعت مشغول کار و توسعه سیستم رتبه‌بندی شهروندان بر اساس تک‌تک فعالیت‌های اجتماعی ایشان خصوصا فعالیت‌های آنلاین است. در این سیستم انتقاد از حکومت، شرکت در یک حرکت اعتراضی و حتی لایک‌کردن یک پست

انتقادی و اخبار تاییدنشده توسط رسانه‌های حکومتی می‌تواند دسترسی شما را به بسیاری از امتیازات اجتماعی حتی تا خرید یک کامپیوتر و تلفن کاهش دهد اما در عوض شرکت در تجمعات و طرح‌های حکومتی، پست مقاله و فعالیت در شبکه‌های اجتماعی به نفع حزب کمونیست و بسیاری فعالیت‌های دیگر حکومتی می‌تواند رتبه شهروندان را بالا ببرد و آنان را از بسیاری از تسهیلات بانکی و دیگر مشوق‌ها بهره‌مند سازد. مواردی که مستقیما در بالا و پایین‌رفتن رتبه شهروندان نقش دارند و مکانیسم‌های تاثیر آنان غیرشفاف‌اند، مثل مواردی چون شکایت همسایه از شما به دلیل دشمنی، به مقامات سیاسی محلی و پلیس، رتبه شما پایین می‌آید. همچنین در رتبه‌بندی اجتماعی شمار غیرقابل‌باوری از متغیرهای برآمده از حجم انبوه داده - مثلا از مصرف آب و برق گرفته تا دیدار و ملاقات، کمک و مواظبت از شهروندان سالخورده - در رتبه‌بندی اجتماعی شما نقش ایفا می‌کنند.

دورنمای طرح رتبه‌بندی اجتماعی تکان‌دهنده است، جامعه‌ای که در آن شهروندان بدون هر ایده و اختیاری مانند اجزای یک بازی فقط و فقط به دنبال کسب یک امتیاز بیش‌تر و بهره‌مندشدن از تسهیلات دولتی‌اند.

۴- هوش مصنوعی و سرکوب پیشگیرانه (Predictive Policing)

دو اقلیت اویغور و تبت یا گروهی از ناراضیان سیاسی مثل وکلای حقوق بشر در چین را در نظر آورید، در سال‌های گذشته هر روز بیش‌ازپیش از پدیده سرکوب پیشگیرانه صحبت می‌شود. پلیس پیش‌گیری، به مجموعه‌ای پیچیده از کاربرد الگوریتم‌های هوش مصنوعی، ریاضیات، مدل‌های آماری و تحلیل داده‌های حاصل از مدل‌های آماری برای پیش‌بینی وقوع جرم در ساعت و مکان مشخص مجهز است. مثلا با استفاده از داده‌های سال‌های پیشین، دوربین‌های مداربسته، افزایش فعالیت تردد برخی شماره تلفن‌های خاص، امکان وقوع جرم مثلا قاچاق مواد مخدر و سرقت در نقطه‌ای خاص پیش‌بینی می‌شود.

سرکوب پیشگیرانه، موضوعی بسیار مناقشه‌برانگیز است و در آزادترین جوامع جهان، صاحب‌نظران علی‌رغم اذعان به فواید بسیار آن برای جلوگیری از وقوع جرم و جنایت، مثلا جنایت علیه کودکان و زنان، از عواقب ناخواسته و کنترل‌نشده جانبی آن به‌شدت ابراز نگرانی می‌کنند. مثلا بیم آن می‌رود که الگوریتم‌های هوش مصنوعی یک اقلیت نژادی یا یک گروه اجتماعی را به‌شدت هدف قرار دهد و افراد عضو این اقلیت مثلا به دلیل رنگ

پوست، مشخصات صورت یا طرز لباس‌پوشیدن بارها و بارها توسط پلیس متوقف و مورد بازجویی و آزار قرار گیرند. این پدیده یعنی هر آنچه در دنیای آزاد دغدغه و مایه نگرانی کوشندگان حقوق بشر است، در چین کمونیست ظاهرا هدف دولت برای توسعه چنین الگوریتم‌هایی است. با روش‌های برآمده از هوش مصنوعی و کلان‌داده صدای یک فرد یا اعضای یک گروه معترض از خلال میلیاردها تماس صوتی شناسایی می‌شود. حتی بدون اطلاع و بعضا با اجبار این افراد اپلیکیشن‌های جاسوسی روی تلفن‌های همراهشان نصب می‌شود. همه رفت‌وآمدهای ایشان از خلال تکنولوژی تشخیص چهره، تشخیص پلاک ماشین و مکان‌یاب تلفن آن‌ها کنترل می‌شود. با کنترل کامل تماس‌ها، ارتباطات و دیگر فعالیت‌های اینترنتی آنان کم‌ترین زمینه برای اعتراض و جمع‌آوری شواهد توسط ناراضیان آلارم‌های بسیاری را برای دولت و نهادهای امنیتی به صدا درمی‌آورد و با بازداشت و ارعاب فرد، اعتراض حتی قبل از وقوع آن خفه می‌شود.

آزمون ارزیابی

لطفا با دقت به پرسش‌ها پاسخ دهید. این کار کمک می‌کند درک خود از مطالب درس را ارزیابی کنید. پاسخ‌های درست در بخش پاسخ‌نامه در پایان کتاب در دسترس است.

۱- واکنش مناسب دنیای آزاد به سرکوب دیجیتال شهروندانِ جوامع بسته؟

الف) انسداد تمام سرویس‌های اینترنتی نظیر گوگل و یوتیوب برای آن جوامع

ب) تحریم، فشار و مقابله با صدور و گسترش تکنولوژی تجسس و سرکوب شهروندان

ج) همکاری با مراجع قانونی آن کشورها و پاسخ به درخواست‌های ایشان

د) تمرکز بر توسعه تکنولوژی دیجیتال در جوامع باز

۲- مهم‌ترین راهبرد دولت‌های مستبد در جلوگیری از گردش آزاد اطلاعات چیست؟

الف) فیلترینگ و انسداد دسترسی شهروندان به دنیای اطلاعات آزاد و بدون سانسور

ب) هدف قراردادن منتقدین و کنشگران مدنی

ج) فشار بیش‌تر به زندانیان سیاسی و ارعاب منتقدین

د) تلاش برای هک ایمیل و سایر اکانت‌های منتقدین و ناراضیان

۳- راهکار اصلی دولت‌های مستبد در سرکوب فعالیت دیجیتال کنشگران چیست؟

الف) افزایش قیمت خدمات اینترنتی با هدف کاهش استفاده کنشگران از چنین سرویس‌هایی

ب) شنود، رصد و مراقبت آنلاین، هک، تهدید و ارعاب کنشگران

ج) ایجاد سرویس‌ها و پیام‌رسان‌های جایگزین یوتیوب، اینستاگرام و گوگل

د) انتشار اخبار دروغ درباره منتقدان و مخالفان

پاسخ‌نامه

در این بخش پاسخ‌های پرسش‌های آزمون ارزیابی درس‌ها را مشاهده می‌کنید.

درس یک: ۱: ج / ۲: ج / ۳: د
درس دو: ۱: الف / ۲: د / ۳: ب
درس سه: ۱: ب / ۲: الف / ۳: ج
درس چهار: ۱: ج / ۲: د / ۳: ج
درس پنج: ۱: ج / ۲: الف / ۳: د
درس شش: ۱: الف / ۲: ب / ۳: د
درس هفت: ۱: ج / ۲: د / ۳: الف
درس هشت: ۱: ب / ۲: الف / ۳: ب