چالش‌ها و راهکارهای مدیریت فضای مجازی

سخنرانی حجت‌الاسلام والمسلمین دکتر حمید شهریاری
در دبیرخانه مجلس خبرگان قم

اشاره

آنچه پیش رو دارید، سخنرانی حجت‌الاسلام والمسلمین دکتر حمید شهریاری است که در تاریخ سی‌ام دی‌ماه سال ۱۳۹۵، در دبیرخانه مجلس خبرگان قم بیان نموده‌اند. در این جلسه که اعضای کارگروه فرهنگی کمیسیون سیاسی مجلس خبرگان رهبری نیز حضور داشتند، آقای دکتر شهریاری ضمن تبیین اهمیت مسئله مدیریت فضای مجازی و نگرش‌های متضادّ موجود در این باره، به آشفتگی‌های سیاست‌گذاری در این حوزه اشاره کردند و راه‌حل‌های پنج‌گانه‌ای را نیز برای بهبود وضعیت فضای مجازی در کشور پیشنهاد دادند. آنچه در ادامه می‌آید، بررسی چالش‌ها و راهکارهای مدیریت فضای مجازی است که امیدواریم مورد توجه مسئولان امر قرار گیرد.

نکته اوّل: اهمیت فضای مجازی

فضای مجازی، مسئله بسیار مهم و بزرگی است. اگر این مسئله را کوچک فرض کنیم، به دنبال راه‌حل‌های کوچک خواهیم بود و توقعات ما نیز در قبال این مسئله، ساده خواهد بود و به صورت طبیعی، آن راه‌حل‌ها نمی‌تواند ما را از مشکلات پیچیده و بزرگ موجود نجات دهند و نخواهیم توانست از فرصت‌هایی که در اختیارمان قرار دارد، به شکل بهینه استفاده نماییم. برای اینکه بزرگی و پیچیدگی فضای مجازی را نسبت به امکانات موجود در کشور تشبیه کنم، باید مقایسه ناو هواپیمابر با یک قایق تندرو را مثال بزنم. چرا چنین مثالی می‌زنم؟ می‌خواهم بیان کنم که هر نوع راه‌حلی، نیازمند دو پیش‌نیاز از سوی ارائه‌دهنده راهکار است؛ اوّل اینکه فرد باید وسط میدان باشد و دستی در اجرا داشته باشد تا مشکلات اجرایی مملکت را بشناسد. هستند افرادی که در سراسر عمر خود هیچ کاری جز انتقاد و نظریه‌پردازی نداشته‌اند؛ آنها نمی‌توانند راه‌حل‌های عملی عرضه کنند. دوم اینکه فضای مجازی، عرصه نوینی است که احتیاج به ایده‌پردازی دارد. کسانی که صرفاً کار اجرایی کردند نیز نمی‌توانند راه‌حل‌های بادوامی را برای چالش‌های آن عرضه کنند. باید طرح‌های اجرایی با پشتوانه نظریه‌پردازی و ایده‌پردازی در این فضا صورت گیرد. افرادی که پیشنهادهای متقن می‌دهند، کسانی هستند که حتماً باید نگاه راهبردی و ایده‌پردازی داشته و آینده‌نگر باشند.

عده‌ای در برخی شوراهای عالی نشسته‌اند و می‌گویند آقا این طور بشود، این طور نشود؛ این اشخاص تا حالا هیچ کار یا مسئولیت اجرایی نداشته‌اند؛ اما مدام می‌گویند باید این چنین بشود. یک عده هم فقط در امور اجرایی هستند و کاری به مباحث تئوریک و نظریه‌پردازی ندارند؛ اما به نظر می‌رسد که یک راه‌حل قاطع باید از سوی کسانی عرضه گردد که در هر دو حوزه حضور داشته باشند؛ هم در فضای مجازی اهل نظر باشند و هم دستی در اجرا داشته باشند.

در حال حاضر، ما فناوری لازم برای ساخت برخی امور را نداریم؛ مثلاً نمی‌توانیم پردازنده اصلی رایانه را بسازیم؛ البته تحصیل دانش آن دشوار نیست؛ فقط ابزارهای لازم برای اینکه آن همه اتصالات را درون یک قطعه سه‌سانتی قرار دهیم، نداریم یا مثلاً نمی‌توانیم ناو هواپیمابر بسازیم؛ یعنی فناوری آن را نداریم؛ اما می‌توانیم قایق تندرو بسازیم که کارآمدهایی هم در خلیج فارس داشته باشد و نیاز ما را برطرف کند و امنیت خلیج فارس را برایمان تضمین نماید. در خصوص فضای مجازی هم این‌گونه است؛ دانش، فناوری و سرمایه موجود فعلی، برای اینکه بتوانیم مسائل فضای مجازی را به‌خوبی حلّ‌وفصل کنیم، کافی نیست. با امکانات موجود ما به هیچ رو نمی‌توانیم در فضای مجازی از فرصت‌ها و همه ابعاد مثبت آن استفاده کنیم و از تهدیدهایش فرار نماییم. این حرف را می‌زنم، چون مسئله فضای مجازی، موضوع بزرگی است؛ اما به اندازه بزرگی آن، هزینه نمی‌کنیم؛ البته چالش‌های فضای مجازی، بسیار بزرگ است و پیچیدگی ساخت پردازنده رایانه، موتور یا ناو هواپیمابر را دارد.

ما از سال‌های گذشته، ابعاد مدیریت فضای مجازی را خیلی مطالعه و پیگیری کرده‌ایم. در سال گذشته، گفتیم اگر بخواهیم از یک جایی شروع کنیم، باید اوّل مبلغ و هزینه این کار برآورد و تأمین شود که پول کمی هم نخواهد بود. امروزه، اگر یک دیتاسنتر یا مرکز داده کوچک بخواهید در جایی ایجاد کنید، ده میلیارد تومان هزینه آن خواهد شد. ما در مرکز تحقیقات کامپیوتری علوم اسلامی، در حدّ نیاز، دیتاسنتری ایجاد کرده‌ایم که بتوانیم دیتاها و اطلاعات و منابع اسلامی را روی آن نگهداری کنیم. تاکنون چیزی بیش از ده میلیارد تومان هزینه شده است که این فقط

دانش، فناوری و سرمایه موجود فعلی، برای اینکه بتوانیم مسائل فضای مجازی را به‌خوبی حلّ‌وفصل کنیم، کافی نیست. با امکانات موجود ما به هیچ رو نمی‌توانیم در فضای مجازی از فرصت‌ها و همه ابعاد مثبت آن استفاده کنیم و از تهدیدهایش فرار نماییم. این حرف را می‌زنم، چون مسئله فضای مجازی، موضوع بزرگی است؛ اما به اندازه بزرگی آن، هزینه نمی‌کنیم

هزینه ایجاد آن است؛ نه نگهداری آن.

حالا شما ببینید شرکت گوگل ده‌ها دیتاسنتر وسیع و پیچیده در سراسر جهان دارد که همه در مالکیت اوست. وسعت یکی از این دیتا سنترها، حدود ۶۵۰۰ متر مربع است. این شرکت، صاحب هزاران سِرور است که صدها میلیارد تومان ارزش دارد و در سراسر جهان مستقر است. ارزش مجموع دارایی گوگل با بیش از ۵۷ هزار نفر کارمند، بیش از ۱۳۱ میلیارد دلار تخمین زده شده است و درآمد ناخالص آن در سال ۲۰۱۴، بالغ بر ۶۶ میلیارد دلار و سود خالص آن، بیش از ۱۴ میلیارد دلار بوده است. توجه کنید که بودجه کل کشور ما در سال ۹۴ ، کمی بیش از ۹۷۸ هزار میلیارد تومان معادل ۲۵۰ میلیارد دلار بوده؛ یعنی درآمد ناخالص شرکت گوگل نزدیک به یک چهارم بودجه کل کشور ماست. موتور جست‌وجوی گوگل نیز در کل دنیا از نظر رتبه در میان دیگر سایت‌های جست‌وجوگر، شماره یک است؛ جست‌وجوگری که ده‌هامیلیارد مراجعه کاربران و درخواست‌کنندگان اطلاعات را در روز پاسخ می‌دهد. امروز، بزرگ‌ترین تاجران دنیای فناوری اطلاعات، شرکا و صاحبان شرکت گوگل هستند. وقتی می‌گوییم بزرگ‌ترین تاجران، یعنی اینکه زمانی مثلاً شرکت فورد سرمایه‌دار اصلی در دنیای تکنولوژی بود؛ یعنی سرمایه، تجهیزات سخت‌افزاری محض بود؛ اما امروز سرمایه‌ها، ترکیبی از سخت‌افزار و نرم‌افزار هستند که به عنوان هسته اصلی ثروت و سرمایه در دست شرکت‌های گوگل یا مایکروسافت قرار دارد. در بودجه امسال به وزارت ارتباطات جهت اجرای وظایف حاکمیتی و توسعه زیرساخت‌ها و خدمات و کاربردهای فناوری اطلاعات و شبکه ملی اطلاعات و امور دیگر فناوری اطلاعات، جمعاً بیش از دو هزار میلیارد تومان که برای کشور ما پول کمی هم نیست، در لایحه بودجه ۹۵ اختصاص داده‌ایم که نشان می‌دهد دولت و مجلس شورای اسلامی نیز عظمت کار را قبول کرده و این مبلغ را تصویب کرده است؛ اما فکر می‌کنم به جهت شرایط مملکت، تا کنون چیزی کمتر از پنج درصد از این پول، برای کارهایی که گفتیم، اختصاص یافته است.

نکته دوم: رویکردهای دوگانه مسئولان

رویکردهای متفاوتی در نظام ما برای تعامل با فضای مجازی هست؛ یک دسته از مسئولان اجرایی ارشد نظام هستند که همه جا قائل به فضای آزادند؛ اینان حقوق شهروندی را هم همین طوری می‌نویسند، اقتصاد مقاومتی را نیز همین گونه تعریف می‌کنند و سعی می‌نمایند انرژی هسته‌ای را هم در این فضا ببینند. اینان اصولاً توسعه کشور را ملازم با آن فضای باز می‌دانند. این آقایان می‌گویند ما تا به آن فضای باز نرسیم، اصلاً توسعه در مملکت ما شکل نمی‌گیرد. نگاه این گروه به فضای مجازی، گوشه‌ای از سیاست «درب‌های باز» است که به آن قائل‌اند. اینها می‌گویند: آقا بگذارید فضای مجازی باز باشد، باید دسترسی به اطلاعات، آزاد باشد. البته این را هم می‌گویند که بازبودن، به معنای دسترسی به فساد و فحشا نیست. هیچ‌کس این

به نظر من، ما تا به اجماع نخبگانی نرسیم، نمی‌توانیم به مدیریت یکپارچه فضای مجازی برسیم. اوّل باید داخل مملکت خودمان یا به اجماع نخبگانی برسیم، یا اگر به اجماع نخبگانی نمی‌رسیم، همگی سازوکاری را برای تصمیم نهایی و قطعی بپذیریم

را قبول ندارد. یعنی اجماع نخبگانی می‌گوید ما با جریان فساد و فحشا و سایر تهدیدهایی که برای فضای مجازی فهرست شده، مخالفیم؛ ولی اجمالاً عرض کنم که تفکر تسامح و تساهلی نیز در این موضوع هست. ازاین‌رو، قائلان به این نظریه، در جلسه‌ای در مورد یک سایت بازی برخط که اخیراً بستند، می‌گویند: آقا چه کسی به شما گفت این بازی را ببندید؟ این سایت، بیش از یک میلیون نفر کاربر دارد. چیزی که بیش از یک میلیون نفر کاربر دارد، حقوق شهروندی محسوب می‌شود و حتی کمیته تعیین مصادیق نیز حقّ بستنش را ندارد. باید این موضوع را در شورای فضای مجازی تصمیم‌گیری کرد.

طبق فرمایش ایشان، وقتی این کار در شورا آمد، یعنی در دستورکار شورای عالی فضای مجازی قرار می‌گیرد و در فهرست کارهای رئیس شورا قرار خواهد گرفت. رئیس شورا نیز آن را در نوبت می‌گذارد و هر وقت صلاح دانست آن را مطرح می‌کند یا شاید هم اصلاً مطرح نکند. بنابراین، این یک طرز تفکر است که در نظام جمهوری اسلامی جدّی است و طرف‌داران آن، از مسئولان ارشدند. اینها می‌گویند: آقا مگر بچه‌حزب‌اللهی‌های لبنان در فضای باز سیاسی و اجتماعی لبنان که ترکیبی از سنّی، شیعه، مسیحی، بی‌دین و غیر از اینهاست و همه مخلوط و با هم هستند، ساخته نشدند؟ خب، با این فضای باز، می‌بینید از درون آنها حزب‌الله لبنان درآمده است. در آنجا، فضای جامعه باز است و همه چیز و هر موضوعی هم در شبکه‌های مجازی و ماهواره‌های آنجا ردوبدل می‌شود و هیچ‌کس هم مانع چاپ کتاب، راه‌اندازی سایت و تولید انواع فیلم نیست؛ خلاصه اینکه جامعه آنجا باز است؛ اما از درون آن، حزب‌الله سر بر آورده است. ما هم باید به این سمت برویم و ایجاد فیلتر و مانع، چاره‌ساز تهدیدات امروزی نیست. این طرز تفکر، دلایل خودش را هم دارد. یکی از دلایلش این است که می‌گویند اگر بستر و فضا باز نباشد، این جوان به خارج می‌رود و همان‌کاری که شما در اینجا مانعش شدی، آنجا انجام می‌دهد.

در مقابل این اندیشه، یک تفکر دیگری وجود دارد که تحفظ بیشتری بر حریم حاکمیتی دارد. این رویکرد می‌گوید: حریم حاکمیتی، باید محفوظ بماند؛ هرچند مجبور شویم مقداری از فضای آزاد کشور را ببندیم؛ یعنی چند سایت یا شبکه اجتماعی را فیلتر کنیم؛ مثلاً چند سال پیش نرم‌افزاری بود مشابه همین تلگرام امروزی که اسمش ویچت بود. آقای خرم‌آبادی دبیر کمیته

الآن در کشور نرخ نفوذ اینترنت، پنجاه‌ویک درصد است؛ یعنی پنجاه‌ویک درصد مردم به اینترنت و شبکه دسترسی دارند و حدود بیست‌وپنج درصدشان تلفن همراه هوشمند دارند که می‌توانند از این شبکه استفاده کنند و شمارشان مرتب رو به افزایش است

هرکسی می‌خواهد فعالیتی در شبکه انجام دهد، اوّل باید احراز هویت بشود. احراز هویت در شبکه، دارای سطوح متعددی است. اوّلین سطح آن، احراز هویت با سیمکارت یا خط تلفن است؛ یعنی هرکس سیمکارت یا خط تلفن می‌خواهد، اوّل باید از طریق مخابرات احراز هویت شود تا سیمکارت یا خط تلفن به نام او صادر گردد؛ به عبارت دیگر، هویتش با نشانی و کد ملی‌اش مشخص شود

تعیین مصادیق، ویچت را با پنج میلیون کاربر بست. چهار یا پنج شبکه اجتماعی دیگر را هم بست؛ اما دولت که عوض شد، دیگر ایشان زورش نرسید که تلگرام را ببندد؛ وگرنه اگر همان روال ادامه داشت، همچنان‌که ایشان پنج شبکه اجتماعی را بست، ششمی آن را هم می‌بست. وقتی دولت جدید آمد، ترکیب کمیته تعیین مصادیق، به نفع دولت فعلی تغییر کرد. دولت جدید هم نظریه فضای باز را داشت. به همین جهت، گسترش و همه‌گیری شبکه‌های مجازی به حال خود رها شد. این تلگرامی که با دو میلیون عضو در کشور شروع به فعالیت کرده بود، الآن بیست میلیون کاربر دارد. ما می‌خواهیم آن را ببندیم؛ ولی می‌بینیم با بیست میلیون جمعیت مواجه هستیم و همین‌طور به اعضای آن نیز اضافه می‌شود. هرکس تلفن همراه هوشمند می‌خرد، به این شبکه اضافه می‌شود. الآن در کشور نرخ نفوذ اینترنت، پنجاه‌ویک درصد است؛ یعنی پنجاه‌ویک درصد مردم به اینترنت و شبکه دسترسی دارند و حدود بیست‌وپنج درصدشان تلفن همراه هوشمند

دارند که می‌توانند از این شبکه استفاده کنند و شمارشان مرتب رو به افزایش است؛ در عین حال، طرف‌داران سیاست بسته می‌گویند باید همه شبکه‌هایی را که مجرای هرگونه فسادی است، فوراً بست و نباید به آنها فرصت فعالیت داد. این خدمات، بستر استفاده مخالفان نظام و بهره‌برداری مجرمان و مفسدان می‌شود. اگر مقابله نشود، اصل نظام خدشه‌پذیر خواهد شد. بی‌توجهی به آن، موجب می‌شود ارکان نظام با القائات شیطانی سست گردد و اگر ادامه یابد، می‌تواند آثار مخربی در اذهان عمومی ایجاد کند. دامن‌زدن به شایعات و القای ناامیدی و یأس به مردم و مواجهه افراد کم‌سن‌وسال با فساد و فحشا و تزلزل ارکان حاکمیت، از پیامدهای قطعی بی‌توجهی به این شبکه‌هاست. باید با آن مقابله کرد و تاوقتی که نتوانیم آن را مدیریت کنیم، باید آنها را ببندیم. این عده می‌گویند ما در قبال جامعه مسئولیت و وظیفه داریم؛ نمی‌شود حیوان درنده را آزاد کنی. باید گردنش را ببندی و میخش را بکوبی که هرکسی را آزار ندهد. باید سیل را مهار کرد. این سیل اگر مهار نشود، تبدیل به یک جریان ویرانگری می‌شود و می‌آید همه را با خود می‌برد؛ همان‌طورکه در اسپانیا سیل فساد و فحشا جوانان مسلمانش را نابود کرد و اسلام از اروپا برچیده شد. ممکن است، این اتفاق برای کشور ما هم بیفتد. این هم یک ایده و تفکر، با استدلال خودش.

پس به طور کلی، ما این دو طرز تفکر را در مملکت داریم و هریک رهبرانی پیدا یا پنهان دارند. اینها دارند خودشان و طرز تفکرشان را به وسیله روزنامه‌ها، مجلات و فضای مجازی عرضه می‌کنند.

به نظر من، ما تا به اجماع نخبگانی نرسیم، نمی‌توانیم به مدیریت یکپارچه فضای مجازی برسیم. اوّل باید داخل مملکت خودمان یا به اجماع نخبگانی برسیم، یا اگر به اجماع نخبگانی نمی‌رسیم، همگی یک سازوکاری را برای تصمیم نهایی و قطعی بپذیریم.

راه‌حل‌های مشکلات فضای مجازی

به طور کلی، بنده پنج راه‌حل را برای مدیریت فضای مجازی مطرح می‌کنم:

راه‌حل اوّل: مدیریت وی‌پی‌ان (VPN) یا مدیریت فراراه‌ها در اینترنت

برای شرح راه‌حلّ اوّل، یک مقدمه لازم است و آن اینکه حاکمیت در کشور ما، خود یک راه‌هایی را در فضای مجازی برای نوعی از دسترسی‌ها باز گذاشته که شما هرچه هم بخواهید موردی را در فضای مجازی ببندید، چون راه‌های دسترسی توسط حاکمیت باز گذاشته شده، قادر نخواهید بود. این راه‌های باز، VPN یا فیلترشکن نام دارد. وی‌پی‌ان یا فیلترشکن، پاشنه آشیل هر نوع راهبرد در فضای مجازی است؛ یعنی من بعداً هر چیزی که می‌خواهم بگویم، اگر شما این راه باز را درست نکنید، آن چیزهایی که بعداً می‌خواهم بگویم، کف روی آب یا «هَباءً مَنْثُورا» است. وی‌پی‌ان (Virtual Private Network)، یعنی با تونل‌زدن یا رمزنگاری و مانند آن، بتوان امنیت و حریم خصوصی داده‌های مبادله‌شده را چنان حفظ کرد که حتی‌المقدور هویت طرفین مخفی بماند و محتوای اطلاعات مبادله‌شده رمزگذاری شود و محل دریافت و ارسال اطلاعات نامعلوم گردد؛ مثلاً من از اینجا به خانه‌ام یک تونل بزنم؛ به‌طوری‌که نه وزارت اطلاعات ایران و نه سی‌آی‌ای آمریکا بفهمد که من از اینجا به آنجا چه فرستادم و چه گرفتم. این فرایند را وی‌پی‌ان یا فیلترشکن می‌گویند. کار فیلترشکن آن است که به این واسطه‌ها اجازه نمی‌دهد رفت‌وآمدها را کنترل کند؛ مثلاً من یک پاسبان وسط راه گذاشته‌ام و می‌گویم آقا ببین اگر فحشا می‌خواهد، به او نده؛ اگر فساد می‌خواهد، به او نده؛ مواد مخدر می‌خواهد، جلویش را بگیر. خب، نگهبان هم نگهبانی می‌دهد؛ اما این فیلترشکن می‌آید

یک تونل می‌زند و پاسبان هم هرچه به این تونل یا اطلاعات رمزشده نگاه می‌کند، چیزی نمی‌بیند که چه مطلب یا خدمتی از این طرف به آن طرف، ردّوبدل می‌شود. در حال حاضر، حاکمیت تصمیم دارد وی‌پی‌ان، باز باشد. منظور ما از حاکمیت در اینجا، نهادهای امنیتی و حاکمیتی مثل وزارت اطلاعات و اطلاعات سپاه است؛ یعنی مراجعی که الآن کار اطلاعات و امنیت مملکت دست آنهاست. این گروه با فیلترشکن کار دارند؛ یعنی مثلاً با یک خارجی می‌خواهند ارتباط بگیرند و نمی‌خواهند که دیگران بفهمند که ما به آن فرد چه چیزهایی گفته‌ایم و یا دقیقاً از کجا ارتباط گرفته شده است. در اینجاست که از تونلینگ استفاده می‌کنند. اگر شما تونل‌ها را جمع و منع کنید، این نوع ارتباطات بسته می‌شود؛ هم کار اطلاعاتی‌ها می‌خوابد و هم خیلی مشکلات دیگر پیش می‌آید؛ مثلاً کار بانک‌ها، سفارتخانه‌ها و بسیاری از کارهای دیگر مثل کارمندان دور از محل کار برای مبادله پیام‌های محرمانه که بر مبنای پروتکل وی‌پی‌ان است نیز تعطیل می‌گردد. پس، ما یک‌سری فعالیت‌هایی در فضای مجازی داریم که باید به صورت

شرکت‌های اینترنتی می‌توانند بفهمند که چه کسانی در چه زمانی به اینترنت وصل شده‌اند و حتی به دستور مرجع قضایی می‌توانند اطلاعات دیگری را نیز از هر یک از کاربران در اختیار مراجع قانونی قرار دهند که این آقا کجا رفته و با چه سایت‌هایی تماس داشته است

وی‌پی‌ان باشد و نمی‌توان آنها را آشکارا انجام داد.

مشکل اینجاست که به جای اینکه قضیه را حل کنیم و راهکاری برایش تعریف نماییم تا این امور در چارچوب خود قرار گیرد، گفته‌ایم فضای مجازی را بی‌دروپیکر باز بگذارید و تونلینگ و فیلترشکن را هم هرکس خواست، می‌تواند استفاده کند. این مسئله، مثل قصهٔ ماهواره است. یکی به ما گفت: آقا می‌دانید چرا ماهواره در مملکت جمع نشده است؟ گفتم: چرا؟ گفت: چون رؤسای اجرایی مملکت همه از ماهواره استفاده می‌کنند. اگر بخواهی ماهواره را جمع کنی، اوّل باید با مسئولان برخورد کنی. هرکسی هم دلیل خودش را دارد؛ یکی می‌گوید من نماینده مجلس شورا هستم، آن می‌گوید من فرهنگی هستم، دیگری می‌گوید من فلان مسئولیت را دارم و همه یک دلیلی دارند که دیش ماهواره را بالای ساختمان خود کار بگذارند. بدیهی است که اگر این طور بود، مردم هم نگاه می‌کنند و می‌گویند: اینها خودشان دارند از ماهواره استفاده می‌کنند، چرا ما استفاده نکنیم.

در زمان آقای اخوان، اوّلین دبیر شورای فضای مجازی، ما اجماع کوچک نخبگانی ایجاد کردیم که وی‌پی‌ان را مدیریت کنند؛ نه اینکه ببندند. آمدیم گفتیم یک سایت راه می‌اندازیم هرکس وی‌پی‌ان نیاز دارد، اسم خود و علت نیازش را بنویسد، آن وقت

یک عده‌ای که متخصص اطلاعاتی کشور هستند، باید بنشینند ببینند چطور می‌توانیم وی‌پی‌ان را مدیریت کنیم؛ به‌طوری‌که وی‌پی‌ان از دست یک بچه چهارده ساله خارج بشود؛ در عین حال، نیاز نهادها و سازمان‌ها نیز برطرف شود

آن مجموعه و مدیران سایت تصمیم بگیرند که این شخص از وی‌پی‌ان استفاده کند یا نکند. یک مدتی هم راه افتاد، اما دیدند اگر این کار ساماندهی بشود، یعنی اینکه ما بسیاری از امور خودمان را فاش سازیم. وقتی که هزاران نفر دیگر با هویت‌های متفاوت و مقاصد مختلف از این تونل استفاده می‌کنند، در این صورت، معلوم نمی‌شود که چه کسی این طرف است و چه کسی آن طرف.

یک عده‌ای که متخصص اطلاعاتی کشور هستند، باید بنشینند ببینند چطور می‌توانیم وی‌پی‌ان را مدیریت کنیم؛ به‌طوری‌که وی‌پی‌ان از دست یک بچه چهارده ساله خارج بشود؛ در عین حال، نیاز نهادها و سازمان‌هایی که به آنها اشاره شد، برطرف شود. در جلسه آخر این هفته شورای عالی فضای مجازی برخی گفتند: آقا اینها بازی را بستند، می‌دانید چه اتفاقی افتاد؟ بچه‌های چهارده‌ساله که این بازی را به صورت عادی باز می‌کردند، رفتند فیلترشکن روی کامپیوترشان نصب کردند تا بتوانند به بازیشان ادامه بدهند. فیلترشکن که نصب شد، غیر از بازی، ده‌ها سایت مزخرف و مستهجن دیگر هم در دسترس نوجوان چهارده‌ساله قرار گرفت. آقایانی که این بازی را بستید، برای چه بستید که جوان چهارده‌ساله ما ناخواسته به این سایت‌ها دسترسی پیدا کند؟

به نظر می‌رسد، جامعه نخبگانی کشور باید از نظام مطالبه کند که این وی‌پی‌ان را مدیریت کنید و این طور نباشد که هرکه خواست، بتواند از وی‌پی‌ان استفاده کند؛ به طور کلی، استفاده از وی‌پی‌ان باید تابع مقرراتی خاص باشد. البته وقتی از مدیریت می‌گوییم، فضایی به وجود می‌آید که یک عده‌ای در این فضا کاسبی می‌کنند. این کاسب‌ها هم گاهی داخل وزارتخانه‌های

خودمان هستند؛ یعنی آنها تازه می‌روند شروع می‌کنند به فروش وی‌پی‌ان؛ می‌گویند خیلی خب، وی‌پی‌ان را مدیریت می‌کنیم؛ یعنی می‌فروشیم و واگذار می‌کنیم. بعد هم یک مرتبه شروع می‌کنند به یک کاسبی تازه و گسترده. آن وقت خود این می‌شود یک معضل که همراهی نهادها را مشکل می‌سازد. این مدیریت، باید توسط کسی یا نهادی اعمال شود که اهمیت مسئله را به‌خوبی درک کند، مسائل اقتصادی این حوزه را بشناسد، مسائل امنیتی آن را بداند و از مسائل ارتباطی و اطلاعاتی آن هم آگاه باشد و در عین حال، برای خود کیسه نیندوخته باشد. فروش وی‌پی‌ان که الآن عمومی است، نباید دولتی شود تا مبادا خود خطر بزرگ دیگری شود.

راه‌حل دوم: مدیریت احراز هویت در شبکه

۱. احراز هویت از طریق سیمکارت یا سیم تلفن:

هرکسی می‌خواهد فعالیتی در شبکه انجام دهد، اوّل باید احراز هویت بشود. احراز هویت در شبکه، دارای سطوح متعددی است. اوّلین سطح آن، احراز هویت با سیمکارت یا خط تلفن است؛ یعنی هرکس سیمکارت یا خط تلفن می‌خواهد، اوّل باید از طریق مخابرات احراز هویت شود تا سیمکارت یا خط تلفن به نام او صادر شود؛ به عبارت دیگر، هویتش با نشانی و کد ملی‌اش مشخص شود. ما حدوداً دو میلیون سیمکارتِ بی‌نام داشتیم و معلوم نبود صاحبان آن چه کسانی هستند. این، یعنی ایجاد بستر جرم و فساد؛ چون یک سیمکارتِ بی‌نام، مثل یک شماره تلفنی که صاحبش معلوم نیست کیست، ممکن است ابزار جرم و تخلف و فساد قرار گیرد. مفسدان و مجرمان از این نوع سیمکارت‌ها یا شماره تلفن‌ها استقبال می‌کنند؛ چون هر عملی که با آن انجام دهند، قابل ردیابی نیست. اما اگر سیمکارت، صاحبِ مشخصی داشته باشد و فعلیِ مجرمانه با آن صورت گیرد، قابلیت ردیابی دارد؛ مثلاً فردِ اوّل می‌گوید فرد دومی به من پیامک زد و گفت فلانِ خدمت را به شما می‌دهم. وقتی سر قرار حاضر شدم، مرا اغفال کرد و مرتکب جرم شد. اگر سیمکارتی که پیامک فرستاده بی‌نام باشد، قابل ردیابی پلیس و دستگاه قضایی نیست. این، سطح اوّل امنیت است که هرکسی مسئولیت ارتباطات و رفتارهایی را که به وسیله سیمکارت خودش صورت می‌گیرد، بپذیرد.

۲. احراز هویت از طریق دستگاه سخت‌افزاری مثل تلفن همراه:

سطح دوم احراز هویت، با مشخصات تلفن همراه است. یعنی فردی که سیمکارت خریده، ممکن است آن را در دستگاه‌های مختلف قرار دهد. هر دستگاهی برای خودش شناسه دارد که در شبکه قابلیت ردیابی دارد. باید جلوی قاچاق تلفن همراه و دستگاه‌هایی که قابلیت اتصال به شبکه (فضای مجازی) را دارند، گرفته شود. هر دستگاه باید به فرد خاصی با مشخصات معیّنی استناد یابد. این، می‌شود سطح دوم امنیت ارتباطات. این دستگاه نیز باید از محلی خریداری شده باشد که مجوز فروش این نوع تلفن همراه یا تبلت را داشته باشد.

به عنوان مثال، وقتی با کسی تماس می‌گیرم، از دو جهت شناخته

به نظر می‌رسد، جامعه نخبگانی کشور باید از نظام مطالبه کند که این وی‌پی‌ان را مدیریت کنید و این طور نباشد که هرکه خواست، بتواند از وی‌پی‌ان استفاده کند؛ به طور کلی، استفاده از وی‌پی‌ان باید تابع مقرراتی خاص باشد

می‌شوم: یکی اینکه تلفن همراه مال من بوده و دیگر اینکه سیمکارت هم به نام من بوده است. حالا اگر این گوشی را کسی از من دزدید و از آن استفاده کرد، قبل از هر چیز، باید بروم پاسگاه و بگویم آقا بیست‌وچهار ساعت است که تلفن همراه من گم شده است؛ مثل ماشین می‌ماند؛ اگر ماشین شما را بدزدند و نروی کلانتری بگویی که ماشین من را دزدیده‌اند، هر جرمی که با آن ماشین مرتکب بشوند، اوّل می‌آیند گریبان شما را می‌گیرند. می‌گویند آقا این ماشین سندش به نام شما خورده، شما با این وسیله، آدم کشتی. می‌گویی: نه آقا من نکشتم؛ دیروز دزدیده بودند و من هم رفتم کلانتری گفتم دزدیده‌اند. به هر حال، احراز هویت در سطح سیمکارت و سخت‌افزار گوشی، در شمار گام‌های اوّل و دوم مدیریت فضای مجازی است.

۳. احراز هویت، از طریق بهره‌برداری از شبکه و اینترنت:

سطح سوم احراز هویت، از طریق اتصال به شبکه و اینترنت است.

اگر کسی سیمکارت خرید و در تلفن همراه مشخصی قرار داد و آن دو را هم به نام خود ثبت کرد، هنوز نمی‌تواند به اینترنت یا شبکه‌های داخلی سازمان‌های مختلف وصل شود. به محض اینکه بخواهد وصل شود، از او می‌پرسند شما چه کسی هستی که می‌خواهی به اینترنت وصل شوی. آیا مجوز داری؟ باید بگوید بنده همان شخصی هستم که فلان مجوز اتصال به اینترنت را از شرکت شما خریدم. بنابراین، باید شناسه کاربری و رمز عبور خود را به شرکت مربوطه بدهم تا او بنده را به اینترنت وصل کند. هر بار که قصد اتصال دارم، این شناسه کاربری و رمز عبور من تصدیق می‌شود و بعد بنده در خانه به اینترنت وصل می‌شوم و آن شرکت هم مطابق مصرف من از اعتبار مالی‌ام کم می‌کند و اگر اعتبارم تمام شود، اینترنتم را قطع می‌کند تا مجدداً واریز انجام گیرد. این، می‌شود احراز هویت سوم.

توضیح اینکه همین الآن در دنیا، هرکه فعالیتی در فضای فیزیکی می‌کند که از نظر حاکمیتی اهمیت دارد، به آن می‌گوید: مجوزت کجاست؟ یعنی ما برای هر نوع رفتار ساختاری در نظام اجتماعی، باید مجوز داشته باشیم. می‌گویند: آقا بقالی می‌خواهد راه بیندازد، باید مجوز داشته باشد؛ دکه می‌خواهد بزند، می‌گویند که چه کسی به شما اجازه داده اینجا دکه بزنی؟ روزنامه می‌خواهد نشر بدهد، می‌گویند چه کسی به شما اجازه داده؟ کتاب و جزوه می‌خواهد چاپ کند، می‌گویند چه کسی به شما اجازه نشر داده؟ پس، ما باید در مملکت یک ساختاری داشته باشیم که برای رفتارهای سازمان‌یافته اجتماعی، اعطای مجوز کنیم که الحمدلله داریم و افراد هم برای اینکه آن کار شخصی، سازمانی یا نهادی را انجام دهند، باید بروند مجوزش را بگیرند و تا نگیرند، اجازه ندارند این کار را بکنند. این موضوع، تا حدودی در کشور هست؛ یعنی شرکت‌هایی که اعطای مجوز دسترسی به اینترنت می‌دهند یا به تعبیر عامه اینترنت می‌فروشند، خودشان از وزارت ارتباطات مجوز این کار را گرفته‌اند و باید طبق قانون، اطلاعات کاربرانی را که اینترنت خریداری کرده‌اند و به شبکه وصل می‌شوند، تا مدتی نگهداری کنند تا اگر لازم شد به دستور قاضی برای کشف جرم آن اطلاعات را در اختیار مراجع قانونی قرار دهند. پس، شرکت‌های اینترنتی می‌توانند بفهمند که چه کسانی در چه زمانی به اینترنت وصل شده‌اند و حتی به دستور مرجع قضایی می‌توانند اطلاعات دیگری را نیز از هریک از کاربران در اختیار مراجع قانونی قرار دهند که این آقا کجا رفته و با چه سایت‌هایی تماس داشته است.

یک سطح دیگری از احراز هویت داریم به معنای احراز هویت در سطح دریافت خدمت؛ یعنی هر وقت بخواهیم خدمتی را دریافت کنیم، این خدمت‌دهنده می‌گوید: من مستقل از ذی‌نفعان دیگر در شبکه، باید اوّل شما را احراز هویت کنم و بعد به شما مجوز عرضه خدمت بدهم

٤. احراز هویت برای دریافت خدمت:

حال فرض کنید شما به اینترنت وصل هستید و دارید از خدمات مختلفی استفاده می‌کنید؛ مثلاً می‌گویید در فضای مجازی من رفتم در سایت قوه قضائیه ابلاغم را گرفتم و رفتم در سایت بانک پول واریز کردم و بعد رفتم فلان کار را انجام دادم. هرکدام از این کارها، اگر دارای اهمیت باشد، از شما احراز هویت مضاعف

می‌خواهد. این نوع، احراز هویت دریافت خدمت نامیده می‌شود؛ یعنی مثلاً برای گرفتن خدمت بانکی از سرویس‌دهنده اینترنت شاتل، او به شما می‌گوید: بله، الآن به شبکه اینترنت وصل شدی و من فهمیدم شما حمید شهریاری هستی؛ اما بانک که نفهمیده شما کیستی. اگر می‌خواهی از حساب خودت پول برداری و بریزی به حساب فلان آقا، باید احراز هویت بشوی. آن سیستم بانکی می‌گوید: من تا نفهمیدم شما حمید شهریاری هستی، این کار را نمی‌کنم. پس، ما یک سطح دیگری از احراز هویت داریم به معنای احراز هویت در سطح دریافت خدمت؛ یعنی هر وقت بخواهیم یک خدمتی را دریافت کنیم، این خدمت‌دهنده می‌گوید: من مستقل از ذی‌نفعان دیگر در شبکه، باید اوّل شما را احراز هویت کنم و بعد به شما مجوز عرضه خدمت بدهم.

درهرحال، یک عده آدم‌های بسیار حرفه‌ای هستند که بلدند قفل‌ها را بشکنند و رمزها را کشف کنند؛ مثل سارقان خودرو که در زمانی بسیار کوتاه درِ ماشین را بازمی‌کنند و ماشین را می‌برند. مشابه صحنه فیزیکی، در صحنه دیجیتال و فضای مجازی نیز عده‌ای هستند که واقعاً حرفه‌ای هستند. آیا دیگر کشورها این موضوع را به حال خود رها کرده‌اند؟ نخیر، رها نکرده‌اند؛ بلکه برای این مشکل هم راه‌حل دارند

برای احراز هویت در ارائه خدمت، دو راه وجود دارد:

الف. احراز هویت از طریق اوتی‌پی (OTP - One Time Password): به این روش می‌گویند رمز یک‌بار مصرف؛ یعنی دستگاه‌هایی هست که برخی بانک‌ها مثل بانک ملی دارند. وقتی با شبکه به بانک متصل می‌شوید، به شما می‌گوید: کد شما چیست؟ می‌گویید: کد من، این است. می‌گوید: خیلی خب، من یک شماره یا رمز یک‌بار مصرف را برای شما تولید می‌کنم و روی تلفن همراهت می‌فرستم. سپس، چند ثانیه منتظر می‌مانید و یک شماره پنج رقمی برایتان ارسال می‌شود. شما آن را دریافت کرده، برای بانک ارسال می‌کنید. سیستم بانک به شما می‌گوید: من الآن هویت شما را احراز کردم. آنگاه اجازه دسترسی به سرویس بانک و دریافت خدمت مورد نظرتان را می‌دهد.

ما الآن این سیستم را در قوه قضائیه راه اندخته‌ایم. به این ترتیب که اوّل خود شخص به صورت حضوری برای شناسایی و مطابقت چهره با کارت ملی و اسناد هویتی در دفاتر خدمات الکترونیک قضایی حاضر می‌شود. سپس، با دریافت شماره تلفن همراهش و تأیید آن، به او می‌گوییم: دیگر از این به بعد ما از طریق تلفن همراه و شبکه مکانیزه قوه قضاییه، شما را شناسایی می‌کنیم. از این پس، این آقا برای گرفتن خدمت از قوه قضاییه، از طریق تلفن همراهش وصل می‌شود و می‌گوید: آقا من می‌خواهم ابلاغم را ببینم. می‌گوییم: شما حمید شهریاری هستی. رمزی که به شما داده‌ایم را وارد کن. وقتی رمزش را وارد نمود، می‌گوییم: الآن روی تلفن همراهت یک عدد پنج رقمی می‌فرستم. چند ثانیه منتظر می‌ماند. سپس، آن پنج رقم را دریافت کرده، برای سیستم می‌فرستد. آنگاه وی با ارسال آن ارقام به سامانه، احراز هویت

آنچه ما مطرح می‌کنیم، راه‌حلّ ملی است که هم هزینه دارد و هم عزم ملی را می‌طلبد. برای مدیریت فناوری در کشور برای سال گذشته، منابع مالی کافی تزریق نشده است و با کمبودهای شدیدی مواجه بودیم. اگر این پول تزریق می‌شد، هر مدیری می‌توانست یکی دو پروژه در همین زمینه به دست گرفته و انجام دهد؛ اما چون پول نبود، خود وزارت ارتباطات هم کاری از پیش نبرد

می‌شود و به او امکان دسترسی داده می‌شود. توجه داشته باشید، اگر حتی دیگری فهمیده باشد رمز شما در شبکه قوه قضاییه چیست، چون رمز یک‌بار مصرف امنیتی دیگری به تلفن همراه شما ارسال می‌شود و گوشی شما دست او نیست، آن پنج رقم به دست وی نمی‌رسد و او نمی‌تواند به اسم شما وارد سیستم شود و به اطلاعاتتان دسترسی پیدا کند. اگر کسی هم با رمز شما بخواهد در سامانه قوه قضاییه اطلاعات قضایی شما را ببیند، این سامانه به تلفن همراهتان هشدار می‌دهد که شما درخواست رمز یک‌بار مصرف کرده‌اید و شما متوجه می‌شوید و می‌گویید: این کیست؟ چه کسی بوده که یک چنین چیزی از طرف من درخواست کرده؟ بنابراین، می‌توان فوری قضیه را پیگیری کرد.

این اوتی‌پی که شرح دادم، الآن در قوه قضاییه راه افتاده است و حدود شش ماه وقت صرف آن شد تا اینکه با آیین‌نامه‌ای در قوه قضاییه عملیاتی شد. می‌دانید در قوه قضاییه تا شرح یک عملیات را بنویسید و آیین‌نامه اجرایی برای آن تنظیم کنید و آن هم مورد قبول نخبگان قوه قضاییه قرار گیرد، خیلی زحمت دارد.

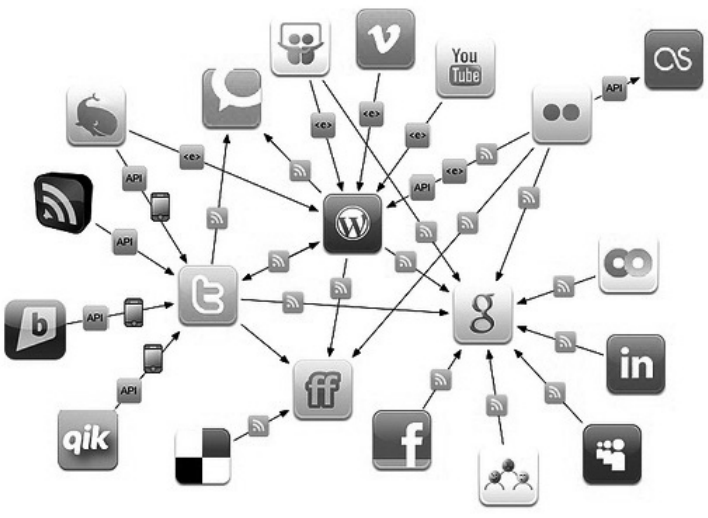
ب. احراز هویت از طریق توکن (Security Token): بانک ملی، از این روش استفاده می‌کند؛ یعنی یک دستگاهی سخت‌افزاری هست به اندازه نیمی از کف دست که به آن «توکن» گویند که رمز شش رقمی تولید می‌کند. هر بار که می‌خواهید به سامانه بانک ملی وصل شوید، باید رمز شخصی محفوظ خود را به توکن بدهید تا توکن برای شما یک رمز شش رقمی تولید کند و چون این ارقام از قبل در سامانه دسترسی بانک برای شما تعریف شده و در سِرور مرکزی خدمات بانک قرار گرفته است، با زدن این شش رقم در سامانه، می‌توانید خدمت خود را از طریق شبکه دریافت کنید؛ مثلاً صورت‌حساب خود را ببینید. این کار، برای دریافت اطلاعات از بانک است؛ اما اگر بخواهید علاوه بر اطلاعات، مبادله‌ای انجام دهید، مثلاً پولی از حساب خود به دیگری واریز کنید، راه سخت‌تری قرار داده شده. اوّل با رمز محفوظتان توکن را روشن می‌کنید. بعد از سامانه درخواست انتقال پول به حساب

دیگری می‌کنید و اطلاعات آن دیگری را وارد می‌کنید. سپس، سامانه به شما سه عدد پنج رقمی می‌دهد که باید به نوبت آن را به توکن خود وارد کنید. بعد توکن به شما یک عدد شش رقمی می‌دهد که باید در سامانه وارد کنید و با این کار، پول از حساب شما به حساب دیگری منتقل می‌شود.

در حال حاضر، هر سازمان و بنگاه و شرکتی برای خودش راه مستقلی برای احراز هویت دارد که اشکالی هم ندارد؛ ولی بنده در دانمارک دیدم که برای احراز هویت دریافت خدمات دولتی و حاکمیتی، تنها یک سایت وجود داشت که همه سازمان‌ها و بنگاه‌ها و شرکت‌های دولتی، از طریق آن احراز هویت می‌شدند. ما این بستر را در قوه قضاییه با سامانه ثنا مهیا کرده‌ایم که باید در جای خودش توضیح داده شود. سامانه ثنا می‌تواند درگاهی برای احراز هویت همه خدمات حاکمیتی باشد؛ ولی فعلاً فقط برای قوه قضاییه این کار را انجام می‌دهد.

۵. احراز هویت از طریق کارت هوشمند ملی:

کارت‌های هوشمند این امکان را دارند که اطلاعاتی را درون خود ذخیره کنند تا در مواقع لزوم، سیستم اطلاعات واردشده را با اطلاعات ذخیره‌شده در کارت تطبیق دهد و سپس، خدمت مورد نظر عرضه گردد؛ مثلاً الآن درون آن، اثر انگشت سبابه افراد نهاده شده است. اگر کسی بخواهد با کارت هوشمند دیگری در سامانه بانک وارد شود و خدمتی بگیرد، بانک می‌تواند درخواست کند که انگشت خود را روی اثرانگشت‌خوان دستگاه قرار دهد یا بکشد؛ آنگاه اگر تطبیق صورت گرفت، بانک از پشت شبکه می‌فهمد که این آقا چه کسی است؛ یعنی احراز هویت می‌شود. در حال حاضر، درون کارت هوشمند ملی، یک قطعه الکترونیکی می‌گذارند که ان‌شاءالله در آینده حتی تصویر قرنیه چشم یا هر اطلاعات دیگر از کاربر را درون آن قرار دهند. این کارت‌ها یک حافظه دارد و مثل فلش، اطلاعات هویتی شما در آن دخیره می‌شود. آن کارت هوشمند، به جای کارت ملی کنونی می‌آید.



ما می‌توانیم بسیاری از خدمات تحت شبکه را به احراز هویت منوط کنیم؛ مثلاً بگوییم کسانی می‌توانند به فلان شبکه اجتماعی وصل شوند که به یکی از روش‌های فوق احراز هویت شده باشند. مجرمی که می‌داند احراز هویت شده است، رفتار تحت شبکه خود را مدیریت می‌کند و این کار، نوعی پیشگیری از وقوع جرم است

خلاصه آنکه ما می‌توانیم بسیاری از خدمات تحت شبکه را به احراز هویت منوط کنیم؛ مثلاً بگوییم کسانی می‌توانند به فلان شبکه اجتماعی وصل شوند که به یکی از روش‌های فوق احراز هویت شده باشند. مجرمی که می‌داند احراز هویت شده است، رفتار تحت شبکه خود را مدیریت می‌کند و این کار، نوعی پیشگیری از وقوع جرم است. می‌توانیم بگوییم کسانی می‌توانند از فیلترشکن استفاده کنند که به یکی از راه‌های فوق، احراز هویت شده باشند. در این حال، می‌توان سامانه‌ای طراحی کرد که در صورت لزوم، رفتارهای اشخاص کاملاً مدیریت شود و در صورت نیاز و با دستور قاضی نیز ردیابی گردد.

باید این کارها را در کنار هم انجام دهیم تا تهدیدها در فضای مجازی به حداقل میزان کاهش یابد. تهدیدها مطلقاً رفع نمی‌شود؛ ولی به حداقل کاهش پیدا می‌کند؛ مثل مرزی که الآن ما داریم؛ بالأخره یکی می‌آید ضربه می‌زند و می‌گریزد. الآن مرز واقعی کشور، دست ماست؛ ولی مرز مجازی، دست ما نیست. اگر آنچه در این نوشته می‌آید، تحقق یابد، مرز مجازی هم به دست ما می‌افتد و می‌توانیم فضای مجازی را مدیریت کنیم.

درهرحال، یک عده آدم‌های بسیار حرفه‌ای هستند که بلدند قفل‌ها را بشکنند و رمزها را کشف کنند؛ مثل سارقان خودرو که در زمانی بسیار کوتاه درِ ماشین را بازمی‌کنند و ماشین را می‌برند. مشابه صحنه فیزیکی، در صحنه دیجیتال و فضای مجازی نیز عده‌ای هستند که واقعاً حرفه‌ای هستند. آیا دیگر کشورها این موضوع را به حال خود رها کرده‌اند؟ نخیر، رها نکرده‌اند؛ بلکه برای این مشکل هم راه‌حل دارند که در ادامه، توضیح می‌دهم.

راه‌حلّ سوم: استفاده از دانش فرانزیک

برای این مورد هم باید مقدمه‌ای عرض کنم. یک ماه پیش، چین بودم. بریکس (BRICS) یک انجمن از کشورهای خاور دور هستند. برخی کشورها از جمله ایران در اجلاسی که از سوی

این انجمن برگزار شده بود، به عنوان میهمان دعوت شده بودند؛ دادستان‌های این کشورها جمع بودند و ما هم همراه دادستان محترم رفته بودیم. آقای دادستان به من گفت: شما هم همراه بنده بیا برویم چین، ببینیم راه‌حلّ مشکلات فضای مجازی چیست؟ ما هم در چین از طریق سفارت با دو سه تا شرکت که در مورد این کاری که الآن می‌خواهم توضیح بدهم، مسئولیتی روی دوششان بود، تماس گرفتیم. یکی از شرکت‌ها کارهای بسیار عالی کرده بود. کارهایشان را پرزنت کردند. کسی همراهم نبود. آنها هم می‌دانستند من از ناحیه دولت و حاکمیت ایران هستم. آنها کاسب این حوزه بودند؛ یعنی کسانی بودند که برای دولت چین این کار را راه‌اندازی نموده بودند و این شرکت، اوّلین اپراتور نسل چهارم تلفن همراه در چین بود. آن شرکت فکر کرد من از طرف دولت ایران آمده‌ام قرارداد ببندم و این محصول را از آنها بخرم؛ به همین جهت، هر توانایی در فضای مجازی داشتند، نشان دادند. آخرش به آنها گفتم: آقا می‌شود یک نسخه از این را به ما ارائه بدهید؟ گفتند: نه، آقا این کسب‌وکار ماست. نمی‌توانیم آن را در اختیار شما قرار بدهیم. فقط برای شما نشان دادیم که اگر می‌خواهید، آن را بخرید.

خب، حالا محصولشان چه بود؟ یک اصطلاحی هست به نام فرانزیک، به معنای بررسی ادله و شواهد محکمه‌ای؛ یعنی شواهد و مدارکی را که در محکمه مورد تأیید است، مورد بررسی و تأیید قرار می‌دهد. این فرانزیک، یک دانش است؛ مثلاً شخصی می‌گوید: آقا من یک سند دارم که این آقا این مِلک را به من فروخته است. بعد محکمه می‌آید آن را بررسی می‌کند. این بررسی، یک دانش است. شما باید دانشی داشته باشید تا بتوانید مستندات را تأیید یا رد کنید. یا مثلاً گفته می‌شود این، خونی که در صحنه جرم ریخته شد، برای آقای فلانی است. شما باید با دانش مربوطه بتوانید آن را تأیید یا رد کنید. این، یک دانش آکادمیک است که با آن می‌شود شاهدی برای محکمه یافت. امروزه، بررسی، مطالعه و کشف شواهدی که برای محکمه‌هایی که به جرایم در فضای مجازی رسیدگی می‌کنند و می‌تواند مستند واقع شود، تبدیل به یک دانش شده است. اگر کسی در فضای مجازی مرتکب جرمی بشود، با استفاده از ابزارهایی که ترکیبی از نرم‌افزار، سخت‌افزار، شبکه و دانش علوم اجتماعی و پلیسی است، پی‌گیری و مستندسازی می‌گردد. این چند دانش که جمع شود، روی هم دانش فرانزیک را در حوزه فضای مجازی تأسیس می‌کند. کارکرد این دانش، این‌گونه است که وقتی در فضای مجازی جرمی رخ می‌دهد، به جای اینکه همه مردم را بگیرند و تلفن همراه‌هایشان را چک کنند، به یک‌سری علائم در این شبکه نگاه می‌کنند و آنها را در فضای مجازی پی‌گیری و رصد

می‌کنند و مجرم یا مجرمان اصلی را می‌یابند؛ یعنی از طریق این دانش می‌روند و یک مرتبه می‌رسند به ده نفر که در بروز جرم، نقش اصلی را داشتند و یا می‌گویند یکی از این ده نفر، از کسانی هستند که فلان سایت مستهجن را نیز راه انداخته‌اند. حالا چگونه این دانش سرنخ‌ها را بررسی و مطالعه و مجرم را کشف می‌کند، چینی‌ها حدود دو ساعت توضیح دادند که الآن قصد ورود به این حوزه دانشی را ندارم؛ ولی یک دانشی در این زمینه وجود دارد که بخش‌هایی از آن را هم‌اکنون پلیس فتا در اختیار دارد.

بنده فقط یکی دو تا مثال در فضای عینی می‌زنم که در عرصه دیجیتالش هم وجود دارد. یک آقایی که دارد زندگی‌اش را می‌کند، یک مرتبه به مشهد و از آنجا به سرخس می‌رود. نهادهای نظارتی می‌گویند اینها که می‌روند سرخس، چه کار دارند؟ آقایی که کار و زندگی‌اش و کسب‌وکارش در تهران است، با سرخس چه نسبتی دارد؟ از میان این همه شهر، چرا به سرخس رفته است؟ می‌گویند خب، حالا شاید رفته کاری داشته است. پلیس‌ها که رصد می‌کنند، یک فهرست زرد درست می‌کنند و می‌گویند اینها آدم‌هایی هستند که غیر از روال‌های عادی زندگی که داشتند، یک مرتبه بلند شدند و به مرز سرخس رفته‌اند و بعد هم با تلفن به چند نفر زنگ زده‌اند. پس، این شخص را بگذار در فهرست معیّنی؛ همه این کارها را با اطلاعات و رایانه‌های خاصی انجام می‌دهند. بعد می‌بینند هم‌زمان یک آدمی که قبلاً به دلیل مواد مخدر مجرم بوده و به پنج سال زندان محکوم شده، این آقا هم به سرخس رفته و در هتل ابریشم اقامت گزیده است و در همین ایامی که آن آقا از تهران به آنجا رفته بود، اتفاقاً ایشان هم در دو شب از اقامتش در همان هتل بوده است. می‌گویند این، یک علامت است. این می‌رود در فهرست صورتی. آنها را هم که با آن شخص در یک هتل بوده‌اند، زیر

هر نوع خدمتی که در فضای مجازی صورت می‌گیرد، باید بومی‌سازی شود؛ یعنی از ابزارهای خارجی استفاده نکنیم؛ این مسئله، شامل مواردی همچون: موتور جست‌وجو، پست الکترونیکی، شبکه اجتماعی و نرم‌افزارهای زیرساختی بانکداری الکترونیک، انواع نرم‌افزارهای سیستمی و کاربردی می‌شود

ذره‌بین می‌گذارند و همه تماس‌های او را کنترل می‌کنند. آرام‌آرام قضیه را رصد می‌کنند تا اینکه یک مرتبه مچ مجرم اصلی را می‌گیرند و می‌گویند شما همان بودی که رفتی در بندرعباس یک خانه فساد درست نمودی و فیلم هم گرفتی و در اینترنت منتشر کردی. این کاری است که از دانش فرانزیک برمی‌آید و بیشتر ادواتش، مبتنی بر محاسبات رایانشی و رصد میدانی است.

امروزه، در دنیا فقط مجرم را می‌گیرند؛ نه اینکه همه چیز را مسدود کنند و همه را بگیرند. ما اگر دانش به‌روز و لازم را نداشته باشیم و سرمایه‌گذاری در این زمینه نکنیم، فتنه هشتادوهشت که بشود، در خیابان جمهوری یا هفت تیر، افراد مفسد به هم پیامک می‌زنند و یک جا جمع می‌شوند اگر دانش لازم را نداشته باشیم، سرشاخه‌ها و سرنخ‌ها را کشف نمی‌کنیم. چه کار می‌کنیم؟ می‌گوییم همه پیامک‌ها را تا فردا ببندید و همه را کلاً می‌بندیم. دانش امروز می‌گوید این کار، درست نیست. شما حاکم خوبی نیستی. حاکم خوب، آن است که به مردم عادی و درستکارش خدمت بدهد و افراد بزهکار و بدکارش را محروم کند. شما باید پیامک کسانی را ببندید که از قبل شناسایی کردید و می‌دانید اینها فتنه‌گرند و ممکن است از آن طرف مرزهای کردستان و سیستان و بلوچستان و یا از جاهای دیگر به تهران بیایند تا شرّ

فردا ممکن است آمریکا هوس کند ما را در اینترنت تحریم کند. ما باید زیرساخت خودمان را داشته باشیم؛ یعنی شهروند ما از حاکمیت توقع دارد که از خانه‌اش کار بانکی انجام دهد. بعد اگر نتوانست، به حاکمیت اعتراض می‌کند که چرا این کار ممکن نیست. ما می‌گوییم: ببخشید آمریکا ما را تحریم کرده است. آن وقت مردم ما می‌گویند: شما توانایی نداشتید کاری کنید که اگر تحریم شدیم، بتوانیم نیاز خودمان را برطرف کنیم و وابسته نباشیم. اینجا کارکرد شبکه ملی اطلاعات روشن می‌شود

درست کنند. شما اینها را ردیابی کنید و ده روز تلفن همراهشان را ببندید یا مدیریت کنید.

بنده مدتی که در خارج کشور بودم، شاهد بودم که پلیس در آنجا راهکاری برای کنترل برخی هیجانات اجتماعی دارد؛ مثلاً بعضی از این آدم‌هایشان که در اجتماعات عمومی خیلی شرّ درست می‌کنند، پلیس به اینها می‌گوید آقای فلانی، من شما را شناسایی کرده‌ام. بازی فوتبال امروز که در فلان شهر انجام می‌شود، یکی دو ساعت قبل از بازی می‌آیید کلانتری، اینجا کنار بنده در این اتاق می‌نشینید. دو ساعت بعد از بازی هم بلند می‌شوید و می‌روید؛ یعنی حاکمیت در آنجا می‌آید برای اینکه آن رفتارهای خشن را مدیریت کند، به جای اینکه بگوید آقا هیچ‌کس نباید برود استادیوم، می‌آید آن آدم شرور را پیدا می‌کند و می‌گوید من شما را مدیریت می‌کنم. هر از چندی هم فهرست افراد شرور را بر اساس آن دانشی که در فهرست مجرمانه دارد، به‌روز می‌کند. حاکمیت باید بتواند با اعمال فرانزیک، مجرم را بگیرد؛ نه اینکه درِ دکان همه را ببندد.

عده‌ای در قوه قضاییه به ما گزارش دادند آیا خبر دارید اصل مواد مخدر از مرز رسمی وارد می‌شود و قاچاق نیست؟ گفتیم حالا چگونه جلوی آن را بگیریم؟ گفت بروید یک دستگاه از این اسکنرهای کامیونی بخرید و در اختیار ما قرار دهید تا ما با آن، بار کامیون‌ها و کانتینرها را به‌راحتی ببینیم؛ زیرا ما که نمی‌رسیم در روز بار هزار کامیون را کنترل کنیم. تازه اگر هم برسیم، بعضی در کار قاچاق خیلی حرفه‌ای هستند و وسایل خود را جایی مخفی می‌کنند که ما ابزارش را نداریم تا بتوانیم آنها را شناسایی کنیم. وقتی خطّ گمرک ما به دستگاه اسکنر مجهز باشد، کامیون‌ها بدون معطلی و بازرسی دستی و سنّتی، از آنجا گذر می‌کنند. یک اسکنر گذاشتند و وقتی شما رد می‌شوی، می‌فهمند که در بار شما چه چیزهایی وجود دارد؛ اگر قاچاق بود، مأموران دستش نمی‌زنند، می‌گذارند برود تا با رصد و پیگیری و تعقیب آن، چهار تا آدم مجرم دیگر را هم که در بیرون گمرک منتظر هستند، شناسایی کنند و به سرنخ اصلی برسند و او را بگیرند.

برخی، از سخنان ما چنین برداشت نکنند که ما با فیلترینگ مخالفم؛ بلکه معتقدیم باید فضای مجازی را مدیریت کرد. بنابراین، فرانزیک را چنین تعریف می‌کنیم: کشف موارد تخلف با استفاده از فناوری، به اضافه اشراف اطلاعاتی نهادهایی چون: وزارت اطلاعات، نیروی انتظامی، اطلاعات سپاه و قوه قضاییه که اگر این دو، یعنی به‌کارگیری فناوری به همراه کار اطلاعاتی با هم ترکیب شود، همان فرانزیک خواهد شد. روی این دو مورد، یعنی کشف موارد تخلف با استفاده از فناوری و اشراف اطلاعاتی، باید سرمایه‌گذاری شود.

آن شرکت چینی حاضر بود بیاید و کار کند؛ می‌گفت سیستم ما با آدم‌هایی که از خارج از چین وارد می‌شود، کار دارد؛ او را رصد می‌کنیم تا بیاید تمام تماس‌ها و ارتباط‌هایش را برقرار کند. آنگاه سرنخ‌ها را کشف کرده، بعد اقدام می‌کنیم. این کار، با روش‌های سنّتی اصلاً ممکن نیست و فقط به کمک فناوری و روش‌های الکترونیکی امکان‌پذیر است. این ابزار، در دنیا تهیه شده و در چین نمونه آن وجود دارد. به‌تازگی، شنیدم یکی از این شرکت‌ها به ایران آمده است.

راه‌حلّ چهارم: ترویج خدمات الکترونیکی بومی

هر نوع خدمتی که در فضای مجازی صورت می‌گیرد، باید بومی‌سازی شود؛ یعنی از ابزارهای خارجی استفاده نکنیم؛

این مسئله، شامل مواردی همچون: موتور جست‌وجو، پست الکترونیکی، شبکه اجتماعی و نرم‌افزارهای زیرساختی بانکداری الکترونیک، انواع نرم‌افزارهای سیستمی و کاربردی، حتی در رایانه‌های خانگی هست؛ مثل خود این سیستم کامپیوتر که روبه‌روی ماست و بعضاً نمی‌دانیم داخلش چیست؟ ما ایرانی‌ها یک برند سخت‌افزاری را می‌خریم؛ درحالی‌که نمی‌دانیم داخل آن چیست؟ بعد یک سیستم عامل دارد که کارکردهای آن نیز برای ما معلوم نیست. گاهی اوقات می‌بینیم کامپیوتر که به شبکه اینترنت متصل است، خودبه‌خود مشغول کارکردن است؛ یعنی بدون اینکه من بخواهم، مشغول دادوستد اطلاعات است. نمی‌دانیم چه چیزی دارد می‌گیرد و چه کار می‌کند. واقعیتش این است که وقتی به اینترنت وصل می‌شویم، معلوم نیست ویندوز با دستگاه و اطلاعات من و شما چه کار می‌کند. یک ابهام هم در اپلیکیشن‌ها و برنامه‌های کاربردی روی سیستم‌هاست که روشن نیست پشت پرده آنها چیست؟

برای ترویج خدمات الکترونیکی بومی، به پنج مورد به عنوان نمونه و شاخص که تا حدودی در آن ورود کرده‌ایم، اشاره می‌کنم:

۱. تأسیس شبکه ملی اطلاعات، به جای شبکه اینترنت؛ یعنی زیرساخت‌های خودمان را از اینترنت جدا کنیم. فردا ممکن است آمریکا هوس کند ما را در اینترنت تحریم کند. ما باید زیرساخت خودمان را داشته باشیم؛ یعنی شهروند ما از حاکمیت توقع دارد که از خانه‌اش کار بانکی انجام دهد. بعد اگر نتوانست، به حاکمیت اعتراض می‌کند که چرا این کار ممکن نیست. ما می‌گوییم ببخشید آمریکا ما را تحریم کرده است. آن وقت مردم ما می‌گویند شما توانایی نداشتید کاری کنید که اگر تحریم شدیم، بتوانیم نیاز خودمان را برطرف کنیم و وابسته نباشیم. اینجا کارکرد شبکه ملی اطلاعات روشن می‌شود. البته شبکه ملی اطلاعات، مثل سیم تلفن است. بیش از این نیست؛ بعضی خیلی بزرگش می‌کنند و اموری را درونش اضافه می‌کنند که انجام آن سخت می‌شود و در نتیجه، آن را نشدنی تلقی می‌کنند که این فکر، غلط است.

۲. پست الکترونیک ملی، مانند چاپار؛ همه از چاپار تعریف می‌کنند که به جای جی‌میل آمده و امنیت ایمیل‌های سازمانی و شخصی ایرانیان را از دست خارجی‌ها تضمین کرده است.

۳. نرم‌افزار اشتراک عکس و تصویر و فیلم موسوم به یوتیوپ که بیشترین قطعات فیلم و تصویر که در اینترنت است و جوان‌ها با وی‌پی‌ان می‌بینند. در مقابلش تعدادی از جوانان ایرانی آمدند یک شبکه ایرانی درست کردند به نام آپارات که هم‌اکنون فعال است و محتوای آن را هم مدیریت می‌کنند. موارد بد و خلاف اخلاق

برخی، از سخنان ما چنین برداشت نکنند که ما با فیلترینگ مخالفیم؛ بلکه معتقدیم باید فضای مجازی را مدیریت کرد. بنابراین، فرانزیک را چنین تعریف می‌کنیم: کشف موارد تخلف با استفاده از فناوری، به اضافه اشراف اطلاعاتی نهادهایی چون: وزارت اطلاعات، نیروی انتظامی، اطلاعات سپاه و قوه قضاییه که اگر این دو، یعنی به‌کارگیری فناوری به همراه کار اطلاعاتی با هم ترکیب شود، همان فرانزیک خواهد شد

هم در آن نیست. به‌شدت هم کارش گرفته و مراجعات بسیاری دارد و جوان‌ها و خانواده‌ها استقبال می‌کنند. افراد ایرانی هم وقتی می‌خواهند فیلم یا تصویری ببینند و به یوتیوپ مراجعه نکنند، به آپارات مراجعه می‌کنند و می‌توانند فیلم و عکس مورد نظرشان را به‌راحتی پیدا کنند. این، یک پروژه موفق ملی در کشور بوده است که به جای یوتیوپ و اینستاگرام آمده است.

۴. موتور جست‌وجوی ملی پارسی‌جوی، یوز و غیر آن، به جای گوگل مطرح است که هنوز موفق نشدیم و سرمایه‌گذاری لازم در آن نکرده‌ایم. این کار، مثل درست کردن ناو هواپیمابر است. انجام آن، نسبتاً دشوار است؛ اما به اعتقاد من، شدنی است.

۵. نرم‌افزارهای پیام‌رسان بومی، مثل بیس‌فون و ساینا که می‌توانند به جای تلگرام و ویچت مطرح شوند. البته در حال حاضر، این نرم‌افزارها امکان پاسخگویی به بیش از یکی دو میلیون عضو را ندارند؛ درحالی‌که تلگرام ۲۰ میلیون کاربر دارد. باید زیرساخت‌های نرم‌افزاری آنها عوض شود. این کار هم مثل همان ناوهواپیمابر است که به سرمایه‌گذاری ملی نیاز دارد.

میانگین نیاز ما در انجام هر خدمت، مثلاً همین پنج خدمت که برشمردم، ده میلیارد تومان است که با چینش یک تیم پنج یا ده نفره از جوان‌های متخصص، در طول پنج سال می‌توان خروجی گرفت. هرکس تجربه و توان کار جمعی در مدیریت فناوری اطلاعات را داشته باشد، می‌تواند مدیریت کند و اگر پشتیبانی مالی کافی باشد، می‌تواند این طرح‌ها را عملیاتی نماید.

وقتی می‌گوییم می‌توانیم فناوری را بومی‌سازی کنیم، این یک کلمه است؛ اما پشت این ادعا، یک دنیا کار و هزینه و توانمندی

آخرین راه‌حلّ مدیریت فضای مجازی، مدیریت شبکه‌های خارجی است. در حال حاضر، شبکه‌های اجتماعی خارجی در کشور ما جولان می‌دهند. اگر یک اجماع نخبگانی شکل بگیرد، می‌توانیم با شبکه‌های خارجی، یک دادوستدهایی انجام دهیم

خوابیده که عملیاتی‌کردن آن، همت بلند می‌طلبد. متأسفانه، مملکت ما پانزده سال است در این زمینه کار و هزینه لازم را پیش‌بینی نکرده است. مدارک و نامه‌های آن نیز موجود است و الآن داریم چوب این کم‌کاری‌ها را می‌خوریم.

راه‌حلّ پنجم: مدیریت شبکه‌های خارجی

پنجمین و آخرین راه‌حلّ مدیریت فضای مجازی، مدیریت شبکه‌های خارجی است. در حال حاضر، شبکه‌های اجتماعی خارجی در کشور ما جولان می‌دهند. اگر یک اجماع نخبگانی شکل بگیرد، می‌توانیم با شبکه‌های خارجی، یک دادوستدهایی انجام دهیم؛ مثلاً در چین هر کاری کردم، به گوگل وصل نشدم. این نشان می‌دهد حاکمیت آنجا یک سازوکارهایی ترتیب

داده و گوگل کارهای خاصی را برای چین کرده است؛ چراکه اگر گوگل این کار را نمی‌کرد، چینی‌ها آن را می‌بستند؛ یعنی به گوگل گفته‌اند اگر شما این کار را نکنی، شما را می‌بندیم. خودشان هم دست به کار شدند و موتور جست‌وجوی خودشان را به نام «بایدو» ساختند. و چون دارای مزیتی‌های نسبی خط و زبان چینی بود، مورد استقبال شهروندان چینی قرار گرفت. گوگل زورش به کشورهایی مثل چین و روسیه نمی‌رسد؛ چون دست این کشورها خالی نیست و اگر اراده کنند، می‌توانند موتور جست‌وجوی لازم به همراه صدها سِرور و ابررایانه مورد نیاز خویش را برپا می‌کنند؛ اما این قدرت‌ها، هزینه – فایده‌ای عمل می‌کنند؛ گوگل هم چون زورش به آنها نمی‌رسد، مجبور می‌شود برخی از شرایط حاکمیتی آنان را بپذیرد؛ اما زورش به امثال ما می‌رسد؛ چون دست ما خالی است. او هم در کشور ما موتور جست‌وجوی خودش را همان جور که دلش می‌خواهد، به کار می‌اندازد. شبکه‌های اجتماعی خارجی هم بر همین وضع‌اند. البته الحمدلله ما یک مبادله خیلی کوچک با صاحبان تلگرام کرده‌ایم و با آنها قرار گذاشته‌ایم که اگر در تلگرام گزارش کردیم که یک کانال مستهجن است، فوری آن را می‌بندند؛ ولی اگر بگویی این کانال منافقان است یا مواد مخدر است، نمی‌بندند؛ یعنی چیزی که در کشور آنان و از نظر خودشان ممنوع نیست، نمی‌بندند. این، یک تفاهم خیلی کوچک است که اتفاق افتاده است و سرویس خیلی ناچیزی به ما می‌دهند. این، اوّلین باری است که ما با یک نهاد خارجی در فضای مجازی به تفاهم رسیدیم و به نظر من، توفیق دوستان در وزارت ارتباطات بوده است که مقدمه‌ای است برای گام‌های بعدی.

مطلب دیگر، انتقال سِرورها به داخل کشور، نیازمند سرمایه بسیاری است. همچنین، بستن و فیلترکردن سرویس‌ها و امکانات نرم‌افزاری فضای مجازی که مشابه داخلی دارد و نمونه بومی آن، مورد استفاده و قبول مردم واقع شده است؛ یعنی هر جا سرویسی داخلی راه انداختیم که زمینه موفقیت را داشت، می‌توانیم موانعی برای نمونه‌های خارجی ایجاد کنیم که آن‌هم باید در موقع خودش انجام شود؛ مثل گمرکی که از ماشین‌های خارجی می‌گیریم تا صنعت داخلی را حمایت کنیم. بنابراین، اوّل باید صنعت بومی خودمان را در فضای مجازی توسعه دهیم، بعد به محدودسازی صنعت خارجی بپردازیم.

سخن پایانی

اگر این راه‌حل‌ها را نتوانستیم عملیاتی کنیم، آن وقت باید آن بخش از فضای مجازی را که حاکمیتِ ما را هدف قرار داده است

اگر اعتبار لازم در اختیار مرکز تحقیقات کامپیوتری علوم اسلامی قرار گیرد، با توجه به پشتوانه‌های بیست‌ساله‌ای که در قم و نیز در قوه قضاییه صورت گرفته و جوانانی لایق ایرانی که با ما ارتباط دارند، می‌توانیم به این اهداف دست پیدا کنیم؛ چنان‌که این مرکز تا کنون برنامه‌هایی تولید کرده که همه دارند از آن استفاده می‌کنند و برخی از آنها نیز جنبه ملی دارد؛ مثل سامانه ثنا (احراز هویت الکترونیکی قوه قضاییه)، دادگان زبان فارسی، خطایاب، پست الکترونیک چاپار، سامانه کشف سرقت ادبی (سمیم نور) و طرح‌های ملی دیگر

و هنوز نتوانسته‌ایم مدیریتش نماییم، فیلتر کنیم؛ وگرنه مملکت از دستمان می‌رود. من معتقدم اگر حاکمیت نمی‌تواند فضای مجازی را مدیریت کند، باید آن را ببندد. بنده در شورای عالی فضای مجازی، همین پنج راه‌حل را مطرح کردم و آخرش هم گفتم: اگر نمی‌توانید آنها را اجرایی نمایید، فعلاً فیلتر کنید و ببندید. آقایان هم ده دقیقه صحبت کردند که نباید ببندیم؛ چون این، حقوق شهروندی است؛ مگر می‌شود شبکه‌ای را که بیست میلیون عضو دارد، بست. به هر صورت، پیشنهادهای ما در آنجا به نتیجه نرسید. آنچه ما مطرح می‌کنیم، راه‌حلّ ملی است که هم هزینه دارد و هم عزم ملی را می‌طلبد. برای مدیریت فناوری در کشور برای سال گذشته، منابع مالی کافی تزریق نشده است و با کمبودهای شدیدی مواجه بودیم. اگر این پول تزریق می‌شد، هر مدیری می‌توانست یکی دو پروژه در همین زمینه به دست گرفته و انجام دهد؛ اما چون پول نبود، خود وزارت ارتباطات هم کاری از پیش نبرد. یکی از این پروژه‌های ملی، خط و زبان فارسی در محیط رایانه‌ای و فضای مجازی است که خود این طرح، ده‌ها زیرپروژه دارد و صد میلیارد تومان برآورد این کلان‌پروژه است؛ مثلاً خطایاب، ترجمه ماشینی، فونت‌های اصیل فارسی، حروف‌خوان نوری فارسی، پردازشگرهای متنی و صوتی فارسی، از جمله آنهاست. برای پاسداشت زبان فارسی در فضای مجازی، باید عملیاتی صورت گیرد که خود، یک پروژه ملی است. مع‌الوصف، از سویی، در این زمینه سرمایه‌گذاری نمی‌شود و از طرفی، فیلترکردن هم به مذاق برخی آقایان خوش نمی‌آید. ازاین‌رو، وضع همین جور مثل پانزده سال گذشته باقی مانده است.

در حال حاضر، شبکه‌های اجتماعی خارجی در کشور ما جولان می‌دهند. اگر یک اجماع نخبگانی شکل بگیرد، می‌توانیم با شبکه‌های خارجی، یک دادوستدهایی انجام دهیم؛ مثلاً در چین هر کاری کردم، به گوگل وصل نشدم. این نشان می‌دهد حاکمیت آنجا یک سازوکارهایی ترتیب داده و گوگل کارهای خاصی را برای چین کرده است

آنچه گفتم، مورد قبول اجماع نخبگان فناوری است که اگر پول به آن تخصیص داده شود، همه این کارها شدنی است. البته بعضی کارها انجام شده؛ مثل فرانزیک که ناجا این کار را تا حدودی عملیاتی کرده است و الآن هم اگر بودجه‌اش را به ناجا بدهند، می‌رود مثل آن شرکت چینی را برای تمام‌کردن این کار می‌آورد؛ منتها پول در این حوزه تزریق نمی‌شود. آن اهتمامی که به انرژی هسته‌ای یا صنایع موشکی می‌شود، به این حوزه نمی‌شود. همان‌طورکه از سازمان انرژی هسته‌ای یا برنامه موشکی حمایت شد و به واسطه همت برخی مدیران کارآمد و جهادی نظام، کار به اینجا رسیده است، اگر همین حمایت برای فضای مجازی هم باشد، کار به‌خوبی پیش می‌رود؛ البته یک اجماع نخبگانی می‌خواهد که بودجه لازم بدون سروصدا و هیاهو و با آرامش، حداقل برای این پنج مورد که برشمردم، تخصیص داده شود و عملیاتی گردد. غیر از فیلترینگ که یک امر سلبی است، موارد دیگر، ایجابی است و ربطی هم به شورای عالی فضای مجازی ندارد؛ بلکه انجام آنها فقط هزینه مالی دارد و پول می‌خواهد و جوانانی هستند که این کارها را انجام دهند.

بنده عرض می‌کنم اگر اعتبار لازم در اختیار مرکز تحقیقات کامپیوتری علوم اسلامی قرار گیرد، با توجه به پشتوانه‌های بیست‌ساله‌ای که در قم و نیز در قوه قضاییه صورت گرفته و جوانانی لایق ایرانی که با ما ارتباط دارند، می‌توانیم به این اهداف دست پیدا کنیم؛ چنان‌که این مرکز تا کنون برنامه‌هایی تولید کرده که همه دارند از آن استفاده می‌کنند و برخی از آنها نیز جنبه ملی دارد؛ مثل سامانه ثنا (احراز هویت الکترونیکی قوه قضاییه)، دادگان زبان فارسی، خطایاب، پست الکترونیک چاپار، سامانه کشف سرقت ادبی (سمیم نور) و طرح‌های ملی دیگر.■