بیم‌ها و امیدهای عصر دیجیتال و درس‌های مایکروسافت برای مدیران

ابزارها و سلاح‌ها

برد اسمیت / کارول ان براون

مترجم: محمد رهبان

چاپ دوم

انتشارات راه پرداخت

نسخه نمونه

برای دانلود نسخه کامل به وبسایت
فروشگاه انتشارات راه پرداخت مراجعه کنید
way2pay.shop

سرشناسه : اسمیت، برد، ۱۹۵۹- م. Smith, Brad (Brad Lee), ۱۹۵۹-
عنوان : ابزارها و سلاح‌ها: بیم‌ها و امیدهای عصر دیجیتال
نویسندگان : برد اسمیت ، کارول ان براون
مترجم: محمد رهبان
مشخصات نشر : تهران: راه پرداخت، ۱۳۹۹
مشخصات ظاهری : ۳۵۶ص. ۱٤/۵×۲۱/۵س‌م
شابک: ۹۷۸-۶۲۲-۹۷۸۲۹-۰-۳
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: Tools and Weapons: The Promise and the Peril of the Digital Age
موضوع : ابزار، Tools
موضوع: سلاح‌ها، Weapons
شناسه افزوده : براون، کارول ان ، Browne, Carol Ann
شناسه افزوده : رهبان، محمد، ۱۳۶۷-، مترجم
رده بندی کنگره: TJ۱۱۹۵
رده بندی دیویی : ۶۲۱/۹
شماره کتابشناسی ملی : ۷۵۳۳۲۱۲
وضعیت رکورد : فیپا

بیم‌ها و امیدهای عصر دیجیتال و درس‌های مایکروسافت برای مدیران

ابزارها و سلاح‌ها

برد اسمیت / کارول ان براون

مترجم: محمد رهبان

عنوان:	ابزارها و سلاح‌ها: بیم‌ها و امیدهای عصر دیجیتال
ناشر:	راه‌پرداخت
نویسنده:	محمد رهبان
مترجم:	مینا والی
ویراستار ارشد	مینا والی
ویراستار ادبی:	یلدا شایسته‌فر
بازبینی نهایی متن:	رضا قربانی
صفحه‌آرا:	علیرضا کیوان
ناظر چاپ:	قادر شهبازی
نوبت چاپ:	دوم ۱۴۰۴
شمارگان:	۱۰۰
شابک:	۹۷۸-۶۲۲-۹۷۸۲۹-۰-۳
تلفن:	۰۲۱-۴۴۴۴۳۹۶۶
دورنگار:	publisher@way2pay.press
ایمیل:	way2pay.press
وب‌سایت:	w2ppress.ir
لیتوگرافی:	هنر اشکان
چاپ و صحافی:	واژه

همه حقوق چاپ و نشر این اثر برای «**انتشارات راه‌پرداخت**» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتال و ...) بدون اجازه کتبی ناشر ممنوع است.

نشانی فروشگاه انتشارات راه‌پرداخت:

تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

@way2paypress Way2Pay.press @way2paypress

فهرست

فصل اول: نظارت الکترونیک؛ چاشنی سه‌ساعته ۲۷
فصل دوم: فناوری و امنیت عمومی؛ «ترجیح می‌دهم بازنده باشم تا دروغگو» ۴۷
فصل سوم: حریم خصوصی؛ یکی از حقوق بنیادین بشر ۶۵
فصل چهارم: امنیت سایبری؛ زنگ خطری برای جهان ۸۷
فصل پنجم: حفاظت از دموکراسی؛ «حکومت جمهوری البته اگر بتوانید حفظش کنید!» ۱۰۳
فصل ششم: رسانه‌های اجتماعی؛ آزادی‌هایی که بین ما فاصله می‌اندازند ۱۱۵
فصل هفتم: دیپلماسی دیجیتال؛ ژئوپلیتیک فناوری ۱۳۵
فصل هشتم: حریم خصوصی مصرف‌کننده؛ «ورق برمی‌گردد» ۱۵۷
فصل نهم: اینترنت پرسرعت روستایی الکتریسیته قرن بیست‌ویکم ۱۷۹
فصل دهم: خلاء استعداد؛ ضلع سرمایه انسانی فناوری ۱۹۷
فصل یازدهم: هوش مصنوعی و اخلاقیات ۲۲۱
فصل دوازدهم: هوش مصنوعی و تشخیص چهره ۲۴۱
فصل سیزدهم: هوش مصنوعی و نیروی کار ۲۶۱
فصل چهاردهم: ایالات متحده و چین؛ دنیای فناوری دوقطبی ۲۷۹
فصل پانزدهم: دموکراتیک کردن آینده ضرورت انقلاب داده باز ۲۹۹
فصل شانزدهم: جمع‌بندی؛ مدیریت فناوری بزرگ‌تر از خودمان ۳۱۹

[یادداشت ناشر]

کتاب ابزارها و سلاح‌ها به موضوعات مهمی می‌پردازد که به آنها مبتلا شده‌ایم؛ ۴۰ سال پیش قرار نبود به این مسائل فکر کنیم و در توشه فیلسوفان و جامعه‌شناسان و اقتصاددانان راه‌حل‌هایی برای مدیریت آنها وجود ندارد. این راه‌ها نو و بدیع هستند و راه‌حل‌های جدید می‌خواهند. هرچند برخی مسائل بدیهی هستند و تاریخی به اندازه تاریخ بشریت دارند، ولی حل‌وفصل آنها به مدل‌های ذهنی متفاوتی نسبت به گذشته نیاز دارد.

نظارت الکترونیکی، فناوری و امنیت عمومی، حریم خصوصی، امنیت سایبری، حفاظت از دموکراسی، رسانه‌های اجتماعی، دیپلماسی دیجیتال، حریم خصوصی مصرف‌کننده، اینترنت پرسرعت روستایی، سرمایه انسانی، هوش مصنوعی و ابعاد گوناگون تأثیرگذاری‌اش بر جامعه، نقش مهم چین و تقابلش با آمریکا، از جمله موضوعات دنیای جدید است. اقتصاددانان و سیاست‌مداران ممکن است از زوایای محدود این موضوعات را بررسی کنند و راه‌حل‌هایی هم برای آنها داشته باشند؛ اما زاویه دید کسب‌وکارها متفاوت است. مدیران کسب‌وکارها باید از زاویه‌ای متفاوت نسبت به سیاست‌مداران این مسائل را ببینند؛ به گونه‌ای که هم خیر و صلاح جامعه را رعایت کرده و هم منافع کسب‌وکارهایشان را دنبال کنند.

اهمیت این کتاب در این است که توسط حقوقدانانی نوشته شده که کسب‌وکارهای

فناوری را درک می‌کنند و سال‌ها کنار یکی از مهم‌ترین کسب‌وکارهای فناوری جهان یعنی مایکروسافت بوده‌اند. بیل گیتس، بنیان‌گذار مایکروسافت، در مقدمه به نقش مهم نویسندگان کتاب بر سرنوشت مایکروسافت تأکید کرده‌اند. زبان حقوق فناوری اهمیت زیادی در آینده کسب‌وکاری فناوری دارد و بدون درک و تبیین این زبان نمی‌توانیم انتظار داشته باشیم که رشد سالم کسب‌وکارهای حوزه اقتصاد نوآوری را شاهد باشیم. این کتاب از منظر بررسی متفاوت مسائل کلان حاکم بر کسب‌وکارها اهمیت ویژه‌ای دارد. معمولاً در چنین کتاب‌هایی دیدگاه‌هایی سرد و بی‌روح ارائه می‌شود؛ یا معمولاً با محتواهای انگیزشی و چگونگی مدیریت روبه‌رو می‌شویم. کمتر کسی به مسائل کلان حاکم بر کسب‌وکارها از زاویه‌ای چنین پرداخته است. این مسائل در همه جای جهان مانند هم هستند، هرچند راه‌حل‌های نقاط گوناگون جهان قطعاً با هم تفاوت دارند و باید هم تفاوت داشته باشند. قطعاً نمی‌توان برای نقاط گوناگون جهان راه‌حل‌های یکسانی را به کار برد.

این کتاب هم در پی ارائه راه‌حلی جهان‌شمول نیست و تلاش کرده مسائل مهمی را که به آنها مبتلا شده‌ایم، تبیین کند. قاعدتاً اولین گام در راه‌حل مسائل شناخت آنهاست. ما بدون شناخت مسائل نمی‌توانیم انتظار مدیریت چالش‌ها را داشته باشیم.

این چالش‌ها مسائل روزمره‌ای را ایجاد می‌کنند و هیچ راه‌حل دائمی هم برای آنها وجود ندارد و احتمالاً در سال‌های آینده حجم مسائل بیشتر هم می‌شود. بنابراین آنچه اهمیت دارد، تلاش فکری مداوم برای بررسی و شناخت ابعاد گوناگون چالش‌های دنیای جدید است. دنیای جدید مبتنی بر فناوری و نوآوری، بی‌رحم است و ما بدون درک آنها قطعاً در آینده نزدیک چالش‌های پرشمارتری خواهیم داشت.

امیدوارم انتشار این کتاب در انتشارات راه پرداخت زمینه تفکر بیشتر درباره مسائل مهم اقتصاد دیجیتال را فراهم کند؛ صمیمانه از حمایت‌های مجموعه ایرانسل در انتشار این کتاب نیز تشکر می‌کنم. ان‌شاءالله با همتی که همکاران خوب من در انتشارات راه پرداخت دارند، بتوانیم در آینده این روند را پرقوت‌تر از گذشته ادامه دهیم.

رضا قربانی
انتشارات راه پرداخت

مقدمه

اولین بار زمانی برای مشاوره به برد اسمیت مراجعه کردم که دشوارترین دوران زندگی حرفه‌ای‌ام را سپری می‌کردم. دو دهه از آن زمان می‌گذرد و همچنان برای مشاوره به او مراجعه می‌کنم.

«برد» سال ۱۹۹۳ به تیم حقوقی مایکروسافت پیوست، اما تازه در اواخر دهه ۱۹۹۰ و در پرونده «شکایت ضدانحصار دولت ایالات متحده علیه مایکروسافت» بود که با هم آشنا شدیم (پرونده برجسته‌ای که در آن دولت ایالات متحده مایکروسافت را متهم کرد که با ایجاد محدودیت‌های قانونی و فنی در توانایی تولیدکنندگان کامپیوترهای شخصی و کاربران برای حذف اینترنت اکسپلورر و استفاده از سایر برنامه‌ها جایگاه انحصاری‌اش در بازار کامپیوترهای شخصی را حفظ می‌کند). ساعات زیادی را در کنار هم کار می‌کردیم. خیلی زود متوجه شدم چه متفکر خبره‌ای است. به‌تدریج هم به شخصیت برد علاقه‌مند شدم و هم به تشخیص و نظر حرفه‌ای‌اش اعتماد پیدا کردم.

برد به استراتژی حقوقی‌مان در آن پرونده شکل داد و بعد کاری کرد که دست‌کم به همان اندازه مهم بود؛ باعث و بانی تغییر فرهنگی و استراتژیک بزرگی در شرکت شد. آن تغییر محور مباحث این کتاب است.

در اوایل کار مایکروسافت افتخار می‌کردم که زمان خیلی کمی را به گفت‌وگو با مسئولان دولت فدرال سپری می‌کنیم. به افراد می‌گفتم «عالی نیست که بدون داشتن حتی یک دفتر کار در واشنگتن دی‌سی می‌توانیم موفق باشیم؟» بعداً به بهایی گزاف؛ یعنی پرونده ضدانحصار فهمیدم که این دیدگاه هوشمندانه نبوده است.

بعد از توافق در مورد آن پرونده، برد؛ من و بسیاری از افراد دیگر در مایکروسافت را متقاعد کرد که باید رویکرد متفاوتی را اتخاذ کنیم. سپس به ما نشان داد که چطور این رویکرد را عملی کنیم. برد وکیل است، نه توسعه‌دهنده نرم‌افزار و هرچند تسلط بسیار خوبی بر فناوری دارد، اما خیلی شبیه بقیه ما فکر نمی‌کند (این حرفم در واقع تعریف و تمجید است). متوجه شده بود که باید وقت و انرژی بیشتری را به برقراری ارتباط با ذی‌نفعان گوناگون مثل دولت، شریک‌ها و حتی گاهی اوقات رقبایمان اختصاص دهیم. برد می‌توانست دیپلمات بسیار خوبی باشد. توانایی‌اش در این زمینه با توجه به علاقه‌اش به روابط بین‌الملل در جوانی منطقی به نظر می‌رسد.

اینکه تفکر برد به منافع مایکروسافت محدود نبود، نشانه گویایی از شخصیت اوست. اهمیت زیاد فناوری و سیاست‌های تأثیرگذار بر آن را درک کرده و به این نتیجه رسیده بود که بیرون گود ایستادن نه فقط برای شرکت ما؛ بلکه برای کل صنعت اشتباه است. هرچند موقعیت‌هایی وجود دارد که باید هر شرکتی راه خودش را برود، اما موقعیت‌های زیاد دیگری هم وجود دارد که همه می‌توانیم از طریق همکاری منافع بیشتری کسب کنیم (برای مثال در مواردی که پای هوش مصنوعی، تشخیص چهره و امنیت سایبری در میان است).

همان‌طور که برد در این کتاب استدلال می‌کند، موقعیت‌هایی هم وجود دارد که مداخله دولت از طریق رگولیشن بیشتر به نفع همه است (برد آن‌قدر آگاهی دارد که متوجه شود چقدر عجیب است که یک رهبر کسب‌وکار به جای قوانین دولتی کمتر، به‌دنبال قوانین بیشتر باشد). در همین راستا می‌دانست که مایکروسافت و سایر شرکت‌های فناوری باید با رهبران ایالات متحده، اروپا و دیگر نقاط جهان تعامل بیشتری داشته باشند. روزهای فخرفروشی به نداشتن دفتر کار در واشنگتن دی‌سی به سر آمده بود.

نگرش برد هیچ‌وقت به اندازه امروز مناسب و مهم نبوده است. دولت‌های سراسر دنیا بسیاری از شرکت‌های فناوری و در مجموع این صنعت را زیر ذره‌بین برده‌اند و می‌پرسند چطور از فناوری‌شان استفاده می‌شود؟ این فناوری چه پیامدهایی دارد؟ شرکت‌های فناوری‌محور چه مسئولیت‌هایی دارند؟ دولت‌ها و جامعه چطور باید به این مسائل بپردازند؟

هرچند این پرسش‌ها همان پرسش‌هایی نیستند که ما ۲۰ سال پیش با آنها مواجه بودیم، اما بینش‌هایی که برد آن زمان داشت، امروز نیز به همان اندازه ارزشمند هستند.

به‌عنوان مثال به مسائلی توجه کنید که فناوری تشخیص چهره به وجود آورده است. این مبحث هنوز آنچنان اهمیت پیدا نکرده که موضوع بحث‌های عمومی شود، اما این اتفاق می‌افتد. شرکت‌های نرم‌افزاری چه محدودیت‌هایی را باید برای ابزارهای تشخیص چهره در نظر بگیرند؟ صنعت فناوری چه رویکردی باید نسبت به این

موضوع داشته باشد و در این زمینه چه نوع رگولیشن دولتی مناسب است؟

برد در پیش‌بینی این پرسش‌ها و ایجاد مشارکت‌هایی برای بحث در مورد آنها پیشگام بوده است. صنعت فناوری باید دور هم جمع شود و با مشتریان و دولت‌های سراسر جهان همکاری کند. شاید نتوانیم به توافقی جهانی دست یابیم، اما به نفع مشتریان، صنعت فناوری و جامعه نخواهد بود که اجازه دهیم آن‌قدر چندپارگی ایجاد شود که قوانین کشورها تفاوت‌های بسیار زیادی پیدا کنند.

کتاب «ابزارها و سلاح‌ها» به طیف بسیار گسترده‌ای از مسائل شامل ۱۵ مسئله از جمله امنیت سایبری، تنوع نیروی کار فناوری اطلاعات و رابطه ایالات متحده و چین پرداخته است. اگر قرار بود مهم‌ترین فصل را انتخاب کنم، فصل مربوط به حریم خصوصی را انتخاب می‌کردم. توانایی جمع‌آوری مقادیر عظیم داده، شمشیری دولبه است. از طرفی دولت‌ها، کسب‌وکارها و افراد را برای اتخاذ تصمیمات بهتر توانمند می‌کند، اما از طرف دیگر پرسش‌های مهمی را در مورد نحوه استفاده از داده‌ها همراه با حفاظت از حق افراد برای برخورداری از حریم خصوصی مطرح می‌کند.

با این حال همان‌طور که برد نشان می‌دهد هرچند فناوری به‌نسبت جدید است، اما پرسش‌های مربوط به آن جدید نیستند. انسان‌ها قرن‌هاست که با نسخه‌های متفاوتی از این مشکل درگیر بوده‌اند. البته شاید غیرمنتظره نباشد که در فصلی در مورد حریم خصوصی داده‌ها، این مسئله مطرح شود که دولت آلمان نازی چطور اطلاعات مردم کشورش را جمع‌آوری می‌کرد. احتمالاً انتظار نخواهید داشت که در این فصل به جنگ ۱۸۱۲ ایالات متحده و امپراتوری بریتانیا اشاره شود یا تاریخچه‌ای از «معاهده‌های معاضدت قضایی دوجانبه» (Mutual Legal Assistance Treaties) ارائه شود.

این امر نشان‌دهنده علایق بسیار متنوع برد و توانایی‌اش در بررسی عمیق تقریباً هر موضوعی است. اما هیچ‌کدام از بحث‌ها مانند خلاصه پرونده‌ای خسته‌کننده نشده‌اند. برد و نویسنده همکارش، «کارول ان براون» داستان‌گوهای توانمندی هستند که تصویری بی‌واسطه از حال و هوای چکش‌کاری این مسائل در لحظه، در سالن‌های همایش و در دادگاه‌های سراسر دنیا ارائه می‌دهند. برد در گوشه‌ای به تحلیل مسائل ننشسته؛ بلکه افراد را کنار هم جمع می‌کند تا به راه‌حل برسند.

برد و من پیوسته به‌صورت حضوری و ایمیلی در مورد این مسائل بحث می‌کنیم. همچنان به تشخیص و درایتش اتکا می‌کنم. تجربه و هوش برد او را به مناسب‌ترین راهنما برای فکر کردن در مورد پرسش‌های پیش روی صنعت فناوری تبدیل کرده است.

این مسائل مدام مهم‌تر می‌شوند. کتاب ابزارها و سلاح‌ها تصویری روشن از پرسش‌های برآمده از فناوری‌های جدید ارائه می‌کند و مسیری بالقوه پیش روی شرکت‌های فناوری و جامعه قرار می‌دهد. برد راهنمایی روشن و جذاب، در مورد برخی از اضطراری‌ترین بحث‌های امروز حوزه فناوری نوشته است.

بیل گیتس

آوریل ۲۰۱۹

پیش‌گفتار

ابر؛ قفسه بایگانی جهان

تمدن همواره بر قدرت داده اتکا داشته است.

تاریخ بشر زمانی شروع شد که انسان‌ها، توانایی صحبت کردن را در خود پرورش دادند. با ابداع زبان افراد توانستند ایده‌ها، تجربه‌ها، خواسته‌ها و نیازهایشان را با هم در میان بگذارند.

سرعت پیشرفت زمانی بیشتر شد که انسان‌ها به توانایی نوشتن دست یافتند. ایده‌ها خیلی آسان‌تر و دقیق‌تر، نه فقط بین افراد؛ بلکه از مکانی به مکان دیگر منتقل می‌شدند.

بعد جرقه‌ای زده شد که شعله دانش را روشن کرد. آن جرقه توانایی ذخیره‌سازی، بازیابی و اشتراک‌گذاری نوشته‌های افراد بود. ساخت کتابخانه‌ها به یکی از نمادهای دنیای باستان تبدیل شد. این بایگانی‌های اسناد و کتاب‌ها باعث شدند افراد علاوه بر بعد مکانی، در بعد زمانی هم بتوانند با یکدیگر ارتباط برقرار کنند و اطلاعات را از نسل خود به نسل بعد انتقال دهند. چند قرن بعد که «یوهانس گوتنبرگ» ماشین چاپ مکانیکی را اختراع کرد، شعله دانش به آتشی تبدیل شد که قدرت تازه‌ای به نویسندگان و خوانندگان بخشید.

این آتش تمام جهان را فراگرفت و قرن‌ها بعد با رشد انفجاری تجارت همراه شد که همزمان علت و معلول افزایش ارتباطات بود. اوایل قرن بیستم هر دفتر کاری به تأسیساتی برای ذخیره‌سازی اسناد نیاز داشت. اتاق‌ها پر از قفسه‌های بایگانی بودند.

هرچند داده همیشه برای جامعه مهم بوده، اما هرگز نقش پررنگی مانند امروز نداشته است. حتی وقتی رشد تجارت کم می‌شود یا اقتصادها ضعیف می‌شوند، باز هم داده با سرعتی پایدار به رشد ادامه می‌دهد. برخی می‌گویند داده به نفت قرن بیست‌ویکم تبدیل شده، اما این کوچک نشان‌دادن واقعیت است. یک قرن پیش خودروها، هواپیماها و بسیاری از قطارها با نفت حرکت می‌کردند. در حالی که امروز محرک همه ابعاد زندگی انسان داده است. در تمدن مدرن داده بیشتر از آنکه شبیه نفتی باشد که می‌سوزانیم، شبیه هوایی است که تنفس می‌کنیم.

داده بر خلاف نفت به منبعی تجدیدپذیر تبدیل شده که خودمان می‌توانیم تولیدش کنیم. در انتهای دهه ۲۰۱۰ تقریباً ۲۵ برابر بیشتر از ابتدای دهه، داده دیجیتال وجود داشت. در واقع اکنون با وجود هوش مصنوعی بیش از همیشه از داده بهره می‌بریم.

زیرساخت دیجیتالی که از این داده‌ها پشتیبانی می‌کند، ابر خوانده می‌شود. هرچند نامش از نرمی و پشمالویی حکایت می‌کند، اما ابر در واقعیت مانند یک قلعه است. هر بار با تلفن هوشمندتان جست‌وجویی انجام می‌دهید، داده‌ها را از مرکز داده عظیمی بیرون می‌کشید. این مراکز داده یکی از عجایب عصر مدرن هستند که تقریباً هیچ‌کس اجازه ورود به آنها را ندارد.

اما اگر آن‌قدر خوش‌اقبال باشید که بتوانید از مرکز داده‌ای بازدید کنید، سازوکار دنیای امروز را بهتر درک می‌کنید.

یکی از بهترین مکان‌ها برای مشاهده طرز کار داخلی ابر، پایتخت سیب دنیاست. شهر کوچک «کوئینسی» (Quincy) در ایالت واشنگتن و تقریباً ۱۵۰ مایلی شرق سیاتل قرار دارد. این مکان تصادفی انتخاب نشده است. کوئینسی در مرکز حوزه کشاورزی این ایالت و در نزدیکی معبر تنگ شیب‌داری قرار دارد که هزاران سال با رود بزرگ و مواج کلمبیا، بزرگ‌ترین آبراه غرب ایالات متحده تراشیده شده است. انرژی این شهر با شبکه‌ای از نیروگاه‌های برق‌آبی شامل سد «گرند کولی» (Grand Coulee Dam)، بزرگ‌ترین نیروگاه ایالات متحده تأمین می‌شود؛ محیطی ایدئال برای بزرگ‌ترین مصرف‌کننده برق جهان یعنی مرکز داده مدرن.

چند چهارراه آن‌طرف‌تر از خیابان اصلی کوئینسی مجموعه‌ای از ساختمان‌های بی‌نام و نشان را می‌بینید که با نرده‌ها و دیوارهای بلندی محصور شده‌اند. روی برخی از این ساختمان‌ها لوگوی شرکت‌های فناوری امروز نصب شده است، اما سایر ساختمان‌ها هیچ نشانه‌ای ندارند. بزرگ‌ترین تأسیسات در این مجموعه مرکز داده کلمبیا نام دارد که متعلق به مایکروسافت است.

نگاه‌کردن به عظمت یک مرکز داده، هیجان‌انگیز (و کمی وهمناک) است. تأسیسات ما در کوئینسی دیگر فقط یک ساختمان نیست. این تأسیسات فضای دو محوطه مرکز داده با بیش از ۲۰ ساختمان را پر کرده‌اند که در مجموع دو میلیون فوت مربع مساحت دارند. هر ساختمان به اندازه دو زمین فوتبال است، یعنی آن‌قدر بزرگ است که دو هواپیمای تجاری در آن جا می‌شود. این مجموعه ساختمان‌ها میزبان صدها هزار سرور و میلیون‌ها هارددیسک است که هر کدام هر سه سال با مدل‌های سریع‌تر و بهره‌ورتر جایگزین می‌شوند.

بهترین راه برای درک مقیاس یک مرکز داده این است که پیاده از گوشه بیرونی آن به سمت

مرکزش بروید. بیرون از هر کدام از این ساختمان‌ها، شماری از بزرگ‌ترین ژنراتورهای برق جهان قرار دارند و آماده‌اند که اگر شبکه برق منطقه قطع شد، در عرض چند ثانیه برق را تأمین کنند تا مرکز داده لحظه‌ای خاموش نشود. هر ژنراتور بیش از ۲۰ فوت ارتفاع دارد و می‌تواند برق بیش از دو هزار خانه را تأمین کند. این ژنراتورها به مخزن‌های گازوئیلی متصل هستند که می‌توانند انرژی مرکز داده را تا ۴۸ ساعت تأمین کنند. تمهیداتی هم برای تأمین سوخت مجدد اندیشیده شده تا در صورت نیاز فعالیت مراکز داده تا مدت بسیار بیشتری متوقف نشود. در مراکز داده جدیدترمان، مانند مرکز داده مستقر در شهر «شاین» ایالت وایومینگ، ژنراتورها از گاز طبیعی پاک‌تر استفاده می‌کنند و برای شبکه برق منطقه برق پشتیبان فراهم می‌کنند. ده‌ها عدد از این ژنراتورهای بسیار بزرگ در کنار ساختمان‌های مرکز داده قرار دارند و آماده تأمین انرژی در صورت قطع برقی هستند که نیروگاه برق‌آبی سد گرند کولی تأمین می‌کند.

داخل هر ساختمان ردیفی از اتاق‌های امن بزرگ به‌عنوان پست‌های برق عمل می‌کنند و معمولاً توان را در ۲۳۰ هزار ولت از شبکه برق دریافت و به ۲۴۰ ولت تبدیل می‌کنند تا توان مورد نیاز کامپیوترهای مرکز داده را تأمین کنند. این اتاق‌های پست برق با ردیف‌هایی از رک‌های شش‌فوتی پر شده‌اند که در هر کدام ۵۰۰ باتری یا بیشتر قرار دارد. این باتری‌ها شبیه باتری خودروی شما هستند. درهای اتاق‌ها ضدگلوله و دیوارها نسوز هستند تا آتش از اتاقی به اتاق‌های دیگر سرایت نکند. هر ساختمان مرکز داده معمولی چهار اتاق از این نوع یا بیشتر دارد و این ساختمان‌ها با توجه به پیکربندی ممکن است تا پنج هزار باتری داشته باشند. این باتری‌ها دو کاربرد دارند. اول اینکه برق شبکه از این رک‌ها عبور می‌کند تا باتری‌ها شارژ نگه داشته شوند و از نوسان‌های بالقوه جلوگیری کنند تا روانی و پایداری جریان برق کامپیوترها حفظ شود. دوم اینکه در صورت قطع برق شبکه، این باتری‌ها تا فعال‌شدن ژنراتورها توان مورد نیاز مرکز داده را تأمین می‌کنند.

در میان مجموعه دیگری از درهای ضدگلوله و دیوارهای نسوز، فلزیابی فرودگاهی وجود دارد که دو نگهبان یونیفرم‌پوش آن را اداره می‌کنند و بین شما و حریم داخلی مجموعه قرار گرفته‌اند. فقط کارمندان تمام‌وقت مایکروسافت که نام‌شان در فهرستی از پیش تأییدشده وجود دارد، می‌توانند از اینجا جلوتر بروند. وقتی به اتاق پذیرش کوچکی وارد می‌شوید، دری فولادی پشت سر شما بسته می‌شود. درون این اتاق دربسته منتظر می‌مانید تا کارمندان

حفاظتی شما را از طریق دوربین بررسی کنند و بعد از تأیید در ضدگلوله بعدی را باز کنند.

سرانجام به اتاقی غارمانند، معبد عصر اطلاعات و سنگ بنای زندگی دیجیتال ما وارد می‌شوید. صدایی آرام ورود شما به این مرکز عصبی را خوشامد می‌گوید. اینجا رک‌های بلند کف به سقفی حاوی کامپیوترها به شکلی ردیف شده‌اند که انتهایشان از میدان دید شما خارج است. این کتابخانه عظیم فولاد و مدار دارای سرورهایی است که از لحاظ شکل و فضای اشغال‌شده مثل هم هستند، اما حجم داده در هر کدام منحصربه‌فرد است. اینجا قفسه بایگانی دنیای دیجیتال است.

جایی در یکی از اتاق‌های این ساختمان‌ها فایل‌هایی وجود دارند که متعلق به شما هستند. ایمیلی که امروز صبح نوشتید، سندی که دیشب روی آن کار کردید و عکسی که دیروز بعدازظهر گرفتید، در یکی از این اتاق‌هاست. همچنین احتمالاً دارای اطلاعات شخصی شما نزد بانک، پزشک و کارفرمایتان هستند. این فایل‌ها فقط بخش بسیار کوچکی از هارددیسک یکی از هزاران کامپیوتر اینجا را اشغال کرده‌اند. همه فایل‌ها رمزنگاری شده‌اند، یعنی اطلاعات به نحوی کدگذاری شده‌اند که فقط کاربران تأییدشده آن داده‌ها می‌توانند آنها را مشاهده کنند.

هر ساختمان مرکز داده چند اتاق این شکلی دارد که به‌نوعی محصور شده‌اند تا در صورت وقوع آتش‌سوزی، آتش به اتاق‌های دیگر سرایت نکند. هر مجموعه از کامپیوترها به سه منبع توان درون ساختمان متصل شده است. هر ردیف نیز به نحوی طراحی شده که گرمای تولیدی کامپیوترها را در ساختمان به گردش درآورد تا در زمستان نیاز به گرمایش و در نتیجه نیاز به برق کاهش یابد.

هنگام خروج از ساختمان نیز باید تمام فرایند امنیتی را دوباره از سر بگذرانید. دوباره باید برای عبور از فلزیاب کفش‌ها و کمربندتان را درآورید. در حالی که با خود فکر می‌کنید که هنگام خروج از فرودگاه نیز چنین روالی وجود ندارد، میزبان‌تان به شما یادآوری می‌کند که این تدابیر امنیتی دوطرفه بی‌دلیل نیستند. مایکروسافت می‌خواهد اطمینان حاصل کند که هیچ‌کس داده‌ها را روی یواس‌بی فلش کپی نمی‌کند یا هارددیسکی با اطلاعات شخصی را به سرقت نمی‌برد. حتی دیسک‌های سخت نیز از خروجی ویژه‌ای عبور می‌کند. وقتی زمان جایگزینی آنها می‌رسد، داده‌هایشان روی کامپیوتری جدید کپی و فایل‌ها پاک می‌شوند. بعد

هارددیسک ازرده‌خارج‌شده به دستگاه فلز خردکن بزرگی وارد می‌شود که تقریباً همان کار کاغذخردکن‌ها را در مورد دیسک‌ها انجام می‌دهد.

احتمالاً برجسته‌ترین ویژگی برای انتهای گشت‌وگذار نگه داشته شده است. راهنما توضیح می‌دهد که به ازای هر کدام از این مراکز داده، مجموعه دیگری از ساختمان‌ها مشابه همین ساختمان‌ها وجود دارد تا در جایی دیگر بی‌وقفه از داده‌های کسب‌وکارها، دولت یا سازمان‌های غیرانتفاعی پشتیبان‌گیری شود. بدین ترتیب اگر زلزله، گردباد یا هر نوع فاجعه طبیعی یا مصنوعی دیگری اتفاق بیفتد، مرکز داده دوم وارد می‌شود تا خدمات ابری شما بدون مشکل به کارش ادامه بدهد. یکی از تجربه‌هایی که در این زمینه داشتیم این بود که وقتی زلزله‌ای شدید شمال ژاپن را به لرزه درآورد، مرکز داده ما در جنوب ژاپن از بروز هر گونه اختلالی در خدمات جلوگیری کرد.

در حال حاضر مایکروسافت مالک، اداره‌کننده و اجاره‌کننده مراکز داده‌ای با اندازه‌های گوناگون در بیش از ۱۰۰ مکان در بیش از ۲۰ کشور است (این ارقام در حال افزایش هستند) که ۲۰۰ خدمت آنلاین ارائه می‌دهند و از بیش از یک میلیارد مشتری در بیش از ۱۴۰ کشور پشتیبانی می‌کنند.

وقتی در سال ۱۹۹۳ به مایکروسافت پیوستم، افراد برای راه‌اندازی شرکت نرم‌افزاری به سرمایه زیادی نیاز نداشتند. «بیل گیتس» و «پل آلن»، بنیان‌گذاران مایکروسافت، جدیدترین افراد از گروهی از توسعه‌دهندگان فناوری بودند که شرکت‌شان را از گاراژ خانه یا اتاق خوابگاه دانشگاه راه‌اندازی کرده بودند. منظورم این است که آن زمان ساخت نرم‌افزار به پول زیادی نیاز نداشت. برای شروع کامپیوتری درست‌وحسابی، پس‌اندازی کم و میل زیاد به پیتزا خوردن کافی بود.

در فاصله تبدیل‌شدن مایکروسافت از استارت‌آپی کوچک به شرکتی چندملیتی، زیاد این شرایط را در مورد شرکت‌های دیگر مشاهده کردیم. در سال ۲۰۰۴ به‌دنبال خرید شرکت نرم‌افزاری ضدجاسوس‌افزاری به نام «جاینت کمپانی سافت‌ویر» (Giant Company Software) بودیم. وقتی تیم‌مان با آنها تماس گرفت، با شماره تلفنی تماس گرفتیم که پشتیبانی فنی ارائه می‌داد. وقتی تماس‌گیرنده مایکروسافت خواست تماس به مدیرعامل شرکت متصل شود، در واقع تلفن به تنها کارمند دیگری داده شده که آن طرف میز نشسته بود. جای تعجب نداشت که مذاکرات

خیلی سریع پیش رفت.

وقتی از یکی از مراکز داده شرکت بازدید می‌کنم، نمی‌توانم به جاینت کمپانی سافت‌ور فکر نکنم. هنوز می‌توانیم همان‌طور که بیل و پال شروع کردند، نرم‌افزاری جدید بسازیم. توسعه‌دهندگان منبع‌باز مدام این کار را می‌کنند، اما فراهم‌کردن پلتفرم‌های مورد نیاز برای رایانش ابری در مقیاس جهانی مقوله‌ای کاملاً متفاوت است. وقتی میان هزاران کامپیوتر با چراغ‌های چشمک‌زن، رک‌های باتری و ژنراتورهای عظیم قدم می‌زنم، احساس می‌کنم نه در عصری دیگر؛ بلکه در سیاره‌ای دیگر قرار دارم. ساخت مراکز داده صدها میلیون دلار هزینه دارد. وقتی هم که ساخته شوند، تازه کار نگهداری و ارتقای آنها شروع می‌شود. این محوطه‌ها مدام گسترش پیدا می‌کنند و سرورها، دیسک‌های سخت و باتری‌ها ارتقا می‌یابند یا با تجهیزات جدیدتر و بهره‌ورتر جایگزین می‌شوند. در مراکز داده مقوله‌ای به نام پایان کار معنی ندارد.

مرکز داده مدرن از بسیاری جهات محور عصر دیجیتال جدیدی محسوب می‌شود که جهان به آن وارد شده است. این مجموعه‌های عظیم متشکل از داده، فضای ذخیره‌سازی و قدرت رایانش، پلتفرمی بی‌سابقه برای پیشرفت در اقتصادهای سراسر جهان ایجاد کرده‌اند و در عین حال عامل ظهور بسیاری از چالش‌برانگیزترین مشکلات دوران ما هستند. در این عصر جدید چطور تعادل مناسب را بین امنیت عمومی، راحتی و آسایش فردی و حریم خصوصی برقرار می‌کنیم؟ در برابر حملات سایبری که از این فناوری برای ایجاد اختلال در کشورها، کسب‌وکارها یا زندگی شخصی افراد استفاده می‌کنند، چطور از خودمان محافظت می‌کنیم؟ چطور موج آثار اقتصادی را مدیریت می‌کنیم که در جامعه‌های ما به راه افتاده‌اند؟ آیا در حال ساختن دنیایی هستیم که برای فرزندان‌مان شغل فراهم می‌کند؟ آیا این دنیایی را که می‌سازیم، اصلاً می‌توانیم کنترل کنیم؟

برای پاسخگویی به همه این پرسش‌ها ابتدا باید بهتر درک کنیم که در حال حاضر فناوری چطور در حال تغییر است؛ مسئله‌ای که تا حدی به درک نحوه تغییر فناوری در گذشته وابسته است.

از ابتدای آفرینش این امکان وجود داشته که از هر ابزاری در راه خیر یا شر استفاده شود. حتی از جارو هم می‌توان برای جارو کردن زمین یا ضربه‌زدن به سر استفاده کرد. هرچه ابزاری قدرتمندتر باشد، فایده یا زیان بیشتری می‌تواند ایجاد کند. هرچند موج تحول دیجیتال

بسیار نویدبخش است، اما دنیا، فناوری اطلاعات را به ابزاری قدرتمند و در عین حال سلاحی ترسناک تبدیل کرده است.

این عصر فناوری جدید به شکل فزاینده‌ای دوران جدیدی از اضطراب و تشویش را به همراه داشته است. این تنش‌ها در حکومت‌های دموکراتیک جهان برجسته‌تر هستند. این کشورها که تحت فشار مشکلات مربوط به مهاجرت، تجارت و نابرابری درآمدی هستند، بیش از پیش با شکاف‌های ناشی از اقدامات عوام‌گرایانه و ملی‌گرایانه مواجه می‌شوند که تا حدی نتیجه تغییرات بنیان‌برافکن فناوری هستند. مزیت‌های فناوری منصفانه و برابر توزیع نشده‌اند و ماهیت و سرعت تغییر افراد، جامعه‌ها و کشورها را به چالش می‌کشد. جوامع دموکراتیک در مجموع با چالش‌های مشترکی روبه‌رو شده‌اند که بزرگ‌تر از چالش‌های تقریباً صد سال اخیر آنها هستند. در برخی موارد هم کشورهای دیگر از فناوری برای سوءاستفاده از این آسیب‌پذیری بهره می‌برند.

این کتاب این مسائل را از جایگاه سکان‌داری یکی از بزرگ‌ترین شرکت‌های فناوری جهان بررسی می‌کند. داستان بخش فناوری را می‌گوید که می‌خواهد نیروهایی را درک کند، بپذیرد و با آنها کنار بیاید که از یک شرکت یا حتی تمام صنعت بزرگ‌تر هستند. در عین حال داستان نه فقط در مورد روندها و ایده‌ها؛ بلکه در مورد افراد، تصمیمات و فعالیت‌هایی برای پاسخگویی به نیازهای جهانی است که به‌سرعت تغییر می‌کنند.

داستان هیجان‌انگیزی است که به‌مرور گره‌هایش باز می‌شوند و ما در مایکروسافت گاهی اوقات آن را از دیدگاه متفاوتی می‌بینیم. دو دهه پیش در موقعیتی قرار گرفتیم که شاید بتوان آن را اولین برخورد فناوری اطلاعات مدرن با جهان نامید. در ایالات متحده وزارت دادگستری و ۲۰ ایالت شکایت ضدانحصاری را علیه ما تنظیم کردند و می‌خواستند مایکروسافت را چندتکه کنند. دولت‌های سایر کشورها نیز پرونده‌های مشابهی را دنبال کرده‌اند. مسئولان رقابت به این جمع‌بندی رسیده بودند که سیستم‌عامل ویندوز آن‌قدر مهم است که نباید رگوله‌نشده باقی بماند.

هرچند با موفقیت از تجزیه شرکت جلوگیری کردیم، اما تجربه‌ای دشوار، مشقت‌بار و حتی دردناک بود. وقتی در سال ۲۰۰۲ به سمت رئیس اداره حقوقی شرکت منصوب شدم، وظیفه‌ام این بود که با دولت‌های نقاط گوناگون جهان و شرکت‌های بخش فناوری به توافق‌هایی شبیه

پیمان صلح دست یابم. این کارها تقریباً یک دهه طول کشید و اشتباهات زیادی را هم در این مسیر مرتکب شدیم. با توجه به جایگاهم شخصاً به نحوی مسئول تقریباً همه این اشتباهات بوده‌ام.

اما از این چالش‌ها باتجربه‌تر و هوشمندتر بیرون آمدیم. یاد گرفتیم که باید به آینه نگاه می‌کردیم و چیزی را می‌دیدیم که دیگران در ما می‌بینند، نه آنچه خودمان می‌خواستیم ببینیم. انگار اولین فارغ‌التحصیلان مدرسه‌ای جدید بودیم. لزوماً شاگرداول نبودیم، اما مزیت‌مان این بود که پیش از همه مدرسه را تمام می‌کردیم.

مسائل فناوری امروز گسترده‌تر و عمیق‌تر از ۲۰ سال پیش هستند. به نقطه‌عطفی برای فناوری و جامعه رسیده‌ایم، دورانی که مملو از فرصت‌هاست، ولی در عین حال نیازمند برداشتن گام‌هایی فوری برای پرداختن به مسائل اضطراری است.

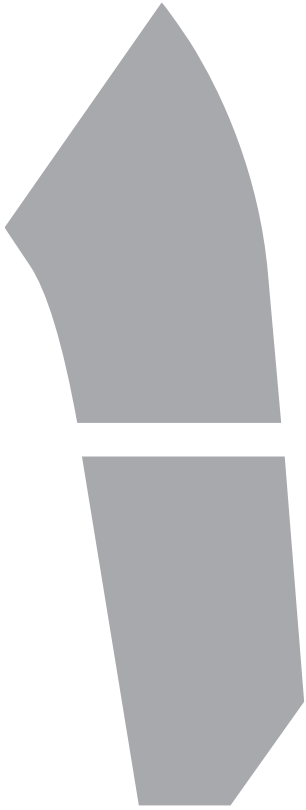
در نتیجه بخش فناوری هم باید درست مانند مایکروسافت دو دهه پیش تغییر کند. وقت آن رسیده که اصلی اساسی را بپذیریم؛ وقتی فناوری ما جهان را تغییر می‌دهد، مسئولیت داریم که به چالش‌های جهانی که در ایجادش نقش داشته‌ایم، رسیدگی کنیم. شاید بدیهی به نظر برسد، اما نه در بخشی که از دیرباز به‌شدت بر رشد سریع متمرکز بوده و گاهی اوقات خود تحول‌آفرینی را هدف نهایی می‌دیده است. به‌طور خلاصه شرکت‌هایی که فناوری خلق می‌کنند، باید مسئولیت بیشتری در برابر آینده بپذیرند.

اما اصلی دیگر و به همان اندازه مهم وجود دارد؛ بخش فناوری به‌تنهایی نمی‌تواند به این چالش‌ها رسیدگی کند. جهان به ترکیبی از خودتنظیمی و اقدامات دولتی نیاز دارد. در این زمینه نیز پیامدهای تأثیرگذارتری کشورهای دموکراتیک جهان را تهدید می‌کند، زیرا در دورانی که فناوری به نیروی تحول‌آفرین قدرتمندی تبدیل شده، این کشورها بیش از همه به حفظ اجماع اقتصادی و اجتماعی فراگیر وابسته هستند. به نظر می‌رسد برای بسیاری از دولت‌های دموکراتیک جلب اراده برای اقدام بیش از همیشه دشوار شده است. اما اکنون زمانی است که دولت‌های دموکراتیک باید جداگانه، با هم و با شکل نوینی از همکاری با بخش فناوری، سیاست‌ها و برنامه‌های جدیدی را به پیش ببرند. به بیان ساده دولت‌ها باید سریع‌تر حرکت کنند و خود را با سرعت فناوری همگام سازند.

دفترچه راهنما یا تجربه ویژه‌ای برای حل این چالش‌ها وجود ندارد، اما بینش‌های مهمی

از گذشته وجود دارند که در هر حال می‌توان آنها را آموخت و به کار گرفت. از زمان شروع انقلاب صنعتی اول در میانه قرن هجدهم، موج‌های مختلفی از تغییر فناورانه را در سراسر دنیا شاهد بوده‌ایم. در برابر هر چالش تازه و در ظاهر بی‌سابقه‌ای، اغلب بدیلی تاریخی وجود دارد که اگرچه کاملاً مثل چالش جدید نیست، اما بینش‌هایی برای اکنون دارد. در این کتاب با کمک‌گرفتن از درس‌های گذشته به فرصت‌ها و چالش‌های آینده می‌پردازیم و ایده‌هایی را برای عبرت‌گرفتن از این درس‌ها ارائه می‌دهیم.

این پرسش‌ها در نهایت شامل فناوری و پیامدهایش برای شغل‌های ما، امنیت ما و بنیادین‌ترین حقوق بشر می‌شود. باید عصر تغییرات فناورانه سریع را با ارزش‌های قدیمی و حتی همیشگی آشتی بدهیم. برای رسیدن به این هدف باید اطمینان حاصل کنیم نوآوری تداوم می‌یابد، اما به نحوی که فناوری و شرکت‌های سازنده آن را تابع جوامع دموکراتیک و توانایی جمعی ما برای تعیین سرنوشت‌مان می‌کند.



فصل اول
نظارت الکترونیک
چاشنی سه ساعته

ششم ژوئن ۲۰۱۳ بود. در شهر «ردموند» ایالت واشنگتن خورشید اوایل تابستان از پشت ابرها درمی‌آمد که «دومینیک کار» (Dominic Carr) در دفتر طبقه پنجمش در مجموعه مایکروسافت پرده کرکره‌ای را کمی بیشتر باز کرد. هرچند در شرق آمریکا هنوز یک ماه تا گرم‌شدن هوا و تابستان واقعی مانده، اما تابش آفتاب از پنجره نوید روزهای گرم‌تر (و کاهش سرعت کار) را می‌داد.

دومینیک تلفن همراهش را برداشت و به سمت آسانسور رفت تا ساندویچی از رستوران شرکت در ساختمان کناری بخرد. در حالی که از مسیر شلوغ بین ساختمان‌ها عبور می‌کرد، تلفنش که در جیب پشتی‌اش است، زنگ خورد. دومینیک مدیر تیم روابط عمومی و ارتباطاتی بود که به من گزارش می‌دادند و برخی از پردردسرترین مسائل شرکت در ارتباط با رسانه‌ها را مدیریت می‌کردند. همیشه تلفنش همراهش بود و به‌ندرت خیلی از میزش دور می‌شد.

اعلان ایمیلی با عنوان «مایکروسافت/پریزم» صفحه نمایش را روشن کرد. در آن زمان «پریزم» عنوان گردهمایی سالانه رهبران فروش شرکت بود. به نظر می‌رسید اطلاع‌رسانی روزمره‌ای در مورد کارهای روزانه شرکت باشد.

اما این ایمیل به هیچ‌وجه روزمره و عادی نبود. چاشنی سه‌ساعته بمبی خبری بود که اگر خنثی نمی‌شد، به‌زودی صدایش را در سراسر دنیا می‌شنیدند.

ایمیل این‌طور شروع می‌شد: «این پیام را فرستاده‌ایم تا به شما اعلام کنیم گاردین در حال آماده‌سازی مقاله‌ای در مورد پریزم، برنامه مخفی همکاری چند شرکت بزرگ فناوری ایالات متحده با آژانس امنیت ملی است. قصد داریم این مقاله را امشب منتشر کنیم.»

ایمیل را دومینیک دیگری، «دومینیک روش» (Dominic Rushe)، خبرنگار روزنامه بریتانیایی گاردین نوشته بود. ابتدا به ایمیل یکی از مدیران روابط عمومی مایکروسافت در بوستون فرستاده شده بود و او هم با برچسب «هشدار قرمز» برای ما ارسال کرده بود؛ برچسبی که یعنی «همین حالا باید این ایمیل را بخوانید».

پیام شامل فهرست ۹ماده‌ای پیچیده‌ای بود که از ما خواسته بود در موردشان توضیح بدهیم و مهلتی تعیین کرده بود که پاسخگویی به آن را غیرممکن می‌کرد. «دومینیک

روش» توضیح داده بود که «به‌عنوان خبرنگاران متعهد علاقه‌مندیم به شما این فرصت را بدهیم که به هر گونه اشتباه ویژه موجود در مواد بالا پاسخ بدهید. پیش از این با کاخ سفید هم در مورد این مقاله ارتباط برقرار کرده‌ایم. با توجه به ماهیت حساس این برنامه زودتر از این نمی‌توانستیم برای پاسخگویی با شما تماس بگیریم.» او خواسته بود پاسخ‌مان را حداکثر تا ساعت شش بعدازظهر به وقت منطقه زمانی شرقی یا سه بعدازظهر به وقت سیاتل ارسال کنیم.

گاردین اسناد اطلاعاتی محرمانه‌ای را به دست آورده بود که نشان می‌داد ظاهراً ۹ شرکت فناوری آمریکایی (شامل مایکروسافت، یاهو، گوگل، فیس‌بوک، پل‌تاک، یوتیوب، اسکایپ، ای‌اوال و اپل) با برنامه‌ای داوطلبانه به نام پریزم موافقت کرده‌اند که دسترسی مستقیم به ایمیل، چت، ویدئو، عکس، جزئیات فعالیت در شبکه‌های اجتماعی و سایر داده‌ها را به آژانس امنیت ملی می‌دهد.

برنامه‌های دومینیک برای ناهار (و بیشتر روزهای آینده) لغو شدند. از وسط راه چرخید، پله‌ها را دو تا یکی کرد و به طبقه پنجم برگشت. حدس می‌زد این مسئله به مقاله مسئله‌سازی ربط دارد که گاردین آن روز صبح منتشر کرده بود. این روزنامه دستور محرمانه دادگاهی را منتشر کرده بود که غول مخابراتی آمریکایی ورایزون را ملزم کرده بود «به‌صورت مستمر و روزانه» سوابق تماس‌های داخلی ایالات متحده و تماس‌های بین ایالات متحده و سایر کشورها را به مسئولان دولتی تحویل دهد. این سوابق را آژانس امنیت ملی تحلیل می‌کرد که ساختمان مرکزی‌اش در شهر «فورت مید» ایالت مریلند قرار داشت و مدت‌ها مشغول شنود الکترونیکی و جمع‌آوری داده‌ها از سراسر جهان بود. در این مقاله آمده بود که در فرایند جمع‌آوری اطلاعات، انبوه میلیون‌ها آمریکایی هم، صرف‌نظر از اینکه خطایی کرده بودند یا خیر، هدف قرار گرفته بودند.

اگر در مایکروسافت فردی از پریزم خبر داشت، آن فرد حتماً «جان فرنک» بود. او مسئول تیمی حقوقی بود که به کارهای امنیت ملی مربوط به شرکت می‌پرداخت. دومینیک به‌سرعت به دفتر جان رفت.

جان که همواره فرد دقیق و قاعده‌مندی است، به‌آهستگی پیام گاردین را که از روی تلفن دومینیک می‌خواند، هضم کرد. عینکش را برداشت، به صندلی‌اش تکیه داد و

به آسمان آفتابی خیره شد. ناگهان خستگی در ظاهرش نمایان شد؛ «این گزارش به هیچ‌وجه منطقی نیست. هیچ‌کدام از این اطلاعات درست به نظر نمی‌رسند.»

جان نه‌تنها می‌دانست شرکت کدام درخواست‌های مجریان قانون را بررسی کرده و پاسخ داده و چگونه در این زمینه عمل کرده است؛ بلکه خودش در طراحی فرایند پاسخگویی هم کمک کرده بود. مایکروسافت داده‌های مشتریان را فقط در پاسخ به فرایند قانونی معتبر و در مورد حساب یا فرد مشخص‌شده در هر حکم تحویل می‌داد. در واقع رویه‌ای برای تحویل اطلاعات انبوه وجود نداشت.

وقتی جان و دومینیک به اتاقم رسیدند، اطلاعات آنچنان بیشتری از پیام خبرنگار نداشتند که با من در میان بگذارند. جان گفت: «اگر آنها این کار را می‌کنند، بدون اطلاع ماست.»

ملزم بودیم که درخواست‌ها برای تحویل داده‌های کاربران را طبق قانون بررسی کنیم و به آنها پاسخ بدهیم. فرایند تعریف‌شده‌ای برای بررسی و پاسخگویی بادقت به همه درخواست‌های داده مجریان قانون داشتیم. اما مایکروسافت شرکت بزرگی است. آیا ممکن بود کار کارمندی خودسر باشد؟

این پرسشی بود که خیلی زود رد شد؛ چراکه از سیستم‌های مهندسی و فرایند دریافت، بررسی و پاسخگویی به درخواست‌های دولتی آگاه بودیم. یادداشت گاردین با شواهد سازگار نبود.

در مایکروسافت هیچ‌کس اسم پریزم را نشنیده بود. گاردین حاضر نبود اسناد افشاشده‌ای را به ما بدهد که مقاله را بر اساس آنها نوشته بود. با افرادی که در کاخ سفید می‌شناختیم، تماس گرفتیم. آنها هم حاضر نبودند در مورد اطلاعات «محرمانه» صحبت کنند. همین‌طور که بعدازظهر می‌گذشت، به شوخی به جان و دومینیک گفتم: «شاید عضوی از گروهی مخفی هستیم که آن‌قدر مخفی است که خودمان هم نمی‌دانیم عضو آن هستیم.»

باید صبر می‌کردیم مقاله منتشر شود و تازه بعد از آن شروع به پاسخگویی به آن خبرنگار کنیم.

گاردین ساعت سه بعدازظهر به وقت منطقه زمانی اقیانوس آرام بمب خبری‌اش

را منتشر کرد: «برنامه پریزم آژانس امنیت ملی به داده‌های کاربران اپل، گوگل و شرکت‌های دیگر دسترسی دارد.» تازه فهمیدیم پریزم، برنامه نظارت الکترونیکی آژانس امنیت ملی، مخفف «ابزار برنامه‌ریزی برای یکپارچه‌سازی، همگام‌سازی و مدیریت منبع» است. چه کسی چنین عبارت قلمبه‌سلمبه‌ای به ذهنش رسیده بود؟ اگر نمی‌دانستیم چیست، فکر می‌کردیم محصول بدی است که بخش فناوری آن را توسعه داده است. طبق اطلاعات این رسانه خبری پریزم برنامه نظارت الکترونیکی برای رصد دستگاه‌های موبایل، تماس‌ها، ایمیل‌ها، گفت‌وگوهای آنلاین، عکس‌ها و ویدئوها بود.

مقاله گاردین و گزارش مشابهی از واشنگتن‌پست در عرض چند ساعت در سراسر دنیا بازتاب پیدا کردند. سیلی از تماس‌های مشتریان روانه تیم‌های فروش و وکلایمان شد.

همه پرسش یکسانی داشتند؛ «خبر درست است؟»

ابتدا مشخص نبود که این رسانه اطلاعاتش را از کجا می‌گیرد. افراد در مورد واقعی و معتبر بودن یا نبودن این اطلاعات بحث می‌کردند، اما سه روز بعد گاردین بمب خبری بزرگ دیگری تقریباً به اندازه همان گزارش‌ها منتشر کرد. این روزنامه منبع اطلاعات را به درخواست خودش افشا کرد. آن منبع ادوارد اسنودن، کارمند ۲۹ساله شرکت «بوز آلن همیلتون» (Booz Allen Hamilton)، یکی از پیمانکاران وزارت دفاع بود. اسنودن در مرکز عملیات‌های تهدید (Threat Operations Center) آژانس امنیت ملی در هاوایی به‌صورت قراردادی به‌عنوان مدیر سیستم‌های کامپیوتر مشغول به کار بود. او بیش از یک میلیون سند بسیار محرمانه را دانلود کرده و ۲۰ مه ۲۰۱۳ سوار هواپیمایی به مقصد هنگ‌کنگ شده بود. در آنجا با خبرنگارانی از گاردین و واشنگتن‌پست تماس گرفته و شروع به انتشار اطلاعات پنهان آژانس امنیت ملی برای مردم جهان کرده بود.

تابستان و پاییز آن سال اسناد اسنودن به مجموعه‌ای از مقالات خبری تبدیل شدند. اولین سند افشاشده پاورپوینتی محرمانه با ۴۱ اسلاید بود که برای آموزش کارمندان امنیتی استفاده می‌شد. اما آن سند تازه آغاز کار بود. خبرنگاران انتشار فایل‌های محرمانه اسنودن را تا سال بعد ادامه دادند و با موجی پیاپی از تیترها، آتش نگرانی

و دلهره را برافروخته نگه داشتند. با طرح ادعاهایی مبنی بر اینکه دولت‌های ایالات متحده و بریتانیا به سوابق تلفن و داده‌های کاربران و از جمله اطلاعات رهبران خارجی و میلیون‌ها آمریکایی بی‌گناه دسترسی دارند، موج عظیمی از بی‌اعتمادی عمومی شکل گرفت.

این اخبار خشم مردم را برانگیخت؛ خشمی که کاملاً منطقی و موجه بود. این گزارش‌ها در تضاد با حقوق حفاظت از حریم خصوصی در جوامع دموکراتیک بود که افراد به مدت بیش از دو قرن آن را بدیهی پنداشته بودند. این حقوق که ما برای حفاظت از اطلاعات شما در مرکز داده کوئینسی به آنها اتکا داریم، در پی اعتراضات شدید خیابان‌های لندن در قرن هجدهم پایه‌گذاری شدند. این توفان سیاسی را فردی به نام «جان ویلکس» (John Wilkes) آغاز کرد که خودش در پارلمان حضور داشت.

می‌توان گفت جان ویلکس پرماجراترین (و تندروترین) سیاست‌مدار زمانه خودش بود. در دهه ۱۷۶۰ نه‌تنها نخست‌وزیر؛ بلکه حتی شاه را هم با سخنانی به چالش کشید و شرمنده کرد که برخی از سیاست‌مداران امروز را هم (تقریباً) شرمنده می‌کند. ویلکس در آوریل ۱۷۶۳ در نشریه‌ای مخالف نقدی ناشناس نوشت. این مقاله عصبانیت «چارلز یورک»، دادستان کل بریتانیا را برانگیخت که حدس می‌زد نویسنده مطلب ویلکس است. طولی نکشید که دولت حکم تفتیش بسیار گسترده‌ای صادر کرد که به مأموران اجرای قانون اجازه می‌داد تقریباً هر مکانی را در هر زمانی تفتیش کنند.

با ناموجه‌ترین اطلاعات نیمه‌شب به خانه چاپخانه‌داری وارد شدند، او را از بستر خواب در کنار همسرش بردند، همه اوراق شخصی‌اش را ضبط کردند و ۱۴ کارگر و خدمتکار را دستگیر کردند. مراجع قدرت بریتانیا به‌سرعت چهار خانه دیگر را هم تفتیش و در مجموع ۴۹ نفر را دستگیر کردند که تقریباً همه بی‌گناه بودند. درها را تخریب کردند، صندوق‌های درشکه‌ها را تفتیش کردند و صدها قفل را شکستند. سرانجام آن‌قدر مدرک به دست آوردند تا مردی را دستگیر کنند که می‌خواستند؛ جان ویلکس بازداشت شد.

ویلکس از آن آدم‌هایی نبود که زود تسلیم شود. در عرض یک ماه چندین شکایت ثبت کرد و به دادگاه رفت تا قدرتمندترین مسئولان مملکت را به چالش بکشد. این

اقدامات آنچنـان عجیب نبودند، امـا آنچه در ادامه اتفـاق افتاد، طبقه حاکـم و به‌ویژه دولت را غافلگیـر کرد. دادگاه‌هـا به نفع ویلکـس رأی دادنـد. دادگاه‌ها با پایـان‌دادن به قدرتی که قرن‌ها پادشاه و زیردستانش از آن استفاده می‌کردند، حکم دادند که مراجع قدرت برای تفتیش باید شـواهد و ادله محکم‌تری داشته باشـند و حتی در این صورت هم باید این کار را به سبک و روشی محدودتر انجام دهند. مطبوعات بریتانیا این احکام را سـتودند و به این عبارت معروف اشـاره کردند که «خانه هر انگلیسـی قلعه اوسـت و قاصدان سرکش پادشاه حق ندارند آن را تفتیش یا در اوراقش فضولی کنند».

شـکایت‌های جان ویلکـس از جهـات مهمـی شـروعی بـرای پیدایش حقـوق حریم خصوصی مدرن بودند. این حقوق مایه حسرت انسان‌های آزاد، از جمله بریتانیایی‌های مستعمره‌نشین سـاکن آمریکای شـمالی بود. آنها تنها دو سـال پیش نزاعی به همین انـدازه شـدید را در نیوانگلند دنبـال کرده و شکسـت خـورده بودند. در آن زمـان «جان آدامز» در بیست‌وچندسـالگی و در حالی که هنوز وکیل نشـده بـود، در انتهای صحن دادگاهی در بوسـتون می‌نشسـت تا یکی از بزرگ‌تریـن رویارویی‌های حقوقـی این قاره را در اوایـل دهـه ۱۷۶۰ تماشـا کند. «جیمـز اوتیس پسـر»، یکـی از پرشـورترین وکلای ماساچوسـت اعتراض کرده بـود که سـربازان بریتانیایی از همان روشـی از قدرت‌شـان استفاده می‌کنند که ویلکس به آن معترض بود. وقتی بازرگانان محلی کالاهای وارداتی را بـدون پرداخت مالیاتی قاچاق می‌کردنـد که ناعادلانه می‌دانسـتند، بریتانیایی‌ها در واکنش از احکام به‌اصطـلاح عمومی اسـتفاده می‌کردند تا خانه به خانـه بروند و بدون هیچ مدرک خاصی به‌دنبال تخلفات گمرکی بگردند.

اوتیس اسـتدلال کرده بـود که ایـن کار نقض اساسـی آزادی‌های مدنی اسـت و آن را «بدترین جلوه قدرت اسـتبدادی» خوانده بود. هرچند اوتیس در این پرونده شکست خورد، اما سـخنانش اولین گام برای حرکت مستعمره‌نشـین‌ها به سمت شورش شد. آدامز حتـی در اواخر عمـرش همچنان حرف‌هـای اوتیـس در دادگاه را به یـاد می‌آورد و نوشته بود این سـخنان «نیروی حیات را در کالبد این کشور دمید». تا روز مرگش گفته بود آن روز، آن پرونده، آن دادگاه و آن مسئله بود که ایالات متحده را در مسیر استقلال قرار داد.

باید ۱۳ سال از اعلامیه استقلال ایالات متحده می‌گذشت تا افراد، اصلی را درک کنند که اوتیس آنچنان پرشور از آن دفاع کرده بود. آن زمان یعنی سال ۱۷۸۹ پیگیری این مسئله به نیویورک و تشکیل جلسه اولین کنگره ایالات متحده در وال‌استریت رسیده بود. «جیمز مدیسون» در پیشگاه مجلس نمایندگان ایستاد و منشور پیشنهادی حقوق ایالات متحده را ارائه داد. این طرح شامل موادی بود که به متمم چهارم قانون اساسی تبدیل شد و تضمین می‌کرد که شهروندان آمریکایی در برابر «تفتیش و ضبط غیرمنطقی افراد، املاک، اوراق و اموال‌شان» از سوی دولت و از جمله استفاده از احکام عمومی مصون خواهند بود. بعد از آن مراجع قدرت برای گرفتن حکم تفتیش خانه یا دفتر کار باید به قاضی مستقلی مراجعه می‌کردند و شواهد و ادله کافی ارائه می‌دادند. در عمل یعنی دولت باید به قاضی نشان می‌داد مدارکی وجود دارد که باعث می‌شود «فردی با ادراک منطقی» به این عقیده برسد که فرد یا افرادی در حال ارتکاب جرم هستند.

اما آیا این حراست اطلاعاتی را هم دربر می‌گیرد که از خانه فرد خارج می‌شود؟ وقتی «بنجامین فرانکلین» اداره پست را تأسیس کرد، متمم چهارم در بوته این آزمایش قرار گرفت؛ وقتی نامه‌ای می‌فرستید، پاکت را مهر می‌کنید و به عامل دولت می‌دهید. دیوان عالی در قرن نوزدهم به‌راحتی حکم داد که افراد در مورد نامه‌های مهروموم‌شده نیز دارای حق حریم خصوصی هستند. در نتیجه متمم چهارم شامل نامه‌ها هم می‌شود و هرچند اداره پست پاکت‌های نامه را در اختیار دارد، اما نمی‌تواند بدون حکم تفتیش صادرشده بر اساس شواهد و ادله کافی پاکتی را باز کند.

دادگاه‌ها در طول قرن‌ها به این موارد توجه کردند که آیا «انتظار افراد برای حفظ حریم خصوصی منطقی است» و وقتی فرد اطلاعاتش را نزد دیگری نگهداری می‌کند، چه تفسیری می‌توان از این انتظار منطقی ارائه کرد. به بیان ساده اگر اطلاعات در جایی مثل محفظه ذخیره‌سازی قفل‌شده‌ای نگهداری می‌شد و کلید آن در دسترس دیگران نبود، قاضی‌ها نتیجه می‌گرفتند که چنین انتظاری منطقی است و مشمول متمم چهارم می‌شود. اما اگر فرد اسنادش را در جعبه‌ای از پرونده‌ها نگهداری می‌کرد که در کنار جعبه‌های دیگران قرار داشت و افراد می‌توانستند به‌راحتی رفت‌وآمد کنند، پلیس

نیازی به حکم تفتیش نداشت؛ زیرا دادگاه‌ها نتیجه‌گیری کرده بودند که در این شرایط طبق متمم چهارم انتظار منطقی برای حفظ حریم خصوصی وجود ندارد.

به نظر می‌رسد مراکز داده حفاظت‌شده امروز با لایه‌های امنیت فیزیکی و دیجیتال فراوان، کاملاً با شرایط محفظه نگهداری قفل‌شده مطابقت دارند.

در تابستان ۲۰۱۳ خبرنگاران پی‌درپی و با توجه به اسناد محرمانه افشاشده جدید برای پیگیری ماجرای اسنودن به ما مراجعه می‌کردند. اتفاقی مدام تکرار می‌شد؛ هر وقت می‌دیدم دومینیک در اتاق جان حضور دارد، می‌دانستم قرار است مقاله دیگری منتشر شود. بیشتر اوقات نمی‌دانستیم گزارشی که به آن پاسخ می‌دهیم، چه محتوایی دارد. دومینیک می‌گوید: «آن چند هفته اول تقریباً هر روز گفت‌وگویی یکسان را با خبرنگاران مختلف تکرار می‌کردم. می‌گفتند دومینیک بالأخره این وسط یکی دروغ می‌گوید، مایکروسافت یا ادوارد اسنودن.»

گزارش گاردین در مورد پریزم فقط یکی از بخش‌های مقاله‌ای بلندتر در مورد تلاش‌های آژانس امنیت ملی برای به دست آوردن داده‌ها از بخش خصوصی بود. همان‌طور که اسناد خارج‌شده از طبقه‌بندی محرمانه با جزئیات زیاد نشان می‌دهند، این سازمان پس از فاجعه ۱۱ سپتامبر ۲۰۰۱ به‌دنبال مشارکت‌های داوطلبانه با بخش خصوصی بود تا داده‌های کاربران را خارج از فرایند احضاریه و حکم قانونی جمع‌آوری کند.

مایکروسافت مانند سایر شرکت‌های فناوری برجسته با این مسئله کلنجار می‌رفت که داوطلبانه چنین داده‌هایی را در اختیار دولت بگذارد یا خیر. وقتی در داخل شرکت در مورد این پرسش‌ها بحث می‌کردیم، شرایط ژئوپلیتیک آن زمان را هم در نظر داشتیم. حملات ۱۱ سپتامبر بر کشور سایه افکنده بود. نیروهای ائتلاف «عملیات آزادی بلندمدت» (Operation Enduring Freedom) را در افغانستان آغاز کرده بودند، کنگره از اشغال عراق پشتیبانی می‌کرد و مردم نگران آمریکا خواستار تلاش‌های مقتدرانه‌تری علیه تروریسم بودند. شرایط عادی نبود و همان‌طور که بسیاری از افراد می‌گفتند، نیازمند واکنشی بی‌سابقه بود.

اما رویکردی که از شرکت‌ها می‌خواست اطلاعاتی مثل اطلاعات توصیف‌شده در

گزارش‌های خارج‌شده از طبقه‌بندی محرمانه را داوطلبانه تحویل دهند، یک مشکل اساسی داشت؛ داده‌های درخواستی آژانس امنیت ملی متعلق به شرکت‌های فناوری نبود، به مشتریان تعلق داشت و شامل برخی از خصوصی‌ترین اطلاعات آنها می‌شد.

مانند برنامه پریزم، تلاش‌های آژانس امنیت ملی بعد از ۱۱ سپتامبر برای جمع‌آوری داوطلبانه اطلاعات مشتریان از بخش خصوصی نیز پرسشی بنیادین را مطرح می‌کرد؛ اینکه چطور می‌توانیم هم به مسئولیت‌مان در قبال مشتریان عمل کنیم و هم وظیفه‌مان برای حفاظت از کشور را به جا آوریم؟

از نظر من پاسخ روشن بود. قانون باید بر این مسئله حاکم می‌بود. در کشور ایالات متحده در همه مسائل قانون حاکم است. اگر دولت ایالات متحده سوابق مشتریان ما را می‌خواست، باید از قوانین کشور پیروی می‌کرد و برای این کار از دادگاه حکم می‌گرفت و اگر مسئولان قوه مجریه فکر می‌کردند قانون به اندازه کافی مؤثر نیست، می‌توانستند به کنگره مراجعه کنند و قدرت بیشتری بخواهند. روال کار در حکومت جمهوری دموکراتیک باید به این صورت باشد.

هرچند در سال ۲۰۰۲ نمی‌توانستیم ادوارد اسنودن و پرواز معروفش را پیش‌بینی کنیم، اما می‌توانستیم به تاریخ بنگریم تا پیش‌بینی کلی‌تری از آینده داشته باشیم. قربانی‌کردن آزادی‌های فردی در برابر امنیت ملی در زمان وقوع بحران ملی مسئله جدیدی نبود.

اولین بحران آمریکا از این نوع کمی بیشتر از یک دهه بعد از تصویب قانون اساسی رخ داد. سال ۱۷۹۸ بود که در دریای کارائیب «شبه‌جنگی» بین ایالات متحده و فرانسه در گرفت. فرانسوی‌ها می‌خواستند به ایالات متحده فشار بیاورند تا وام‌هایی را بازپرداخت کند که پادشاه سرنگون‌شده فرانسه داده بود، پس بیش از ۳۰۰ کشتی تجاری آمریکا را ضبط کردند و در ازای آزادی آنها باج خواستند. برخی آمریکایی‌های خشمگین خواستار جنگی تمام‌عیار بودند. افراد دیگری مثل رئیس‌جمهور «جان آدامز» فکر می‌کردند این کشور تازه‌تأسیس حریف فرانسوی‌ها نمی‌شود. آدامز که می‌ترسید این بحث‌های عمومی سم مهلکی برای این حکومت نوپا شود، تلاش کرد با امضای مجموعه‌ای متشکل از چهار قانون، مخالفان را ساکت کند. این چهار قانون

به‌عنوان «قوانین بیگانگان و فتنه‌انگیزی» (Alien and Sedition Acts) شناخته شدند. این قوانین به دولت اجازه می‌دادند که خارجی‌های «خطرناک» را زندانی یا از کشور اخراج کند و انتقاد از دولت را جرم می‌شمردند.

تقریباً ۶۰ سال بعد، در دوران جنگ داخلی، ایالات متحده دوباره یکی از اصول کلیدی دموکراسی این کشور را کنار گذاشت. در آن زمان «آبراهام لینکلن»، رئیس‌جمهور وقت، چند بار قرار احضار زندانی را تعلیق کرد تا شورشی‌های مؤتلفه را سرکوب کند. لینکلن برای اعمال قانون خدمت اجباری در ارتش این تعلیق را گسترش داد و حق محاکمه منصفانه را در سراسر کشور تعلیق کرد. در دوران جنگ داخلی در مجموع ۱۵ هزار نفر از مردم آمریکا بدون برگزاری دادگاه زندانی شدند.

در سال ۱۹۴۲ کمی بعد از بمباران «پرل هاربر»، رئیس‌جمهور «فرانکلین روزولت» تحت تأثیر ارتش و نظر مردم فرمانی اجرایی را امضا کرد که ۱۲۰ هزار نفر از آمریکایی‌های ژاپنی‌تبار را روانه اردوگاه‌های دورافتاده‌ای می‌کرد که در حصار سیم خاردار و نگهبانان مسلح بودند. دوسوم از افراد زندانی در ایالات متحده به دنیا آمده بودند. وقتی سه سال بعد این فرمان لغو شد، بیشتر آنها خانه، مزرعه، کسب‌وکار و جامعه‌شان را از دست داده بودند.

هرچند کشور در بحبوحه بحران ملی، این بی‌عدالتی‌ها را پذیرفته بود، اما مردم آمریکا بعدها به هزینه‌ای که برای امنیت جامعه داده شده بود، با تردید نگاه کردند. در ذهن من پرسش اصلی این بود که «۱۰ سال بعد وقتی دیگر شرایط کنونی حاکم نباشد، چطور قضاوت خواهیم شد؟ آیا می‌توانیم بگوییم به تعهدمان به مشتریان احترام گذاشته‌ایم؟»

وقتی سؤال مشخص شد، پاسخ روشن بود. نمی‌توانیم بدون آنکه فرایند قانونی معتبر طی شود، داده‌های مشتریان را داوطلبانه تحویل دهیم. به‌عنوان ارشدترین وکیل شرکت، باید مسئولیت این موضع را می‌پذیرفتم (و هر گونه انتقاد را تحمل می‌کردم). در هر حال مگر کسی بهتر از وکلا برای دفاع از حقوق مشتریان‌مان وجود دارد؟

در این شرایط تقریباً همه شرکت‌های فناوری برجسته در تابستان سال ۲۰۱۳ در حالت تدافعی قرار گرفتند. ناراحتی‌مان را به اطلاع مسئولان کشور در واشنگتن دی‌سی

رساندیم. لحظه‌ای تاریخی بود و تضادهایی را آشکار کرد که در شکاف میان دولت‌ها و بخش فناوری تا امروز نقش داشته‌اند. دولت‌ها به رأی‌دهندگانی خدمت می‌کنند که در جغرافیایی تعریف‌شده، برای مثال یک ایالت یا کشور، زندگی می‌کنند. اما فناوری جهانی شده و ما تقریباً از همه جای دنیا مشتری داریم.

ابر علاوه بر ایجاد تغییر در مکان و دریافت‌کنندگان خدمات‌مان، رابطه‌مان با مشتریان را هم بازتعریف کرده است. ابر شرکت‌های فناوری را به مؤسساتی تبدیل کرده که از جهاتی شبیه بانک‌ها هستند. افراد پول‌شان را نزد بانک می‌گذارند و نزد شرکت‌های فناوری خصوصی‌ترین اطلاعات‌شان (ایمیل‌ها، عکس‌ها، اسناد و پیام‌های متنی) را ذخیره می‌کنند.

این رابطه جدید پیامدهایی هم ورای بخش فناوری دارد. درست همان‌طور که مسئولان در دهه ۱۹۳۰ به این جمع‌بندی رسیدند که بانک‌ها آن‌قدر برای اقتصاد مهم شده‌اند که نمی‌توان رگوله‌نشده رهایشان کرد، امروزه شرکت‌های فناوری هم آن‌قدر مهم شده‌اند که نمی‌توان با رویکرد سیاست عدم مداخله با آنها برخورد کرد. باید تابع حاکمیت قانون و رگولیشن فعال‌تر باشند. اما دامنه فعالیت شرکت‌های فناوری امروز بر خلاف بانک‌های دهه ۱۹۳۰ جهانی است که مسئله رگولیشن را بسیار پیچیده‌تر می‌کند.

با افزایش نارضایتی مشتریان سراسر جهان در سال ۲۰۱۳ متوجه شدیم بدون ارائه توضیحات بیشتر به هیچ‌وجه نمی‌توانیم به نگرانی‌هایشان پاسخ بدهیم. از محدودیت‌های روشنی که در مورد خدمات خودمان وضع کرده بودیم و کارهای گاهی اوقات پیچیده، برای پرداختن به ایرادهای شیوه‌های از پیش موجود در شرکت‌هایی که خریده بودیم، کاملاً آگاهی داشتیم. می‌خواستیم توضیح بدهیم که اطلاعات مشتریان را تنها در پاسخ به احکام تفتیش، احضاریه‌ها و دستورات امنیت ملی تحویل داده‌ایم، اما وقتی پیشنهادمان برای اطلاع‌رسانی عمومی این مطالب را مطرح کردیم، وزارت دادگستری به ما اعلام کرد که این اطلاعات محرمانه هستند و نمی‌توانیم منتشرشان کنیم. احساس ناامیدی و درماندگی بر ما غالب شد.

تصمیم گرفتیم کاری کنیم که تا به حال انجام نداده بودیم؛ می‌خواستیم از دولت ایالات

متحده شکایت کنیم. به‌عنوان شرکتی که یک دهه دعوی قضایی ضدانحصار در برابر دولت را با موفقیت پشت سر گذاشته و یک دهه وقت گذاشته بود تا با دولت به صلح برسد، در آستانه ورود به مسیری بودیم که راه برگشتی نداشت. دادخواستی را در دادگاه نظارت بر اطلاعات خارجی (FISC-Foreign Intelligence Surveillance Court) مطرح کردیم که ابتدا پنهان نگه داشته شد.

دادگاه نظارت بر اطلاعات خارجی، دادگاهی ویژه است که برای بررسی دستورات نظارتی دولت تأسیس شده است. این دادگاه در طول جنگ سرد ایجاد شد تا برای شنودهای تلفنی، جمع‌آوری داده‌های الکترونیکی و نظارت بر تروریست‌ها و جاسوس‌های احتمالی مجوز صادر کند. فعالیت‌های این دادگاه بسیار محرمانه است تا از اقدامات اطلاعاتی برای نظارت بر تهدیدهای امنیتی و برطرف‌کردن آنها محافظت شود. هر حکمی که تحت قانون نظارت بر اطلاعات خارجی (Foreign Intelligence Surveillance Act) صادر می‌شود، همراه با دستور منع انتشار است که ما را از اطلاع‌رسانی به مشتری در مورد دریافت حکم برای داده‌هایش منع می‌کند. هرچند این موضوع قابل درک بود، اما پرونده حقوقی ما تصریح می‌کرد که بر اساس متمم اول قانون اساسی و الزام آن به آزادی اظهارنظر، این حق را داریم که اطلاعات کلی‌تر را با مردم به اشتراک بگذاریم. استدلال کردیم که دست‌کم این حق را داریم که در مورد تعداد و انواع دستوراتی که گرفته‌ایم، اطلاع‌رسانی کنیم.

کمی بعد فهمیدیم که گوگل هم همین کار را کرده است. این مسئله به نقطه‌عطف دیگری منجر شد. پنج سال بود که اختلافات‌مان را نزد رگولاتورهای سراسر دنیا مطرح می‌کردیم. گوگل در حمایت از اعمال محدودیت بر ویندوز استدلال می‌کرد. مایکروسافت هم در حمایت از اعمال محدودیت بر جست‌وجوهای گوگل استدلال می‌کرد. به‌خوبی یکدیگر را می‌شناختیم. احترام زیادی برای «کنت واکر»، رئیس اداره حقوقی گوگل قائل بودم، اما هیچ‌کس نمی‌توانست بگوید رفقای صمیمی هستیم.

به یکباره در مبارزه‌ای جدید و مشترک در برابر دولت خودمان در یک طرف قرار گرفته بودیم. تصمیم گرفتم با کنت تماس بگیرم و پیشنهاد همکاری بدهم. ابتدا به تبادل پیام اقدام کردم و به نتیجه‌ای نرسیدم. در یکی از صبح‌های ماه جولای در حالی که از

گردهمایی با کارمندان در یکی از ساختمان‌های تیم «ایکس‌باکس» خارج می‌شدم، تلفنم را از جیبم درآوردم تا دوباره تلاش کنم. به‌دنبال گوشه‌ای خلوت گشتم و به سمت ماکتی مقوایی و در اندازه واقعی از «مستر چیف» (Master Chief) رفتم. شخصیت خیالی مستر چیف سربازی است که در بازی «هیلو» (Halo) رهبری سربازان را در جنگ علیه ارتش موجودات فضایی بر عهده دارد. حس خوبی داشتم، احساس می‌کردم مستر چیف هوایم را دارد.

کنت تلفن را جواب داد. هرچند قبلاً زیاد با هم صحبت کرده بودیم، بحث‌مان تقریباً همیشه به شکایت‌های شرکت‌هایمان از یکدیگر مربوط می‌شد، اما اکنون پیشنهاد متفاوتی داشتم. گفتم «بیا متحد شویم و ببینیم می‌توانیم با هم با وزارت دادگستری مذاکره کنیم».

اگر کنت فکر می‌کرد این پیشنهاد نوعی فریب است، سرزنشش نمی‌کردم، اما حرفم را شنید و فردای آن روز به سراغم آمد و گفت مایل به همکاری است.

تماسی مشترک با دولت برقرار کردیم تا در مورد توافقی مشترک مذاکره کنیم. به نظر می‌رسید به توافق نزدیک می‌شویم، اما در اواخر آگوست مذاکرات ناگهان با شکست به پایان رسید. احساس می‌کردیم آژانس امنیت ملی و اف‌بی‌آی در این زمینه هم‌عقیده نیستند. در اواخر تابستان و اوایل پاییز ۲۰۱۳، افشاهای ادامه‌دار اسنودن شکافی عمیق‌تر بین دولت ایالات متحده و بخش فناوری ایجاد کرد و شرایط از بد هم بدتر شد.

واشنگتن‌پست ۳۰ اکتبر مقاله‌ای منتشر کرد که غافلگیری شدید صنعت فناوری را به‌دنبال داشت. عنوان مقاله این بود: «اسناد اسنودن نشان می‌دهند که آژانس امنیت ملی به ارتباطات مراکز داده یاهو و گوگل در سراسر دنیا نفوذ کرده است». یکی از نویسندگان این مقاله «بارت گلمن» بود؛ خبرنگاری که از زمانی او را می‌شناختم و به او احترام می‌گذاشتم که برای روزنامه دانشجویی «دیلی پرینستونین» در دانشگاه پرینستون می‌نوشت. آن موقع هر دو دانشجوی دوره کارشناسی این دانشگاه بودیم. در مقاله او آمده بود که آژانس امنیت ملی با کمک دولت بریتانیا مخفیانه به کابل‌های فیبر نوری زیردریایی دسترسی پیدا کرده تا داده‌های شبکه‌های یاهو و گوگل را کپی کند. هرچند نمی‌توانستیم مطمئن شویم که این سازمان کابل‌های ما را هم هدف قرار داده

یا خیر، اما اسناد اسنودن به خدمات ایمیل و پیام‌رسانی شخصی ما هم اشاره کرده بودند. این مسئله باعث شد شک کنیم که از ما هم شنود می‌کنند. تا امروز دولت‌های ایالات متحده و بریتانیا هک‌کردن کابل‌های داده ما را به‌صورت عمومی انکار نکرده‌اند.

بخش فناوری با ترکیبی از شگفتی و خشم به این گزارش واکنش نشان داد. این مقاله حلقه‌ای گم‌شده را فراهم می‌ساخت که به درک ما از اسناد اسنودن کمک می‌کرد. مقاله نشان می‌داد که داده‌های آژانس امنیت ملی بسیار بیشتر از آن است که به‌صورت قانونی و به واسطه دستورات امنیت ملی و احکام تفتیش ارائه کرده بودیم. اگر این گزارش واقعیت می‌داشت، دولت در عمل در حال تفتیش و ضبط اطلاعات خصوصی افراد در مقیاسی گسترده بود.

مقاله واشنگتن‌پست نشان می‌داد که آژانس امنیت ملی در همکاری با همتای بریتانیایی‌اش، احتمالاً بدون بررسی یا نظارت قضایی، در حال استخراج داده‌ها از کابل‌های مورد استفاده شرکت‌های فناوری آمریکایی است. نگران بودیم که این اتفاق در تقاطع ورودی کابل‌ها به بریتانیا در حال وقوع است. در حالی که وکلای سراسر صنعت فناوری در حال تبادل نظر بودند، به این فرضیه رسیدیم که آژانس امنیت ملی به خودش قبولانده که با همکاری با دولت بریتانیا یا اتکا به این کشور و فعالیت در خارج از مرزهای آمریکا، مشمول متمم چهارم قانون اساسی ایالات متحده نمی‌شود و در نتیجه الزامی ندارد که فقط مطابق با تشریفات قانونی و دستور دادگاه به تفتیش و ضبط اطلاعات بپردازد.

مایکروسافت و سایر شرکت‌های فناوری به‌سرعت واکنش نشان دادند. ما و سایر شرکت‌ها در هفته‌های بعد از انتشار مقاله اعلام کردیم که روی همه داده‌هایی که از طریق کابل‌های فیبر نوری بین مراکز داده جابه‌جا می‌شوند و همچنین داده‌هایی که در سرورهای مراکز داده خودمان ذخیره می‌شوند، رمزنگاری قدرتمندی را اجرا می‌کنیم. این کار گامی اساسی در حفاظت از مشتریان بود؛ چراکه در این صورت حتی اگر دولتی با نفوذ به کابل‌ها، داده‌های مشتریان را سرقت می‌کرد، تقریباً غیرممکن بود که بتواند داده‌ها را رمزگشایی کند و بخواند.

حرف‌زدن از این نوع پیشرفت‌ها در رمزنگاری خیلی آسان‌تر از عملی‌کردن آن بود.

این اقدامات شامل افزایش شدید بار کاری رایانش مراکز داده و مستلزم کار مهندسی بسیار زیاد بود. برخی رهبران مهندسی شرکت اشتیاقی برای انجام این کار نداشتند. نگرانی‌هایشان قابل درک بود. توسعه نرم‌افزار معمولاً شامل بده‌بستان در انتخاب قابلیت‌ها می‌شود؛ چراکه منابع مهندسی در دسترسی که می‌توان در چارچوب زمانی متناسب با پروژه به کار گرفت، محدود هستند. این پروژه رمزنگاری آنها را مجبور می‌کرد که توسعه سایر قابلیت‌های محصولی را که مشتریان می‌خواستند اضافه کنیم، به تأخیر بیندازند. بعد از مدتی بحث پویا و فعال، «استیو بالمر»، مدیرعامل وقت مایکروسافت و تیم رهبری ارشد تصمیم گرفتند با سرعت و عزم بیشتر پروژه رمزنگاری را به پیش ببرند. سایر شرکت‌های فناوری هم همین کار را انجام دادند.

نوامبر آن سال و در حالی که این اتفاقات می‌افتادند، رئیس‌جمهور باراک اوباما از سیاتل بازدید کرد. در جلسه‌ای برای جذب کمک‌های مالی شرکت کرده بود و کاخ سفید گروهی از رهبران و حامیان محلی را بعد از رویداد رسمی به میهمانی کوچکی در سوئیتی خصوصی در هتل «وستین سیاتل» دعوت کرده بود. من هم به‌عنوان نماینده مایکروسافت دعوت شده بودم.

امیدوار بودم در این موقعیت چنددقیقه‌ای فرصت نصیبم شود تا با رئیس‌جمهور درباره مسائلی حرف بزنم که در رابطه با متمم اول در شکایت‌مان مطرح کرده بودیم. اما وکلای وزارت دادگستری از ما خواسته بودند در مورد این پرونده با رئیس‌جمهور صحبت نکنیم. می‌گفتند «موکل‌شان» (یعنی دولت یا رئیس‌جمهور) وکیل دارد و همه گفت‌وگوها باید از طریق آنها انجام شود، اما کمی قبل از ورود رئیس‌جمهور اوباما به محل میهمانی از دستیارش، «ولری جرت» پرسیدم آیا اشکالی ندارد از رئیس‌جمهور پرسش متفاوتی بپرسم که به شکایت‌مان ربطی نداشت. می‌خواستم بپرسم فکر می‌کند تدابیر حفاظتی متمم چهارم در برابر تفتیش‌ها و مصادره‌های غیرمنطقی دولت، حتی خارج از ایالات متحده هم شامل شهروندان آمریکایی می‌شود یا خیر.

با توجه به گزارش واشنگتن‌پست درباره نفوذ آژانس امنیت ملی در کابل‌های مورد استفاده شرکت‌های آمریکایی در خارج از ایالات متحده، فکر می‌کردم این پرسش اهمیت ویژه‌ای دارد. ولری فکر می‌کرد این موضوع برای رئیس‌جمهور جالب باشد.

حق با او بود. وقتی با رئیس‌جمهور در این مورد صحبت می‌کردم، آن اوبامایی نمود پیدا کرد که سال‌ها استاد حقوق اساسی بود. هرچند رئیس‌جمهور به‌روشنی بیشتر از آنچه من به یاد داشتم، در حقوق اساسی تبحر داشت، اما آن‌قدر از این حوزه به خاطر می‌آوردم که بتوانم گفت‌وگوی آبرومندی داشته باشم.

اما بعد موضوع را عوض کرد.

رئیس‌جمهور پرسید: «شنیدم نمی‌خواهید در مورد شکایت‌تان با ما به توافق برسید. فکر می‌کنید اگر دیگران ببینند با دولت درافتاده‌اید، جلوه بهتری دارد. این‌طور است؟» از آن لحظاتی بود که محاسبات ذهنی فوری لازم داشت. بی‌شک وکلای وزارت دادگستری هرگز به ما نگفته بودند که به پرسش‌های مستقیم رئیس‌جمهور ایالات متحده جواب ندهیم، پس جواب دادم. توضیح دادم که ما می‌خواستیم توافق کنیم، اما به نظر می‌رسید دولت نمی‌خواهد. نگرانی‌هایمان را شرح دادم و گفتم معتقدیم اگر افراد مناسبی را دور هم جمع کنیم، می‌توانیم شاهد پیشرفت واقعی باشیم.

اوباما چند هفته بعد گروهی از رهبران فناوری را به کاخ سفید دعوت کرد. هشت روز تا کریسمس مانده بود و کارها در بال غربی کاخ سفید که به مناسبت سال نو تزئین شده بود، با شتاب زیادی به پیش می‌رفت؛ چراکه کارمندان عجله داشتند تا پیش از رفتن رئیس‌جمهور به تعطیلات سالانه‌اش در هاوایی، کارهای باقی‌مانده را به اتمام برسانند. کاخ سفید به‌صورت عمومی اعلام کرده بود که این جلسه در مورد «مسائل مربوط به سلامت، تدارکات فناوری اطلاعات و نظارت الکترونیکی» است. مانند این بود که به طرفداران بیس‌بال بگوییم به رویدادی می‌روید که شامل سرود ملی، مسابقه هات‌داگ‌خوری و اولین بازی لیگ جهانی بیس‌بال می‌شود. همه می‌دانستیم هدف اصلی‌مان از حضور در واشنگتن در آن صبح سرد زمستانی چیست.

گروهی بسیار برجسته از رهبران صنعت فناوری به بال غربی آمده بودند؛ افرادی مثل تیم کوک، مدیرعامل اپل؛ اریک اشمیت، رئیس هیئت‌مدیره گوگل؛ شریل سندبرگ، مدیر ارشد عملیات فیس‌بوک؛ رید هیستینگز، مدیرعامل نت‌فیلیکس و چندین نفر دیگر حضور داشتند. بیشتر ما همدیگر را می‌شناختیم. از میان حاضران ما و هفت شرکت دیگر (که تقریباً همه رقیب بودیم) به‌تازگی متحد شده بودیم تا با تشکیل

ائتلافی جدید بـه نام «اصـلاح نظارت دولتـی» در مورد همان مسـائلی همـکاری کنیم که امروز آمده بودیم در موردشـان بحث کنیم. بعد از احوال‌پرسی مشتاقانه تلفن‌های هوشمندمان را در راهرو در محفظه‌های مکعبی گذاشتیم و به اتاق روزولت رفتیم.

اتاق روزولت به افتخار نه یـک رئیس‌جمهور؛ بلکه دو رئیس‌جمهور نام‌گذاری شـده است؛ «تئودور روزولت» که بال غربی را ساخت و «فرانکلین روزولت» که آن را گسترش داد. در حالی که روی صندلی‌ام در پشت میز همایش بلند و صیقلی اتاق می‌نشستم، به نقاشی‌ای چشم دوختم که بالای شـومینه قرار داشت و پیش خود خندیدم. تصویر «تئودور روزولت» با لباس «سوارکاران سرسخت» (لقب اولین گروه سواره نظام داوطلب ایالات متحده که تئودور روزولت یکی از فرماندهانش بود) سوار بر اسب چموشش بود. امیدوار بودم این جلسه ۹۰دقیقه‌ای به آن سختی نباشد.

کاخ سـفید با تمام قوا و متحد به اسـتقبال ما آمده بـود. رئیس‌جمهـور اوباما و معاون او، جو بایدن، در جایگاه مرسوم یعنی در میانه میز نشستند و در دو طرف آنها نیز تقریباً تمام تیم ارشـد کاخ سفید حضور داشـتند. در حالی که اهالی رسـانه عکس می‌گرفتند، رئیس‌جمهور از رید هیسـتینگز چند پرسـش بی‌مخاطـره در مورد فصل آینده سـریال «خانه پوشالی» پرسید.

بعد از خروج اهالی رسانه از اتاق گفت‌وگو جدی شد. رسم این جلسات در دوره اوباما این بود که هر میهمان اظهارنظر اولیه‌ای داشته باشد. با توجه به تعداد زیاد میهمانان، این بخش کمی طول کشید. رئیس‌جمهور از مهارت‌های «پرسشگری سقراطی» (روشی برای مباحثه که بر اساس سؤال و جواب متوالی و هدفمند بنا شده، به‌طوری‌که با اختیار موضع طـرف مقابل، ابتـدا موافقـت و همراهی او جلب می‌شـود و سـپس تناقض‌های استدلال‌های او آشکار شده و با استفاده از موضع خود شخص، مدعایش رد می‌شود) خود استفاده می‌کرد و با پرسـیدن برخی پرسش‌ها و بازگویی نکات مطرح‌شده از سوی میهمانان گفت‌وگو را هوشمندانه‌تر می‌کرد.

به‌جز چند استثنا، همه رهبران استدلال قدرتمندی برای محدود کردن جمع‌آوری انبوه داده، ایجاد شفافیت بیشـتر و کنترل بیشـتر قدرت و اختیارات آژانس امنیت ملی ارائه دادند. بیشتر وقت جلسه اشاره مستقیمی به ادوارد اسنودن نکردیم، اما وقتی نوبت به

«مارک پینکوس»، بنیان‌گذار شرکت توسعه‌دهنده بازی‌های اجتماعی «زینگا» (Zynga) رسید که نزدیک اوباما نشسته بود، استدلال کرد که اسنودن قهرمان است. پینکوس گفت: «باید او را عفو کنید و مانند قهرمانان ورزشی برایش جشن قهرمانی بگیرید.»

در حالی که بایدن به‌وضوح یکه خورده بود، اوباما گفت: «این کار را به هیچ‌وجه انجام نخواهم داد.» رئیس جمهور توضیح داد که فکر می‌کند اسنودن با سرقت اسناد بسیار زیاد و خارج‌کردن آنها از کشور عملی غیرمسئولانه انجام داده است.

بعد نوبت به «ماریسا میر»، مدیرعامل یاهو رسید. او که در کنار پینکوس نشسته بود، پرونده‌ای از جنس کاغذ مانیل را باز کرد که در آن سرفصل‌های صحبتش بادقت آماده شده بودند. ابتدا گفت: «با همه موافقم.» بعد مکثی کرد و سرش را بالا گرفت. بعد خیلی سریع به پینکوس اشاره و اضافه کرد: «البته به‌جز این آقا، با حرف‌های او موافق نیستم.» همه خندیدند.

این گفته‌ها بازتاب‌دهنده کار چالش‌برانگیزی بود که همه می‌خواستیم انجام دهیم. تقریباً همه ما به کاخ سفید رفته بودیم تا رئیس جمهور را به تغییر رویه دولت ترغیب کنیم، اما بخش فناوری رابطه صمیمی و گرمی با اوباما داشت. در ضمن وقتی به دیدار فردی در خانه‌اش می‌روید، به چالش کشیدن او همیشه دشوارتر است؛ به‌ویژه حالا که آن خانه کاخ سفید بود.

هرچند همه مبادی آداب بودیم، اما قاطعانه بر سر حرف‌مان ایستادیم و دلایل‌مان را برای ایجاد اصلاحات در نظارت اعلام کردیم. از فهرست مسائلی که اوباما فکر می‌کرد دولت باید به آنها رسیدگی کند، روشن بود که وقت زیادی را صرف بررسی این موضوع کرده است. در برخی موارد با ما مخالفت می‌کرد و می‌گفت هرچند افراد نگران داده‌هایی هستند که آژانس امنیت ملی در اختیار دارد، اما شرکت‌های حاضر در آن جلسه در مجموع بسیار بیشتر از دولت داده در اختیار دارند. اوباما گفت: «این احتمال را می‌دهم که در آینده جایگاه‌مان در این بحث عوض شود.»

در انتهای جلسه رئیس جمهور به‌روشنی اعلام کرد که علاقه‌مند به پیگیری چند تغییر هرچند محدود؛ اما مهم در سیاست ایالات متحده است. زیرمجموعه‌ای از مسائل را نام برد و از افراد خواست اطلاعات بیشتری ارائه دهند تا به افزایش جزئیات بحث کمک کنند.

یک ماه بعد در تاریخ ۱۷ ژانویه ۲۰۱۴ رئیس‌جمهور اولین گام مهم به سوی اصلاحات در نظارت را برداشت. شب قبل از سخنرانی اوباما و رونمایی از این برنامه‌ها، وکلای وزارت دادگستری با ما تماس گرفتند. پیشنهاد دادند که در مورد شکایت‌های مایکروسافت و گوگل با شرایطی توافق کنند که بسیار مطلوب‌تر از آن شرایطی بود که در مذاکرات ماه آگوست سال قبل گفته بودیم که می‌پذیریم. بعد از قطعی‌شدن توافق بر اساس گزارش‌های شفاف‌سازی جدیدی به کار ادامه دادیم تا داده‌های بیشتری را در مورد احکام و دستورات امنیت ملی منتشر کنیم. گوگل در اقدامی تحسین‌برانگیز سریع‌تر از همه مدلی کارآمد را ارائه کرد که بقیه ما تصمیم گرفتیم از آن پیروی کنیم.

از نظر بسیاری از مشتریان و حامیان حریم خصوصی، سخنرانی اوباما گام اولی بود که باید با گام‌های زیاد دیگری تکمیل می‌شد. بخش فناوری از این دیدگاه‌ها پشتیبانی کرد. می‌دانستیم که این مسائل آسان نیستند و هنوز پرسش‌های دشواری باقی مانده‌اند. چطور می‌توانستیم دولت‌ها و مشتریان خارجی را متقاعد کنیم که دولت ایالات متحده به مراکز داده تحت مدیریت شرکت‌های آمریکایی دست‌درازی نخواهد کرد؟ همزمان چطور می‌توانستیم گام‌های قانونی مورد نیاز برای تأمین امنیت عمومی را برداریم؟ حل‌کردن این مسائل سال‌ها طول می‌کشید.

تغییرات این هفت ماه یعنی از زمانی که اسنودن اسناد دزدیده‌شده را به گاردین ارائه داده بود، ما را شگفت‌زده می‌کرد. افراد از دامنه نظارت دولت آگاه شده بودند. رمزنگاری قدرتمندتر رایج شده بود. شرکت‌های فناوری از دولت خودشان شکایت کرده بودند و رقبا در چارچوب‌های جدیدی همکاری می‌کردند.

با گذشت چند سال افراد همچنان در مورد قهرمان یا خائن‌بودن ادوارد اسنودن بحث می‌کنند. از دیدگاه برخی افراد هم قهرمان بود، هم خائن. در هر صورت تا اوایل سال ۲۰۱۴ دو مسئله مشهود بود؛ اسنودن جهان را تغییر داده بود و در بخش فناوری هم ما را تغییر داده بود.

فصل اول

فناوری و امنیت عمومی

«ترجیح می‌دهم بازنده باشم تا دروغگو»

حفظ امنیت جامعه به مجریان قانون وابسته است. در عین حال برای دستگیری مجرمان یا تروریست‌ها ابتدا باید آنها را پیدا کرد و این کار نیز مستلزم دسترسی مؤثر به اطلاعات است. در قرن بیست‌ویکم این اطلاعات اغلب در مراکز داده بزرگ‌ترین شرکت‌های فناوری جهان نگهداری می‌شوند.

بخش فناوری در تلاش برای ایفای نقش و عمل به تعهدات خود در حفظ امنیت جامعه و در عین حال حفاظت از حریم خصوصی افراد روی لبه شمشیر حرکت می‌کند. تعادلی ظریف و شکننده است که باید آن را در پاسخگویی به نیازهای دنیای سیال و پرشتاب امروز حفظ کنیم.

رخدادهای نیازمند واکنش ما، ناگهانی و بدون هشدار قبلی اتفاق می‌افتند. این واقعیتی است که اولین بار در سال ۲۰۰۲ آن را از نزدیک لمس کردم. «دنیل پرل»، خبرنگار وال‌استریت‌ژورنال ۲۳ ژانویه آن سال در کراچی پاکستان ربوده شد. آدم‌رباها از کافی‌نتی به کافی‌نت دیگر می‌رفتند و از خدمات ایمیل هات‌میل مایکروسافت برای اعلام خواسته‌هایشان استفاده می‌کردند. پلیس پاکستان نیز مذبوحانه به‌دنبال آنها بود. آدم‌رباها در ازای آزادی پرل خواستار آزادی مظنونان تروریستی در پاکستان و توقف برنامه انتقال جنگنده‌های اف-۱۶ از ایالات متحده بودند. واضح بود که دولت پاکستان با این باج‌خواهی‌ها موافقت نخواهد کرد. تنها راه نجات پرل پیدا کردن او بود.

مراجع قدرت در پاکستان خیلی سریع همکاری مخفی با اف‌بی‌آی در ایالات متحده را شروع کردند. اف‌بی‌آی نیز به ما مراجعه کرد. کنگره استثنایی اضطراری برای قانون حریم خصوصی ارتباطات الکترونیکی (Electronic Communications Privacy Act) در نظر گرفته بود تا «در موارد اضطراری که خطر مرگ یا آسیب فیزیکی جدی وجود دارد»، دولت بتواند بلافاصله اقدام کند و شرکت‌های فناوری بتوانند سریع همکاری کنند. به‌وضوح زندگی پرل در خطر بود.

جان فرنک نزد من آمد و موقعیت را توضیح داد. مجوز همکاری با پلیس محلی و اف‌بی‌آی را صادر کردم. هدف‌مان تحت نظر گرفتن حساب هات‌میل مورد استفاده آدم‌رباها و استفاده از آدرس آی‌پی ایمیل‌های جدید آنها برای پیدا کردن مکان کافی‌نت‌هایی بود که آدم‌رباها در آن سر دنیا از آنها استفاده می‌کردند. تیم‌های ما به

مدت یک هفته همکاری نزدیکی با اف‌بی‌آی و مراجع قدرت محلی در پاکستان داشتند و رد آدم‌رباها را در حالی می‌گرفتند که برای دسترسی به اینترنت از یک نقطه اتصال به نقطه اتصال دیگر می‌رفتند.

به آنها نزدیک شدیم، اما کافی نبود. آدم‌رباها پیش از دستگیری، پرل را کشتند. حال‌مان بد بود. مرگ بی‌رحمانه او مخاطرات و مسئولیت عظیمی را برجسته می‌کرد که بر دوش ما بود؛ مسئله‌ای که به‌ندرت به بحث‌های عمومی راه می‌یافت.

این حادثه نشانه‌ای اولیه از حوادث آینده بود. امروزه فضای سایبری دیگر مسئله‌ای حاشیه‌ای نیست و بیش از پیش به مکانی تبدیل شده که افراد در آن به سازمان‌دهی خود می‌پردازند و اتفاقات دنیای واقعی را تعیین می‌کنند.

حادثه غم‌انگیز دنیل پرل اهمیت تشخیص و درایت در زمینه حریم خصوصی را هم برجسته می‌کند. از جهاتی تعادلی بین حریم خصوصی و امنیت وجود دارد. این تعادل حاصل فعالیت‌های گروه‌های حامی حریم خصوصی و نهادهای مجری قانون است که جهت‌گیری‌های مخالفی را دنبال می‌کنند، اما مانند قاضی‌هایی که در مورد این مشاجرات تصمیم‌گیری می‌کنند، شرکت‌های فناوری هم به مکان‌هایی تبدیل شده‌اند که باید به این مسائل رسیدگی کنند. باید هر دو طرف این معادله را درک و به‌خوبی بررسی کنیم.

یکی از چالش‌های بزرگ این است که چطور این کار را به‌خوبی انجام دهیم. توانایی ما در تغییر رفتار سریع در واکنش به احکام تفتیش فرایندی است که از طریق آزمون‌وخطا از ابتدای ظهور ایمیل و اسناد الکترونیکی در دهه ۱۹۸۰ رشد کرده است.

رئیس‌جمهور رونالد ریگان در سال ۱۹۸۶قانون حریم خصوصی ارتباطات الکترونیکی را امضا کرد که وکلای حریم خصوصی امروز با علاقه از آن یاد می‌کنند. در آن زمان کسی نمی‌دانست که آیا متمم چهارم از مقوله‌ای مثل ایمیل محافظت می‌کند یا خیر، اما هم جمهوری‌خواهان و هم دموکرات‌ها می‌خواستند این نوع سپر حفاظتی قانونی را ایجاد کنند.

همان‌طور که گاهی در واشنگتن دی‌سی اتفاق می‌افتد، کنگره در سال ۱۹۸۶ نیت درستی داشت، اما نتیجه بر پیچیدگی شرایط افزود. بخشی از قانون حریم خصوصی

ارتباطات الکترونیکی، قانون ارتباطات ذخیره‌شده (Stored Communications Act) است که نوع جدیدی از حکم تفتیش را ایجاد کرد. بر اساس این قانون دولت می‌توانست با ادله کافی به قاضی مراجعه کند، برای ایمیل شما حکم تفتیش بگیرد و حکم را نه به شما؛ بلکه به شرکت فناوری‌ای ابلاغ کند که ایمیل و اسناد الکترونیکی شما در آنجا ذخیره شده است. آن شرکت هم ملزم بود ایمیل را استخراج کند و به دولت تحویل دهد. این قانون در برخی شرایط شرکت‌های فناوری را در عمل، به کارگزاران دولت تبدیل کرد.

این قانون شرایط جدیدی را هم ایجاد کرد. اگر دولت حکم تفتیشی را به خانه یا دفتر فرد ابلاغ می‌کرد، احتمالاً فردی وجود داشت و می‌فهمید چه اتفاقی می‌افتد. آن فرد نمی‌توانست از اجرای حکم جلوگیری کند، اما خبردار می‌شد و اگر فکر می‌کرد حقوقش نقض شده‌اند، می‌توانست پا جای پای جان ویلکس بگذارد و به دادگاه برود.

اما کنگره در مورد اطلاع‌رسانی به افراد و کسب‌وکارهایی که دولت ایمیل‌ها و اسنادشان را از شرکت‌ها می‌گرفت، رویکردی پیچیده‌تر را اتخاذ کرد و قانونی گذاشت که به دولت این اختیار را می‌داد که دستور منع انتشاری را بگیرد که شرکت فناوری را مجبور می‌کند حکم را محرمانه نگه دارد. طبق این قانون دولت می‌تواند بر پنج مبنای متفاوت تقاضای محرمانگی کند. این مبانی در ظاهر غیرمنطقی به نظر نمی‌رسیدند. برای مثال اگر افشای اطلاعات به نابودی مدارک و شواهد یا ارعاب شاهدی منجر می‌شد یا به هر صورت تحقیقات را به خطر می‌انداخت، قاضی می‌توانست حکم را به همراه دستور عدم افشا صادر کند. شرکت فناوری ممکن است هر دو دستور را با هم دریافت کند که دستور اول آن شرکت را به تحویل داده‌های الکترونیکی و دستور دوم به مخفی نگه‌داشتن درخواست ملزم می‌کند.

وقتی هنوز به‌ندرت از ایمیل استفاده می‌شد، این احکام و دستورات منع انتشار جدید بسیار کم بودند، اما با رشد انفجاری اینترنت و ظهور مراکز داده‌ای با صدها هزار کامپیوتر شرایط بسیار پیچیده‌تر شد. در حال حاضر تیم «اجرای قانون و امنیت ملی» ما از ۲۵ کارمند تمام‌وقت (شامل متخصصان تطبیق، وکلا، مهندسان و متخصصان امنیت) تشکیل شده است. این تیم از کمک گسترده شرکت‌های حقوقی بی‌شماری در سراسر دنیا بهره می‌برد. در مایکروسافت این تیم را به‌عنوان تیم «لنز» (LENS)

می‌شناسیم. مأموریت‌شان سرراست است، اما کارشان به هیچ‌وجه ساده نیست. آنها باید درخواست‌های مجریان قانون در سراسر جهان را بر اساس قوانین کشورهای گوناگون و طبق تعهدات قراردادی شرکت نسبت به مشتریان بررسی کنند و به آنها پاسخ بدهند. تیم لنز در هفت مکان در شش کشور از سه قاره حضور دارد. این تیم هر سال معمولاً به بیش از ۵۰ هزار حکم و احضاریه از طرف بیش از ۷۵ کشور پاسخ می‌دهد که فقط سه درصد از این تقاضاها برای دریافت محتواست. مراجع قانونی در بیشتر موارد به‌دنبال آدرس آی‌پی، فهرست مخاطبان و داده‌های ثبت‌نام کاربر هستند.

وقتی مایکروسافت حکمی دریافت می‌کند، معمولاً از طریق ایمیل ارسال می‌شود. مدیر تطبیق تقاضا را بررسی می‌کند تا مطمئن شود معتبر است و قاضی آن را امضا کرده، مراجع قانونی برای آن شواهد و ادله کافی دارند و آن اطلاعات در حوزه اختیارات آن سازمان قرار دارد. اگر همه شرایط برقرار باشند، مدیر تطبیق مدارک درخواستی را از مرکز داده ما استخراج می‌کند. داده‌ها دوباره بررسی می‌شوند تا اطمینان حاصل شود که دقیقاً همان اطلاعاتی را ارائه می‌دهیم که در حکم مشخص شده است. بعد اطلاعات به مرجع قانونی مورد نظر ارسال می‌شود. آن‌طور که یکی از کارمندان لنز برای من توضیح داد؛ «ساده به نظر می‌رسد، اما انجام وظیفه درست خیلی زمان‌بر است. باید خود حکم و اطلاعات حساب مربوط به آن را بررسی کنید، اطلاعات را استخراج کنید و بعد دوباره این اطلاعات را بررسی کنید تا مطمئن شوید که اطلاعات مناسب را ارائه می‌دهید».

وقتی مدیر تطبیق به این جمع‌بندی می‌رسد که حکم بیش از حد گسترده است یا از حوزه اختیارات آن سازمان فراتر می‌رود، پرونده به یک وکیل ارجاع می‌شود. گاهی اوقات از سازمان متقاضی می‌خواهیم حکم را محدودتر کند. در موارد دیگر حکم را غیرقانونی تلقی می‌کنیم و از آن پیروی نمی‌کنیم.

یکی از اعضای تیم لنز همواره آماده‌باش است، یعنی هر هفته یک نفر کنار تلفنی می‌خوابد که اگر موردی اضطراری یا حادثه‌ای تروریستی در نقطه‌ای از دنیا اتفاق افتاد که نیازمند اقدام فوری بود، پاسخگو باشد. در هفته‌هایی که اوضاع جهان خیلی به‌هم‌ریخته است، اعضای تیم لنز به‌نوبت آماده‌باش هستند تا همه به‌اندازه کافی

بخوابند و در زمان کار هوشیار باشند.

در سال ۲۰۱۳ که ادوارد اسنودن رازهای آژانس امنیت ملی را افشا کرد و مشکلات ناشی از حجم عظیم داده‌ها بروز پیدا کردند، وکیلی جدید به مایکروسافت ملحق شد تا این تیم را رهبری کند. نام این وکیل «ایمی هوگن برنی» است. ایمی با تیزهوشی و شوخ‌طبعی هوشمندانه‌اش خیلی زود حمایت تیم را جلب کرد. ایمی سه سال قبل را به‌عنوان وکیلی در واحد امنیت ملی ساختمان مرکزی اف‌بی‌آی سپری کرده بود. این تجربه او را به‌خوبی برای کار در مایکروسافت آماده کرده بود؛ هرچند احتمالاً قرار بود روزهایی برسد که در پرونده‌هایی در مقابل همکاران سابقش در واشنگتن دی‌سی قرار بگیرد.

ایمی به‌سرعت با نقش جدیدش سازگار شد. دفتر کارش در طبقه پایین دفتر من قرار داشت و حضور من در راهروی دفتر او مدام بیشتر می‌شد. دفترش کنار دفتر «نِیت جونز» بود که اوایل همان سال بعد از بیش از یک دهه خدمت در دولت ایالات متحده به مایکروسافت پیوسته بود. در سابقه دولتی جونز حضور در کمیته قضایی سنا، وزارت دادگستری و در نهایت بخش مبارزه با تروریسم شورای امنیت ملی دوران ریاست‌جمهوری اوباما وجود داشت.

«ایمی» کار تیم لنز و «نیت» استراتژی تطبیق کلی ما، روابط‌مان با سایر شرکت‌های فناوری و مذاکرات با دولت‌های بین‌المللی را مدیریت می‌کردند. آنها و تمام تیم لنز باید همگام با تحول جهان تعادلی ظریف را برقرار می‌کردند. باید با سازمان‌های مجری قانون سراسر جهان همکاری می‌کردند، اما در عین حال در خط مقدم دفاع از حقوق حریم خصوصی مقررشده در متمم چهارم و قوانین سایر کشورها قرار داشتند. از آنجایی که با چند متخصص حریم خصوصی که از قبل در شرکت حضور داشتند، همکاری می‌کردند، خوشحال بودم که دفاترشان به من نزدیک است.

نیت و ایمی به‌سرعت به یک تیم دونفره تبدیل شدند که آن‌قدر هماهنگ و قدرتمند بودند که سایر اعضای تیم آنها را «نِیمی» می‌خواندند. در مایکروسافت افراد بر همکاری نیت و ایمی برای اتخاذ رویکرد مناسب نسبت به حساس‌ترین مسائل اتکا داشتند. مدیران تطبیق ما به مسئله‌ای داغ که به ایمیل‌شان ارسال شده بود، نگاهی

می‌انداختند، با هم بحث می‌کردند و تصمیم می‌گرفتند که باید سریع به نِیمی ارجاع شود.

تیم نِیمی مسئول تصمیم‌گیری‌های مهم و دشوار برای حفاظت از قفسه بایگانی دنیا بود؛ مسئولیتی که اغلب به شکل ناگهانی و غافلگیرکننده دشوارتر می‌شد.

روز چهارشنبه، ۷ ژانویه ۲۰۱۵ در حالی که کارمندان سراسر فرانسه برای وقت استراحت ناهار آماده شده بودند، دو برادر به ساختمان مرکزی مجله فکاهی «شارلی ابدو» وارد شدند و بی‌رحمانه ۱۲ نفر را کشتند. این دو نفر به القاعده وابسته بودند و مانند بسیاری از مسلمانان از کاریکاتورهای اهانت‌آمیز این مجله در مورد پیامبر اسلام، محمد (ص) خشمگین شده بودند. اما این برادران بر خلاف بسیاری از افراد دیگر خودشان دست به کار شده بودند.

شبکه‌های خبری به تفصیل این حادثه غم‌انگیز را پوشش دادند. ما هم از ردموند مثل بقیه دنیا اخبار این رخداد وحشتناک را دنبال می‌کردیم. وقتی ماگ قهوه‌ام را در اتاق استراحت پر می‌کردم، گروهی از افراد تلویزیون را تماشا می‌کردند که نشان می‌داد پلیس فرانسه در حال جست‌وجو برای پیدا کردن این دو برادر است که توانسته بودند فرار کنند. خیلی زود سربازان ارتش فرانسه نیز به عملیات تعقیب گسترده ملی ملحق شدند و عضو دیگری از القاعده نیز حمله تروریستی مجزایی را در سوپرمارکتی فرانسوی اجرا کرد. خیابان‌ها و محله‌های درگیر در این حادثه را می‌شناختم. سه سال اول حضور در مایکروسافت را در مقر اروپایی شرکت در پاریس گذرانده بودم.

این ماجرا برای دنیا مهم بود، اما به‌جز بررسی وضعیت کارمندان حاضر در آن منطقه که همه در امنیت کامل بودند، این ماجرا به شغلم ربطی نداشت. اما فردا صبح که خورشید در ردموند طلوع کرد، دیگر این‌طور نبود. پلیس ملی فرانسه که خیلی زود فهمیده بود این دو تروریست دارای حساب ایمیل مایکروسافت هستند، از اف‌بی‌آی کمک خواسته بود. در ردموند ساعت ۵:۴۲ صبح بود که اف‌بی‌آی در نیویورک به این مورد اضطراری واکنش نشان داد و از ما ایمیل و سوابق حساب این آدمکش‌ها را درخواست کرد که شامل آن دسته از آدرس‌های آی‌پی می‌شد که می‌توانستند مکان کامپیوتر یا تلفن در زمان ورود کاربر به حساب را نشان دهند. تیمی در مایکروسافت

این درخواست اضطراری را بررسی کردند و اطلاعات را در عرض ۴۵ دقیقه در اختیار اف‌بی‌آی گذاشتند. روز بعد مراجع قانونی فرانسه در عملیات تعقیب ملی این دو تروریست را پیدا کردند که در درگیری مسلحانه با پلیس کشته شدند.

حوادث پاریس، فرانسه و جهان را تکان داد. یکشنبه بعد از حمله بیش از دو میلیون نفر در خیابان‌های پایتخت فرانسه راهپیمایی کردند تا برای این خبرنگاران سوگواری کنند و با همبستگی پشتیبانی‌شان از آزادی رسانه را به نمایش بگذارند.

متأسفانه این حمله تروریستی آخرین حادثه غم‌انگیز پاریس در سال ۲۰۱۵ نبود. بعدازظهر جمعه‌ای در ماه نوامبر که شهروندان پاریسی در حال اتمام کار هفتگی بودند، تروریست‌ها دوباره در حملاتی هماهنگ به نقاط مختلفی از شهر هجوم بردند. در کنسرتی درون یک سالن نمایش، در مجاورت یک استادیوم و در چند رستوران و کافه با اسلحه‌های خودکار بر مردم آتش گشودند. صحنه‌های آن حوادث تکان‌دهنده بود. تروریست‌ها ۱۳۰ نفر را کشتند و بیش از ۵۰۰ نفر را مجروح کردند. این حمله، مرگبارترین حمله‌ای بود که پاریس از زمان جنگ جهانی دوم تجربه کرده بود. هرچند هفت نفر از مهاجمان کشته شدند، اما دو نفر دیگر توانستند فرار کنند.

فرانسوا اولاند، رئیس‌جمهور فرانسه بلافاصله در سراسر کشور حالت فوق‌العاده اعلام کرد. دولت اسلامی عراق و سوریه (داعش) مسئولیت این حوادث را پذیرفت و کمی بعد مشخص شد که شماری از مهاجمان از بلژیک آمده بودند. عملیات تعقیب جدیدی شروع شد که این بار دو کشور را دربر می‌گرفت.

باز هم اف‌بی‌آی در همکاری با مراجع قانونی اروپایی احکام و احضاریه‌هایی را برای ایمیل‌ها و سایر حساب‌های متعلق به مظنونان به شرکت‌های فناوری ابلاغ کرد. از حادثه «شارلی ابدو» درس گرفته بودیم که زمان وقوع حملات تروریستی باید برای انجام اقدامات لازم آماده باشیم. مراجع قانونی فرانسه و بلژیک این بار ۱۴ دستور به ما ابلاغ کردند. تیم مسئول آنها را بررسی کرد، قانونی‌بودن آنها را تأیید کرد و اطلاعات درخواستی را در هر مورد در کمتر از ۱۵ دقیقه تحویل داد.

این دو حادثه غم‌انگیز پاریس توجه دنیا را به خود جلب کرد، اما این روزها به هیچ‌وجه تنها روزهایی نبودند که به توجه ما نیاز داشتند. در اوایل ظهور ایمیل،

دولت‌ها به‌ندرت به ما مراجعه می‌کردند، اما وقتی در سال ۵۰ هزار حکم تفتیش و دستور دولتی از بیش از ۷۰ کشور دریافت کردیم، باید فعالیت‌هایمان را در مقیاس جهانی عملیاتی می‌کردیم.

«ساتیا نادلا» به تعریف مسیر پیش روی ما کمک کرد. پیش از قرار گرفتن در جایگاه مدیرعاملی شرکت در اوایل سال ۲۰۱۴، کسب‌وکار ابری شرکت را مدیریت می‌کرد. بیش از همه خدمات ابری را می‌شناخت. به‌علاوه حساسیت ارزشمند دیگری را به همراه خود به این مسئله پیچیده اضافه کرده بود. او پسر مدیری دولتی در هند بود. پدرش به‌عنوان رهبر دانشکده‌ای که نسلی از مدیران دولتی در دهه‌های بعد از استقلال این کشور را پرورش داده بود، مورد احترام قرار می‌گرفت. چنین پدری او را بزرگ کرده بود. این پیشینه حس ششمی از سازوکار دولت به ساتیا داده بود. شباهت ساتیا نادلا و بیل گیتس برایم جالب بود. بیل گیتس هم پسر یکی از برجسته‌ترین و محترم‌ترین وکلای سیاتل بود. بیل و ساتیا هر دو به‌نوعی نمونه تمام‌عیاری از یک مهندس بودند، اما بیل می‌توانست مانند یک وکیل فکر کند و ساتیا می‌توانست مانند فردی در دولت فکر کند. برای من فرصت بحث‌کردن با هر دوی اینها در مورد مسائل دشوار بسیار ارزشمند بود.

در حالی که سعی می‌کردیم دامنه کامل مسائل نظارت را درک کنیم، ساتیا در اواخر سال ۲۰۱۴ پیشنهاد داد که رویکردی اصولی را توسعه دهیم. گفت: «باید بدانیم چطور تصمیمات سخت را بگیریم و مشتریان‌مان هم باید بدانند چطور این کار را انجام می‌دهیم. به مجموعه‌ای از اصول هم نیاز داریم تا ما را در این زمینه هدایت کنند.»

در دهه قبل رویکرد مشابهی را در مورد مسائل دشوار به کار گرفته بودیم. از جمله برای پرداختن به مسائل ضدانحصاری شرکت «اصول ویندوز: ۱۲ اصل برای ترویج رقابت» را منتشر کردیم. در سال ۲۰۰۶ در باشگاه ملی مطبوعات (National Press Club) در واشنگتن دی‌سی از آن اصول رونمایی کردم. «جان لیبوویتز» که در آن زمان عضو کمیسیون فدرال تجارت (Federal Trade Commission) بود و در بحبوحه پرونده‌های ضدانحصار برجسته‌ای که داشتیم، ما را به این کار ترغیب کرده بود، در مراسم سخنرانی حاضر شده بود. بعد از سخنرانی به سراغ من آمد و گفت: «اگر یک دهه پیش این اصول

را منتشر کرده بودید، فکر نمی‌کنم دولت از شما شکایت می‌کرد.»

هرچند مأموریتی که ساتیا بر عهده ما گذاشته بود، ساده و سرراست به نظر می‌رسید، اما در واقعیت این‌طور نبود. به اصولی نیاز داشتیم که برای تمام کسب‌وکارمان از سیستم‌عامل‌ها تا ایکس‌باکس مناسب باشد. این اصول باید ساده و به‌یادماندنی می‌بودند، نه ۲۰ پاراگرافی که با اصطلاحات حقوقی و فنی پر شده‌اند. ارائه محتوای کوتاه‌تر و ساده‌تر همیشه دشوارتر است.

اگرچه خود مسئله دشوار بود، اما نقطه شروع واضحی داشت. همیشه در ذهن‌مان روشن بود که اطلاعاتی که افراد در مراکز داده ما ذخیره می‌کنند، متعلق به ما نیست. افراد همچنان صاحب ایمیل‌ها، عکس‌ها، اسناد و پیام‌های فوری‌شان هستند. ما کارگزار دارایی‌های افراد هستیم، مالک این داده‌ها نیستیم و به‌عنوان کارگزار شایسته باید از این داده‌ها در راستای منافع صاحبان‌شان استفاده می‌کردیم، نه اینکه فقط به خودمان فکر کنیم.

بر مبنای این نقطه شروع تیمی را تشکیل دادیم که چهار اصل را تدوین کردند. این اصول را «تعهدات ابری» خودمان می‌خوانیم و شامل حریم خصوصی، امنیت، تطبیق و شفافیت می‌شوند. از اینکه به رهبران بازاریابی شرکت می‌گفتم وکلا راهی پیدا کرده‌اند که مبحثی پیچیده را به چهار واژه تبدیل کنند، لذت می‌بردم. عجیب نبود که به‌سرعت اشاره می‌کردند چنین اتفاقی بی‌سابقه است.

با این حال تدوین اصول واضح و به‌کارگیری آنها دو چالش مجزا و متفاوت بودند. تیم هر اصل را به همراه جزئیات و آموزش مربوط تدوین کرده بود. آزمون واقعی زمانی پیش می‌آمد که شرایط جدید پرسش‌های دشواری را مطرح می‌کردند و آن موقع باید تصمیم می‌گرفتیم که تا کجا حاضریم به تعهداتی پایبند بمانیم که طراحی کرده بودیم.

خیلی زود با یکی از دشوارترین انتخاب‌ها روبه‌رو شدیم که به تعهدمان نسبت به شفافیت مربوط می‌شد. پذیرفته بودیم که شفافیت رکن اساسی همه مسائل دیگر است. اگر افراد نمی‌فهمیدند چه کار می‌کنیم، نمی‌توانستند در مورد هیچ مسئله دیگری به ما اعتماد کنند.

به‌طور ویژه این مشتریان تجاری‌مان بودند که می‌خواستند بدانند چه زمانی حکم

یا احضاریه‌ای برای تفتیش ایمیل‌ها یا سایر داده‌ها دریافت کرده‌ایم. معتقد بودیم به‌ندرت دلیل خوب و درستی وجود دارد که دولت دستورات قانونی را به جای مشتریان سازمانی به خود ما ابلاغ کند. بر خلاف افراد مجرم یا مظنونان تروریستی، بسیار بعید بود که شرکت یا کسب‌وکاری معتبر از کشور فرار کند یا دست به عملی غیرقانونی بزند تا تحقیقات را منحرف کند. حتی اگر دولت نگران پاک‌سازی بالقوه داده‌ها بود، می‌توانستیم با دریافت «دستور انسداد» محدود نسخه‌ای از داده‌های مشتری تهیه کنیم تا دولت پیش از دسترسی به داده‌ها با خیال راحت مشکلات حقوقی را با مشتری حل‌وفصل کند.

در سال ۲۰۱۳ به‌طور علنی اعلام کردیم که اگر دستوری قانونی در مورد داده‌های مشتریان تجاری یا دولتی‌مان دریافت کنیم، به آنها اطلاع خواهیم داد. اگر دستور منع انتشاری به ما اجازه این کار را ندهد، آن دستور را در دادگاه به چالش می‌کشیم. همچنین به سازمان‌های دولتی می‌گوییم که برای دریافت اطلاعات یا داده‌های مربوط به کارمندان مشتریان‌مان، به‌طور مستقیم به خود مشتریان مراجعه کنند؛ همان‌طور که قبل از انتقال فعالیت این مشتریان به ابر این کار را می‌کردند. علاوه بر این به دادگاه می‌رویم تا این رویه را همیشگی کنیم.

با اولین آزمون زمانی مواجه شدیم که اف‌بی‌آی یک نامه امنیت ملی را به ما ابلاغ کرد که داده‌های متعلق به یکی از مشتریان سازمانی را درخواست می‌کرد. این دستور به ما اجازه نمی‌داد به مشتری بگوییم اف‌بی‌آی داده‌هایش را می‌خواهد. بگذریم از اینکه دلیلی برای درخواست داده‌ها از ما به جای درخواست مستقیم از خود مشتری وجود نداشت، بعد از مطالعه نامه به این جمع‌بندی رسیدیم که جلوگیری از اطلاع‌رسانی به مشتری نیز مبنایی منطقی ندارد. از نامه تبعیت نکردیم، شکایتی ثبت کردیم و به دادگاه فدرال در سیاتل رفتیم. قاضی با استدلال ما موافق بود. اف‌بی‌آی پیام حرکت ما را دریافت کرد و نامه را پس گرفت.

در طول سال بعد وکلای شرکت در متقاعد کردن وزارت دادگستری به مراجعه مستقیم به مشتریان سازمانی برای دریافت داده‌هایشان پیشرفت خوبی داشتند. با این حال در ژانویه ۲۰۱۶ دستیار دادستانی در ناحیه‌ای دیگر درخواست ما را نپذیرفت

و حکم تفتیش مهروموم‌شده‌ای را به ما ابلاغ کرد که خواستار داده‌های متعلق به یکی از مشتریان تجاری می‌شد. این حکم دستور منع انتشار نامحدودی را به همراه داشت که تا همیشه برقرار بود. اعتراض کردیم. معمولاً وقتی موضع‌مان را توضیح می‌دادیم، دولت از خواسته‌اش عقب‌نشینی می‌کرد، اما این بار دادستان فدرال با پافشاری بر خواسته‌اش، ما را مجبور به مراجعه به دادگاه کرد.

در سفری اروپایی بودم و صبح زود که از خواب بیدار شدم، ایمیل «دیوید هاوارد» را دیدم که مسئول کارهای دادخواهی و چند حوزه دیگر در شرکت بود. دیوید پنج سال پیش به ما پیوسته بود و پیش از آن مسیر شغلی موفقی را به‌عنوان مدعی‌العموم فدرال و شریک شرکتی حقوقی گذرانده بود. در همه مسائل دشوار با طرز برخورد آرام و تشخیص و درایت خوبش به ما کمک می‌کرد. رهبری او در ایجاد الگوی تکرارشونده پیروزی در ۹۰ درصد پرونده‌های سالانه شرکت نقشی اساسی داشت. زمانی نیمه‌شوخی نیمه‌جدی به هیئت‌مدیره مایکروسافت گفته بودم «از دیوید یاد گرفته‌ام که به دست آوردن نتایج خوب در دادخواهی‌ها دشوار نیست. فقط باید در پرونده‌هایی که سزاوار پیروزی هستید، بجنگید و در پرونده‌هایی که سزاوار شکست هستید، با طرف مقابل به توافق برسید». کلید موفقیت، وجود فردی مثل دیوید بود که تفاوت این پرونده‌ها را از هم تشخیص می‌داد.

در این پرونده دیوید نسبت به احتمال موفقیت‌مان خوش‌بین نبود. قاضی با ما هم‌رأی نبود و تهدید کرده بود به‌دلیل اهانت به دادگاه محکوم‌مان می‌کند. دیوید نوشته بود که تیم دادخواهی می‌خواهد داده‌های مشتری را تحویل بدهد تا جریمه نشویم. آن روز در تماس تلفنی گروهی به تیم گفتم که نمی‌خواهم تسلیم شویم. به مشتریان‌مان قول داده بودیم با این نوع دستورات مقابله کنیم و این قول شامل رفتن به دادگاه و مبارزه در نبردهای دشوار هم می‌شد.

یکی از اعضای تیم گفت مشخص است که در این مبارزه شکست می‌خوریم و این شکست می‌تواند برای ما بسیار گران تمام شود. گفتم: «ترجیح می‌دهم بازنده باشم تا دروغگو. قول، قول است.» احساس می‌کردم هزینه شکستن آن قول بیشتر از هر گونه جریمه پولی است، حتی اگر نتیجه محرمانه و پنهان می‌ماند.

به تیم دادخواهی گفتم که اگر در این پرونده بجنگند، اما نبرد را بازنده شوند و جریمه را کمتر از ۲۰ میلیون دلار نگه دارند، نتیجه را پیروزی اخلاقی می‌دانم. همه می‌دانستیم که امکان نداشت بیشتر از کسری از آن مقدار جریمه بشویم. با این حرف در واقع می‌خواستم به اعضای تیم (که خوشبختانه می‌خواستند در همه پرونده‌ها پیروز شوند) بگویم از نظر من هر نتیجه‌ای به دست بیاید، ما پیروز شده‌ایم.

تیم مایکروسافت شبانه‌روزی و آخر هفته‌ها را به همراه وکلای خارج از شرکت تلاش کرد. در آن پرونده شکست خوردیم، اما از جریمه اهانت به دادگاه در امان ماندیم و این توانایی را حفظ کردیم که با مشتریان‌مان شفاف بمانیم و بدون ذکر جزئیات اعلام کنیم که در یکی از این نوع پرونده‌ها شکست خورده‌ایم. مهم‌تر از همه به قول‌مان وفادار مانده بودیم.

نگران بودیم که همچنان پرونده به پرونده به این روش امتحان شویم. باید موضع تهاجمی می‌گرفتیم. دیوید می‌گفت: «اگر به دولت اجازه دهیم انتخاب‌کننده باشد، در این پرونده‌ها پیروز نمی‌شویم. این نوع دستورات منع انتشار باید در موارد استثنایی صادر شوند، نه اینکه به روال عادی تبدیل شوند. دولت در حال عادی‌کردن آنهاست. باید از دادگاه بخواهیم در مورد این شیوه فراگیر حکم بدهد.»

دیوید نقشه‌ای هوشمندانه کشید. تصمیم گرفتیم مقوله‌ای به نام «حکم تفسیری» (declaratory judgment) را دنبال کنیم که حقوق ما را شفاف می‌کرد. استدلال کردیم که دولت با عادی‌کردن صدور دستور منع انتشار بر اساس قانون حریم خصوصی ارتباطات الکترونیکی از اختیاراتش ذیل قانون اساسی سوءاستفاده می‌کند. سوابق احکام در دسترس از یک سال و نیم قبل را جست‌وجو کردیم و فهمیدیم که بیش از نیمی از تقاضاهای دریافت داده دولت برای افراد با دستور منع انتشار محدود شده بودند و نیمی از این موارد نیز حکم را برای همیشه پنهان نگه می‌داشتند.

به دادگاه فدرال در سیاتل برگشتیم تا از دولت خودمان شکایت کنیم. استدلال کردیم که استفاده افراطی از دستور منع انتشار حق ما بر اساس متمم اول برای اطلاع‌رسانی به مشتریان در مورد مصادره ایمیل‌هایشان توسط دولت را نقض می‌کند. همچنین مدعی شدیم که این دستورات منع انتشار، حق مبتنی بر متمم

چهارم مشتریان‌مان برای حفاظت در برابر تفتیش و ضبط غیرقانونی را نقض می‌کند؛ زیرا افراد اطلاع نداشتند چه اتفاقی در حال وقوع است و نمی‌توانستند از حقوق قانونی‌شان دفاع کنند.

این پرونده به‌طور جدی این مسئله را مطرح می‌کرد که آیا در محیط ابری از حقوق افراد حفاظت می‌شود یا خیر. با اتکا به روند پرونده‌های اخیر دیوان عالی خوش‌بین بودیم. قاضی‌های دیوان عالی در سال ۲۰۱۲ در تصمیمی با آرای پنج به چهار اعلام کرده بودند که متمم چهارم پلیس را ملزم می‌کند که برای قرار دادن مکان‌یاب جی‌پی‌اس روی خودروی مظنون حکم تفتیش بگیرد. هرچند سایر قاضی‌ها «نفوذ فیزیکی» با نصب دستگاهی به خودروی فردی دیگر را مستلزم حکم تفتیش می‌دانستند، اما قاضی «سونیا سوتومایور» به این مسئله اشاره کرد که مجریان قانون در قرن بیست‌ویکم لزوماً نیازی ندارند که برای ردیابی مکان فرد نفوذ فیزیکی داشته باشند. تلفن‌های هوشمند دارای قابلیت جی‌پی‌اس که سوابقی از مکان فرد ایجاد می‌کنند، در حال گسترش بودند. این تلفن‌های هوشمند انواع گوناگونی از اطلاعات شخصی را برملا می‌کردند که دولت می‌توانست تا سال‌ها از آنها بهره‌برداری کند. همان‌طور که سوتومایور می‌گوید؛ مگر اینکه این نوع نظارت در متمم چهارم قانونی لحاظ شده باشد، وگرنه می‌تواند «رابطه بین شهروند و دولت را به نحوی تغییر دهد که برای جامعه دموکراتیک زیان‌آور است».

قاضی سوتومایور مسئله دیگری را توصیف می‌کرد که ما فکر می‌کردیم مسئله‌ای بنیادین است. به مدت تقریباً دو قرن دیوان عالی می‌گفت متمم چهارم نمی‌تواند از اطلاعاتی محافظت کند که به‌صورت گسترده به اشتراک گذاشته می‌شوند. مبنای این قضاوت این فرض بود که افراد دیگر نمی‌توانستند «انتظاری منطقی برای حفظ حریم خصوصی» داشته باشند، اما اکنون سوتومایور می‌گفت حریم خصوصی به این معنی است که افراد باید هم بتوانند اطلاعات را به اشتراک بگذارند و هم تعیین کنند چه افرادی می‌توانند آن را مشاهده کنند و چگونه می‌توانند از آن استفاده کنند. او اولین قاضی دیوان عالی بود که این تغییر را تشریح می‌کرد و پرسش مهم این بود که سایر قاضی‌ها هم آن را می‌پذیرند یا خیر.

دو سال بعد به‌تدریج پاسخی برای این پرسش پیدا شد. «جان رابرتس»، قاضی ارشد دیوان عالی تابستان سال ۲۰۱۴ نظری را بر اساس اتفاق آرای دیوان عالی مکتوب کرد. قاضی‌ها به این نتیجه رسیدند که پلیس برای تفتیش تلفن همراه فرد، حتی اگر آن فرد به واسطه ارتکاب جرم بازداشت شده باشد، باید حکم بگیرد. رابرتس نوشته بود: «تلفن‌های همراه مدرن صرفاً ابزار رفاهی مبتنی بر فناوری نیستند. با وجود همه محتوایی که دارند و مسائلی که می‌توانند افشا کنند، برای بسیاری از مردم آمریکا حریم خصوصی محسوب می‌شوند.»

رابرتس توضیح داده بود که هرچند متمم چهارم برای حفاظت از افراد در خانه‌هایشان تصویب شده است، اما تلفن‌های مدرن «معمولاً اطلاعاتی بسیار بیشتر از کامل‌ترین تفتیش خانه برملا می‌کنند. تلفن همراه علاوه بر اینکه حاوی سوابق حساسی در قالب دیجیتال است که در گذشته در داخل خانه پیدا می‌شد، حاوی طیف گسترده‌ای از اطلاعات خصوصی نیز هست که هرگز و در هیچ قالبی در خانه پیدا نمی‌شدند». در نتیجه متمم چهارم شامل تلفن همراه هم می‌شود.

وقتی حرف‌های بعدی رابرتس را خواندیم، فریاد شادی سر دادیم. اولین‌بار بود که دیوان عالی در عمل به فایل‌های ذخیره‌شده در مراکز داده ما مثل مرکز داده کوئینسی می‌پرداخت. رابرتس نوشته بود: «داده‌هایی که کاربران در تلفن‌های همراه مدرن‌شان مشاهده می‌کنند، ممکن است در عمل در خود دستگاه ذخیره نشده باشد. نوعی داده یکسان ممکن است برای کاربری در خود دستگاه و برای کاربری دیگر در ابر ذخیره شده باشد.» دیوان عالی برای اولین‌بار اذعان کرد که تفتیش تلفن دامنه‌ای فراتر از دستگاه فیزیکی فرد دارد. در واقع فناوری جدید زمینه جدیدی برای حفاظت قدرتمند از حریم خصوصی در ابر فراهم کرده بود.

هرچند این سخنان ارتباط مستقیمی با اعتراض ما به دستورات منع انتشار گسترده در سیاتل نداشت، اما نیروی پشتیبانی برای آرمان حریم خصوصی گسترده‌تر ما را فراهم می‌کرد. حال باید از این نیروی پشتیبان بهره می‌بردیم.

با ثبت شکایتی در ۱۴ آوریل ۲۰۱۶ اجرای برنامه دیوید را شروع کردیم. این پرونده به قاضی «جیمز روبارت» واگذار شد که پیش از انتصاب به‌عنوان قاضی فدرال در سال

۲۰۰۴، یکی از برجسته‌ترین و پرنفوذترین افراد جامعه حقوقی سیاتل بود. پیش از این و از جمله در دادگاه مهمی مربوط به پتنت با ایشان روبه‌رو شده بودیم. قاضی سختگیر اما باهوش و منصفی بود. اعضای تیم دادخواهی ما را هوشیار و آماده نگه می‌داشت.

همزمان با ثبت شکایت، داده‌هایمان از ۱۸ ماه گذشته را هم به اشتراک گذاشتیم که نشان می‌داد بیش از ۲۵۰۰ دستور منع انتشار در مورد داده‌های افراد دریافت کرده‌ایم که به ما اجازه نداده‌اند در مورد اقدامات قانونی‌ای که برای مطالبه اطلاعات شخصی مشتریان‌مان انجام شده، به آنها اطلاع‌رسانی کنیم. به شکل قابل توجه و حتی غافلگیرکننده‌ای ۶۸ درصد از این دستورات هیچ تاریخ انقضای مشخصی نداشتند. در واقع یعنی تا ابد اجازه نداشتیم به مشتریان‌مان اطلاع دهیم که دولت به داده‌هایشان دسترسی داشته است.

متوجه بودیم که باید دغدغه‌هایمان در مورد شیوه کنونی وزارت دادگستری را با نقشه راهی برای رویکردی بهتر همراه کنیم. خواستار شفافیت بیشتر و «بی‌طرفی دیجیتال» بودیم. منظورمان از بی‌طرفی دیجیتال پذیرفتن این حق بود که از اطلاعات افراد باید صرف‌نظر از مکان و چگونگی ذخیره‌سازی محافظت شود. گفته بودیم در این زمینه باید با تعیین اصل ضرورت به تعادل برسیم تا امکان صدور دستور منع انتشار وجود داشته باشد، اما با ضرورت‌های تحقیقات مورد نظر متناسب باشد.

دولت پیش از شروع دادگاه با ارائه دادخواست رد و مختومه اعلام‌کردن شکایت‌مان واکنش نشان داد. استدلال کرده بود که هیچ حقی برای اطلاع‌رسانی به مشتریان تحت عنوان متمم اول نداریم و هیچ مبنایی هم نداریم که از حقوق مشتریان بر اساس متمم چهارم دفاع کنیم. خیلی زود به این جمع‌بندی رسیدیم که اگر بتوانیم از این دادخواست عبور کنیم، احتمالاً نقطه‌عطف مهمی برجا خواهیم گذاشت. اگر از این مرحله عبور می‌کردیم، به داده‌های دولت در مورد استفاده گسترده از دستورات حفظ محرمانگی دسترسی پیدا می‌کردیم و با این اتفاق احتمالاً به سایر حقایقی دست می‌یافتیم که برای پیروزی استدلال‌هایمان نیاز داشتیم.

به این نتیجه رسیدیم که باید ائتلافی فراگیر از حامیان ایجاد کنیم. بنابراین تابستان را صرف کمپین جذب حامی کردیم. تا روز کارگر (اولین دوشنبه ماه سپتامبر) بیش از

۸۰ حامی با ارسال یادداشت‌های مشاور دادگاه به پرونده ملحق شدند. در این گروه نمایندگانی از همه بخش‌های صنعت فناوری، جامعه کسب‌وکار، رسانه‌ها و حتی مسئولان سابق و مورد احترام وزارت دادگستری و اف‌بی‌آی حضور داشتند.

وکلا و مردم روز ۲۳ ژانویه ۲۰۱۷ به دادگاه قاضی روبارت رفتند. یک سال و دو روز از تصمیم‌مان برای مقابله با دستور منع انتشار مهروموم‌شده به جای تسلیم می‌گذشت. اکنون فرصت برگزاری دادگاهی عمومی در مورد دادخواست دولت برای ما فراهم شده بود. دادگاه در حالی برگزار می‌شد که مسئولان سابق وزارت دادگستری در ردیف جلو برای حمایت از ما حضور یافته بودند.

روبارت دو هفته بعد دادخواست دولت را رد کرد و حکم داد که پرونده‌مان می‌تواند در دادگاه بررسی شود. هرچند قاضی استدلال دولت را پذیرفته بود که نمی‌توانیم از حقوق متمم چهارم مشتریان‌مان دفاع کنیم، اما موافقت کرد که ادعایمان در مورد متمم اول می‌تواند موجه باشد. از این مرحله به سلامت عبور کرده بودیم و باید برای مبارزه بعدی آماده می‌شدیم.

وزارت دادگستری بیشتر حواسش را جمع کرد و خواسته‌های ما را جدی‌تر گرفت. بعد از چند جلسه بحث، این وزارتخانه سیاست جدیدی را منتشر کرد که محدودیت‌های روشنی را برای درخواست دستور منع انتشار از سوی مدعی‌العموم‌ها تعیین می‌کرد. این وزارتخانه همراه با این سیاست راهنمای جدیدی را هم ارائه داد که از نماینده‌های دادستانی می‌خواست در مورد احکام مربوط به سازمان‌ها پیش از مراجعه به ارائه‌دهندگان خدمات ابری به خود سازمان‌ها مراجعه کنند. از این اتفاقات راضی بودیم و به‌طور علنی اعلام کردیم که فکر می‌کنیم رویکرد جدید کمک می‌کند اطمینان حاصل شود که دستورات محرمانگی فقط در موارد ضروری و برای مدت‌زمان تعریف‌شده استفاده می‌شوند. هر دو طرف توافق کردیم که به پرونده شکایت دستور منع انتشار خاتمه دهیم.

این نتیجه تعادل ظریف بین حریم خصوصی و امنیت را برجسته کرد. دعوی قضایی معمولاً ابزارهای کم‌اثری هستند. به خودی خود فقط می‌توانند تعیین کنند که فرایندهای موجود قانونی هستند یا خیر. نمی‌توان با آنها پیشنهاد جدیدی تهیه

کرد که به نحوه حکمرانی بر فناوری رسیدگی کند. رسیدن به این خواسته مستلزم گفت‌وگوی واقعی و گاهی اوقات مذاکره و حتی قانون‌گذاری جدید است. در این مورد دعوی قضایی کاری را انجام داد که لازم بود؛ همه را دور هم جمع کرد تا در مورد آینده صحبت کنند، اما جمع‌کردن همه برای گفت‌وگو در مورد مسائل دیگر، چالشی ادامه‌دار باقی ماند؛ چالشی که در ادامه دشوارتر و مهم‌تر شد.

فصل سوم

حریم خصوصی

یکی از حقوق بنیادین بشر

در زمستان ۲۰۱۸ بعد از روزی پرمشغله از رویدادهای عمومی و جلسات پشت سر هم در برلین، آماده بودیم که به استراحت برویم، اما «درک بورنمن» و «تانیا بوم» از تیم آلمانی شرکت نظر دیگری داشتند. تأکید کردند که به‌عنوان آخرین ایستگاه از زندانی قدیمی در شمال شرقی شهر بازدید کنیم.

یک هفته قبل، چنین فرصت سرگرم‌کننده‌ای کنجکاوی‌مان را برانگیخته بود، اما هوای بسیار سرد و خستگی ناشی از پرواز اشتیاق‌مان را فرونشانده بود. با این حال این تغییر مسیر به یکی از به‌یادماندنی‌ترین روزهای آن سال تبدیل شد.

در حالی که از خیابان‌های پایتخت برلین عبور می‌کردیم، نور زمستانی به‌مرور محو می‌شد. از شیشه ماشین معماری شهر را می‌دیدیم که به‌سرعت از پیش چشم‌مان رد می‌شد و داستان گذشته شهر را تعریف می‌کرد. هرچه به مقصد نزدیک می‌شدیم، عمارت‌های بزرگی که تاریخچه‌شان به دوره‌های پروس، امپراتوری آلمان، جمهوری وایمار و آلمان نازی برمی‌گشت، جای خود را به بلوک‌های بتنی بی‌روح دوره کمونیسم می‌دادند. مقصد زندان سابق «هونشونهازن» (Hohenschönhausen) جمهوری دموکراتیک آلمان (آلمان شرقی) بود.

این زندان زمانی مجموعه نظامی بسیار محرمانه و مقر اشتازی یا به عبارت دیگر وزارت امنیت آلمان شرقی بوده است. اشتازی نقش «سپر و شمشیر» آلمان شرقی را داشت و با نظارت سرکوبگرانه و مهندسی افکار عمومی بر کشور حکومت می‌کرد. هنگام سقوط دیوار برلین اشتازی تقریباً ۹۰ هزار مأمور داشت که با شبکه‌ای مخفی شامل بیش از ۶۰۰ هزار «شهروند ناظر» پشتیبانی می‌شدند که در آلمان شرقی، جاسوسی همکاران و همسایگان‌شان و گاهی اوقات خانواده خودشان را می‌کردند. اشتازی مقادیر سرسام‌آوری از پرونده‌ها، اسناد، عکس‌ها و نوارهای ویدئویی و صوتی را جمع‌آوری کرده بود که اگر کنار هم ردیف می‌شدند، ۶۹ مایل طول می‌داشتند. از پایان جنگ جهانی دوم تا انتهای جنگ سرد، شهروندانی که احتمال داده می‌شد از کشور فرار کنند یا رژیم آنها را تهدید یا مردم‌گریز می‌دانست، دستگیر و تهدید می‌شدند و در هونشونهازن بازجویی می‌شدند.

وقتی در ورودی این زندان سابق باز شد، از روبه‌روی یک برج دیدبانی بتنی عبور

کردیم. آنجا با زندانی سابق ۷۵ساله‌ای به نام «هانس یوخن شیدلر» ملاقات کردیم. اندام ورزشکاری و لبخند بی‌ریایش نه با سن و سالش و نه با سختی‌هایی که در این زندان کشیده بود، همخوانی نداشت. به گرمی دستان‌مان را فشرد و ما را به سمت ساختمان خاکستری بزرگی راهنمایی کرد که هفت ماه تاریک و سخت را در آن سپری کرده بود.

شیدلر سال ۱۹۶۸ برلین را ترک کرده بود تا برای گذراندن دوره دکتری فیزیک به دانشگاه «چارلز» در پراگ برود. با یادآوری دوره معروف به بهار پراگ و کاهش محدودیت‌ها و آزادسازی سیاسی که آن سال در پایتخت چکسلواکی اتفاق افتاده بود، می‌گفت: «بهار پراگ یکی از شادترین دوره‌های زندگی‌ام بود. همه آخر هفته‌ها بهار پراگ را جشن می‌گرفتم.» اما با ورود نیم‌میلیون سرباز پیمان ورشو به چکسلواکی و سرکوب اصلاحات، حرکت این کشور به سمت آزادی خیلی زود متوقف شد.

آگوست آن سال، شیدلر ۲۴ساله در خانه‌اش در برلین بود که این اخبار ناگوار را شنید. رویای عصری جدید، عصری که آن را «نسخه‌ای انسانی‌تر» از سوسیالیسم توصیف می‌کرد، بر باد رفته بود. شیدلر و چهار نفر از دوستانش در اعتراض به این اتفاقات اعلامیه‌های کوچکی چاپ می‌کنند که از رژیم شوروی انتقاد می‌کند و همان شب آنها را به صندوق پستی خانه‌های مردم برلین شرقی می‌اندازند.

آن شب اشتازی هر پنج نفر را هنگام انجام این کار دستگیر می‌کند و به همین مکانی می‌فرستد که اکنون ما ایستاده بودیم. هفت ماه را در یکی از همین سلول‌های کوچک و تاریکی گذرانده که ما بازدید کردیم. در این مدت اجازه نداشته سایر زندانیان را ببیند، با افراد دیگر صحبت کند یا حتی یک صفحه مطلب بخواند. والدینش نمی‌دانستند کجاست و چرا ناپدید شده است. شکنجه‌های روانی بی‌رحمانه‌ای را تحمل کرده بود. شیدلر حتی بعد از آزادی نیز اجازه نداشته در رشته مورد نظرش یعنی فیزیک مطالعه یا کار کند.

ناگهان هدف بازدید آن روز ما روشن شد.

امروزه مانند دوران شیدلر نیست که بخش زیادی از کنشگری سیاسی از کف خیابان شروع شود؛ بلکه از اینترنت شروع می‌شود. ارتباطات الکترونیکی و رسانه‌های

اجتماعی بستری را برای افراد فراهم کرده‌اند تا حامیان‌شان را بسیج، پیام‌شان را منتشر و نظر مخالف‌شان را ابراز کنند و در عرض چند روز به هدفی برسند که دستیابی به آن در بهار پراگ هفته‌ها طول می‌کشید. اقدام هانس یوخن در دهه ۱۹۶۰ معادل ایمیل‌فرستادن امروزی بود و انگار هنگام فشردن دکمه «ارسال» دستگیر شده بود.

وقتی در مورد مسائل حریم خصوصی در مایکروسافت صحبت می‌کردیم، اغلب از نقش دولت آلمان در تصویب و اجرای قوانین جدید حرف می‌زدیم. درک و تانیا می‌خواستند بی‌واسطه ببینیم چرا آنها و سایر آلمانی‌ها اهمیت زیادی به این مسائل می‌دهند. شرکت‌های فناوری به‌عنوان کارگزاران مقادیر زیادی از داده‌های شخصی، باید ریسک‌های قرار گرفتن داده‌ها در اختیار افراد نامناسب را به‌اندازه‌ای درک کنند که احتمالاً فقط افراد تحت ظلم نازی‌ها و اشتازی می‌توانند درک کنند. درک می‌گفت: «بسیاری از افرادی که به این زندان می‌افتادند، برای کارهایی دستگیر می‌شدند که در حریم خصوصی خانه‌هایشان انجام داده بودند. سیستم نظارت مطلقی وجود داشت که برای کنترل افراد طراحی شده بود.»

توضیح می‌داد که تجربه‌های دوران نازی و اشتازی، آلمانی‌های عصر مدرن را نسبت به نظارت الکترونیکی محتاط کرده و افشاگری‌های اسنودن این بدگمانی‌ها را تقویت کرده است. درک می‌گفت: «وقتی داده‌ها جمع‌آوری می‌شوند، همیشه امکان سوءاستفاده وجود دارد. وقتی در نقاط مختلف دنیا فعالیت می‌کنیم، باید به یاد داشته باشیم که دولت‌ها می‌توانند با گذشت زمان تغییر کنند. به حوادث اینجا دقت کنید. داده‌هایی که در مورد افراد (دیدگاه‌های سیاسی، مذهبی و اجتماعی آنها) جمع‌آوری می‌شوند، ممکن است به دست افراد نامناسبی بیفتند و مشکلات گوناگونی ایجاد کنند.»

در ردموند وقتی با کارمندان در مورد حریم خصوصی حرف می‌زدم، داستان شیدلر به من کمک کرد مسائلی را تشریح کنم که هنگام مدیریت داده‌های مشتریان‌مان در معرض خطر هستند. حریم خصوصی فقط رگولیشنی نیست که باید از آن پیروی کنیم؛ بلکه یکی از حقوق بنیادین بشر است که تعهدی اخلاقی به حفاظت از آن داریم.

این داستان همچنین به افراد کمک کرد درک کنند جهانی‌شدن رایانش ابری فقط به

معنی کار گذاشتن کابل‌های فیبر نوری در کف اقیانوس‌ها و ایجاد مراکز داده در سایر قاره‌ها نیست؛ بلکه در عین حال به معنی انطباق با فرهنگ سایر کشورها و همزمان پایبندی به تعهدات‌مان به ارزش‌های محوری با احترام‌گذاشتن به حقوق حریم خصوصی افراد و حفاظت از این حقوق است.

یک دهه پیش برخی افراد حاضر در بخش فناوری فکر می‌کردند می‌توانند صرفاً از طریق مراکز داده مستقر در ایالات متحده به مشتریان سراسر جهان خدمت‌رسانی کنند، اما تجربه عملی، این تفکر را رد کرد. افراد انتظار داشتند صفحات وب، ایمیل‌ها و اسناد تصویری و گرافیکی به‌صورت آنی در تلفن‌ها و کامپیوترهایشان بارگذاری شوند. آزمایش مشتریان نشان داد که تأخیری فقط نیم‌ثانیه‌ای افراد را کلافه می‌کند. طبق قوانین فیزیک، مراکز داده باید در کشورهای بیشتری ساخته می‌شدند تا لازم نباشد محتوا برای رسیدن به دست کاربر، نصف دنیا را در کابل‌ها طی کند. این نزدیکی جغرافیایی کلید کاهش مقوله‌ای به نام «تأخیر داده» یا تأخیر در انتقال است.

حتی پیش از شروع ساخت مرکز داده‌مان در کوئینسی نیز به‌دنبال میزبانی اروپایی برای اولین مرکز داده‌مان در خارج از ایالات متحده بودیم. پیشگام اولیه، بریتانیا بود، اما کمی بعد ایرلند هم خودی نشان داد.

ایرلند از دهه ۱۹۸۰ به‌نوعی خانه دوم بخش فناوری آمریکا بود. مایکروسافت اولین شرکت فناوری بود که سرمایه‌گذاری زیادی در این کشور انجام داد. مشوق‌های مالیاتی و نیروی کار انگلیسی‌زبان اولین عوامل جذب شرکت‌ها به «جزیره زمرد» (لقب کشور ایرلند) بودند. ایرلند در آن زمان از عضویتش در اتحادیه اروپا و روحیه میهمان‌نوازی‌اش به‌منظور جذب افراد از نقاط مختلف اروپا و سپس سراسر جهان برای زندگی و کار در این کشور و به‌ویژه ناحیه دوبلین استفاده می‌کرد. دولت ایرلند با این کار اقتصاد کشور را رشد داد و رفاه پایداری برای این کشور ایجاد کرد. ما در مایکروسافت به ارتباطات و مشارکت‌مان در این رشد افتخار می‌کردیم.

در دهه ۱۹۸۰ مشتریان اروپایی‌مان نرم‌افزارهای ما را با سی‌دی‌هایی نصب می‌کردند که در ایرلند تولید می‌شد، اما به‌تدریج که نرم‌افزارها به ابر منتقل شدند، ایرلندی‌ها متوجه شدند که کسب‌وکار سی‌دی سرانجام منقرض خواهد شد. باید فرصت

اقتصادی جدیدی را برای کشورشان ایجاد می‌کردند.

وزارت تشکیلات، تجارت و اشتغال ایرلند در پیش‌بینی این آینده و ایجاد زیربنایی که مراکز داده را به این کشور جذب کند، کار فوق‌العاده‌ای انجام داد. وقتی هنوز برنامه تعریف‌شده‌ای برای ابر نداشتیم، هیئتی از این وزارتخانه به دیدار من و دیگران آمدند و استدلال و توجیه‌شان را برای استقرار اولین مرکز داده اروپایی‌مان در نزدیکی دوبلین ارائه کردند. در این هیئت نمایندگی مقام ارشدی به‌نام «رونالد لانگ» حضور داشت که وقتی در شرکت «کاوینگتون اند برلینگ» در لندن کار می‌کردم، همکارم بود. زمانی یک روز بعدازظهر را در دوبلین صرف بحث و گفت‌وگو با او در مورد مسئله چالش‌برانگیزی در زمینه سیاست عمومی کرده بودم.

در جلسه‌مان در ردموند با اکراه مکثی کردم و توضیح دادم که ساخت اولین مرکز داده اروپایی‌مان در ایرلند امکان‌پذیر نیست. هیچ کابل فیبر نوری پرسرعتی وجود نداشت که ایرلند را به اروپای قاره‌ای (خشکی اصلی اروپا منهای جزایر این قاره) متصل کند و در نبود چنین زیرساختی، ساخت مرکز داده در ایرلند منطقی نبود.

پاسخ ران ساده بود: «سه ماه به ما فرصت بدهید.»

چطور می‌توانستیم به چنین خواسته‌ای پاسخ منفی بدهیم.

در عرض سه ماه دولت ایرلند مذاکرات برای احداث زیرساختی با همان نوع کابل مورد نیاز را انجام داد و ما فرایند ساخت مرکز داده‌ای در جنوب دوبلین را شروع کردیم. در ابتدا با ساختمانی کوچک شروع کردیم، سپس مدام ساختمان‌های بیشتری را اضافه کردیم.

مایکروسافت در سال ۲۰۱۰ شروع به ذخیره‌سازی داده‌های مشتریان سراسر اروپا در ایرلند کرد. امروزه مراکز داده‌ای در چند کشور دیگر سراسر اروپا داریم، اما هیچ‌کدام به بزرگی مرکز داده ایرلند نیستند که معادل بزرگ‌ترین تأسیسات‌مان در ایالات متحده است. مساحت این مرکز دو مایل مربع است. این مرکز داده و مراکز داده بزرگ تحت مدیریت آمازون، گوگل و فیس‌بوک کمک کرده‌اند ایرلند از جزیره‌ای کوچک به ابرقدرت داده‌ای تبدیل شود.

در حال حاضر ایرلند یکی از بهترین مکان‌های دنیا را برای مراکز داده فراهم کرده

است. هرچند برخی افراد ممکن است فکر کنند مشوق‌های مالیاتی دلیل اصلی این مسئله است، اما سایر عوامل بسیار مهم‌تر هستند. یکی از این عوامل آب‌وهواست. در دوره‌ای که مراکز داده در مجموع بزرگ‌ترین مصرف‌کننده برق جهان هستند، آب‌وهوای معتدل ایرلند دمای ایدئال را برای کامپیوترها فراهم می‌کند. ساختمان‌ها نیازی به سیستم سرمایش ندارند و گرمای در گردش ناشی از سرورها اغلب برای گرم‌کردن ساختمان‌ها در زمستان کافی است.

اما مهم‌تر از آب‌وهوا فضای سیاسی ایرلند است. این کشور هم بخشی از اتحادیه اروپاست و هم از اجماع محلی پایداری بهره می‌برد که به حقوق بشر احترام می‌گذارد و از آن محافظت می‌کند. سازمان حفاظت از داده قدرتمند، اما واقع‌بینی وجود دارد که فناوری را به‌خوبی می‌شناسد و در عین حال اطمینان حاصل می‌کند که شرکت‌های فناوری از اطلاعات شخصی کاربران‌شان محافظت می‌کنند.

زمانی که از کشورهای خاورمیانه بازدید می‌کردم، به مسئولان گفتم: «رابطه ایرلند با داده مثل رابطه سوئیس با پول است.» به عبارت دیگر این کشور مکانی است که افراد باید به‌دنبال ذخیره‌سازی ارزشمندترین اطلاعات شخصی‌شان در آن باشند. به نظر می‌رسد در ایرلند کمتر از همه نقاط دنیا این احتمال وجود دارد که معادلی مدرن برای آن زندان اشتازی ایجاد شود.

متأسفانه عملیات جهانی مراکز داده بسیار پیچیده‌تر از آن شده که بتوان به‌سادگی همه داده‌ها را در مکانی مثل ایرلند ذخیره کرد. یکی از دلایل این پیچیدگی این است که اکنون کشورهای بیشتری خواستار ذخیره‌سازی داده‌هایشان درون مرزهای خودشان هستند. هرچند این دیدگاه هرگز مورد علاقه بخش فناوری نبوده، اما از برخی جهات قابل درک است و تا حدی به مسئله حیثیت ملی مربوط می‌شود. این کار همچنین تضمین می‌کند که دولت قوانین خودش را اعمال کند و مطمئن شود که احکام تفتیش می‌توانند به همه داده‌های کشور دسترسی داشته باشند.

فشار برای استقرار مراکز داده در کشورهای بیشتر به پیدایش مسئله‌ای منجر شده که به‌سرعت در حال تبدیل‌شدن به یکی از مهم‌ترین مسائل حقوق بشری جهان است. با توجه به ذخیره‌سازی اطلاعات شخصی همه در ابر، رژیمی مستبد و مصمم

به نظارت فراگیر می‌تواند به‌دنبال این خواسته‌های ظالمانه برود که نه‌تنها بر ارتباطات افراد؛ بلکه بر آنچه می‌خوانند و تماشا می‌کنند نیز نظارت کند. دولت‌ها با داشتن چنین اطلاعاتی می‌توانند افرادی را که تهدید به حساب می‌آورند، تحت تعقیب قانونی قرار دهند، اذیت کنند و حتی اعدام کنند.

این مسئله یکی از واقعیت‌های بنیادین زندگی است که همه افراد شاغل در بخش فناوری باید هر روز به خودشان یادآوری کنند. خوش‌اقبالیم که در یکی از سودآورترین بخش‌های اقتصادی دوران زندگی‌مان کار می‌کنیم، اما در این زمینه منافع مالی در معرض خطر، بسیار کم‌اهمیت‌تر از مسئولیتی است که در برابر آزادی و زندگی افراد داریم.

به همین دلیل هر تصمیمی برای استقرار مرکز داده مایکروسافت در کشوری جدید مستلزم ارزیابی حقوق بشری مفصل است. در این موارد خودم یافته‌ها را بازبینی می‌کنم و هر وقت این یافته‌ها نگرانی ایجاد کنند، به‌ویژه وقتی پاسخ نهایی باید منفی باشد، شخصاً مداخله می‌کنم. کشورهایی وجود دارند که مرکز داده‌ای در آنها مستقر نکرده‌ایم و نخواهیم کرد؛ زیرا از لحاظ حقوق بشر پرریسک هستند. در کشورهای دیگری که کم‌ریسک‌تر هستند نیز نه داده‌های مشتریان؛ بلکه فقط داده‌های کسب‌وکارها را ذخیره می‌کنیم، تمهیدات حفاظتی بیشتری را در نظر می‌گیریم و در موردشان هوشیار و گوش‌به‌زنگ هستیم. خواسته‌های جدید می‌توانند به‌ناگهان بحران‌های بی‌سروصدا، اما شدیدی به وجود بیاورند. شب و روزهایی هستند که شهامت اخلاقی مسئولان خدمات ابری را به بوته آزمایش می‌کشند.

حتی وقتی همه این شرایط برقرار است، باز هم مسئله دیگری می‌تواند همه سپرهای حفاظتی ناشی از ذخیره‌سازی داده‌ها در مکانی مثل ایرلند را بی‌اثر کند. چنین اتفاقی زمانی می‌افتد که دولت کشوری یک شرکت فناوری را ملزم به تحویل داده‌های ذخیره‌شده در کشوری دیگر می‌کند. اگر فرایند قاعده‌مندی وجود نداشته باشد که از حقوق بشر محافظت کند، کشورهای سراسر دنیا می‌توانند به مرزهای یکدیگر و حتی به مکان‌های امنی مثل ایرلند نفوذ کنند.

از جهاتی مسئله جدیدی نیست. قرن‌هاست که دولت‌های سراسر جهان توافق

کرده‌اند که قدرت هر دولتی، از جمله احکام تفتیش آن، به مرزهایش محدود می‌شوند. دولت‌ها این قدرت را داشتند که افراد را دستگیر کنند و خانه‌ها، اداره‌ها و ساختمان‌های موجود در حوزه استحفاظی خودشان را تفتیش کنند، اما نمی‌توانستند به کشور دیگری وارد شوند، فردی را بربایند یا اسنادی را بردارند و باید از طریق دولت همان سرزمین مستقل اقدام می‌کردند.

دولت‌ها در مواردی این سیستم را نادیده گرفته و خودسرانه اقدام کرده‌اند. در یکی از این موارد این نوع بی‌توجهی به مرزها تنش‌های بین‌المللی را افزایش داد و در وقوع رخدادهایی نقش داشت که در نهایت به جنگ ۱۸۱۲ بریتانیا و ایالات متحده منجر شد. خصومت‌های دو کشور زمانی افزایش یافت که نیروی دریایی پادشاهی بریتانیا بر دریاها حاکم بود، اما همیشه برای جنگ دریایی‌اش با ناپلئون سرباز کم داشت. بریتانیایی‌ها برای برطرف‌کردن مشکل کمبود نیرو «گروه‌های سربازگیری» را به کشتی‌های خارجی و بندرهای بیگانه می‌فرستادند تا افراد را بربایند و به خدمت اجباری ببرند. هرچند فرض بر این بود که نیروی دریایی پادشاهی مشمولان بریتانیایی را می‌گیرد، اما گروه‌های سربازگیری به گذرنامه افراد نگاه نمی‌کردند. وقتی آشکار شد که این گروه‌ها افراد را بدون استثنا می‌برند و برخی شهروندان آمریکا را به خدمت اجباری نیروی دریایی پادشاهی درآورده‌اند، ایالات متحده خواستار برخوردی در این زمینه شد. کشور تازه‌تأسیس آمریکا به‌طور کامل ورود کشتی‌های بریتانیایی به بندرهای آمریکا را ممنوع کرد. پیام روشن بود: یا به قانون‌مان احترام بگذارید یا از کشورمان بروید.

از قرار معلوم جنگ ۱۸۱۲ لازم بود تا هر دو دولت به منطق بازگردند و در مورد احترام به حاکمیت یکدیگر به توافق برسند. بنابراین نوع جدیدی از پیمان‌های بین‌المللی ظهور کرد که استرداد مجرمان و دسترسی به اطلاعات کشورهای دیگر را امکان‌پذیر می‌ساخت. بسیاری از این توافق‌نامه‌های جدید، معاهده معاضدت قضایی دوجانبه خوانده می‌شدند. با این حال در طول دهه گذشته آشکار شد که این معاهدات اغلب برای عصر رایانش ابری مناسب نیستند. نهادهای مجری قانون از کندی فرایند این معاهدات ناراحت بودند، مسئله‌ای که قابل درک است، اما هرچند دولت‌ها در مورد روش‌هایی برای به‌روزرسانی این توافق‌نامه‌ها و افزایش سرعت فرایند بحث می‌کردند،

اما سرعت پیشرفت در این زمینه کم بود.

وقتی داده‌ها به ابر منتقل شدند، عوامل اجرای قانون در پی راهی برای دور زدن فرایند معاهده معاضدت قضایی دوجانبه رفتند. آنها سعی می‌کردند حکمی را برای یک شرکت فناوری مستقر در حوزه استحفاظی خودشان بگیرند و خواستار ایمیل‌ها و فایل‌هایی شوند که در مرکز داده‌ای مستقر در کشوری دیگر ذخیره شده بودند. از نگاه آنها دیگر لازم نبود که به معاهدات معاضدت قضایی دوجانبه اتکا کنند. حتی نیاز نبود به دولت دیگر بگویند چه کار می‌کنند.

با این حال مشخص بود که بیشتر دولت‌ها از اینکه یک شرکت فناوری داده‌های شهروندان‌شان را استخراج کند و به کشوری خارجی بدهد و در نتیجه تمهیدات حفاظتی قانونی آنها را دور بزند، راضی نبودند. در سال ۱۹۸۶ که کنگره ایالات متحده قانون حریم خصوصی ارتباطات الکترونیکی را تصویب کرد، بندی را در آن قرار داد که اطمینان حاصل می‌کرد کشورهای دیگر نمی‌توانند چنین کاری انجام دهند. نمی‌خواستند ببینند کشورهای خارجی اقدامی شبیه کار گروه‌های سربازگیری را در مورد داده‌های دیجیتال انجام می‌دهند. بر اساس این قانون شرکت‌های فناوری آمریکایی در صورت تحویل برخی از انواع داده‌های دیجیتال مثل ایمیل، حتی در پاسخ به درخواست قانونی دولتی خارجی نیز جرم مرتکب شده‌اند. قانون «شنود» سال ۱۹۶۸ نیز به همین ترتیب رهگیری یا شنود ارتباطات درون ایالات متحده را برای کشورهای خارجی جرم شناخت. در حقیقت افراد باید بر مبنای معاهده معاضدت قضایی دوجانبه از طریق فرایند بین‌المللی تعیین‌شده عمل می‌کردند.

قوانین اروپا به این روشنی نبودند، اما می‌دانستیم دیدگاه‌های آنها به‌اندازه افراد درون کشور خودمان اهمیت دارند. آنها هم درست مانند مسئولان آمریکایی علاقه‌ای به نفوذ دولت‌های خارجی به سرزمین‌شان نداشتند، به‌ویژه به این دلیل که اتحادیه اروپا و اعضایش قوانین سخت‌گیرانه‌ای را برای حفاظت از حقوق حریم خصوصی شهروندان‌شان تصویب کرده بودند. می‌دانستیم که مانند کشتی‌های بریتانیایی در بندرهای آمریکایی در اوایل قرن نوزدهم، مراکز داده ما هم فقط زمانی در خاک اروپا پذیرفته خواهند شد که موافقت کنیم به قوانین محلی احترام بگذاریم.

با این حال وقتی رایانش ابری فراگیرتر و داده‌ها در دسترس‌تر شدند، دولت‌ها دیگر نتوانستند در برابر وسوسه اقدام یک‌جانبه برای دسترسی به داده‌های موجود در کشورهای دیگر مقاومت کنند. وقتی پرونده به پرونده و مجزا بررسی می‌کردیم، چنین اقداماتی قابل درک بودند. بازرس یکی از نهادهای مجری قانون به اطلاعاتی نیاز دارد و می‌خواهد هرچه سریع‌تر به آن برسد. وقتی می‌تواند شرکت فناوری مستقر در همان نزدیکی را مجبور کند که کارش را سریع‌تر راه بیندازد، چه دلیلی دارد که فرایند زمان‌بر استفاده از معاهده معاضدت قضایی دوجانبه با دولتی دیگر را طی کند؟ اگر آن دولت دیگر معترض می‌شد، کسی با دادستان محلی کاری نداشت و آن شرکت فناوری بود که باید با عواقب آن اقدام دست‌وپنجه نرم می‌کرد.

طولی نکشید که ما هم در مایکروسافت در میانه این نبردهای جدید قرار گرفتیم. سعی می‌کردیم به‌نوعی جلوی گلوله‌های دو طرف جاخالی بدهیم. بررسی پرونده‌هایی در دو کشور تصویر روشنی از این چالش ارائه می‌دهد.

یکی از این کشورها برزیل بود. صبح یکی از روزهای ژانویه ۲۰۱۵ یکی از رهبران شرکت زیرمجموعه‌مان در برزیل برای جلسه فروش در ردموند حضور داشت که از اتاق جلسه به راهرو رفت تا پاسخ تماس همسرش را بدهد. آن خانم در منزل‌شان در سائوپائولو بود و سراسیمه به نظر می‌رسید. پلیس برزیل برای دستگیری شوهرش آمده و خواسته بود در آنجا حاضر شود. با زور از ورودی‌های ساختمان عبور کرده و آپارتمانش را پلمب کرده بودند. جرمش چه بود؟ کار کردن برای مایکروسافت.

پلیس برزیل پافشاری می‌کرد که ارتباطات شخصی مربوط به تحقیقات جنایی در جریانی را طبق قانون برزیل تحویل دهیم، اما در آن زمان مرکز داده‌ای در برزیل نداشتیم و در نتیجه در واقع این کار باید در ایالات متحده انجام می‌شد. توضیح دادیم که طبق قانون ایالات متحده این کار جرم محسوب می‌شود و ترغیب‌شان کردیم که به جای این کار از فرایند معاهده معاضدت قضایی دوجانبه موجود بین دو کشور استفاده کنند. مسئولان برزیلی مخالف پیشنهاد ما بودند. پیش از این در موقعیتی مشابه علیه یکی دیگر از مدیران ارشد محلی ما در سائوپائولو پرونده‌ای کیفری تشکیل داده بودند و جریمه‌ها بر ضد مایکروسافت ماه به ماه بیشتر می‌شدند.

از نیت جونز خواستیم تلاش کند از طریق مذاکره با مسئولان برزیلی به توافق برسد. بعداً گفته بود: «در موقعیت بسیار دشواری قرار داشتیم و مسئولان برزیلی نمی‌خواستند کوتاه بیایند.»

برای نیت پرداختن به این مسئله از دفتر امنش در ردموند آسان بود، اما رهبران محلی ما در برزیل از چنین نعمتی برخوردار نبودند. مراجع قانونی سائوپائولو یکی از مدیران ارشدمان را مدت کوتاهی به زندان انداختند و تا چند سال حاضر نشدند پرونده کیفری علیه او را مختومه اعلام کنند. بی‌درنگ هزینه‌های دفاع از او در دادگاه را پذیرفتیم و گفتیم اگر بخواهند او و خانواده‌اش را از برزیل خارج می‌کنیم. همچنین در مورد بیش از ۲۰ میلیون دلار جریمه علیه شرکت درخواست تجدیدنظر کردیم.

منشاء چالش دوم ایالات متحده بود. در اواخر سال ۲۰۱۳ حکمی به دست‌مان رسید که خواستار سوابق ایمیل مربوط به تحقیقاتی در مورد قاچاق مواد مخدر می‌شد. هرچند چنین حکمی عادی بود، اما بررسی حساب مورد نظر به‌سرعت نشان داد که مسئله‌ای غیرعادی وجود دارد. به نظر می‌رسید این ایمیل‌ها به فردی تعلق دارد که شهروند ایالات متحده نیست. اطلاعات هم نه در خاک آمریکا؛ بلکه در ایرلند ذخیره شده بودند.

امیدوار بودیم اف‌بی‌آی و وزارت دادگستری در این مورد از دولت ایرلند کمک بخواهند. در هر حال ایالات متحده و ایرلند متحدان و دوستان نزدیکی هستند که معاهده معاضدت قضایی دوجانبه به‌روزشده‌ای را امضا کرده‌اند. با مسئولان در دوبلین صحبت کردیم و آنها اعلام کردند مایل به همکاری هستند، اما مسئولان وزارت دادگستری به رویه‌ای که با این شیوه ایجاد می‌شد، علاقه‌ای نداشتند و نمی‌خواستند آن را دنبال کنند. گفتند باید از حکم پیروی کنید.

رویه برای ما هم به همان اندازه مهم بود. اگر دولت ایالات متحده می‌توانست بی‌اعتنا به قانون ایرلند یا حتی خبر دادن به دولت این کشور، به این کشور نفوذ کند، هر کشور دیگری هم می‌توانست این کار را انجام دهد و می‌توانستند تلاش کنند این کار را در هر جایی انجام دهند. بنابراین تصمیم گرفتیم به جای پذیرش حکم، شکایت کنیم. دسامبر ۲۰۱۳ پرونده‌مان را به دادگاه فدرال نیویورک بردیم. وقتی به سمت ساختمان

دادگاه در میدان «فولی» در منهتن جنوبی حرکت می‌کردیم، به یاد سال‌های اول دوران شغلی‌ام افتادم. اولین سال بعد از فارغ‌التحصیلی از مدرسه «حقوق کلمبیا» در سال ۱۹۸۵ را برای قاضی ناحیه‌ای و در طبقه بیست‌ودوم همین ساختمان باریک در نزدیکی وال‌استریت کار کرده بودم. این کار منشی‌گری دیدگاهی از درون سیستم به سازوکار قانون به من داد.

نیویورک با جایی که در آن بزرگ شده بودم، یعنی «اپلتون» (Appleton) در شمال شرقی ایالت ویسکانسین تفاوت زیادی داشت. هرچند فضای این شهر بزرگ با فضای تربیتی «میدوسترنی» (ایالت‌های غرب میانه آمریکا) من فرق داشت، اولین روز کاری متوجه نبودم که خودم هم نوعی پدیده جدید هستم. علاوه بر اینکه اشتیاق یک فارغ‌التحصیل تازه دانشکده حقوق را داشتم، ظاهرم نیز برای این ساختمان دادگاه بلند غیرعادی بود؛ کارمندی جدید که کامپیوتر شخصی سنگین اما قدرتمندی را با خود حمل می‌کرد.

اولین کامپیوترم را پاییز سال قبل خریده بودم؛ زمانی که این دستگاه‌ها هنوز برای بسیاری از افراد رایج نبود. راستش را بگویم آی‌بی‌ام پی‌سی جونیور (IBM PCjr) که خیلی زود تولیدش متوقف شد، آنچنان هم کامپیوتر محسوب نمی‌شد، اما نرم‌افزاری را روی آن نصب کرده بودم که سال آخر دانشکده حقوق را متحول کرده بود. آن نرم‌افزار نسخه ۱٫۰ مایکروسافت ورد بود. آن‌قدر دوستش داشتم که هنوز دیسک‌ها، دفترچه راهنما و قاب پلاستیکی‌اش را در دفتر خانگی‌ام دارم. در مقایسه با خودکار و کاغذ یا ماشین تحریری که در دانشکده از آن استفاده کرده بودم، پردازش ورد شگفت‌انگیز بود. می‌توانستم هم سریع‌تر و هم بهتر بنویسم. بنابراین همسرم، «کتی» را که خودش هم وکیل تازه‌کاری بود، متقاعد کردم که باید پیش از شروع شغل اولم ۱۰ درصد از حقوق ۲۷ هزار دلاری سالانه‌ام را برای خرید کامپیوتری بهتر صرف کنم و در دفتر کارم نصب کنم. خدا را شکر که از تصمیم من حمایت کرد.

قاضی‌ای که برایش کار می‌کردم، آن زمان ۷۲ساله بود و دفتری که میز من در آن قرار داشت پر از طاقچه‌هایی بود که جعبه‌هایی بسیار مرتب و منظم حاوی یادداشت‌های دست‌نویس دقیق او از بیش از دو دهه دادگاه و پرونده روی آنها قرار داشت. سیستم

بایگانی ماهرانه (و آزمایش‌پس‌داده‌ای) وجود داشت به همراه کارت‌های تایپ‌شده برای هر کدام از نکاتی که باید برای راهنمایی هیئت‌منصفه جمع‌آوری می‌شد. ورودم با کامپیوتر شخصی تعجب برخی افراد را برانگیخت. آن موقع بود که اهمیت استفاده از کامپیوتر برای بهتر انجام‌دادن کارهای مورد نیاز (یعنی نوشتن یادداشت‌های اداری و پیش‌نویس حکم‌های قانونی) بدون برهم‌زدن شیوه‌های قدیمی همچنان کارآمد را فهمیدم. درس ارزشمندی بود که همچنان آن را سرلوحه خود قرار داده‌ام؛ از فناوری برای بهبود کارهایی که می‌توانند بهبود یابند و در عین حال احترام‌گذاشتن به شیوه‌های کارآمد موجود استفاده کنید.

به سال ۲۰۱۴ برگردیم که باز هم در حال وارد کردن فناوری رایانش جدید به همان دادگاه بودیم. می‌دانستیم احتمالاً نبردی طولانی را در پیش داریم. این دیدگاه‌مان خیلی زود تأیید شد؛ قاضی بخش، علیه ما حکم داد و زمینه را برای ورود به مسیر طولانی تجدیدنظرخواهی فراهم کرد.

پرونده ما به‌ویژه در اروپا با واکنش عمومی سریعی مواجه شد. یک ماه بعد از شکست در دادگاه اول، برای شرکت در مجموعه‌ای از جلسات سفر کردم که از برلین و با دیدار با مسئولان دولتی، نمایندگان مجلس، مشتریان و خبرنگاران شروع می‌شد. هرچند می‌دانستم پرونده حکم مربوط به ایرلند مورد توجه خواهد بود، اما انتظار نداشتم این پرونده این‌چنین در کانون توجهات قرار بگیرد. وقتی ساعت هشت صبح اولین روز سفر گفت‌وگو با خبرنگاری را شروع کردم، در به یاد آوردن نام قاضی بخشی که حکم اولیه را علیه ما صادر کرده بود، به تقلا افتادم. تیم دادخواهی ما این شکست را فراموش و خودش را احیا کرده بود و برای دور دوم در برابر قاضی ناحیه آماده می‌شد. ما از آن شکست عبور کرده بودیم، اما خیلی زود فهمیدم که آلمانی‌ها هنوز عبور نکرده‌اند.

در انتهای دو روز حضور در برلین، جزئیات حکم و نام قاضی بخشی که آن را صادر کرده بود، در حافظه‌ام ثبت شده بود. هر جا می‌رفتم، افراد تقریباً بلافاصله شروع به حرف‌زدن با من در مورد قاضی فرانسیس می‌کردند. تقریباً هیچ‌کس به‌جز حلقه حقوقی کوچکی در نیویورک، نامش را نشنیده بود، اما در سال ۲۰۱۴ در برلین، «جیمز سی فرانسیس چهارم»، قاضی بخشی که علیه ما حکم داده بود، به نامی آشنا تبدیل

شده بود.

به نظر می‌رسید پرسش‌ها پایانی ندارند. «منظورش از فلان سخن چی بود؟ چرا فلان حرف را زد؟ بعد چه شد؟» آلمانی‌ها رونوشت‌هایی از حکم قاضی فرانسیس آورده بودند که بادقت حاشیه‌نگاری شده بودند. تعداد کمی از افراد فرازهایی از متن را برای من بلند می‌خواندند. بسیاری از افراد نیز تمام صفحات را مطالعه کرده بودند.

تا بعدازظهر روز اول که با مدیر ارشد فناوری اطلاعات شعبه شرکت در یکی از بزرگ‌ترین ایالت‌های آلمان جلسه داشتم، واقعاً خسته شدم. یادم می‌آید آن مدیر ارشد فناوری اطلاعات حکم قاضی فرانسیس را روی میز ساخته‌شده از چوب ماهون بین ما گذاشت. انگشت اشاره‌اش را مستقیم به سمت این حکم قانونی گرفت و گفت: «اگر نتوانید این حکم را عوض کنید، هرگز امکان ندارد ایالت من داده‌های ما را در مرکز داده شرکتی آمریکایی ذخیره کند.»

تمام آن سال این مسئله ما را در سفرهای بین‌المللی دنبال می‌کرد. در توکیو انتظار نداشتم همان واکنشی را ببینم که در برلین تجربه کرده بودم، اما در یک میهمانی جمعی از مشتریان سازمانی من را احاطه کردند و اصرار داشتند که شخصاً به من بگویند نتیجه پرونده مرکز داده ایرلند چقدر برای کسب‌وکارشان مهم است. بارها تکرار کردند که «مایکروسافت باید در این پرونده پیروز شود». آنها هم بادقت مسیر پرونده ما را در دادگاه‌ها دنبال می‌کردند. در حضورهای عمومی سراسر دنیا به‌کرات عهد کردم که پرونده را رها نمی‌کنیم و اگر لازم باشد آن را تا دیوان عالی هم می‌بریم.

در حالی که پرونده به‌آهستگی پیش می‌رفت، متوجه شدیم که حتی اگر برنده شویم، باز هم این دادخواهی محدودیت‌های خودش را دارد. می‌توانست نفوذ احکام تفتیش بر اساس قانون موجود را زیر سؤال ببرد، اما نمی‌توانست قانون جدید یا نسل جدیدی از معاهدات بین‌المللی مورد نیاز برای عبور از معاهدات معاضدت قضایی دوجانبه منسوخ‌شده را مستقر کند.

شروع به تهیه پیش‌نویس پیشنهادهای جدید کردیم و در ادارات دولتی سراسر جهان به‌دنبال متحدانی گشتیم که ممکن بود رهبری طرح‌های گسترده‌تر مورد نیاز را بر عهده بگیرند. قانونی در کنگره ارائه شد، اما باید این قانون را با توافق‌نامه‌های

بین‌المللی جدید همراه می‌کردیم.

در مارس ۲۰۱۵ فرصت مناسبی به دست آوردیم. جلسه‌ای که در کاخ سفید در آن شرکت کردم، فرصتی برای بازبینی مسائل حریم خصوصی و نظارت جاری فراهم کرد. در حالی که پرونده کیفری علیه مدیر ارشد برزیلی‌مان و جریمه‌های مایکروسافت را تشریح می‌کردم، رئیس‌جمهور حرفم را قطع کرد و گفت: «شرایط آشفته به نظر می‌رسد.» حاضران بحث کردند و رئیس‌جمهور از فرصتی برای تدوین رویکردی جدید به توافق‌نامه‌های بین‌المللی، ترجیحاً با یک یا دو دولت متحد کلیدی مثل بریتانیا یا آلمان حمایت کرد.

۱۱ ماه بعد در فوریه ۲۰۱۶ و با کمی سروصدا، بریتانیا و ایالات متحده پیش‌نویسی را برای توافق‌نامه اشتراک‌گذاری اطلاعات دوجانبه مدرن‌تر پیشنهاد دادند. یکی از عناصر مورد نیازمان داشت پدیدار می‌شد، اما این توافق بدون تصویب قانونی جدید در کنگره نمی‌توانست اجرایی شود و با وجود حمایت‌های فراگیر کنگره، وزارت دادگستری همچنان مانع تصویب هر گونه قانونی می‌شد که نحوه استفاده این وزارتخانه از احکام تفتیش برای جمع‌آوری داده‌ها از سراسر دنیا را تغییر می‌داد. با بن‌بستی در قانون‌گذاری مواجه شدیم و بدون توافقی فراگیرتر نمی‌شد در مورد چشم‌انداز موفقیت‌مان خوش‌بین باشیم.

اما در ادامه دیوان عالی بن‌بست را به‌صورت غیرمنتظره‌ای شکست.

تا فوریه ۲۰۱۸ طول کشید، اما سرانجام در صبحی گرم‌تر از انتظار با پای پیاده از خیابان «فرست» در واشنگتن دی‌سی به سمت ساختمان مروارید‌گون بلند دیوان عالی ایالات متحده می‌رفتیم. توقفی کردیم تا نمای باشکوه مکانی را هضم کنیم که قرار بود در آن پیامدهای جهانی رایانش ابری به ۹ قاضی دیوان ارائه شود.

ساختمان چهارطبقه باعظمت دیوان عالی درست روبه‌روی کاخ کنگره است. در واقع در تقاطع فیزیکی قوه‌های قضائیه و مقننه آمریکا قرار داشتیم. به یک جهت که نگاه می‌کردیم، ساختمان گنبدی‌شکل براق کنگره دیده می‌شد و وقتی برمی‌گشتیم، چشم‌مان به پله‌های مرمری عریض و بالای آنها ستون‌های بلند دیوان عالی می‌افتاد. بعد از آن به دو در بلند حکاکی‌شده یعنی ورودی دیوان می‌رسیدیم.

وقتی روز ۲۷ فوریه به دیوان رسیدیم، صف بلندی از افراد روی آن راه‌پله‌های نمادین و آن اطراف ایستاده بودند. گروهی از ناظران امیدوار منتظر تماشای نبرد ما با دولت خودمان بودند. این مرحله آخرین رویارویی قضایی نبردی بود که چهار سال پیش شروع شده بود، یعنی زمانی که انتقال ایمیل از آن سوی اقیانوس اطلس به این سو را نپذیرفتیم.

چهارمین باری بود که مایکروسافت برای پرونده‌ای در برابر دیوان عالی استدلال می‌کرد که همیشه برایم تجربه برجسته‌ای بوده است. مسائل ناشی از مدرن‌ترین فناوری‌های جهان را به دادگاهی می‌بریم که همان شکل و شمایلی را دارد که تقریباً یک قرن پیش داشت. همراه داشتن هر گونه تلفن یا لپ‌تاپ ممنوع است. هر بار بعد از تحویل دستگاه‌های همراهم، در صندلی‌ام در تالار سرخ بزرگ می‌نشینم؛ تالاری که شبیه صحنه‌های نمایش پرده‌دار است. بعد به تنها فناوری این دادگاه یعنی ساعت دادگاه نگاه می‌کنم.

به‌تدریج به ارزش توانایی دیوان عالی در بررسی پیامدهای فناوری در محیطی بدون هیچ ابزار فناوری مدرن واقف شده‌ام. اولین پرونده‌مان در این دادگاه که به سال ۲۰۰۷ برمی‌گشت، شامل مسائل مربوط به پتنتی بود که اتفاقاً از عملیات تولید سی‌دی مایکروسافت در ایرلند ناشی می‌شد. یک هفته بعد از دادگاه با یکی از مدیران ارشد دادگاه برخورد کردم که گفت: «وقتی برخی قاضی‌ها صحبت می‌کردند، کمی مضطرب به نظر می‌رسیدید.»

متوجه شدم که در نمایش چهره‌ای خونسرد از خودم موفق نبوده‌ام. هنوز آن موقعیت را به یاد دارم. در آن زمان یکی از قاضی‌ها در حال بحث با وکیل طرف مقابل در مورد پیامدهای «ارسال فوتون‌ها» از نیویورک به کامپیوترهای اروپا از طرف مایکروسافت بود.

با خودم فکر می‌کردم «این پرونده چه ربطی به فوتون دارد؟ چرا در مورد نیویورک صحبت می‌کنیم؟»

اما درس ارزشمندی گرفته بودم که مهم‌تر از نیاز به حفظ چهره خونسرد در طول جلسه استماع بود. قاضی‌ها همیشه همه جزئیات جدیدترین فناوری‌ها را درک

نمی‌کنند، اما منشی‌های جوان‌تری دارند که درک می‌کنند. به‌علاوه قاضی‌ها این درک مبتنی بر واقعیت‌ها را با خرد و درایتی تکمیل می‌کنند که اغلب فراتر از قانون است. با وجود اعتراضات عمومی به فرایند انتخاب قاضی‌ها و برخی پرونده‌های بحث‌برانگیز، دیوان عالی همچنان یکی از نهادهای واقعاً معتبر جهان است. بیشتر روزها ۹ قاضی در کنار هم تلاش می‌کنند با استدلال مسائل چالش‌برانگیز را حل کنند. در دادگاه‌های نقاط مختلف دنیا بوده‌ام و به دستاوردهایی که دیوان عالی ایالات متحده می‌تواند کسب کند، ایمان پیدا کرده‌ام.

آن روز صبح بعد از یک ساعت استدلال شفاهی، ۹ قاضی دادگاه به نحوی جلسه را ترک کردند که هیچ‌کدام از دو طرف به اندازه کافی از پیروزی اطمینان نداشتند. هرچند می‌شد حدس‌های زیادی در مورد طرف پیروز زد، اما پیش‌بینی با اطمینان بالا غیرممکن بود. قاضی‌ها خواسته یا ناخواسته بهترین شرایط را برای ترغیب دو طرف به توافق ایجاد کرده بودند.

اما مانعی بزرگ باقی بود؛ دو طرف تنها زمانی می‌توانستند در مورد ضروری‌نبودن صدور حکم در دیوان عالی به توافق برسند که قانونی جدید تصویب می‌شد. به عبارت دیگر رسیدن به توافق مستلزم قانون جدیدی بود که فقط در آن سمت خیابان فرست، یعنی در ساختمان کنگره می‌توانست تصویب شود.

از جهتی درخواست تصویب قانون از کنگره مانند درخواست معجزه بود. کنگره تقریباً در مورد هیچ مسئله‌ای اتفاق نظر نداشت و به‌ندرت قانون تصویب می‌کرد، اما فرصت کوتاهی پیدا شد. در مورد گزینه‌هایمان با «فرد هامفریز»، از افراد ذی‌نفوذ باسابقه واشنگتن و رهبر تیم امور دولتی شرکت گفت‌وگو کردم. همراه با کاخ سفید به این نتیجه رسیدیم که تلاش کنیم.

اتفاقی که در ادامه افتاد، بدون تلاش‌های چهارساله اعضای هر دو حزب در سنا و مجلس نمایندگان امکان‌پذیر نبود. بعد از دو جلسه استماع در قوه مقننه و بازنویسی‌های متعدد، برای آخرین دور از بحث‌ها با وزارت دادگستری جلسه گذاشتیم. بانی این جلسه سناتور «لیندسی گراهام» بود که بدین منظور از جایگاهش به‌عنوان رئیس کمیته فرعی جرم و تروریسم در کمیته قضایی سنا استفاده کرده بود.

گراهام با اراده محکم تلاش می‌کرد افراد را به همکاری تشویق کند. تقریباً یک سال پیش در مه ۲۰۱۷ جلسه استماعی با تعداد زیادی شرکت‌کننده برگزار کرده بود که من در آن شهادت داده بودم. دولت بریتانیا نیز با توجه به پیامدهای این مسئله برای توافق بین‌المللی‌اش با ایالات متحده، «پدی مک‌گینس»، معاون مشاور امنیت ملی را فرستاده بود تا شهادت بدهد. طبع دلپذیر اسکاتلندی‌اش را با درکی عمل‌گرا، اما سخت‌گیرانه از ملزومات نبرد با تروریسم در بریتانیا ترکیب کرده بود. مشاور امنیت ملی کاخ سفید، «تام بوسرت» به‌طور منظم با مک‌گینس گفت‌وگو می‌کرد و همه را به پیدا کردن وجوه مشترک در کنگره ترغیب می‌کرد.

کمی بعد از بحث در برابر دیوان عالی، متنی جدید برای قانون شکل گرفت که هر دو طرف برای پشتیبانی از آن به توافق رسیدند. نام جدیدی هم به آن داده شد. این نام «قانون شفاف‌سازی کاربرد خارجی قانونی داده‌ها» یا قانون کلود بود.

این قانون بندهایی داشت که برای ما مهم بودند؛ بین نفوذ بین‌المللی احکام تفتیش که وزارت دادگستری خواستار آن بود با به رسمیت شناختن حق شرکت‌های فناوری برای به چالش کشیدن احکام در صورت تعارض قوانین تعادل برقرار شده بود. یعنی اگر ایرلند، آلمان یا کل اتحادیه اروپا می‌خواستند از طریق قوانین محلی‌شان مانع اجرای احکام تفتیش خارجی یک‌جانبه شوند و در عوض رویکرد شفاف‌تر یا مشارکتی‌تری را اتخاذ کنند، می‌توانستند این کار را انجام دهند و ما هم می‌توانستیم در دادگاه‌های ایالات متحده به آن رویکرد استناد کنیم.

مسئله مهم‌تر این بود که قانون کلود اختیار جدیدی را برای توافق‌نامه‌های بین‌المللی مدرن ایجاد می‌کرد که می‌تواند جایگزین این تلاش‌های یک‌جانبه شود. این توافق‌نامه‌ها می‌توانند با فرایندهای سریع‌تر و مدرن‌تر، توانایی دسترسی به داده‌ها در کشوری دیگر را به مجریان قانون بدهند. در عین حال قواعدی بر این فرایندها حاکم هستند که از حریم خصوصی و سایر حقوق بشر حفاظت می‌کنند. این قانون مانند همه قوانین، به‌ویژه آنهایی که با سازش و مصالحه همراه هستند، بی‌نقص نبود، اما بیشتر، آن خواسته‌هایی را دربر می‌گرفت که چهار سال برای پیشبردشان تلاش کرده بودیم.

اما پیدا کردن ابزاری برای الحاق قانون کلود به آن و تصویب این قانون، همچنان مشکل بزرگی بود. بعید بود که سنا و مجلس نمایندگان هر دو در تقویم قانون‌گذاری خود زمانی برای بررسی جداگانه این مسئله پیدا کنند، به‌ویژه با توجه به زمان کمی که تا صدور حکم دیوان عالی مانده بود. در نتیجه باید آن را به قانون دیگری ضمیمه می‌کردیم.

متوجه شدیم که تنها شانس واقعی برای تصویب این پیشنهاد ضمیمه‌کردن آن به لایحه بودجه است. به دو دلیل این کار چالش سختی بود؛ اول اینکه کنگره در تصویب لایحه‌های بودجه با مشکل روبه‌رو بود و دوم اینکه به همین دلیل رهبران کنگره مایل به الحاق پیشنهادهای غیربودجه‌ای به لایحه‌های بودجه نبودند.

با این حال مشخص بود که با پشتیبانی سناتور گراهام، جمهوری‌خواهان سنا نیز ممکن است از این ایده پشتیبانی کنند، اما اگر دموکرات‌های سنا مخالفت می‌کردند، قانون به جایی نمی‌رسید. بلافاصله فهمیدیم فردی وجود دارد که می‌تواند بسیار تأثیرگذار باشد. از بسیاری جهات او را نه‌تنها به‌عنوان رهبری در قوه مقننه؛ بلکه به‌عنوان فردی واقعاً بانفوذ و پرانرژی می‌دانستیم. این فرد «چاک شومر»؛ رهبر اقلیت سنا بود. هرچند آشنایی کمی با این مسئله داشت، اما به‌سرعت در مورد آن تحقیق و هدف ما را درک کرد و پذیرفت.

وقتی بوسرت، گراهام و شومر را پشت سرمان می‌دیدیم، تلاش برای همراه‌کردن رهبران مجلس نمایندگان را آغاز کردیم. طولی نکشید که «پل رایان»، رئیس و «نانسی پلوسی»، رهبر اقلیت مجلس نمایندگان غرق گفت‌وگو در مورد درج قانون کلود در لایحه بودجه شدند. مذاکرات به دور دیگری از اصلاحات منجر شد. چند روز یک‌بار به نظر می‌رسید تلاش‌هایمان بی‌ثمر خواهد شد، اما مدام با بوسرت صحبت می‌کردیم و همه مصمم بودیم که تسلیم نشویم. به طرز شگفت‌آوری بعد از چندین دور تماس و گفت‌وگو تلاش‌هایمان به نتیجه رسید. رئیس‌جمهور دونالد ترامپ ۲۳ مارس ۲۰۱۸ لایحه بودجه‌ای را امضا کرد که این قانون هم در آن وجود داشت. قانون کلود حالا دیگر واقعاً قانون شده بود و می‌توانستیم در فاصله کوتاهی در مورد پرونده دیوان عالی به توافق برسیم.

از زمانی کـه اولین‌بار بـه دادگاه فـدرال در نیویورک رفتـه بودیم، بیش از چهار سـال می‌گذشت، اما از زمانی که از پله‌های ساختمان دیوان عالی پایین آمده بودیم، کمتر از یک ماه سپری شده بود. مراحل نهایی با چنان سـرعتی پیش رفته بود که افراد دخیل در همه جزئیات را غافلگیر کرده بود.

هرچند از نتایـج راضی بودیم، اما احساسـات دوگانه‌ای هم داشـتیم. معتقد بودیم قانون کلود می‌توانـد قانون قدرتمندی باشـد، اما ماننـد همه قوانین و همـه توافق‌های دادگاهی با سازش‌هایی همراه بود. درسی که خیلی وقت پیش گرفته بودیم، این بود که به مبارزه رفتن جذاب‌تر است، اما معامله و توافق‌کردن ثمره بیشتری دارد. معامله‌کردن معمولاً تنها راه پیشرفت بود؛ البته معاملات هم مستلزم مقداری بده‌بستان است.

همچنین مسـتلزم انجام اقدامـات مؤثر برای تشـریح نتیجه هسـتند؛ به‌ویژه وقتی کـه نتیجه پیچیده اسـت. بـه همین دلیـل و دلایل دیگـر معمولاً بـرای طیفـی از نتایج برنامه‌ریزی می‌کردیـم و برای هر مورد محتوای اطلاع‌رسـانی آماده داشـتیم، اما قانون کلود چنـان سـریع به پیـش رفتـه بـود و زمـان بسـیار زیـادی را از مـا بـرای گفت‌وگو با سیاست‌مداران گرفته بود که به اندازه کافی و لازم برای این نتیجه آماده نبودیم.

مشتریان، گروه‌های حامی حریم خصوصی و مسئولان دولتی سراسر جهان شروع به پرس‌وجو در مورد محتوای قانون کلود و سـازوکار واقعی آن کردند. مشـتریان سؤال داشـتند و گروه‌های حامی حریـم خصوصی نگران بودنـد. بنابراین به تکاپـو افتادیم و کمی بعد گزارش‌هایی را به سراسر جهان ارائه دادیم و محتوایی را منتشر کردیم تا این خلأ را پـر کنیم. این اقـدام تقریباً نماینـدگان فروش مایکروسـافت در همه کشـورها را دربر می‌گرفت. این مسـئله را زمانی کاملاً درک کردم که یک ماه بعد در فرانسه یکی از کارمندان مایکروسافت متوقفم کرد. این کارمند در حال شام‌خوردن در رستورانی بود که من را در حال رد شدن از آنجا دیده و شناخته بود. در حالی که شامش سرد می‌شد، من را دنبال کرده بود. وقتی به من رسید، کمی صبر کرد تا نفسش جا بیاید و پرسش‌هایش در مورد این قانون جدید را در ذهنش آماده کند.

نتیجه همزمان نشـان می‌داد تاکنون چه دستاوردهایی داشته‌ایم و جهان همچنان بایـد چـه مسـیری را طـی کنـد. اکنـون چارچوبـی بـرای آینـده‌ای متفـاوت بـر مبنـای

توافق‌نامه‌های جدید میان کشورها وجود دارد. همان‌طور که «ریچارد داونینگ»، معاون دادستان کل ایالات متحده، در سالگرد تصویب قانون کلود گفت، این قانون «صرفاً راه‌حلی برای چالش کنونی ارائه نمی‌دهد؛ بلکه نوعی راه‌حل آرمانی نیز ارائه می‌دهد». بعد توضیح داد که «هدف این راه‌حل ایجاد گروهی از کشورهای هم‌فکر و تکریم‌کننده حقوق بشر است که به حاکمیت قانون وفادار هستند. در این گروه کشورها می‌توانند تعارضات قانونی‌شان با یکدیگر را به حداقل برسانند و منافع دوجانبه‌شان را بر اساس ارزش‌های مشترک و احترام متقابل به پیش ببرند».

اما قانون کلود مانند شالوده‌ای است که خانه‌های جدید باید روی آن ساخته شوند. در جهانی زندگی می‌کنیم که مجریان قانون باید سریع اقدام کنند، حریم خصوصی و سایر حقوق بشر باید محافظت شوند و مرزهای کشورها باید محترم شمرده شوند.

توافق‌نامه‌های بین‌المللی جدید می‌توانند به همه این اهداف برسند؛ البته به شرطی که با تفکر و تأمل تدوین شده و با ثبات قدم دنبال شوند. به عبارت دیگر هنوز باید سال‌های زیادی تلاش کنیم.

فصل چهارم

امنیت سایبری

زنگ خطری برای جهان

«پاتریک وارد» ۱۲ مه ۲۰۱۷ به اتاق آماده‌سازی قبل از جراحی در بیمارستان «سنت بارتالومیو» در بخش مرکزی لندن برده شد. این مرکز درمانی بسیار بزرگ که مردم محلی آن را با نام بارت می‌شناسند، چند خیابان با کلیسای جامع «سنت پل» (St. Paul's Cathedral) فاصله دارد؛ جایی که این بیمارستان در سال ۱۱۲۳ در زمان پادشاهی «هنری اول» بنیان‌گذاری شد. این بیمارستان در دوران بمباران هوایی پیاپی هیتلر بی‌وقفه به فعالیت ادامه داد و با افتخار از جنگ جهانی دوم و بمب‌هایی جان سالم به در برد که مدام لندن را هدف می‌گرفتند و گاهی به این بنای مشهور و زیبا برخورد می‌کردند، اما در تاریخ ۹۰۰ساله بارت، هیچ بمبی بیشتر از اتفاقی که آن صبح جمعه افتاد، ویرانی به بار نیاورد.

«وارد» سه ساعت طول کشیده بود تا از روستای کوچکش در شهرستان «دورست» (Dorset) در نزدیکی شهر جنوبی «پول» (Poole) در انگلستان، به آنجا بیاید. خانواده‌اش از اواخر قرن نوزدهم در این منطقه ساحلی کشاورزی کرده بودند؛ منطقه‌ای با مناظری چشم‌نواز که انگار از وسط کتاب‌های داستان گلچین شده‌اند. شغل «وارد» هم با خانه آرام و باصفایش هم‌خوانی داشت. مدیر فروش باسابقه «پربک آیس‌کریم» (Purbeck Ice Cream)، تولیدکننده بستنی‌های باکیفیت و گران‌قیمت بود. عاشق شغلش بود. به ما می‌گفت: «برای صحبت‌کردن و بستنی‌خوردن حقوق می‌گرفتم و هر دوی این کارها را می‌توانم خیلی خوب انجام دهم.»

دو سال برای گرفتن وقت جراحی در بارت برای ترمیم یک نارسایی جدی قلبی به نام «کاردیومیوپاتی» صبر کرده بود. این بیماری نارسایی ژنتیکی است که دیواره قلب را ضخیم می‌کند و این مرد انگلیسی میانسال اهل کوهنوردی و فوتبال را در انجام بیشتر کارهای روزانه ناتوان کرده بود. آن روز صبح موهای سینه «وارد» تراشیده شد و مجموعه‌ای از آزمایش‌ها روی بدنش انجام شد. روی تخت چرخ‌دار بیمارستان دراز کشیده بود و انتظار عملی را می‌کشید که مدت‌ها به‌دنبالش بود. جراح به او سر زد و گفت: «فقط چند دقیقه دیگر باید منتظر بمانی. به‌زودی در اتاق عمل می‌بینمت.» اما «وارد» هرگز به اتاق عمل نرفت.

بیش از یک ساعت بعد پزشک دوباره آمد و گفت: «هک شده‌ایم. تمام سیستم

بیمارستان از کار افتاده است. نمی‌توانم جراحی را انجام بدهم.» بیمارستانی که در طول جنگ جهانی دوم همواره فعال مانده بود، هدف حمله سایبری گسترده‌ای قرار گرفته و ناگهان فلج شده بود. همه سیستم‌های کامپیوتری بیمارستان از کار افتاده بودند. آمبولانس‌ها به مراکز درمانی دیگر فرستاده می‌شدند، قرارهای ملاقات لغو شده بودند و خدمات جراحی آن روز بسته شده بودند. این حمله یک‌سوم خدمات سلامت ملی (National Health Service) بریتانیا را که بیشتر خدمات مراقبت سلامت در انگلستان را ارائه می‌کند، فلج کرده بود.

آن روز صبح در ردموند تیم رهبری ارشد مایکروسافت در حال برگزاری جلسه عادی جمعه‌ها بود. این گردهمایی‌های هفتگی با ساتیا نادلا و ۱۴ مقام زیردست مستقیم او همیشه ساعت هشت صبح در اتاق هیئت‌مدیره شرکت آغاز می‌شوند. این اتاق در همان طبقه‌ای قرار دارد که دفتر چند نفر از ما در آن واقع شده است. در این جلسات به بحث‌های متنوعی در مورد محصول و طرح‌های کسب‌وکار می‌پردازیم و بعدازظهر جلسه را به اتمام می‌رسانیم. اما جلسه ۱۲ مه ۲۰۱۷ مثل همیشه نبود.

پیش از اتمام بحث در مورد دومین موضوع، ساتیا بحث را قطع کرد و گفت: «از طریق چند ایمیل به من در مورد حمله سایبری گسترده‌ای علیه مشتریان‌مان خبر داده‌اند. چه خبر است؟»

خیلی زود متوجه شدیم مهندسان امنیت مایکروسافت در واکنش به تماس‌های مشتریان به تکاپو افتاده‌اند و تلاش می‌کنند دلیل این حمله به‌سرعت در حال گسترش را پیدا کرده و آثار آن را ارزیابی کنند. تا زمان ناهار دیگر برایمان مشهود بود که این اتفاق هکی عادی نیست. مهندسان مرکز اطلاعات تهدید مایکروسافت (MSTIC-Microsoft Threat Intelligence Center) که ما آن را «میستیک» می‌خوانیم، به‌سرعت آن بدافزار را با کدی تطبیق دادند که گروهی به‌نام «زینک» (روی) دو ماه پیش با آن آزمایشی را انجام داده بودند. میستیک به هر گروه هک دولتی اسم رمزی بر اساس عنصری از جدول تناوبی داده است. در این مورد اف‌بی‌آی معتقد بود زینک به دولت کره شمالی وابسته است. زینک همان گروهی بود که یک سال‌ونیم پیش شبکه کامپیوتری «سونی پیکچرز» را از کار انداخته بود.

جدیدترین حمله آنها از دیدگاه فنی به شکلی غیرعادی پیچیده بود. کد بدافزار جدیدی را به نرم‌افزار اولیه زینک اضافه کرده بودند که به آلودگی این امکان را می‌داد که به‌صورت کرم رایانه‌ای از کامپیوتری به کامپیوتر دیگر برود. کد بعد از تکثیر، دیسک سخت کامپیوتر را رمزنگاری و قفل می‌کرد، بعد پیام باج‌خواهانه‌ای را نمایش می‌داد که برای ارسال کلیدی الکترونیکی که داده‌ها را بازیابی می‌کرد، ۳۰۰ دلار می‌خواست. بدون این کلید نیز داده‌های کاربر تا ابد مسدود و خارج از دسترس می‌ماندند.

آغاز این حمله سایبری از بریتانیا و اسپانیا بود و در عرض چند ساعت در سراسر دنیا پخش شد و در نهایت ۳۰۰ هزار کامپیوتر را در بیش از ۱۵۰ کشور آلوده کرد. پیش از آنکه فرایند تحولش را طی کند، جهان آن را به نام «واناکرای» (می‌خواهم گریه کنم) به خاطر سپرد؛ رشته کد نرم‌افزاری مخربی که نه‌تنها باعث می‌شد مدیران فناوری اطلاعات بخواهند گریه کنند؛ بلکه در نقش زنگ خطری ناخوشایند برای جهان ظاهر شد.

کمی بعد نیویورک‌تایمز گزارش داد که پیچیده‌ترین بخش کد واناکرای را آژانس امنیت ملی ایالات متحده توسعه داده تا از یکی از آسیب‌پذیری‌های ویندوز سوءاستفاده کند. آژانس امنیت ملی احتمالاً این کدها را برای نفوذ به کامپیوترهای دشمنانش ساخته بود. اما ظاهراً این نرم‌افزار دزدیده شده بود و از طریق گروه ناشناسی به‌نام «شدو بروکرز» (Shadow Brokers) به بازار سیاه ارائه شده بود که کدهای مسموم را در محیط آنلاین منتشر می‌کند تا خرابی به بار بیاورد. «شدو بروکرز» سلاح پیشرفته آژانس امنیت ملی را در دسترس همه افرادی قرار داده بود که می‌دانستند کجا می‌توانند آن را پیدا کنند. هرچند ارتباط روشنی بین این گروه با فرد یا سازمان مشخصی وجود نداشت، اما متخصصان جامعه اطلاعات تهدید، حدس می‌زدند که این گروه نماینده کشوری است که تمایل زیادی به ایجاد اختلال دارد. در این مورد زینک باج‌افزار قدرتمندی را به کد آژانس امنیت ملی اضافه کرده و سلاح سایبری آلوده‌کننده‌ای را ایجاد کرده بود که باقدرت در سراسر اینترنت پخش می‌شد.

همان‌طور که یکی از مدیران امنیت شرکت می‌گفت؛ «آژانس امنیت ملی یک راکت توسعه داده بود و کره شمالی آن را به موشک تبدیل کرده بود، تفاوت این دو در کلاهک

است». در واقع ایالات متحده سلاح سایبری پیشرفته‌ای را توسعه داده بود، کنترل آن را از دست داده بود و کره شمالی از آن برای انجام حمله‌ای علیه تمام جهان استفاده کرده بود.

نقشه‌ای که تا چند ماه قبل نامحتمل به نظر می‌رسید، اکنون خبر روز شده بود. اما آن‌قدر وقت نداشتیم که به کنایه‌آمیز بودن موقعیت فکر کنیم. باید تلاش می‌کردیم به مشتریان کمک کنیم سیستم‌های آلوده را شناسایی کنند، گسترش بدافزار را متوقف کنیم و کامپیوترهایی را که غیرفعال شده بودند، احیا کنیم. تا ظهر تیم امنیت ما به این جمع‌بندی رسید که نسخه‌های جدیدتر ویندوز به واسطه وصله‌ای که دو ماه پیش منتشر کرده بودیم، در برابر این حمله مصون بودند، اما دستگاه‌های قدیمی‌تری که ویندوز ایکس‌پی داشتند، مصون نبودند.

این مسئله کم‌اهمیت نبود. هنوز بیش از صد میلیون کامپیوتر در جهان وجود داشتند که از سیستم‌عامل ویندوز ایکس‌پی استفاده می‌کردند. سال‌ها تلاش کرده بودیم مشتریان را متقاعد کنیم که دستگاه‌هایشان را ارتقا بدهند و نسخه جدیدتری از ویندوز را نصب کنند. ویندوز ایکس‌پی در سال ۲۰۰۱، شش سال پیش از اولین آیفون اپل و شش ماه پیش از اولین آیپاد عرضه شده بود. هرچند می‌توانستیم برای آسیب‌پذیری‌های خاصی وصله‌هایی را عرضه کنیم، اما فناوری‌ای بسیار قدیمی مثل ویندوز ایکس‌پی به هیچ‌وجه نمی‌توانست با تهدیدات امنیتی کنونی همگام باشد. اینکه انتظار داشته باشیم نرم‌افزاری با قدمت ۱۶ سال در برابر حملات نظامی‌گونه امروز مقاومت کند، مانند این بود که برای مقاومت در برابر موشک سنگر خاکی حفر کنیم.

با وجود تشویق‌ها، تخفیف‌ها و به‌روزرسانی‌های رایگان، برخی از مشتریان با این سیستم‌عامل قدیمی کار می‌کردند. در حالی که به‌دنبال ارتقای پایگاه سیستم‌عامل‌های نصب‌شده بودیم، در نهایت تصمیم گرفتیم همچنان به ساخت وصله‌های امنیتی برای سیستم‌های قدیمی ادامه دهیم، اما بر خلاف نسخه‌های جدیدتر، مشتریان سیستم‌های قدیمی باید این وصله‌ها را به‌صورت بخشی از خدمات اشتراکی می‌خریدند. البته هدف ما ایجاد مشوقی مالی برای ارتقا به نسخه امن‌تری

از ویندوز بود.

هرچند اتخاذ این رویکرد در بیشتر موقعیت‌ها منطقی به نظر می‌رسید، اما حمله ۱۲ مه متفاوت بود. کرم‌بودن واناکرای به این بدافزار این امکان را می‌داد که با سرعتی غیرعادی گسترش پیدا کند. باید جلوی آسیب را می‌گرفتیم؛ در نتیجه این مسئله به گفت‌وگوهای پرحرارتی درون مایکروسافت منجر شد. آیا باید وصله ویندوز ایکس‌پی برای این حمله را در سراسر جهان در دسترس همه قرار دهیم، حتی افرادی که اشتراک امنیتی تهیه نکرده بودند و از جمله کامپیوترهایی که از نسخه‌های دزدی نرم‌افزار ما استفاده می‌کردند؟ ساتیا بحث را متوقف و اعلام کرد که وصله را به رایگان برای همه منتشر می‌کنیم. وقتی برخی افراد داخل مایکروسافت مخالفت کردند و گفتند این اقدام تلاش ما برای ترغیب افراد به کنار گذاشتن ایکس‌پی را تضعیف می‌کند، ساتیا مخالفان را با ایمیلی آرام کرد که در آن نوشته شده بود: «الان وقت مذاکره نیست. دامنه آلودگی خیلی گسترده شده است.»

در حالی که به پیشرفت‌های فنی برای مهار و کاهش آلودگی واناکرای دست یافته بودیم، پیامدهای سیاسی در حال افزایش بود. ساعت شام آن روز جمعه در سیاتل، صبح شنبه در پکن بود. مسئولان دولت چین با تیم‌مان در پکن تماس گرفتند و به «تری مایرسون» که رهبری واحد ویندوز را بر عهده داشت، ایمیل زدند و در مورد وضعیت وصله‌های ویندوز ایکس‌پی از او سؤال کردند.

با توجه به اینکه چین بیشتر از هر کشوری دستگاه‌های دارای ویندوز ایکس‌پی داشت، این پرس‌وجو برای ما غافلگیرکننده نبود. چین تا حد زیادی از حمله اولیه در امان مانده بود؛ زیرا وقتی بدافزار در بعدازظهر جمعه به وقت محلی منتشر شده بود، بیشتر کامپیوترهای اداری این کشور برای آخر هفته خاموش شده بودند. با این حال دستگاه‌های دارای ویندوز ایکس‌پی منسوخ آنها همچنان آسیب‌پذیر بودند.

اما وصله‌های ایکس‌پی تنها مشغله ذهنی طرف چینی نبود. مسئولی که به تری ایمیل زده بود، در مورد مسئله مطرح‌شده در گزارش آن روز نیویورک‌تایمز سؤال کرده بود. آن گزارش ادعا کرده بود که دولت ایالات متحده در جست‌وجوی آسیب‌پذیری‌های نرم‌افزارها بوده و آنها را جمع‌آوری کرده و به جای اطلاع‌رسانی به شرکت‌های فناوری

بـرای برطرف‌کردن‌شـان، آنها را مخفی نگه داشـته اسـت. واکنـش ما را خواسـته بود. گفتیم در مورد این پرسـش نه با ما؛ بلکه بـا دولت ایالات متحده بایـد گفت‌وگو کنند. البته تعجب‌آور نبـود که این اقـدام دولت آمریـکا برای ما و سـایر شـرکت‌های فناوری خوشایند نباشد. اتفاقاً مدت زیادی بود که از دولت‌ها خواسته بودیم پس از شناسایی آسیب‌پذیری‌ها، آنها را اعلام کنند تا در راستای مصلحت عمومی برطرف شوند.

می‌دانسـتیم که این پرسـش تـازه اولین مورد از پرسـش‌های زیادی اسـت کـه افراد از سراسـر جهان مطـرح خواهند کرد. تا صبح شـنبه متوجه شـدیم که بایـد اقداماتی فراتر از پشتیبانی از مشتریان آسیب‌دیده‌مان انجام دهیم. باید عمومی‌تر به مسائل ژئوپلیتیـک در حـال ظهـور می‌پرداختیم. سـاتیا و مـن آن روز صبح مدتـی را به بحث تلفنی در مورد گام بعدی گذراندیم و به این نتیجه رسیدیم که برای پاسخگویی به موج پرسش‌های پیش رو در مورد واناکرای، اطلاع‌رسانی عمومی را در دستور کار قرار دهیم. بنابرایـن از جزئیات حملـه فاصلـه گرفتیم و بـه چشـم‌انداز فراگیرتر امنیت سـایبری پرداختیم.

به‌روشـنی اعلام کردیم که مایکروسـافت و سایر شـرکت‌های بخش فناوری مسئول اصلی حفاظت از مشتریان در برابر حملات سایبری هستند. این مسئولیت مسلم بود، اما فکر می‌کردیم باید بر این مسئله هم تأکید کنیم که مشتریان هم در امنیت سایبری مسئولیت پیدا کرده‌اند. باید به‌روزرسانی و ارتقای کامپیوترها را برای مشتریان آسان‌تر می‌کردیم، اما یکـی از درس‌های ایـن حادثه این بود که اگر پیشـرفت‌های ما اسـتفاده نشوند، خیلی مفید نخواهند بود.

به نکته سـومی هم اشـاره کردیـم؛ نکته‌ای کـه فکـر می‌کردیم حملـه واناکـرای آن را مشهود کرده است. در حالی که دولت‌های بیشتری توانایی‌های تهاجمی پیشرفته‌ای را توسعه می‌دهند، باید سلاح‌های سایبری‌شان را هم کنترل کنند. گفتیم «معادل سرقت واناکرای در سلاح‌های متعارف این است که تعدادی از موشک‌های «تاماهاک» ارتش ایالات متحده دزدیده شـوند». این حقیقت که سـلاح‌های سـایبری را می‌توان در یک فلش یواس‌بی ذخیره کرد (یا با آن دزدید)، محافظت از آنها را دشوارتر و مهم‌تر می‌کرد. برخی مسـئولان کاخ سـفید و آژانـس امنیت ملـی از اشـاره ما به موشـک تاماهاک

ناراحت شدند. برخی همتایان‌شان در دولت بریتانیا نیز با آنها موافق بودند و استدلال می‌کردند که «مقایسه واناکرای با تفنگ دقیق‌تر از مقایسه آن با موشک است». اما آیا تاکنون کسی با تفنگ همزمان به اهدافی در ۱۵۰ کشور ضربه زده است؟ در عین حال نکته اصلی چیز دیگری بود. این سخنان بیش از همه نشان می‌داد که مسئولان امنیت سایبری چقدر با حرف‌زدن مستقیم در مورد این مسائل در رسانه‌ها یا دفاع از شیوه‌هایشان در برابر مردم ناآشنا هستند.

مسئله‌ای که بیش از همه ما را غافلگیر کرد، جای خالی بحثی گسترده در مورد دلیل کره شمالی برای انجام این حمله بود. هنوز به پاسخ قطعی نرسیده‌ایم، اما نظریه بسیار کنجکاوی‌برانگیزی در این زمینه وجود دارد.

کره شمالی درست یک ماه قبل از حمله شکستی خجالت‌آور را در پرتاب موشکی خبرساز تجربه کرده بود. همان‌طور که «دیوید سنگر» و دو خبرنگار دیگر در آن زمان در نیویورک‌تایمز نوشتند، دولت ایالات متحده به‌دنبال کاهش سرعت برنامه موشکی این کشور «از جمله از طریق روش‌های جنگ الکترونیکی بود».

همان‌طور که این خبرنگاران در نیویورک‌تایمز نوشته بودند، کشف عامل شکست موشک غیرممکن بود، اما «جیمز متیس»، وزیر دفاع در اظهارنظر در مورد این اتفاق مرموز عمل کرده و فقط گفته بود «رئیس‌جمهور و تیم نظامی او از آخرین پرتاب موشک ناموفق کره شمالی آگاه هستند. رئیس‌جمهور هیچ نظر دیگری ندارد». چنین حرفی را از رئیس‌جمهوری می‌شنیدیم که به‌ندرت می‌گوید هیچ نظر دیگری ندارم.

شاید کره شمالی به حمله سایبری به موشکش با حمله سایبری پاسخ داده بود. واناکرای در تأثیرگذاری هیچ تبعیضی قائل نمی‌شد، اما شاید اساساً هدف‌شان همین بوده باشد. شاید با این کار می‌خواستند بگویند «شما می‌توانید در یک نقطه به من ضربه بزنید، اما من می‌توانم در همه جا به شما پاسخ بدهم».

چند جنبه واناکرای با این نظریه هم‌خوانی دارد؛ اول اینکه درست زمانی که همه در آسیای شرقی در حال خاموش‌کردن کامپیوترها و رفتن به خانه برای آخر هفته بودند، حمله علیه اهدافی در اروپا انجام شد. اگر کره شمالی می‌خواست اثرگذاری بر اروپای غربی و شمال آمریکا را به حداکثر برساند و در عین حال اثرگذاری بر چین را کاهش

دهد، زمان ایدئالی را انتخاب کرده بود. آلودگی با حرکت خورشید به غرب و در حالی گسترش یافت که کارمندان کسب‌وکارها و دولت‌های سایر قاره‌ها کار روزانه‌شان را ادامه می‌دادند، اما چینی‌ها پیش از بازگشت به کار در روز دوشنبه، آخر هفته را برای واکنش نشان‌دادن فرصت داشتند.

علاوه بر این کره شمالی قابلیتی اضافه کرده بود که متخصصان آن را «دکمه‌های مرگ» می‌خوانند. این قابلیت جلوگیری از گسترش بیشتر بدافزار را امکان‌پذیر می‌کند. یکی از دکمه‌های مرگ، بدافزار را به جست‌وجوی آدرس اینترنتی مشخصی هدایت می‌کرد که هنوز وجود نداشت. تا وقتی که آن آدرس وجود نداشت، واناکرای همچنان گسترش می‌یافت، اما به محض اینکه فردی آن آدرس را ثبت و فعال می‌کرد که گام فنی ساده‌ای بود، تکثیر کد متوقف می‌شد.

اواخر روز ۱۲ مه پژوهشگر امنیتی در بریتانیا با تحلیل کد واناکرای این دکمه مرگ را پیدا کرد، با هزینه کم ۱۰/۶۹ دلار آن آدرس را ثبت و فعال کرد و جلوی گسترش بیشتر واناکرای را گرفت. برخی گمانه‌زنی می‌کردند که این مسئله نشان‌دهنده متبحر نبودن سازندگان واناکرای است، اما شاید معکوس این گمانه‌زنی درست باشد. شاید طراحان واناکرای می‌خواستند اطمینان حاصل کنند که می‌توانند این بدافزار را پیش از صبح دوشنبه متوقف کنند تا اجازه ایجاد اختلال بیش از حد در چین یا کره شمالی را ندهند.

دست‌آخر هم اینکه مسئله مشکوکی در مورد پیام باج‌خواهی و رویکرد مورد استفاده واناکرای وجود داشت. همان‌طور که متخصصان امنیت گفته‌اند، کره شمالی قبلاً از باج‌افزار استفاده کرده بود، اما شگردهایش متفاوت بود؛ اهداف ارزشمند مثل بانک‌ها را انتخاب و به‌صورت پنهانی مبالغ زیادی را مطالبه می‌کردند، مطالبه ۳۰۰ دلار از همه برای باز کردن قفل یک دستگاه را دست‌کم می‌توان تغییر رویه خواند. شاید استفاده از باج‌افزار پوششی برای منحرف‌کردن رسانه‌ها و مردم از پیام واقعی بوده است؛ پیامی پنهانی که قرار بوده مسئولان ایالات متحده و متحدانش درک کنند.

اگر کره شمالی این حمله را در پاسخ به حمله سایبری ایالات متحده انجام داده بود، حادثه خیلی مهم‌تر از آن بود که افراد به آن توجه می‌کردند. این حادثه نزدیک‌ترین تجربه جهان به جنگ سایبری شدید بود. به این معنی بود که پیامدهای این حمله برای

مردم عادی خسارت جانبی نداشته است؛ پیامدی بوده که مهاجم می‌خواسته است.

صرف‌نظر از پاسخ، خود پرسش مسئله‌ای جدی را بازتاب می‌دهد. سلاح‌های سایبری در طول دهه گذشته خیلی پیشرفته‌تر شده‌اند و احتمالات و فرصت‌های جنگ مدرن را بازتعریف کرده‌اند، اما با روش‌هایی به کار گرفته می‌شوند که رخداد واقعی را می‌پوشانند. عموم مردم هنوز ریسک‌ها یا مسائل اضطراری مربوط به سیاست عمومی را کاملاً درک نمی‌کنند و تا وقتی این مسائل از حاشیه به متن نیایند، خطر همچنان افزایش خواهد یافت.

اگر کسی در مورد تهدید جنگ سایبری شک داشت، باید با حمله سایبری شش هفته بعد دیگر ایمان می‌آورد.

روز ۲۷ ژوئن ۲۰۱۷ حمله‌ای سایبری به اوکراین انجام شد. در این حمله با استفاده از همان کد نرم‌افزاری دزدیده‌شده از آژانس امنیت ملی، حدود ۱۰ درصد از همه کامپیوترهای اوکراین از کار افتادند. ایالات متحده، بریتانیا و پنج دولت دیگر بعداً این حمله را به روسیه نسبت دادند. متخصصان امنیت این بدافزار را «نات‌پتیا» (NotPetya) نامیدند؛ زیرا کدهای مشترکی با باج‌افزار شناخته‌شده‌ای داشت که از روی ماهواره مسلح «پتیا» نام‌گذاری شده بود. این ماهواره بخشی از سلاح تخیلی «گلدن‌آی» (GoldenEye) اتحاد جماهیر شوروی در فیلمی محصول سال ۱۹۹۵ از مجموعه جیمز باند به همین نام بود. آن سلاح می‌توانست ارتباطات الکترونیکی در شعاع ۳۰ مایلی را از کار بیندازد.

در دنیای غیرتخیلی سال ۲۰۱۷، حمله نات‌پتیا دامنه نفوذ بسیار گسترده‌تری داشت؛ در سراسر اوکراین گسترش یافت و کسب‌وکارها، سیستم حمل‌ونقل و بانک‌ها را فلج کرد و بعد به خارج از مرزهای این کشور گسترش یافت و به شرکت‌های چندملیتی مثل «فداکس»، «مرک» و «مرسک» نفوذ کرد. مرسک، غول ترابری دانمارکی شاهد از کار افتادن تمام شبکه کامپیوتری جهانی خود بود.

وقتی مهندسان امنیت مایکروسافت به دفاتر مرک در لندن رسیدند تا در بازیابی کامپیوترها کمک کنند، آنچه مشاهده کردند، با استانداردهای قرن بیست‌ویکم عجیب و ترسناک بود. «مارک امپسون»، مهندس پایکار مایکروسافت که قدبلند و

پرتحرک بود و سریع حرف می‌زد، یکی از اولین افراد حاضر در صحنه بود. او می‌گوید: «همیشه نویز و صداهای محیطی کامپیوترها، چاپگرها و اسکنرها را می‌شنوید. اینجا هیچ صدایی نمی‌آمد. سکوت مطلق بود.»

امپسون می‌گوید وقتی در راهروهای مرسک راه می‌رفتم، احساس می‌کردم انگار این دفتر کار مرده است. امپسون می‌گوید: «در این شرایط فرایند منطقی عیب‌یابی استاندارد را طی می‌کنید و می‌پرسید وضعیت چطور است؟ کدام سرورها قطع هستند؟ چه اتفاقی افتاده است؟ پاسخ دادند همه‌چیز قطع است. بعد پرسیدم تلفن‌ها چطور؟ گفتند قطع هستند. اینترنت چی؟ اینترنت هم قطع است.»

یادآوری ناخوشایندی بود از اینکه چقدر اقتصاد و زندگی ما به فناوری اطلاعات وابسته است. در دنیایی که همه‌چیز به هم متصل هستند، هر چیزی می‌تواند مختل شود. یکی از دلایلی که تأمل در مورد حمله سایبری به شبکه‌های برق امروزی را جدی می‌کند، همین مسئله است.

اگر شهری شبکه برق، تلفن، گاز، آب و اینترنتش را از دست بدهد، می‌تواند به دورانی شبیه عصر حجر برگردد. اگر زمستان باشد، افراد ممکن است از سرما منجمد شوند، اگر تابستان باشد، افراد ممکن است گرمازده شوند. افرادی که برای زنده‌ماندن به دستگاه‌های پزشکی وابسته هستند، ممکن است جان‌شان را از دست بدهند. حمله‌ای سایبری را در آینده‌ای با خودروهای خودران تصور کنید که وقتی خودروها به‌سرعت در حال رانندگی در بزرگراه هستند، به سیستم‌های کنترل‌شان نفوذ می‌کند.

همه این احتمالات به ما یادآوری می‌کنند و هشدار می‌دهند که در چه دنیایی زندگی می‌کنیم. مرسک بعد از حمله نات‌پتیا در اقدامی غیرمعمول به مردم اطمینان داد که کشتی‌هایش تحت کنترل ناخداها هستند. نیاز به این اطمینان خاطر دادن میزان وابستگی جهان به کامپیوترها و پتانسیل اختلال مبتنی بر حمله سایبری را نشان داد.

فراگیری نرم‌افزار در زیرساخت جوامع ما تا حدی نشان می‌دهد که چرا دولت‌ها در توانایی‌های مبتنی بر سلاح‌های سایبری تهاجمی سرمایه‌گذاری می‌کنند. دولت‌ها در مقیاس و سطحی بسیار متفاوت با هکرهای نوجوان و همتایان‌شان در سازمان‌های جنایی بین‌المللی فعالیت می‌کنند. ایالات متحده از اولین سرمایه‌گذاران و همچنان

رهبر این حوزه است. اما سایر کشورها هم در این زمینه به‌سرعت پیشرفت کرده‌اند که از جمله می‌توان به روسیه، چین، کره شمالی و ایران اشاره کرد که به مسابقه تسلیحات سایبری پیوسته‌اند.

حملات واناکرای و نات‌پتیا نشان‌دهنده تقویت شدید توانایی‌های مبتنی بر تسلیحات سایبری در حال رشد جهان بود. با این حال تنها چند ماه بعد مشخص شد که دولت‌های جهان این زنگ خطر را جدی نگرفته‌اند.

در گفت‌وگو با دیپلمات‌هایی از نقاط گوناگون جهان تردید یکسانی را مشاهده می‌کردیم: «کسی کشته نشده است. این حملات به افراد کاری ندارند. صرفاً حمله دستگاه‌ها به دستگاه‌ها هستند.»

در تحقیقات‌مان به این نتیجه رسیدیم که دیدگاه افراد نسبت به امنیت سایبری، بیش از همه پیشرفت‌های قبلی در فناوری تسلیحاتی، به نسل آنها بستگی دارد. نسل‌های جوان‌تر بومی عصر دیجیتال هستند. تمام زندگی‌شان به فناوری اتکا دارد و حمله به دستگاه‌هایشان مانند حمله به خانه‌شان است؛ پای منافع شخصی‌شان در میان است. اما نسل‌های قدیمی‌تر چنین دیدگاهی به آثار حمله سایبری ندارند. بدین ترتیب به پرسش هوشیارکننده‌تری می‌رسیم. آیا این هشدارها جهان را پیش از وقوع ۱۱ سپتامبر دیجیتال بیدار می‌کنند؟ یا دولت‌ها همچنان خواب خوش را ترجیح می‌دهند؟

بعد از حمله نات‌پتیا می‌خواستیم به دنیا نشان دهیم چه اتفاقی در اوکراین افتاده؛ کشوری که هدف چندین حمله سایبری بوده است. هرچند نات‌پتیا آسیب شدیدی به این کشور زده بود، اما خارج از اوکراین پوشش رسانه‌ای کم و پراکنده‌ای در مورد این حادثه وجود داشت. تصمیم گرفتیم تیمی از کارمندان مایکروسافت را بفرستیم تا با افراد در کی‌یف مصاحبه کنند و ببینند دقیقاً چه اتفاقی افتاده است. افرادی را پیدا کردند که کسب‌وکار، مشتریان یا شغل‌شان را از دست داده بودند. کارمندان ما با اوکراینی‌هایی حرف زدند که نتوانسته بودند مواد غذایی بخرند؛ زیرا کارت‌های اعتباری و خودپردازها کار نمی‌کردند. با مادرانی صحبت کردند که وقتی شبکه ارتباطی قطع شده بود، نتوانسته بودند فرزندان‌شان را پیدا کنند. بدیهی است که مانند ۱۱ سپتامبر نبود، اما نشان می‌داد که جهان به کدام سمت حرکت می‌کند.

مردم اوکراین بی‌پرده در مورد تجربه‌هایشان صحبت می‌کردند، اما قربانیان حملات سایبری اغلب ساکت می‌مانند؛ چراکه از امنیت شبکه‌شان خجالت می‌کشند. این رویه به جای حل مسئله، آن را ماندگار می‌کند. مایکروسافت نیز زمانی با همین دوراهی روبه‌رو شد. در سال ۲۰۱۷ وکلای ما ایده شکایت از دو مجرم در بریتانیا را مطرح کردند که با موفقیت بخشی از شبکه ایکس‌باکس ما را هک کرده بودند. هرچند افشای این حادثه پرسش‌های ناخوشایندی را مطرح می‌کرد، اما اجازه دادم این کار انجام شود. اگر خودمان شجاعت بیشتری به خرج ندهیم، هرگز نمی‌توانیم به‌دنبال رهبری مردم باشیم.

اما علاوه بر بیشتر حرف‌زدن، باید بیشتر عمل می‌کردیم.

دیپلمات‌های اروپایی موافق بودند. سفیری اروپایی در دفتر سازمان ملل در ژنو به من گفت: «می‌دانیم باید کارهای بیشتری انجام دهیم، اما هنوز نمی‌دانیم چه کارهایی باید انجام دهیم و حتی اگر بدانیم، در حال حاضر جلب موافقت دولت‌ها در مورد هر کاری آسان نیست. در مورد این مسئله شرکت‌های فناوری باید پیشگام باشند. این کار بهترین راه برای وادار کردن دولت‌ها به ورود به این مسیر است.»

کمی بعد این فرصت مهیا شد. گروهی از مهندسان امنیت به این جمع‌بندی رسیدند که اگر چند شرکت با هم و همزمان اقدام کنند، می‌توانیم بخش مهمی از توانایی بدافزاری گروه وابسته به کره شمالی (زینک) یا همان عامل حمله واناکرای را از کار بیندازیم. می‌توانستیم وصله‌هایی را برای آسیب‌پذیری‌هایی توزیع کنیم که زینک می‌خواست از آنها سوءاستفاده کند، کامپیوترهای شخصی آلوده را پاک کنیم و حساب‌هایی را در مجموعه خدمات‌مان ببندیم که مهاجمان از آنها استفاده می‌کردند. آثار این کارها همیشگی نبود، اما به توانایی‌های این گروه ضربه می‌زد.

در مایکروسافت، فیس‌بوک و شرکت‌های دیگر گفت‌وگوهای مفصلی در مورد اجرا کردن یا نکردن این نقشه و نحوه اجرای آن داشتیم. این اقدام ما را به هدفی برجسته‌تر تبدیل می‌کرد. در مورد آن با ساتیا صحبت کردم و در ماه نوامبر برنامه‌مان برای پیشبرد این کارها را با هیئت‌مدیره مایکروسافت به اشتراک گذاشتیم. به این نتیجه رسیدیم که از همه جهات و از جمله از جنبه قانونی، استدلال قدرتمندی داریم و اگر هماهنگ

با سایر شرکت‌ها عمل کنیم، گامی است که ارزش برداشتن دارد.

همچنین بـه این نتیجه رسـیدیم کـه باید به اف‌بـی‌آی، آژانـس امنیت ملی و سـایر مسـئولان در ایالات متحده و دیگر کشـورها اطلاع بدهیم. از آنها اجـازه نمی‌گرفتیم؛ بلکه صرفاً برنامه‌مـان را به اطلاع آنها می‌رسـاندیم. می‌خواسـتیم مطمئن شـویم که از حسـاب‌های کاربری که مـا می‌خواهیـم غیرفعال کنیـم، در عملیـات اطلاعاتی برای پاسخگویی به تهدید کره شمالی استفاده نمی‌شود.

چند روز بعد به واشـنگتن دی‌سـی رفتـم و بخشـی از روز را در کاخ سـفید گذراندم. در دفاتر زیرزمین بال غربی با تام بوسـرت، مشـاور امنیت ملـی رئیس‌جمهور و «راب جویس»، هماهنگ‌کننده امنیت سـایبری کاخ سـفید جلسه داشـتم. با آنها در مورد برنامه‌هایمـان گفت‌وگـو کـردم؛ برنامه‌هایـی که آن زمـان اجرایشـان برای هفتـه آینده برنامه‌ریزی شده بود.

گفتند که با پشتیبانی کامل رئیس‌جمهور ترامپ به اعلام رسمی عاملیت کره شمالی در حمله واناکرای نزدیک هسـتند. این امـر گامی کلیدی در اعلام عمومی مسـئولیت دولت‌ها در حملات سایبری بود. بوسرت به این جمع‌بندی رسیده بود که دولت ایالات متحده باید به‌صورت رسـمی مخالفتش را با آن دسـته از حملات سـایبری کـه آنها را «نامتوازن و کورکورانه» می‌داند، اعلام کند. علاوه بر این کاخ سفید در این مورد فعالانه با کشـورهای دیگر همکاری می‌کـرد تا بتواننـد برای اولین‌بـار در کنار هـم به‌طور علنی انگشت اتهام را به سمت کره شمالی بگیرند.

بوسـرت ابتدا از ما خواسـت برنامه‌مان را به تعویق بیندازیم و گفـت: «تا یک هفته بعد از برنامه شـما آمادگی نداریم که خبرمان را اعلام کنیم و بهتر خواهد بود اگر همه همزمان عمل کنیم.» گفتم نمی‌توانیم عملیات‌مان را عقب بیندازیم؛ زیرا باید با عرضه برخی از وصله‌ها که مردم در ۱۲ دسامبر منتظر آنها هستند، هماهنگ باشد. مشهور بود که مـا وصله‌ها را در دومین سه‌شـنبه هر ماه عرضـه می‌کنیم. این روز را سه‌شـنبه وصله می‌خواندیم.

گزینـه جایگزینـی پیشـنهاد کـردم. گفتـم: «اجـازه بدهیـد ببینـم در مـورد تعویـق اطلاع‌رسانی‌ها در مورد عملیات‌مان چه کاری می‌توانیم بکنیم و شاید بتوانیم این کار

را با هم انجام دهیم.»

این گفت‌وگو جنبه مهم اما عجیب واکنش دولتی به واناکرای را آشکار کرد. آن‌طور که بوسرت به من توضیح داد و بعداً در کنفرانس مطبوعاتی اعلام کرد، با توجه به تحریم‌های گسترده‌ای که از قبل برقرار بود، دولت ایالات متحده برای واکنش به این حادثه گزینه‌های محدودی در اختیار داشت. او به رسانه‌ها گفت: «رئیس‌جمهور ترامپ تقریباً همه اهرم‌های قابل استفاده، غیر از گرسنگی‌دادن به مردم کره شمالی تا سرحد مرگ را به کار برده تا رفتارشان را تغییر دهد.»

هرچند دولت بعدها نتیجه‌گیری کرد که می‌تواند واکنش‌های بالقوه‌اش به حملات سایبری را گسترش دهد، اما بخش فناوری می‌توانست گام‌هایی بردارد که دولت نمی‌توانست. شرکت‌های فناوری می‌توانستند به‌راحتی برخی از بخش‌های کلیدی توانایی بدافزاری کره شمالی را غیرفعال کنند. بنابراین اگر می‌توانستیم دو بیانیه را تجمیع کنیم، موضع‌گیری قدرتمندتری در برابر بازیگران وابسته به دولت‌ها بروز داده بودیم.

به دو مسیر هماهنگ وارد شدیم؛ مسیر اول اجرای عملیات و مسیر دوم اعلام عمومی آن بود. تیم‌های امنیت مایکروسافت، فیس‌بوک و شرکت فناوری دیگری که نمی‌خواست نامش رسماً اعلام شود، در کنار هم تلاش کردند تا در صبح روز ۱۲ دسامبر، روز وصله، در توانایی‌های سایبری زینک اختلال ایجاد کنند. عملیات بدون هیچ اشکالی انجام شد.

اما تلاش برای اعلام عمومی عملیات پیچیده‌تر بود. متخصصان امنیت (تقریباً در همه حوزه‌ها) از گفت‌وگوی عمومی در مورد کارشان اکراه دارند. یکی از دلایل این اکراه این است که فرهنگ‌شان بر حفاظت (نه به اشتراک گذاشتن اطلاعات) استوار است. به‌علاوه همیشه ریسکی وجود دارد که اقدام مسبب حملات تلافی‌جویانه شود. اما اگر می‌خواستیم اقدام مؤثری علیه حملات سایبری دولتی انجام دهیم، باید بر این اکراه و بی‌میلی غلبه می‌کردیم.

همچنین با پیچیدگی مضاعف رابطه نامساعد بخش فناوری با دولت ترامپ روبه‌رو بودیم. ماه‌های اخیر را به نبردهای مربوط به مسائل مهاجرتی در کنار دیگر مسائل سپری

کرده بودیم. این رابطه نامساعد باعث شده بود برخی افراد میلی به اعلام عمومی هر گونه همکاری با دولت نداشته باشند. اما احساس می‌کردم حتی اگر باید در زمینه‌هایی بر موضع خودمان پافشاری کنیم، در زمینه‌های دیگری که امکان دارد، باید با هم مشارکت کنیم. امنیت سایبری هدفی مشترک است که در مورد آن نه‌تنها می‌توانیم مشارکت کنیم؛ بلکه اگر می‌خواهیم پیشرفت واقعی داشته باشیم، باید همکاری کنیم.

کاخ سفید به ما اعلام کرد بیانیه‌اش را ۱۹ دسامبر صادر می‌کند. به‌سرعت به فیس‌بوک و آن شرکت دیگر گفتیم که اگر همه بخواهیم همگام به پیش برویم، ما حاضریم که اقدام‌مان علیه زینک را علنی کنیم، اما تا صبح روز قبل از اجرای برنامه هنوز منتظر تصمیم‌گیری دو شرکت دیگر بودیم. اعلام کردم که در صورت لزوم به‌تنهایی برنامه را اجرا می‌کنیم. معتقد بودم تنها راه واقعاً مؤثر برای جلوگیری از مشارکت کشورها در این حملات، این است که نشان دهیم توانایی در حال رشدی برای واکنش وجود دارد. باید کسی اولین گام روبه‌جلو را برمی‌داشت. شاید بهتر بود آن کس ما باشیم.

شب خبر خوب رسید که فیس‌بوک همراه ما تلاش‌هایش را علنی می‌کند و در مورد اقدام جمعی‌مان صحبت خواهد کرد. خبر بهتر هم صبح روز بعد از کنفرانس مطبوعاتی بوسرت در کاخ سفید رسید. او توضیح داد که پنج کشور دیگر (استرالیا، کانادا، ژاپن، نیوزیلند و بریتانیا) در اعلام عمومی عامل حمله، به ایالات متحده پیوسته‌اند. اولین‌بار بود که کشورها در اقدامی چندجانبه با یکدیگر همراه می‌شدند تا عاملیت کشوری دیگر در حمله‌ای سایبری را علنی کنند. بعد اعلام کرد که مایکروسافت و فیس‌بوک هفته پیش گام‌های ملموسی برداشته‌اند تا بخشی از توانایی حمله سایبری گروه زینک را از کار بیندازند.

دولت‌ها و شرکت‌های فناوری با همکاری یکدیگر به دستاوردی رسیده بودند که بدون همکاری و به‌طور جداگانه ممکن نبود؛ البته راه‌حل نهایی برای تهدیدات سایبری جهان نبود، پیروزی بزرگی هم به‌شمار نمی‌آمد، اما شروع تازه‌ای بود.

فصل پنجم

حفاظت از دموکراسی

«حکومت جمهوری البته اگر بتوانید حفظش کنید!»

در سال ۱۷۸۷ در حالی که کنوانسیون قانون اساسی آمریکا به کار خود در فیلادلفیا پایان داده بود، از «بنجامین فرانکلین» حین خروج از تالار استقلال پرسیدند نمایندگان چه نوع حکومتی ایجاد کردند. پاسخی داد که بعداً مشهور شد؛ گفت: «حکومت جمهوری، البته اگر بتوانید حفظش کنید.» این جمله در تمام کشور و تا سال‌های زیادی بازتاب یافت. این سخنان این موضوع را برجسته می‌کرد که حکومت جمهوری دموکراتیک فقط نوعی حکومت جدید نیست؛ بلکه نوعی است که حفاظت و حفظ آن مستلزم هوشیاری و در برخی موارد، اقدام عملی است.

در تاریخ آمریکا این هوشیاری و اقدام عملی، اغلب مساوی با اقدام شهروندان در قالب رأی‌دادن، خدمات عمومی و در مواردی حتی گذشتن از جان خود بوده است. در دیگر نقاط عطف، مستلزم بسیج‌شدن کسب‌وکارهای کشور بوده است، مانند کاری که بخش صنعتی آمریکا برای کمک به پیروزی در جنگ جهانی دوم انجام داد. تاریخ به ما آموخته که هوشیاری باید همیشگی باشد؛ زیرا نیاز به اقدام از قبل خبر نمی‌دهد.

نیاز به این هوشیاری ناگهان در یکشنبه‌شبی در جولای ۲۰۱۶ به وجود آمد. در طول دو هفته قبل از این شب، بیشتر زمان را صرف شرکت در کنوانسیون‌های ملی احزاب جمهوری‌خواه و دموکرات در کلیولند و فیلادلفیا کرده بودم. آخر هفته‌ام نیز به انجام کارهای عقب‌مانده، گذشته بود و می‌خواستم کار را تعطیل کنم که ایمیلی با عنوان «اضطراری» دریافت کردم. وقتی داشتم ایمیل را باز می‌کردم، هرگز فکر نمی‌کردم مقدمه کمپینی در حال گسترش و آزمونی برای بخش فناوری باشد که این صنعت را به چالش می‌کشد تا گامی برای دفاع از دموکراسی بردارد.

ایمیل را «تام برت»، یکی از معاونان اداره حقوقی مایکروسافت فرستاده بود. در سطر موضوع نوشته شده بود: «مسئله اضطراری واحد جرائم دیجیتال». واحد جرائم دیجیتال یکی از تیم‌های مایکروسافت است که تام مدیریتش می‌کرد. این واحد را ۱۵ سال پیش ایجاد کردیم و هنوز در بخش فناوری منحصربه‌فرد مانده است؛ مسئله‌ای که فکر می‌کنم تا حدی عجیب است. این تیم از بیش از یکصد نفر در سراسر جهان تشکیل شده و شامل دادستان‌ها و مأموران تحقیق دولتی سابق و همچنین تحلیلگران جرم‌شناسی، داده و کسب‌وکار برجسته می‌شود. واحد جرائم دیجیتال از نتایج تلاش‌های ضدجعل ما در دهه ۱۹۹۰ بود، اما به تیم

ضربت دیجیتالی تبدیل شد که وقتی می‌بیند انواع جدیدی از فعالیت مجرمانه در اینترنت رایج شده است، با مجریان قانون همکاری می‌کند.

۱۰ روز قبل، یعنی جمعه پیش از «کنوانسیون ملی حزب دموکرات» در سال ۲۰۱۶، «ویکی‌لیکس» ایمیل‌هایی را منتشر کرده بود که هکرهای روس از کمیته ملی حزب دموکرات دزدیده بودند. این اتفاق در طول هفته برگزاری کنوانسیون به ماجرای خبری مهمی تبدیل شد. طی این هفته مرکز اطلاعات تهدید ما یا همان «میستیک» تلاش برای هک جدید و مجزایی را شناسایی کرد که «استرانسیوم» عامل آن بود؛ استرانسیوم نامی بود که ما به گروهی از هکرهای روس داده بودیم که با نام‌های «فنسی بر» (Fancy Bear) و «APT28» هم شناخته می‌شود. تیم تام می‌خواستند سه‌شنبه همان هفته ضربه‌ای حقوقی به استرانسیوم بزنند و در فعالیت‌هایش اختلال ایجاد کنند.

اف‌بی‌آی و جامعه اطلاعاتی، استرانسیوم را وابسته به اداره اصلی اطلاعات (GRU)؛ سازمان اطلاعات نظامی روسیه می‌دانستند. تام گزارش داد که استرانسیوم با جعل خدمات مایکروسافت؛ طیفی از مسئولان سیاسی و نامزدهای انتخابات، از جمله حساب‌های متعلق به کمیته ملی حزب دموکرات و کمپین ریاست‌جمهوری هیلاری کلینتون را هدف قرار داده و پای ما را وسط این ماجرا کشیده است.

میستیک فعالیت استرانسیوم را از سال ۲۰۱۴ زیر نظر گرفته بود. این گروه در آن زمان به اجرای حملات به‌اصطلاح فیشینگ اقدام می‌کرد و ایمیل‌های ساختگی بادقت طراحی‌شده‌ای می‌فرستاد تا با فریب اهداف، آنها را به کلیک‌کردن روی لینک‌هایی ترغیب کند که در ظاهر وب‌سایت‌های مورد اعتمادی بودند. در برخی از این وب‌سایت‌ها نام مایکروسافت هم وجود داشت. استرانسیوم از مجموعه‌ای از ابزارهای پیشرفته به‌منظور ذخیره‌سازی کلیدهای فشرده‌شده روی صفحه‌کلید، به دست آوردن ایمیل‌ها و فایل‌ها و جمع‌آوری اطلاعات از کامپیوترهای دیگر استفاده می‌کرد. این گروه حتی از ابزاری برای آلوده‌کردن دستگاه‌های ذخیره‌سازی یواس‌بی استفاده کرده بود تا داده‌های سایر کامپیوترهای ایزوله و خارج از شبکه را نیز جمع‌آوری کند.

استرانسیوم پیشرفته‌تر و همچنین سمج‌تر از سازمان‌های هک مجرمانه بود و در طول دوره‌ای طولانی، ایمیل‌های فیشینگ بسیار زیادی به اهداف انتخابی خود ارسال می‌کرد.

بدون شک کلاهبرداری موفق از هدفی ارزشمند به زحمتش می‌ارزید.

هرچند بسیاری از کاربران کامپیوتر با این روش آشنا هستند، اما مقابله با آن دشوار است؛ چنانچه فردی از همایش سالانه شرکت امنیت شبکه «آراس‌ای» (RSA) در سان‌فرانسیسکو توییت کرده بود: «هر سازمانی دست‌کم یک کارمند دارد که روی هر لینکی کلیک می‌کند.» در واقع در این روش، از کنجکاوی انسان و همچنین بی‌دقتی افراد سوءاستفاده می‌شود. در تحلیل فعالیت‌های هکرها به این نتیجه رسیدیم که نخستین کاری که هکرها پس از نفوذ موفق به حساب ایمیل افراد انجام می‌دهند، این است که به‌دنبال کلیدواژه «رمز عبور» می‌گردند. وقتی رمز عبورهای افراد برای خدمات گوناگون زیاد می‌شود، اغلب افراد ایمیل‌هایی را با واژه رمز عبور برای خودشان می‌فرستند که این امر سرقت این اطلاعات را برای هکرها آسان می‌کند.

در جولای ۲۰۱۶ میستیک مشاهده کرد استرانسیوم به‌دنبال ثبت دامنه‌های اینترنتی جدیدی است تا داده‌های کاربران را سرقت کند. استرانسیوم شروع به استفاده از نام مایکروسافت در این دامنه‌ها کرده و برای مثال دامنه Microsoftdccenter.com را ثبت کرده بود تا این‌گونه به نظر برسد که لینک، مربوط به خدمات پشتیبانی واقعی مایکروسافت است. واحد جرائم دیجیتال آخر هفته را صرف تدوین استراتژی حقوقی برای رسیدگی به این مسئله کرده بود و آن‌طور که تام روز یکشنبه گزارش داد، آماده بودند که با اجرای برنامه‌شان این سایت‌ها را ببندند.

این برنامه بر مبنای یک نوآوری حقوقی و فنی تدوین شده بود که واحد جرائم دیجیتال در گذشته آن را بنیان نهاده بود. طبق این برنامه قرار بود به دادگاه مراجعه کنیم و نشان دهیم که استرانسیوم از نشان تجاری مایکروسافت سوءاستفاده کرده و بر این اساس از دادگاه بخواهیم کنترل دامنه اینترنتی جدید را به واحد جرائم دیجیتال منتقل کند. این بخش از زاویه‌ای نوآورانه بود، اما تقریباً بدیهی هم بود. قانون نشان تجاری از چندین دهه پیش وجود داشت و در حال حاضر نیز افراد را از به‌کارگیری نشان‌های تجاری ثبت‌شده مثل «مایکروسافت» در نام وب‌سایت منع می‌کند.

سپس در بعد فنی، در آزمایشگاه جرم‌شناسی واحد جرائم دیجیتال، «حفره» اینترنتی امنی جدا از بقیه شبکه‌مان می‌ساختیم. این حفره همه ارتباطات کامپیوترهای آلوده

با سرور فرمان و کنترل استرانسیوم را رهگیری می‌کرد. هدف از در اختیار گرفتن کنترل شبکه استرانسیوم، شناسایی مشتریان آلوده و سپس همکاری با کاربران برای پاک‌سازی دستگاه‌های آلوده‌شان بود.

عاشق این ایده بودم. این مورد دقیقاً همه اهداف اولیه ما از ایجاد واحد جرائم دیجیتال را برآورده می‌کرد. با ایجاد این واحد می‌خواستیم کاری کنیم که وکلا و مهندسان به نحوی دست به نوآوری بزنند که نتیجه‌ای واقعی برای مشتریان داشته باشد. هرچند از موفقیت‌مان اطمینان کامل نداشتیم، اما تام خوش‌بین بود و پیشنهاد داد سه‌شنبه صبح بی‌درنگ دادخواست‌مان را در دادگاه فدرال ویرجینیا ثبت کنیم. من نیز موافقتم را اعلام کردم.

یکی از جنبه‌های این رویکرد این بود که در دادگاه راحت برنده می‌شدیم. تقریباً تضمین‌شده بود که هکرها برای دفاع از خود به دادگاه نخواهند آمد. مگر دیوانه باشند؟ چراکه با این کار خودشان را در معرض اختیارات قانونی و حتی تعقیب قانونی قرار می‌دادند. تیم واحد جرائم دیجیتال در دستیابی به هدفی موفق شده بود که همیشه در پی آن بودیم، اما معمولاً دستیابی به آن دشوار بود. استراتژی حقوقی ما نقطه‌قوت هکرها، یعنی توانایی‌شان در مخفی‌شدن در سایه‌ها، را به نقطه‌ضعف‌شان تبدیل کرده بود.

در دادگاه پیروز شدیم، کنترل دامنه‌های اینترنتی را در اختیار گرفتیم و کار برقراری ارتباط و همکاری با قربانیان را شروع کردیم. هرچند اسناد دادگاه در دسترس همه بود و انتشاراتی امنیتی هم از کار ما گزارش تهیه کرده بود، اما سایر رسانه‌ها به آن توجهی نکردند. با اطمینان خاطر به گسترش این روش اقدام کردیم. ۱۴ بار دیگر به دادگاه رفتیم، ۹۰ دامنه استرانسیوم را ضبط کردیم و دادگاه را متقاعد کردیم که قاضی بازنشسته‌ای را به‌عنوان دستیار قاضی ویژه منصوب کند تا درخواست‌های ما سریع‌تر تأیید شوند.

اوایل سال ۲۰۱۷ فعالیت‌هایی را شناسایی کردیم که هدف‌شان هک‌کردن تیم‌های کمپین نامزدهای انتخابات ریاست‌جمهوری فرانسه بود. به کارکنان کمپین و همچنین آژانس امنیت ملی فرانسه اطلاع دادیم تا تمهیدات امنیتی قدرتمندتری را در نظر بگیرند. از توانایی‌های تحلیل داده‌مان برای شناسایی روندهای موجود و در حال پیدایش، استفاده کردیم و یک الگوریتم هوش مصنوعی توسعه دادیم تا نام‌های دامنه‌ای را پیش‌بینی کنیم که هکرها در آینده از آنها استفاده خواهند کرد. با این حال هیچ‌کدام از این کارها راه‌حل جامع و کاملی

نبودند. همچنان به‌نوعی درگیر موش و گربه بازی بودیم. فقط حالا دست‌کم گربه چنگ‌های جدیدی داشت.

متأسفانه در طول رقابت‌های انتخابات ریاست‌جمهوری آمریکا موش داستان ما به نحوی متبحرتر شده بود که هیچ‌کس کاملاً درک نمی‌کرد. روس‌ها در سال ۲۰۱۶ از ایمیل به‌عنوان سلاحی برای جمع‌آوری و افشای ارتباطات بهره بردند و با محتوای این ارتباطات رهبران کمپین هیلاری کلینتون و کمیته ملی حزب دموکرات را نزد افکار عمومی خجالت‌زده کردند.

در سال ۲۰۱۷ تغییری را در نقشه‌شان ایجاد کردند و ترکیبی از ایمیل‌های واقعی و جعلی منتسب به کمپین ریاست‌جمهوری امانوئل مکرون را منتشر کردند. هرچند واحد جرائم دیجیتال مایکروسافت و تیم‌های دیگری در صنعت فناوری، راه‌های جدیدی برای خنثی‌کردن این فعالیت‌ها پیدا کردند، اما خیلی زود مشخص شد که روس‌ها نیز همگام با ما نوآوری می‌کنند.

استرانسیوم را در هک‌های مختلفش در سراسر دنیا دنبال کردیم. شگفت‌آور بود که ردشان را می‌شد در بیش از ۹۰ کشور مشاهده کرد. بیشترین فعالیت‌شان هم در اروپای مرکزی و شرقی، عراق، اسرائیل و کره جنوبی بود.

در شرایط عادی این فعالیت‌ها با واکنش قدرتمند و یکپارچه ایالات متحده و متحدانش در ناتو مواجه می‌شد، اما آن زمان اصلاً شرایط عادی نبود. چون حوادث ایالات متحده با مشروعیت انتخابات ریاست‌جمهوری ۲۰۱۶ از دیدگاه‌های مختلف ارتباط پیچیده‌ای پیدا کرده بود، بنابراین شکل‌گیری بحث‌های دوحزبی امکان‌پذیر نبود. در جلسه‌ای با گروهی دوحزبی از مشاوران سیاسی‌مان در واشنگتن‌دی‌سی، استدلال کردم که هر دو حزب، ما را ناامید کرده‌اند. بسیاری از جمهوری‌خواهان میلی به برخورد با روس‌ها نداشتند؛ چراکه فکر می‌کردند این کار به‌صورت ضمنی باعث تضعیف رئیس‌جمهوری از حزب جمهوری‌خواه می‌شود و به نظر می‌رسید برخی از دموکرات‌ها نیز ترجیح می‌دهند به جای انجام کاری مؤثر در راستای برخورد با دولت روسیه، به دونالد ترامپ انتقاد کنند. در نتیجه یکی از ستون‌های اصلی دفاع از دموکراسی بعد از جنگ جهانی دوم، پیش رویمان فروریخته بود. این ستون، پشتیبانی یکپارچه، فراحزبی و ملی آمریکا از رهبری ایالات متحده بود که می‌توانست متحدان ما در ناتو را متحد کند. وقتی از ناامیدی‌ام حرف زدم، یکی از افراد گفت: «واشنگتن همین است» و

سایر مشاوران هم سری به نشانه تأیید تکان دادند.

بعید به نظر می‌رسید که بخش فناوری بتواند به‌تنهایی شرایط را تغییر دهد. در اواخر سال ۲۰۱۷ هنگام بازدید از اسپانیا و پرتغال، دو کشوری که نگرانی‌های فزاینده‌ای در مورد هک‌های روس‌ها داشتند، مسئولان به‌طور مستقیم از من درخواست کمک کردند. هرچند افراد به‌وضوح پذیرفته بودند و فشار می‌آوردند که باید کارهای بیشتری انجام شود، اما بدون شکل‌گیری بحث‌های شفاف و هدفمند در مورد اتفاقاتی که مشاهده می‌کردیم، جلب حمایت عمومی دشوار بود.

یکی از بزرگ‌ترین چالش‌های ما گفت‌وگو با مردم در مورد این تهدیدات بود. هیچ‌کدام از رهبران بخش فناوری تمایلی به اشاره به کشورها نداشتند، ما هم از این قاعده مستثنی نبودیم. شرکت بودیم، نه دولت و هرچند در گذشته انتقادات دولتی را تحمل کرده بودیم، اما عادت نداشتیم یک دولت خارجی را به سوءاستفاده از پلتفرم‌ها و خدمات‌مان متهم کنیم. با این حال بیش از پیش آشکار شده بود که سکوت ما ریسک عملی‌شدن تهدیداتی را افزایش می‌داد که قصد داشتیم به متوقف‌شدن آن کمک کنیم.

داخل شرکت نیز با «مسئله روسیه» دست‌وپنجه نرم می‌کردیم. نگران بودیم که اگر به‌صورت علنی در مورد ارتباط دولت روسیه با هک‌ها صحبت کنیم، آنها اقدامات تلافی‌جویانه‌ای را علیه منافع تجاری و کارمندان‌مان در روسیه انجام دهند. تلاش کردیم به مشتریان خصوصی و دولتی‌مان در روسیه اطمینان دهیم که نگرانی‌های ما نسبت به دولت آنها به این معنی نیست که به آنها یا کشورشان پشت خواهیم کرد؛ مگر نه اینکه پنج بار در دولت‌های اوباما و ترامپ از دولت خودمان شکایت کرده بودیم. در مورد مسائل مربوط به مهاجرت هم حتی یک لحظه از موضع مخالف‌مان در برابر دولت ترامپ کوتاه نیامده بودیم. این مسائل باعث نمی‌شد به ادامه تعامل و پشتیبانی در سراسر ایالات متحده متعهد نباشیم، اما چطور افرادی در نقاط مختلف جهان می‌توانستند از ما انتظار داشته باشند که منتقد اقدامات نادرست ایالات متحده در زمینه نظارت و مهاجران باشیم، ولی منتقد اقدامات روسیه علیه جوامع دموکراتیک نباشیم؟

در اواخر سال ۲۰۱۷ فعالیت‌های تازه‌ای را برای هک ایمیل در خدمات‌مان مشاهده کردیم که به نظر می‌رسید آن دسته از نمایندگان سنا را هدف گرفته‌اند که در انتخابات میان‌دوره‌ای

ایالات متحده در سال ۲۰۱۸ برای انتخاب مجدد تلاش خواهند کرد. پیش از آنکه حسابی به دست هکرها بیفتد، به دفاتر نمایندگان مورد نظر هشدار دادیم. هیچ‌کس نمی‌خواست به‌صورت علنی در مورد این حملات ناموفق اظهارنظر کند، بنابراین ما هم سکوت کردیم.

در جولای ۲۰۱۸ تام برت در گردهمایی امنیتی «اسپن» (Aspen) سخنرانی کرد و در میزگردی گفت که دو حمله فیشینگ علیه اعضای کنگره و نامزدهای انتخابات آتی را مشاهده و به ناکام گذاشتن‌شان کمک کرده‌ایم. البته اسامی این اعضا را اعلام نکرد و رسانه‌ها نیز توجه زیادی به این سخنان نکردند. اما «دیلی بیست» (The Daily Beast)، وب‌سایت خبری حوزه فناوری، تحقیقاتی انجام داد و به‌درستی «کلر مک‌کسکیل»، سناتور ایالت میسوری را به‌عنوان یکی از این دو عضو شناسایی کرد. ناگهان این مسئله توجه رسانه‌ها را به‌شدت برانگیخت و خیلی زود شنیدیم که نشست‌های اطلاعاتی برای بحث در مورد این شرایط در اتاق وضعیت کاخ سفید در حال برگزاری است. مک‌کسکیل به‌سرعت کاری را کرد که وقتی به کارکنانش درخواست دادیم، امیدوار بودیم انجام دهد؛ بیانیه‌ای با لحنی تند صادر کرد که در آن آمده بود: «هرچند این حمله موفق نبود، اما بسیار وقیحانه است که عاملان این حمله فکر کنند می‌توانند قسر دربروند. مطمئناً مرعوب نخواهم شد.»

درس مهمی گرفتیم. کارکنان نمایندگان کنگره بیشتر از ما سازمان‌ها به بحث علنی در مورد این نوع حملات آشنا نبودند. به‌ویژه اگر مسئله در ابتدا به کارکنان فناوری اطلاعات سازمانی واگذار می‌شد، ماه‌ها بدون هیچ دستاوردی به بحث گذاشته می‌شد و در نهایت هیچ‌کس چیزی نمی‌گفت. اما اگر مسئله به مدیران ارشد سازمان ارجاع می‌شد، تصمیم‌گیری در مورد اظهارنظر علنی آنچنان دشوار نبود.

هرچند اظهارنظر علنی بسیار مهم بود، اما متوجه شدیم که به‌عنوان ارائه‌دهندگان این خدمات آنلاین باید کارهای بیشتری انجام دهیم. تصمیم گرفتیم برنامه ویژه‌ای را تدوین کنیم تا از نامزدها، کمپین‌ها و گروه‌های سیاسی وابسته در برابر مداخلات آنلاین، بهتر محافظت کنیم. نام این برنامه را «اکانت‌گارد» (محافظ حساب) گذاشتیم. این خدمت به‌صورت رایگان به گروه‌های سیاسی و افرادی ارائه می‌شد که از ایمیل و خدمات آفیس ۳۶۵ ما استفاده می‌کردند. میستیک فعالانه فعالیت کشورها را تحت نظر می‌گرفت و وقتی حمله‌ای را شناسایی می‌کردیم با اطلاعات مفصل به کارکنان کمپین هشدار می‌دادیم.

این طرح را دوست داشتم، اما می‌دانستیم اکانت‌گارد فقط بخشی از راه‌حل مسئله است. اگر رهبران دموکرات سراسر دنیا حاضر شده بودند که با قدرت بیشتری با مداخلات انتخاباتی در حال گسترش مقابله کنند، پس زمانش رسیده بود که بخش فناوری هم با شفافیت بیشتری در مورد مشاهداتش اطلاع‌رسانی کند.

فرایند اطلاع‌رسانی در مورد اکانت‌گارد فرصتی برای پیشرفت در این زمینه بود. به‌تازگی مشاهده کرده بودیم که استرانسیوم شش وب‌سایت ساخته که به‌وضوح سیاست‌مداران آمریکایی را هدف گرفته است. سه وب‌سایت روی سنای ایالات متحده متمرکز بودند و دو وب‌سایت دیگر بسیار درخور توجه بودند. به نظر می‌رسید یکی از این سایت‌ها مؤسسه بین‌المللی جمهوری‌خواهان (International Republican Institute) را هدف گرفته که یک سازمان جمهوری‌خواه مطرح است و از اصول دموکراتیک در سراسر دنیا پشتیبانی می‌کند. به نظر می‌رسید سایت دیگر، مؤسسه «هادسن» (Hudson) را هدف گرفته که اندیشکده‌ای محافظه‌کار است و پیش‌تر اعتراضات شدیدی را در مورد طیفی از سیاست‌ها و روش‌های روسیه مطرح کرده بود. قرار دادن این شواهد در کنار هم نشان می‌داد که استرانسیوم فقط دموکرات‌ها را هدف قرار نمی‌دهد و بر هر دو جناح سیاسی آمریکا متمرکز شده است.

واحد جرائم دیجیتال از دادگاه حکمی گرفت تا کنترل هر شش سایت به حفره ما منتقل شود. به این جمع‌بندی رسیدیم که پیش از هک‌شدن فردی اقدام کرده‌ایم. حال پرسش این بود که تا چه حد باید در مورد این اتفاق اطلاع‌رسانی عمومی کنیم. بحث‌های فعالی بین گروه‌های گوناگون مایکروسافت شکل گرفت، اما موقعیت خوبی بود که از بحث‌های عمومی گسترده و متنوع در این زمینه استقبال کنیم؛ به‌ویژه با توجه به اینکه این هک‌ها روی هر دو حزب سیاسی تأثیر می‌گذاشتند.

در نتیجه هفته‌ای از مذاکرات داخلی پرحرارت شروع شد که با تماسی در دفتر کار من در یک صبح جمعه به پایان رسید. تصمیم گرفتیم با رؤسای آن دو سازمان خصوصی و مسئولان سنا تماس بگیریم و از قبل برنامه‌مان برای اعلام خبر در سه‌شنبه هفته آینده را به اطلاع آنها برسانیم.

رهبران هر دو سازمان به‌سرعت از اقدامات ما پشتیبانی کردند. یکی از آنها گفت این حملات از جهاتی «نشان افتخاری» است که اهمیت کارهای آنها را ثابت می‌کند. محتوای

اطلاع‌رسانی در مورد اکانت‌گارد را با اطلاعاتی در مورد این حملات جدید و بیانیه‌ای روشن تلفیق کردیم و در آن اعلام کردیم این شش وب‌سایت را «گروهی وابسته به دولت روسیه به نام استرانسیوم ساخته است که با نام‌های فنسی بر یا APT28 هم شناخته می‌شود». نخستین بار بود که باشفافیت، روسیه را به‌عنوان منشاء حملات معرفی می‌کردیم؛ حرکتی که فیس‌بوک و گوگل نیز چند روز بعد با حذف حساب‌های دروغ‌پراکنی و جعلی از سایت‌هایشان دنبال کردند.

هرچند بدون شک هنوز به پایان مسیر نرسیده بودیم، اما این اتفاق نشان می‌داد بخش فناوری از سال ۲۰۱۶ تاکنون چقدر در این زمینه پیشرفت کرده است. وقتی صنعت گام‌های جدیدی برداشت، رسانه‌ها، دولت ایالات متحده را تحت فشار قرار دادند تا تلاش‌هایی در حد و اندازه تلاش‌های ما انجام دهد. این اتفاق مبنایی را فراهم کرد که امیدوار بودیم به زیربنایی جدید برای اقدام مشارکتی گسترده‌تر و بیشتر تبدیل شود. در برنامه «نیوزاور» (NewsHour) شبکه PBS گفتم: «باید اختلاف‌نظرات‌مان را کنار بگذاریم تا با همکاری یکدیگر اقدامات مورد نیاز را برای حفاظت از دموکراسی آمریکایی در برابر این نوع تهدیدات انجام دهیم.»

فکر می‌کنم جای تعجب نداشت که موضع علنی قدرتمندتر بخش فناوری برای دولت روسیه خوشایند نبود. در نوامبر ۲۰۱۸ یکی از کارمندان مایکروسافت در ردموند برای دریافت ویزا به‌منظور شرکت در همایشی در مسکو درخواست داد. از او خواسته شد فاصله دو هزار مایلی تا سفارت روسیه در واشنگتن‌دی‌سی را برای «مصاحبه ویزا» طی کند. وقتی این کارمند به اتاق مصاحبه وارد می‌شود، مسئول کنسولی پاکتی را به او می‌دهد و مؤدبانه از او می‌خواهد دو سند داخل آن را بخواند. بعد از کارمند می‌خواهد اسناد را به ردموند ببرد و به مدیران ارشد مایکروسافت تحویل دهد. مصاحبه در کمتر از پنج دقیقه به اتمام می‌رسد و ویزای آن کارمند صادر می‌شود.

کمی بعد ایمیلی با دو سند پیوست‌شده دریافت کردم؛ ایمیل حاوی رونوشت‌های چاپ‌شده‌ای از نسخه‌های انگلیسی‌زبان گزارش‌های خبری رسمی روسیه بود. هر دو گزارش اظهاراتم در آگوست آن سال را به تفصیل پوشش داده و اشاره کرده بودند که دولت روسیه سخنان من را رد می‌کند. در جمع‌بندی یکی از گزارش‌ها آمده بود: «مسئولان روسیه بارها هر

گونه مداخله در انتخابات خارجی از جمله با استفاده از حملات هکری را تکذیب کرده‌اند.»

پیام روسیه به مایکروسافت نشان‌دهنده محدودیتی بود که بسیاری از شرکت‌های فناوری آمریکایی با آن مواجه هستند. از طرفی سیاست‌مداران آمریکایی ما را به اتخاذ موضع سرسختانه در برابر فعالیت‌های هک خارجی ترغیب می‌کردند که قابل درک بود، اما از طرف دیگر این اقدامات به فشار کشورهای خارجی به شرکت‌ها منجر می‌شد.

به‌مرور که تصویر کاملی از فعالیت‌های روسیه در این زمینه شکل می‌گرفت، مشخص شد که ایمیل تنها فناوری دیجیتالی نیست که در معرض ریسک تبدیل‌شدن به سلاح قرار دارد. یکی از درس‌های مهم حوزه مدیریت ریسک این است که هم باید به ریسکی فکر کنیم که به احتمال زیاد با آن مواجه خواهیم شد و هم ریسکی را در نظر بگیریم که حتی اگر احتمال بسیار کمی برای وقوع آن وجود دارد، اما بدترین اتفاقی خواهد بود که با آن مواجه خواهیم شد. وقتی ریسک‌های دیجیتال برای دموکراسی را در نظر می‌گیریم، به نظر می‌رسد بدترین اتفاق، هک‌شدن احتمالی دستگاه‌های رأی‌گیری یا اختلال در شمارش دقیق آرای انتخاباتی است. تصور کنید بعد از انتخاباتی نزدیک و مهم خبر برسد که دولتی خارجی سیستم‌های رأی‌گیری را به شکل تأثیرگذاری هک کرده و امکان اصلاح آنها وجود ندارد. از سخن بنجامین فرانکلین وام می‌گیرم و می‌گویم اگر مردم نتوانند اطمینان کنند رأی‌هایی که اعلام می‌شود، همان‌هایی هستند که مردم داده‌اند، پس چطور می‌توانیم «جمهوری را حفظ کنیم»؟

همین حالا هم دنیا شاهد تلاش‌های کشورها برای ارزیابی امکان دست‌کاری دستگاه‌های رأی‌گیری است. پژوهشگران هم آسیب‌پذیری‌های بسیاری از دستگاه‌های رأی‌گیری را مستند کرده‌اند. این دستگاه‌ها نرم‌افزارها و سخت‌افزارهایی دارند که در اوایل دهه ۲۰۰۰ توسعه یافته‌اند. هرچند جذب سرمایه عمومی برای رسیدگی به این مسئله در حال افزایش است، اما برای برطرف‌کردن آسیب‌پذیری مشهود و از مدت‌ها پیش مستندشده این سیستم‌های کامپیوتری قدیمی، باید کارهای بیشتری انجام دهیم.

این موضوع از جمله مسائلی است که بدون کمک بخش فناوری حل نمی‌شود. البته تلاش‌های نوآورانه‌ای در حال گسترش هستند؛ از جمله در مایکروسافت که پژوهش‌ها به راه‌اندازی «الکشن‌گارد» (ElectionGuard؛ محافظ انتخابات) در ماه می ۲۰۱۹ منجر شد. الکشن‌گارد سیستم رأی‌گیری رمزنگاری‌شده‌ای است که از صندوق‌های انتخابات و

آرای جمع‌آوری‌شده در آنها محافظت می‌کند. سیستم نرم‌افزاری منبع‌بازی است که از سخت‌افزارهای ارزان و غیرسفارشی استفاده می‌کند و بهترین ویژگی‌های فناوری‌های قدیمی و جدید را ترکیب می‌کند. رأی‌دهنده، نامزدها را روی صفحه‌نمایش الکترونیکی انتخاب می‌کند، سپس سیستم این انتخاب‌ها را روی برگه رأی کاغذی چاپ می‌کند و رأی‌دهنده برگه رأی را در صندوق می‌اندازد تا برای هر گونه بررسی مورد نیاز بعد از انتخابات، سابقه‌ای کاغذی وجود داشته باشد. رأی‌دهنده همچنین نسخه چاپی شخصی با شماره رهگیری الکترونیکی دریافت می‌کند که از الگوریتمی رمزنگاری‌شده برای ثبت انتخاب‌هایش بهره می‌برد. از این شماره رهگیری می‌توان برای تأیید ثبت دقیق آرای فرد استفاده کرد. این راه‌حل در مجموع امکان شمارش قابل اطمینان و امن همه آرا را فراهم می‌کند و رویکردی حیاتی برای امنیت و کارآمدی دموکراسی است.

در یک دهه پیش، تهدیدات سایبری به‌منظور هک کمپین‌ها و اختلال در رأی‌گیری، مسئله چندان جدی‌ای نبودند، اما اکنون ریسک‌هایی واقعی هستند که در گزارش‌های خبری روزانه مشاهده می‌شوند. همان‌گونه که دولت‌های دموکراتیک و صنعت با همکاری یکدیگر در دهه ۱۹۴۰ تلاش کردند تا در جنگ جهانی پیروز شویم، امروز هم باید برای حفاظت از صلح، واکنشی یکپارچه نشان دهند.

شایان ذکر است آزمایش‌های رژیم‌های مستبد با کمپین‌های دروغ‌پراکنی نشان می‌دهد که چالش‌های بسیار پیچیده‌تری پیش روی ما قرار دارد.

فصل ششم

رسانه‌های اجتماعی؛ آزادی‌هایی که بین ما فاصله می‌اندازند

در موزه‌ای در مرکز تالین، پایتخت استونی که در نزدیکی دریای بالتیک قرار دارد، دو آدمک مرد و زن جوان در دو طرف تخته چوبی باریک و بلندی قرار گرفته‌اند که بی‌وقفه دور می‌زنند. در حالی که این الاکلنگ بزرگ روی تکیه‌گاهی باریک می‌چرخد، اما این دو آدمک با دست‌های باز و نگاه خیره ثابت ایستاده‌اند. این مجسمه عجیب‌وغریب پیامی بدون شک جدی می‌فرستد. این اثر نماد وضعیت شکننده‌ای است که جوامع آزاد سراسر دنیا با آن مواجه هستند؛ این جوامع باید در عصر رسانه‌های اجتماعی از دموکراسی در برابر آزادی‌هایی حفاظت کنند که می‌توانند بین افراد فاصله بیندازند. این مجسمه گردان در واقع آخرین صفحه از روایت این موزه از داستانی است که تقریباً یک قرن از تاریخ به دست آوردن، از دست دادن و دوباره به دست آوردن استقلال در این کشور حوزه دریای بالتیک و تلاش‌ها برای حفظ استقلال را نشان می‌دهد. این داستان چالش‌های فناوری‌محور پیش روی همه دموکراسی‌های مدرن را هم بیان می‌کند. همان‌طور که راهنمای صوتی به بازدیدکنندگان می‌گوید: «استونی یک‌روزه آزاد نشده است. پیوسته به‌دنبال آزادی هستیم. هر روز این کار را می‌کنیم.» موزه دوطبقه «اشغال و آزادی وابامو» (Vabamu Museum of Occupations and Freedom) در پایین‌دست مرکز شهر قرون وسطایی تالین قرار گرفته است. هرچند این ساختمان شیشه‌ای و فولادی از لحاظ اندازه کوچک است، اما در تضادی شکوهمند با مرکز شهر برج و بارودار این پایتخت قرن سیزدهمی قرار دارد که در ارتفاعی بالاتر از این موزه قرار گرفته است. دیوارهای شیشه‌ای که به‌عنوان نمادی از عصر جدید استونی ساخته شده‌اند، نور شمالی را به درون این ساختمان معاصر فرامی‌خوانند؛ نوری که صحنه مدرنی را روشن می‌کند که داستانی پیچیده و غم‌انگیز به قلم اشغالگران روس، آلمان نازی و اتحاد جماهیر شوروی را بیان می‌کند. اما این موزه فقط بر سختی، سرکوب و کشتار متمرکز نیست. انگار شاهد هم‌سرایی افرادی از سراسر جهان هستیم که مشتاق آزادی هستند. مهم‌تر از همه به کشمکش مدام آزادی و مسئولیت‌پذیری می‌پردازد که آن دو آدمک چرخان موزه به ظرافت به نمایش می‌گذارند.

وقتی در پاییز ۲۰۱۸ از استونی بازدید می‌کردیم، تحقیقات کنگره ایالات متحده در مورد کمپین‌های دروغ‌پراکنی در توییتر و فیس‌بوک با بیشترین سرعت در جریان بود.

جهان در مورد این چالش‌های جدید هوشیار شده بود و سؤالاتی برایش پیش آمده بود. چطور این اتفاق افتاد؟ چرا افتاد؟ و چرا زودتر متوجه آن نشدیم؟

یکی از پاسخ‌های این پرسش‌ها را صبح یک روز یکشنبه در موزه وابامو پیدا کردیم. موزه وابامو ایده فردی به نام «اولگا کیستلر ریتسو» از اهالی استونی بود که بعداً ملیت آمریکایی گرفت. اولگا که در سال ۱۹۲۰ در کی‌یف اوکراین همزمان با فروپاشی امپراتوری روسیه به دنیا آمده بود، زیر سلطه مجموعه‌ای از رژیم‌های مستبد بزرگ شده بود. در کودکی به همراه برادر بزرگ‌ترش با فرار از آشوب و قحطی اوکراین به سمت شمال و به استونی مهاجرت کردند. اواخر جنگ جهانی دوم و در حالی که سربازان اتحاد جماهیر شوروی در حال آماده‌سازی برای حمله به کشور کوچک استونی و برگرداندن آن به خاک خودشان بودند، اولگا که حالا زن جوانی بود با سربازان آلمانی که در حال عقب‌نشینی بودند، سوار یکی از آخرین کشتی‌ها شد و از این کشور فرار کرد.

اولگا در سال ۱۹۴۹ به ایالات متحده آمد و در نهایت به همراه شوهر و دخترش در محلی در فاصله چند دقیقه‌ای از مکان امروزی ساختمان‌های اصلی مایکروسافت، در شهر ردموند، ایالت واشنگتن ساکن شد.

هرچند باقی عمرش را در ایالات متحده زندگی کرد، اما فکر استونی هرگز از ذهنش خارج نشد. مدام وضعیت وطن دوران کودکی‌اش را پیگیری می‌کرد که همچنان در اشغال اتحاد جماهیر شوروی بود. این شرایط در سال ۱۹۹۱ تغییر کرد؛ استونی بعد از ۵۰ سال اشغال از سلطه روسیه آزاد شد و شروع به ساختن آینده‌اش به‌عنوان کشوری مستقل کرد.

اولگا که اشتیاق زیادی برای مشارکت در آینده دموکراتیک استونی داشت، پس‌انداز عمرش را برای ساخت موزه‌ای اهدا کرد که داستان مهمی را گرامی می‌داشت. می‌خواست مطمئن شود جهان این داستان را نه فراموش و نه تکرار می‌کند. همان‌طور که «لنارت مری»، یکی از رؤسای جمهور استونی و حامی این مؤسسه، در افتتاحیه موزه در سال ۲۰۰۳ گفته بود این ساختمان بسیار فراتر از یک موزه است؛ «این ساختمان خانه آزادی است و پیوسته باید به ما یادآوری کند که چه مرز ظریف و حساسی بین آزادی و متضادش یعنی تمامیت‌خواهی وجود دارد.»

موزه وابامو هر سال داستان اشغال و آزادی استونی را برای بیش از ۵۰ هزار بازدیدکننده از سراسر جهان بازگو می‌کند و همچنین به آنها نشان می‌دهد فناوری چطور می‌تواند به سلاح تبدیل شود.

اینترنت به استونی کمک کرد تا از سایه کمونیسم دربیاید و زادگاه آینده اسکایپ را به دموکراسی الکترونیکی خودخوانده سرزنده‌ای تبدیل کند. اما در سال ۲۰۰۷ اشغالگر سابق استونی با حمله به پاشنه‌آشیل دیجیتال این کشور، شکنندگی ذاتی دموکراسی را برملا کرد و نشان داد چطور همان فناوری که به تعریف آزادی این کشور کمک کرده، این کشور را آسیب‌پذیرتر هم ساخته است.

بهار آن سال استونی متحمل نخستین حمله سایبری یک دولت علیه کشوری دیگر شد. این حمله محاصره‌ای دیجیتال به نام حمله «منع سرویس»، فعالیت بخش عمده اینترنت این کشور و از جمله سایت‌هایی را متوقف کرد که خدمات دولتی و اقتصاد استونی به آنها وابسته بودند. جهان به روسیه مظنون بود.

«مارینا کایوراند»، وزیر امور خارجه سابق استونی در میهمانی ناهارمان در تالین می‌گفت: «اگر چیزی مانند سگ واق‌واق کند، سگ است. اما در مورد ما، بد سگی بود!» مارینا بدون شک در این زمینه اطلاع داشت؛ چراکه در زمان حمله، سفیر استونی در فدراسیون روسیه بود.

حمله سال ۲۰۰۷، این کشور ۱٫۳ میلیون نفری را در زمینه امنیت سایبری مشهور کرد. در پی این حمله، ناتو مرکز عالی دفاع سایبری مشارکتی خود را در حومه تالین ساخت. قرار گرفتن در تیررس روسیه، این کشور و رهبرانش را وادار کرده بود که نه‌فقط بر جنگ و صلح؛ بلکه بر آزادی و سرکوب هم تمرکز کنند؛ مسائلی که در دو سوی مخالف معادله فناوری اطلاعات کنونی قرار دارند.

موزه‌ای که اولگا ساخته، برخورد فناوری و جامعه را به نحوی نشان می‌دهد که اماکن خیلی کمی قادر به این کار هستند. افراد سرکوب‌شده با میلی مشترک، یعنی طلب آزادی، متحد می‌شوند. اما وقتی افراد آزاد می‌شوند، این پیوند مشترک به‌تدریج محو می‌شود. مردم استونی بی‌واسطه فهمیدند که وقتی پرده آهنین فرو می‌ریزد، آن آزادی چالش‌هایی را به همراه دارد که ممکن است سرسام‌آور باشند.

در توضیحات این موزه آمده است: «از جهتی چنین شرایطی بسیار ترسناک است؛ زیرا همه در فهمیدن خواسته‌های واقعی‌شان دچار مشکل می‌شوند. اگر همه خواسته‌ها مجاز باشند، فرد چه چیزی را باید درخواست کند؟ در این صورت افراد در جست‌وجوی مسیرهای مختلف، خودشان را از پا درمی‌آورند».

مارک زاکربرگ، مدیرعامل فیس‌بوک این پلتفرم آنلاین را برای «بازتر و متصل‌تر» کردن دنیا ساخت. این موضوع از جهتی ستایش تمام‌عیاری از آزادی است، اما در کشوری که مأموران اطلاعاتی کاگ‌ب در آن نسخه‌های چاپی همه ماشین‌های تحریر کشور را ثبت، ردیابی و جمع‌آوری کردند تا از ارتباطات بدون مجوز جلوگیری کنند، مردم به‌خوبی می‌دانند که وقتی جریان اطلاعات و ایده‌ها ناگهان کاملاً آزاد شود، چقدر می‌تواند دردسرساز باشد.

افراد در چنین شرایطی چه کار می‌کنند؟ همان‌طور که موزه نشان می‌دهد، قبیله خودشان، در این مورد قبیله سایبری خودشان را پیدا می‌کنند؛ به‌دنبال گروه‌هایی از افراد هم‌فکر می‌گردند که همواره جزئی از جامعه انسانی بوده‌اند. این گروه‌ها با انتخاب کانال‌های ترجیحی و افرادی که می‌خواهند با آنها تعامل کنند، به‌هم‌پیوسته‌تر اما بسته‌تر می‌شوند؛ اطلاعاتی را به اشتراک می‌گذارند که فقط از یک دیدگاه به مسئله نگاه کرده است؛ مانند دنیای واقعی افراد به‌سرعت بدترین مسائل را در مورد دیگران باور می‌کنند، به‌ویژه آنهایی را که متفاوت می‌دانند؛ مکانیسم‌های دفاعی افراد فعال می‌شوند؛ خلاصه اینکه ایدئال‌گرایی با طبیعت انسانی برخورد می‌کند.

چه افرادی پیش از همه متوجه این مسئله شدند و از آن بهره‌برداری کردند؟ افرادی که مانند اهالی استونی در شرایطی مرکب از سرکوب و آزادی زندگی کرده بودند و شاید زودتر از دیگران متوجه این شرایط شدند؛ آنها همسایگان اهالی استونی در آن سوی مرز روسیه بودند. چه افرادی دیرتر از همه هوشیار شدند؟ آمریکایی‌های ایدئال‌گرای ساکن غرب ایالات متحده که تمام عمرشان را در آزادی گذرانده بودند.

اما برای درک درست این پدیده باید یکی دیگر از پیامدهای فناوری را به یاد بیاوریم که گرایش ما به تجزیه‌شدن به قبیله‌های سایبری را تقویت می‌کند. این پیامد «در کنار هم تنها بودن» است.

مدام بیش از پیش جذب گفت‌وگوهای مجازی با افرادی می‌شویم که از لحاظ فیزیکی در کنار ما نیستند؛ گاهی اوقات یک دنیا از هم فاصله داریم. فناوری دیجیتال دنیا را کوچک‌تر (و افراد را در دسترس‌تر) کرده است، اما در عین حال سکوتی کرکننده بین افرادی ایجاد کرده که در کنار هم قرار دارند. این پدیده جدیدی نیست. بیش از یک قرن است که تقریباً هر فناوری جدیدی که افراد دور از هم را به هم متصل کرده، موانع جدیدی را نیز بین افراد کنار هم و زیر یک سقف ایجاد کرده است.

هیچ فناوری مدرن دیگری مانند خودرو ساختار زندگی ما را تغییر نداده است و این تغییر فقط در چند جای دیگر به اندازه مناطق روستایی آمریکا عمیق بوده است. تا ابتدای قرن بیستم روستانشینان معمولاً خرید، کار، عبادت، یادگیری و معاشرت را در شعاع ۲۰مایلی خود انجام می‌دادند و اسب و درشکه‌هایشان آنها را حمل می‌کرد. فروشگاه همه‌منظوره مرکز شهر بود، کودکان در هر سن و سالی به مدرسه‌ای با یک یا دو کلاس می‌رفتند و همه اهالی از کلیسای روستایی کوچکی برای عبادت استفاده می‌کردند.

اما وقتی خودروهای بنزینی به مناطق روستایی وارد شدند، این شرایط به کلی تغییر کرد. بین سال‌های ۱۹۱۱ تا ۱۹۲۰ خودروهای موجود در مزارع از ۸۵ هزار به بیش از یک میلیون رسید. خودرو و جاده‌های مدرن چشم‌اندازهای جدیدی را با فرصت‌هایی در فاصله‌های دور پیش روی روستانشینان باز کرد و فاصله شهر و روستا را کاهش داد. همان‌طور که تاریخ‌نگاری می‌گوید خودرو «روستاییان را از انزوایی فیزیکی و فرهنگی درآورد که ویژگی بارز زندگی در مناطق روستایی بود».

اما این امکان جابه‌جایی بیشتر بدون هزینه نبود؛ هرچه افراد زمان بیشتری را در جای دیگر سپری می‌کردند، زمان کمتری را با خانواده‌ها و همسایگان‌شان می‌گذراندند. خودرو بافت درهم‌تنیده شهرهای کوچک را تا ابد تغییر داد.

از ابتدای دهه ۱۹۶۰ تلفن ثابت اثری مشابه روی خانواده‌ها گذاشت. اکنون برای نوجوانان وقت گذراندن به‌تنهایی در اتاق خواب به معنی وقت گذراندن با دوستان پای تلفن و چند سال بعد با کامپیوترهایشان بود. اعضای خانواده در خانه و در کنار هم تنها بودند.

۴۰ سال بعد تلفن‌های هوشمند باعث شدند فاصله فیزیکی بچه‌ها از والدین‌شان کمتر بشود، اما ذهن بچه‌ها به‌وضوح جای دیگری بود. مشاجره در مورد کنار گذاشتن تلفن همراه در خانواده‌ها به‌ویژه در هنگام صرف شام، بسیار رایج شد. فناوری در طول زمان پیوسته جهان را به جای کوچک‌تری تبدیل کرده، اما در عین حال ارتباط افراد را با آنهایی که در همسایگی‌شان یا زیر یک سقف در کنارشان زندگی می‌کنند، کمتر کرده است.

این مسئله چالش‌های جدیدی را برای دموکراسی ایجاد می‌کند. صرف زمان بیشتر در محیط آنلاین با غریبه‌ها، افراد را در برابر کمپین‌های دروغ‌پراکنی، آسیب‌پذیرتر کرده است؛ کمپین‌هایی که از علاقه‌مندی‌ها، خواسته‌ها و گاهی اوقات تعصبات آنها سوءاستفاده می‌کنند. این کمپین‌ها برای دنیای واقعی هم پیامدهایی دارند.

تا دهه‌ها یکی از نقاط قوت حکومت‌های جمهوری جهان، توانایی استفاده از ارتباطات باز و بحث عمومی برای ایجاد درک فراگیر و حتی فراحزبی، پشتیبانی در مورد مسائل سیاست خارجی و تعهد به آزادی‌های دموکراتیک بود. به‌ندرت آسان بوده است، اما همان‌طور که «فرانکلین روزولت» اثبات کرد؛ از فناوری‌های ارتباطی جدید مثل رادیو (در زمان او) می‌توان برای جلب حمایت عمومی در مورد اقدامات دشواری مثل پشتیبانی از بریتانیا پیش از ورود ایالات متحده به جنگ جهانی دوم استفاده کرد. ایالات متحده در این دهه‌ها از تمام فناوری‌های موجود؛ از رادیو تا فکس و... برای انتشار اطلاعات و گسترش دموکراسی در جوامع بسته اروپای مرکزی و شرقی استفاده کرد.

اما اکنون دیگران در مورد این نقطه‌قوت جامعه آزاد و باز، ورق را برگردانده‌اند. هک‌کردن ایمیل‌ها فقط نمونه کوچکی از رویکرد جدید روسیه است؛ چراکه بلندپروازی‌های این کشور بسیار گسترده‌تر هستند. شبکه‌های خبری کابلی و بعد رسانه‌های اجتماعی، حباب‌های اطلاعاتی بیش از پیش پراکنده‌ای را در دموکراسی‌های غربی، به‌ویژه در ایالات متحده ایجاد کرده‌اند. چه اتفاقی می‌افتاد اگر اطلاعات (درست یا غلط) را بتوان با استفاده از پلتفرم‌هایی مثل فیس‌بوک و توییتر منتشر کرد تا خشم گروه‌های گوناگون جامعه را برانگیخت و نامزدهای سیاسی احتمالاً متخاصم‌تر نسبت

به منافع روسیه را تضعیف کرد؟ چه اتفاقی می‌افتاد اگر تیم‌هایی از متخصصان فناوری و علوم اجتماعی در سن‌پترزبورگ و مسکو دور هم جمع شده بودند تا با همان خلاقیت و سرعت سازندگان پلتفرم‌ها، روی تصویر سیاسی و اجتماعی آمریکا تأثیر بگذارند؟ و چه اتفاقی می‌افتاد اگر هیچ‌کس در ایالات متحده به اندازه کافی توجه نکرده بود تا اتفاقات پیش رو را پیش‌بینی کند؟

اواخر سال ۲۰۱۸ تیمی از دانشگاه آکسفورد و شرکت آنالیتیکس آمریکایی «گرافیکا» آن دسته از داده‌های فیس‌بوک، اینستاگرام، توییتر و یوتیوب را که به واسطه حکم قانونی به کمیته اطلاعات سنا ارائه شده بود، تحلیل کرد. این تیم اولین گروهی بود که شیوه سازمان تحقیقات اینترنت روسیه (Internet Research Agency) (IRA) «در انجام حمله‌ای گسترده به ایالات متحده با استفاده از پروپاگاندای کامپیوتری به‌منظور ارائه اطلاعات اشتباه به رأی‌دهندگان آمریکایی و دوقطبی‌کردن آنها» را به‌دقت مستند می‌کرد. این تلاش‌های دروغ‌پراکنی معمولاً در حوالی تاریخ‌های کلیدی در تقویم انتخاباتی آمریکا به اوج می‌رسیدند. این استراتژی از ماهیت تعاملی و وایرال پلتفرم‌های رسانه‌های اجتماعی سوءاستفاده می‌کرد. همان‌طور که گزارش این تیم نشان می‌دهد، بین سال‌های ۲۰۱۵ تا ۲۰۱۷ بیش از ۳۰ میلیون کاربر «مطالب فیس‌بوکی و اینستاگرامی سازمان تحقیقات اینترنت را با خانواده و دوستان‌شان به اشتراک گذاشته، لایک کرده، به آنها واکنش نشان داده و پای آنها نظرشان را نوشته بودند».

عوامل روسیه با سوءاستفاده از فناوری ساخت آمریکا، توانسته بودند به محیط سیاسی ایالات متحده دسترسی یابند و در آن مداخله کنند. این نفوذ خارجی به دنیای واقعی هم کشیده شد؛ به‌طور مثال، تلاش موفقی که سازمان تحقیقات اینترنت در سال ۲۰۱۶ برای سازمان‌دهی تظاهرات همزمان گروه‌های مخالف در هیوستون داشت. در آن واقعه همسایگانی که ندانسته از سوی افرادی در سن‌پترزبورگ روسیه تحریک شده بودند، علیه یکدیگر شعار می‌دادند.

تا اواخر سال ۲۰۱۷ این حقیقت بیش از پیش روشن شد. وقتی گزارش‌ها در مورد تلاش‌های روسیه برای دروغ‌پراکنی در فیس‌بوک منتشر شدند، بیشتر افراد در بخش فناوری، از جمله مارک زاکربرگ شک داشتند که این فعالیت‌ها، گسترده یا آنچنان

اثرگذار باشند. اما این دیدگاه خیلی زود تغییر کرد. پاییز سال ۲۰۱۷ فیس‌بوک در تیررس مسئولانی از سراسر جهان قرار گرفته بود. بعد از پرونده‌های ضدانحصار علیه مایکروسافت در تقریباً دو دهه پیش، نخستین بار بود که یک شرکت فناوری تا این اندازه هدف تحقیقات و موشکافی نهادهای عمومی قرار می‌گرفت. از آنجایی که آن سال‌ها را در مایکروسافت گذرانده بودم، درخواست‌های مهم و در حال افزایش دولت از فیس‌بوک را درک می‌کردم. در عین حال مشکلات بسیار بزرگ پیش روی این شرکت را هم درک می‌کردم. فیس‌بوک خدماتش را به‌عنوان پلتفرمی برای دولت‌های خارجی طراحی نکرده بود تا از آن برای ایجاد اختلال در دموکراسی استفاده کنند، اما در عین حال تمهیداتی هم در نظر نگرفته بود تا از چنین فعالیت‌هایی جلوگیری کند یا دست‌کم آنها را شناسایی کند. تا زمانی که روسیه از فیس‌بوک علیه کشور سازنده آن سوءاستفاده نکرده بود، هیچ‌کس در این شرکت (یا در بخش فناوری یا خود دولت ایالات متحده) چنین پدیده‌ای را پیش‌بینی نکرده بود.

وقتی در فوریه ۲۰۱۸ در کنفرانس امنیتی مونیخ شرکت کردم، از تمرکز جهان بر مسئله فیس‌بوک بسیار متعجب شدم. این همایش سالانه که در سال ۱۹۶۳ بنیان‌گذاری شده و اکنون آن را «ولفگانگ ایشینگیر»، دیپلمات آلمانی سابق و مورد احترام مدیریت می‌کند، وزیران دفاع و سایر رهبران نظامی و ملی را از سراسر جهان دور هم جمع می‌کند تا در مورد سیاست امنیت بین‌الملل بحث کنند. در فهرست شرکت‌کنندگان این همایش در سال ۲۰۱۸ نام برخی همتایان من در صنعت فناوری اطلاعات دیده می‌شد.

در حالی که از میان افسران نظامی رده‌بالای حاضر در لابی شلوغ هتل «بایریشر هوف» (Bayerischer Hof) رد می‌شدم، با خود فکر کردم اینجا غریبه‌ام. وقتی در آسانسور کنار «اریک اشمیت»، رئیس وقت هیئت‌مدیره گوگل و تیمش قرار گرفتم، نوعی احساس بازگشت به وطن پیدا کردم. جای عجیبی برای برخورد با فردی از سیلیکون‌ولی بود.

اریک اشمیت پرسید: «تابه‌حال اینجا آمده بودی؟»

پاسخ دادم: «حقیقتش تابه‌حال به ذهنم خطور نکرده بود که باید در این همایش

شرکت کنم.»

اما در سال ۲۰۱۸ زمانه عوض شده بود، حضور هر دوی ما در مونیخ اتفاق مهمی بود.

بیشتر بحث‌های آن هفته بر استفاده از فناوری اطلاعات به‌عنوان سلاح متمرکز بود. از «کریستین لاگارد»، رئیس صندوق بین‌المللی پول در برنامه ناهاری با مدیران عامل پرسیده شد «چرا به همایشی دفاعی آمده است». او توضیح داد که می‌خواهد درک کند که چگونه از فناوری اطلاعات برای آسیب‌رساندن به فرایندهای دموکراتیک استفاده می‌شود و از این درک برای پرداختن به این مسئله استفاده کند که چطور ممکن است از فناوری اطلاعات برای حمله به بازارهای مالی سوءاستفاده شود. گفت‌وگوی هشدارآمیزی بود، اما دوراندیشی‌اش به من اطمینان خاطر داد.

هرچند گفت‌وگوها دشوار و کمی سنگین بودند، اما نمی‌توانستم با «الکس استیموس»، مدیر ارشد امنیت فیس‌بوک که در تمام مدت همایش در حال دفاع از شرکتش بود، کمی احساس همدردی نکنم. در میزگردی که هر دو حضور داشتیم، یکی از اعضای هلندی پارلمان اروپا، او را با پرسش‌های تندوتیز به رگبار بسته بود. همان شب در مراسم شام با شورای آتلانتیک، مسئولان دولتی و سایر شرکت‌کنندگان خشمگین مدام او را به چالش می‌کشیدند و می‌پرسیدند: «چطور فیس‌بوک اجازه داد این اتفاقات بیفتد».

هرچند نگرانی‌ها قابل درک بودند، اما از این بحث‌ها بسیار عصبانی می‌شدم. همه فیس‌بوک را هدف گرفته بودند، اما هیچ‌کس به متهم اصلی اشاره نمی‌کرد. مثل این بود که سر فردی داد بزنیم که یادش رفته در را قفل کند، اما هیچ اشاره‌ای به دزد نکنیم.

پرسش مهم‌تر برای فیس‌بوک، ایالات متحده، حکومت‌های جمهوری دموکراتیک جهان و کل بخش فناوری این بود که چه کار باید بکنیم. واکنش برخی افراد در دولت این بود که فیس‌بوک و سایر شرکت‌های مالک رسانه‌های اجتماعی را مقصر می‌دانستند و پافشاری می‌کردند که این شرکت‌ها باید مسئله را حل کنند. هرچند بخش زیادی از مسئولیت بر عهده این شرکت‌ها بود که این فناوری را ابداع کرده بودند، اما چنین رویکردی ناقص به نظر می‌رسید. پاسخ باید شامل ترکیبی از اقدامات دولت و بخش فناوری می‌شد.

در تابستان ۲۰۱۸ و در حالی که مارک زاکربرگ در کنگره شهادت می‌داد، بخش فناوری لحنش را نسبت به بزرگی مشکل و واکنش لازم، تغییر داده بود. زاکربرگ در آن جلسه گفت: «موضع من این نیست که نباید هیچ رگولیشنی وجود داشته باشد. فکر می‌کنم با افزایش اهمیت اینترنت در زندگی افراد، پرسش واقعی این است که رگولیشن مناسب چیست؛ نه اینکه رگولیشن باید وجود داشته باشد یا خیر.»

همان‌طور که اظهارات زاکربرگ نشان می‌دهد، بین به‌رسمیت‌شناختن مسئله بدیهی لزوم رگولیشن و رسیدن به نوعی رگولیشن منطقی در مورد رسانه‌های اجتماعی، تفاوت زیادی وجود دارد.

یکی از افراد پیشگام در پاسخ‌دادن به پرسش دوم، «مارک وارنر»، از مدیران ارشد مخابراتی سابق است که از سال ۲۰۰۹ به‌عنوان نماینده مردم ویرجینیا در سنای ایالات متحده خدمت می‌کند. وارنر در تابستان ۲۰۱۸ وایت‌پیپری را با مجموعه‌ای از پیشنهادها منتشر کرد که یکی از اهدافش رسیدگی به مسئله کمپین‌های دروغ‌پراکنی از طریق قانون‌گذاری جدید بود. او در این مقاله به برخی مسائل فنی و حریم خصوصی مربوط به این مشکلات اذعان کرده و خواستار بحث بیشتر در این زمینه شده بود.

همان‌طور که وارنر در مقاله‌اش بیان کرده بود، یکی از مسائل نوظهور رسانه‌های اجتماعی اینترنتی نگرانی‌های فزاینده نسبت به مصونیت موجود آنها طبق قانون منزلت ارتباطات (Communications Decency Act) است. کنگره در سال ۱۹۹۶ قانونی را تصویب کرد تا با معافیت ناشران «خدمات کامپیوتری تعاملی» از بسیاری از مسئولیت‌های قانونی ناشران سنتی‌تر، رشد اینترنت را افزایش دهد. برای مثال در ایالات متحده طبق قوانین ایالتی و بسیاری از قوانین فدرال، رسانه‌های اجتماعی بر خلاف تلویزیون و رادیو در برابر محتوای غیرقانونی منتشرشده در سایت‌هایشان مسئولیت قانونی ندارند.

اما اینترنت دیگر مقوله نوظهوری نیست و امروزه آثارش تمام جهان را فراگرفته است. از آنجایی که حکومت‌ها، تروریست‌ها و مجرمان از سایت‌های رسانه‌های اجتماعی در راستای اهداف شرورانه استفاده می‌کنند، رهبران سیاسی بیش از پیش در زیر سؤال بردن معافیت قانونی رسانه‌های اجتماعی با ناشران سنتی همراه می‌شوند.

وارنر به گسترش «جعل عمیق» به‌عنوان دلیل دیگری برای وضع مسئولیت‌های قانونی جدید در مورد سایت‌های رسانه‌های اجتماعی به‌منظور نظارت بر محتوایشان اشاره می‌کند. منظور از جعل عمیق «ابزارهای پیشرفته تلفیق صدا و تصویری است که می‌توانند فایل‌های صوتی یا ویدئویی جعلی تولید کنند و به دروغ نشان دهند که فردی سخنی می‌گوید یا کاری انجام می‌دهد».

هرچه دنیا بیشتر شاهد تقویت فعالیت‌های مشمئزکننده در رسانه‌های اجتماعی شد، فشار سیاسی نیز افزایش یافت. یک دهه بعد، شاید به ماه مارس ۲۰۱۹ به‌عنوان نقطه‌عطف نگاه کنیم. همان‌طور که «کوین روز» در نیویورک‌تایمز نوشت کشتار تروریستی وحشتناک ۵۱ مسلمان بی‌گناه در ۱۵ مارس در دو مسجد شهر «کرایست‌چرچ» (Christchurch) نیوزیلند از برخی جهات «حادثه‌ای بی‌سابقه بود؛ اولین کشتار جمعی مختص عصر اینترنت که کاملاً درون گفتمان عجیب افراط‌گرایی مدرن متولد و عملی شد». همان‌طور که او توضیح می‌دهد؛ «پیش از حمله در مورد آن در توییتر صحبت شده بود، در انجمن گفت‌وگوی «ایت‌چن» (8chan) اطلاعیه آن ارسال شده بود و به‌صورت زنده از فیس‌بوک پخش شده بود. بعد این تصاویر مدام در یوتیوب، توییتر و ردیت بازپخش شد و در حالی که این پلتفرم‌ها تلاش می‌کردند این کلیپ‌ها را حذف کنند، اما بلافاصله نسخه دیگری جایگزین‌شان می‌شد.»

تنها دو هفته بعد در ولینگتون، پایتخت نیوزیلند بودیم. برای این سفر از چند ماه قبل برنامه‌ریزی شده بود. «جاسیندا آردرن»، نخست‌وزیر نیوزیلند که این بحران تکان‌دهنده را با درایت و متانت فوق‌العاده مدیریت کرده بود، در سخنرانی مهمی تغییر چشم‌گیری را در نگاه به رسانه‌های اجتماعی ترسیم کرده بود. گفته بود: «نمی‌توانیم دست روی دست بگذاریم و بپذیریم که این پلتفرم‌ها وجود دارند و در مورد محتوایی که در آنها منتشر می‌شود، هیچ مسئولیتی ندارند.» سپس با تأکید بیشتر به سایت‌های رسانه‌های اجتماعی اشاره کرده و گفته بود: «این سایت‌ها ناشر هستند، پستچی نیستند. نمی‌توانند همه سود را ببرند، اما هیچ مسئولیتی نپذیرند.»

وقتی با آردرن و اعضای کابینه‌اش در نیوزیلند دیدار کردیم، نمی‌توانستم با حرف‌های او مخالفت کنم. این حادثه نشان داده بود که شرکت‌های فناوری باید

کارهای بیشتری انجام دهند. این مسئله شامل مایکروسافت و خدماتی مثل «بینگ»، «ایکس‌باکس لایو»، «گیت‌هاب» و «لینکدین» هم می‌شد. در سطح گسترده‌تر، ناگهان به نظر رسید که نظام رگولاتوری بنانهاده‌شده در تقریباً ۲۵ سال پیش، دیگر برای رسیدگی به تهدیدات کشورهای متخاصم و تروریست‌ها علیه مردم کافی نیست.

هرچند تفاوت‌های روشنی بین سوءاستفاده تروریست‌ها و مهاجمان تحت حمایت دولت‌ها از پلتفرم‌های رسانه‌های اجتماعی وجود دارد، اما شباهت‌هایی هم وجود دارد. هر دو شامل تلاش‌های عمدی برای تضعیف پایداری اجتماعی‌ای می‌شوند که جوامع به آن وابسته هستند. همچنین از قرار معلوم واکنش‌ها به هر دو مسئله، می‌توانند یکدیگر را تقویت کنند و دولت‌ها را به سمت تدوین مدل رگولاتوری جدیدی برای سایت‌های رسانه‌های اجتماعی رهنمون سازند.

اقدام برای رگوله‌کردن رسانه‌های اجتماعی ممکن است بی‌سابقه به نظر برسد، اما خوب است به یاد بیاوریم که ایالات متحده وضعیت مشابهی را تجربه کرده است. بیشتر آنچه اکنون می‌بینیم مشابه تلاش‌ها برای رگوله‌کردن محتوای رادیویی در دهه ۱۹۴۰ است.

اولین برنامه رادیویی بی‌سیم را شرکت «وستینگ‌هاوس» در نوامبر ۱۹۲۰ در ایالات متحده پخش کرد. این برنامه به اعلام خبر پیروزی «ویلیام هاردینگ» در انتخابات ریاست‌جمهوری و جانشینی او به جای «وودرو ویلسون» اختصاص داشت. وقتی رادیو نخستین بار به خانه‌های مردم آمد، معجزه‌ای مدرن در نظر گرفته می‌شد. رادیو جهان را از طریق تجربه‌های مشترک، رویدادهای زنده شاد، سرگرمی و اخبار فوری به هم مرتبط کرد. رادیوی بی‌سیم در دهه ۱۹۳۰ به محبوبیتی فوق‌العاده رسید و تا آخر این دهه به عضو ثابت ۸۳ درصد از اتاق‌های نشیمن خانه‌های آمریکایی‌ها تبدیل شد؛ عصر طلایی رادیو بود و این فناوری به همه‌چیز؛ از فرهنگ و سیاست آمریکا تا زندگی خانوادگی شکل داد.

وقتی رادیو در نیمه دوم دهه ۱۹۳۰ فراگیر شد، نگرانی‌ها نسبت به آثار اجتماعی آن نیز گسترش یافت. همان‌طور که در مقاله‌ای در سال ۲۰۱۰ در مجله «اسلیت» (Slate) آمده بود: «رادیوی بی‌سیم عامل پرت‌شدن حواس کودکان از مطالعه و

افت عملکردشان در مدرسه است؛ کارهایی که آن زمان مناسب و سالم محسوب می‌شدند. مجله موسیقی «گرامافون» در سال ۱۹۳۶ گزارش داد که کودکان به تقسیم توجه‌شان بین آماده‌سازی ملال‌آور تکالیف مدرسه و جذابیت هیجان‌انگیز بلندگوی رادیو، عادت کرده بودند و توصیف کرده بود که چطور برنامه‌های رادیو تعادل ذهن‌های تحریک‌پذیرشان را به هم می‌زند.»

بعد از پایان جنگ جهانی دوم اتفاقی افتاد که «وینسنت پیکارد»، پژوهشگر، آن را «شورش علیه رادیو» توصیف می‌کند. آن‌طور که او مستند کرده، بازار رادیو ابتدا بر اساس مدل کسب‌وکاری رشد کرد؛ بدین نحو که برای فروش دستگاه‌های رادیو، برنامه‌های رادیویی را به‌صورت رایگان ارائه می‌کرد، اما تا دهه ۱۹۴۰ در خانه‌های بیشتر مردم آمریکا یک رادیو یا حتی بیشتر وجود داشت. در نتیجه مدل کسب‌وکار برنامه‌های رادیو به سمت مدل تبلیغات حرکت کرد که در نگاه برخی منتقدان به تولید سریال‌های آبکی و برنامه‌های دیگری منجر شد که به‌مرور بیش از پیش بی‌معنی و حتی مبتذل شدند. آن‌طور که پیکارد می‌گوید: «این انتقاد به جنبش‌های اجتماعی مردمی، یادداشت‌های روزنامه‌ها و مجلات گوناگون و همچنین صدها نامه از شنوندگان عادی به سردبیرها، گوینده‌ها و کمیسیون ارتباطات فدرال راه یافت و در نتیجه قدرت گرفت.»

بی‌تابی به اوج رسید و باعث شد کمیسیون ارتباطات فدرال (Federal Communications Commission) در سال ۱۹۴۶ کتاب «آبی» را منتشر کند. کتاب آبی گزارشی بود که به خاطر رنگ جلدش این عنوان را گرفته بود و می‌خواست «امتیاز برخورداری از مجوز پخش را به رعایت الزامات گسترده‌ای مطابق با منافع عمومی مشروط کند». شرکت‌های پخش تجاری واکنش سیاسی شدیدی علیه این گزارش نشان دادند و پیشنهادهایش را ناکام گذاشتند، اما در هر صورت این اتفاق تاریخ پخش رادیو را عوض کرد و باعث شد شبکه‌های رادیویی بزرگ بودجه‌ای را به برنامه‌های مستند اختصاص دهند و برنامه‌سازی در راستای منافع عمومی را بهبود ببخشند.

برخی ممکن است به شورش علیه رادیو نگاه کنند و از این تاریخچه به این باور برسند

که یک چالش برای رسانه‌های اجتماعی اتفاق سیاسی زودگذر مشابهی خواهد بود که بعید است به تغییر رگولاتوری ماندگاری منجر شود. هرچند در پیش‌بینی آینده هیچ‌وقت قطعیتی وجود ندارد، اما دلایلی وجود دارد که باور کنیم بر خلاف این نظر، مسائل مربوط به رسانه‌های اجتماعی، نه کم‌اثرتر؛ بلکه تأثیرگذارتر خواهند بود. یکی از دلایل این است که نگرانی‌های کنونی مثل دروغ‌پراکنی دولت‌ها و پروپاگاندای تروریستی جدی‌تر از برنامه‌سازی مبتذل در دهه ۱۹۴۰ است. دلیل دوم ماهیت جهانی پیشنهادهای رگولاتوری موجود است. هرچند با توجه به اهمیت متمم اول قانون اساسی و عوامل دیگر، ایالات متحده از گذشته تمایلی به رگوله‌کردن محتوا نداشته است، اما کشورهای دیگر تا این اندازه از آزادی بیان حمایت نمی‌کنند.

اگر در مورد جنبه دوم شکی وجود داشت، اتفاقاتی که در پی حمله در کرایست‌چرچ نیوزیلند در استرالیا افتاد، این شک را کاملاً برطرف کرد. دولت استرالیا در عرض کمتر از یک ماه قانون جدیدی تصویب کرد که رسانه‌های اجتماعی و سایت‌های مشابه را ملزم می‌کرد «محتوای خشن مشمئزکننده» را «به سریع‌ترین شکل ممکن» حذف کنند یا با ریسک تحمل مجازات‌های کیفری مواجه شوند که شامل تا سه سال حبس برای مدیران ارشد فناوری و جریمه‌ای تا ۱۰ درصد درآمد سالانه شرکت می‌شود. هرچند بسیاری از افراد حاضر در بخش فناوری که فکر می‌کردند این قانون ترکیبی از مجازات‌های کیفری شدید و استانداردهای قانونی غیردقیق است، با نگرانی واکنش نشان دادند، اما این تحول نشان‌دهنده استیصال روزافزون رهبران سیاسی سراسر جهان بود که به‌وضوح خواستار جایگزینی مصونیت قانونی خدمات آنلاین با مدل رگولاتوری جدیدی بودند.

با این حال تفاوت زیادی بین نیاز به مدلی جدید و آگاهی دقیق از آن مدل جدید وجود دارد. به نظر می‌رسد پیروی از فرایندهای بازبینی ویراستاری پیش از انتشار در رسانه‌های چاپی، رادیویی یا تلویزیونی مرسوم، برای سایت‌های رسانه‌های اجتماعی غیرممکن باشد. فرض کنید قرار باشد فرد ویراستاری همه عکس‌های فیس‌بوک یا مدخل‌های لینکدین را قبل از نمایش برای کاربران بازبینی کند. این کار «سازوکاری» را از بین می‌برد که به صدها میلیون یا حتی میلیاردها کاربر در سراسر دنیا این امکان

را می‌دهد که محتوا بارگذاری کنند و آن را با خانواده، دوستان و همکاران‌شان به اشتراک بگذارند.

این مسئله باید با ظرافت و با تیغ جراحی؛ نه ساطور حل شود. مواجهه با این چالش، به‌ویژه در شرایط فشار سیاسی آسان نیست. این رویکرد به حدی برای جلوگیری از واکنش قانونی عجولانه بود که وارنر از گفت‌وگو با پلتفرم‌های رسانه‌های اجتماعی حمایت کرد، در حالی که بازخورد بسیار کمی از طرف بیشتر شرکت‌های مطرح دریافت کرد. وارنر با نگرانی از سوءاستفاده فزاینده روسیه از رسانه‌های اجتماعی، فهرستی از رویکردهای متناسب‌تر را ارائه کرد. یکی از ایده‌هایش که سیاست‌مداران استرالیایی آن را جدی‌تر و در سطحی بالاتر اجرا کردند، ملزم‌کردن پلتفرم‌های رسانه‌های اجتماعی به جلوگیری از بارگذاری دوباره محتوای غیرقانونی توسط کاربران بود. این کار در عمل مسئولیت قانونی این سایت‌ها برای اقدام‌کردن بعد از شناسایی مشکل را افزایش می‌داد. نسخه کلی‌تری از این ایده را دولت بریتانیا دو هفته بعد از اقدام استرالیا ارائه داد و «وظیفه قانونی جدیدی را برای مسئولیت‌پذیری بیشتر شرکت‌ها در برابر امنیت کاربران‌شان» پیشنهاد کرد و از این پیشنهاد با نظارت نهاد رگولاتوری مستقل پشتیبانی کرد. وارنر همچنین قوانینی را پیشنهاد کرد که پلتفرم‌های رسانه‌های اجتماعی را به تعیین مبداء حساب‌ها یا مطالب، شناسایی حساب‌های جعلی و هشدار دادن به کاربران در مورد انتشار اطلاعات توسط بات‌ها ملزم می‌کرد.

همان‌طور که این پیشنهادها نشان می‌دهند، احتمالاً می‌توان رویکردهای رگولاتوری مکملی را اتخاذ کرد که «تمرکز محدودتر بر طبقه‌بندی‌های ویژه محتوای نامناسب» را با «تلاش گسترده‌تر برای ارائه اطلاعات بیشتر در مورد منابع محتوا» تلفیق می‌کنند. یکی از ویژگی‌های مهم رویکرد دوم تأکید آن بر پرداختن به مسئله دروغ‌پراکنی، نه با ارزیابی درست یا غلط بودن محتوا؛ بلکه با ارائه اطلاعات درست در مورد هویت افراد به کاربران رسانه‌های اجتماعی است؛ رویکردی عقلانی که در تبلیغات سیاسی مدرن اتخاذ می‌شود. با این کار تشخیص درست یا غلط‌بودن را به مردم واگذار می‌کنیم، اما به آنها این امکان را می‌دهیم که این تصمیم را بر اساس درک درست از ناشر محتوا بگیرند. در قرن بیست‌ویکم باید به مردم اجازه بدهیم بدانند ناشر محتوا انسان است

یا بات خودکار.

جالب است که طرحی غیردولتی از همین رویکرد استفاده می‌کند. این طرح را دو آمریکایی برجسته در بخش رسانه اجرا کردند که یکی محافظه‌کار و دیگری لیبرال است. «گوردون کروویتز»، ناشر سابق وال‌استریت‌ژورنال و «استیون بریل»، روزنامه‌نگار سابقی است که مجله «آمریکن لایر» و شبکه تلویزیونی «کورت تی‌وی» را بنیان‌گذاری کرده است. این دو نفر با هم خدمت «نیوزگارد» (NewsGuard) را ایجاد کرده‌اند که از روزنامه‌نگاران استفاده می‌کند تا برای رسانه‌ها به‌اصطلاح «برچسب مصرف» درست کند.

نیوزگارد از طریق پلاگین رایگان مرورگر اینترنت آیکون‌های سبز یا قرمزی را در کنار لینک‌های موتورهای جست‌وجو و فیدهای رسانه‌های اجتماعی شامل فیس‌بوک، توییتر، گوگل و بینگ به نمایش می‌گذارد که نشان می‌دهند سایتی «می‌خواهد اطلاعات درست ارائه کند یا نیتی پنهان دارد یا با آگاهی، اطلاعات غلط یا پروپاگاندا منتشر می‌کند». نیوزگارد علاوه بر ارزیابی وب‌سایت‌های خبری و اطلاعاتی، آیکون آبی را در مورد سایت‌های پلتفرمی به کار می‌گیرد که از محتوای تولیدی کاربران میزبانی می‌کنند و آیکون نارنجی را برای سایت‌های شوخی و طنزنگاری به کار می‌برد که به نحوی طراحی شده‌اند که واقعی به نظر برسند. در مورد وب‌سایت‌هایی که هنوز ارزیابی و دسته‌بندی نشده‌اند، آیکون خاکستری به کار برده می‌شود.

این تلاش چالش‌هایی را هم در ابتدای کار به همراه داشت؛ به‌ویژه وقتی تیم نیوزگارد فعالیتش را به خارج از ایالات متحده گسترش داد و تلاش کرد معیارهای دسته‌بندی مؤثری را برای سراسر جهان تدوین کند. اما کروویتز و بریل می‌توانند بسیار سریع‌تر و چابک‌تر از دولت‌ها عمل کنند. پیش از آنکه پیشنهادهای وارنر به مرحله جلسه استماع در کنگره برسند، خدمت آنها آماده و فعال شده بود و این تیم پیوسته در حال اصلاح و بهبود عملیات‌هایش است. چون تلاشی غیردولتی است، به‌سرعت می‌تواند دامنه فعالیت‌های بین‌المللی‌اش را گسترش دهد، اما موفقیت این خدمت به تأمین مالی خصوصی و پشتیبانی شرکت‌ها از پلاگین مرورگر و در نهایت به خود کاربران وابسته است که از این خدمت استفاده کنند یا خیر.

در مجموع دو درس کلی‌تر در این زمینه وجود دارد؛ اول اینکه طرح‌های بخش‌های دولتی و خصوصی باید در کنار هم پیش بروند و یکدیگر را تکمیل کنند و دوم اینکه هرچند فناوری کنونی تازگی دارد، اما درس‌های زیادی را می‌توان از چالش‌های گذشته گرفت.

جالب است که مداخله خارجی در دموکراسی تقریباً قدمتی به اندازه خود کشور ایالات متحده دارد. ماهیت حکومت جمهوری دموکراتیک، همیشه آن را در معرض اختلال (خارجی یا داخلی) قرار می‌دهد و این اختلال‌ها از طریق تلاش‌هایی برای تخریب اعتماد و تأثیرگذاری بر نظر مردم اتفاق می‌افتند. نخستین نفری که متوجه این موضوع شد، «ادموند چارلز جنت»، یکی از اولین سفیران فرانسه در ایالات متحده بود. او اوایل آوریل ۱۷۹۳، درست چند هفته پیش از آنکه «جورج واشنگتن» بی‌طرفی ایالات متحده را در جنگ در حال گسترش فرانسه و بریتانیا اعلام کند، به ایالات متحده آمد. جنت مأموریت داشت این حکومت جمهوری نوپا را به پشتیبانی از فرانسه ترغیب کند و از جمله می‌خواست ایالات متحده را متقاعد کند که هم بدهی‌هایش به فرانسه را زودتر پرداخت کند و هم به این کشور کمک کند تا از طریق کشتی‌های تجاری مسلح در بندرهای ایالات متحده، به ناوگان دریایی بریتانیا حمله کند. جنت آماده بود که در صورت لزوم، برای براندازی دولت نوپای ایالات متحده هم تلاش کند.

ورود جنت به ایالات متحده تنش فزاینده‌ای را در کابینه واشنگتن ایجاد کرد. «توماس جفرسون» به فرانسوی‌ها و «الکساندر همیلتون» به بریتانیایی‌ها گرایش داشت. جنت برای رسیدن به هدفش تلاش کرد به‌طور مستقیم به مردم آمریکا مراجعه کند. تاریخ‌نگاری می‌گوید این حرکت محرک مهمی در ایجاد سیستم دوحزبی موجود بود: «هیجان گفت‌وگوهای سیاسی بالا گرفت، در مواردی نزاع‌های خیابانی شکل گرفت و همچنین دوستی‌های قدیمی خراب شدند.» در نتیجه واشنگتن و اعضای کابینه‌اش در سال ۱۷۹۳ اختلاف نظرات‌شان را کنار گذاشتند و یکپارچه خواستار فراخوان جنت برای بازگشت به فرانسه شدند.

این نتیجه برای نسل ما درسی دارد؛ با مداخلات خارجی در فرایندهای دموکراتیک،

می‌توان با موفقیت برخورد کرد؛ به شرط آنکه ذی‌نفعان حکومت جمهوری به اندازه کافی اختلاف‌نظرات‌شان را کنار بگذارند تا بتوانند با همکاری یکدیگر واکنش مؤثری نشان دهند. شاید دشوار باشد که به یاد بیاوریم جفرسون، همیلتون و حامیان‌شان به اندازه جمهوری‌خواهان و دموکرات‌های امروز پرحرارت بودند، اما نمایش موزیکال همیلتون در «برادوی» به یادمان می‌آورد که سیاست‌مداران امروز دست‌کم دیگر به دوئل‌های مسلحانه متوسل نمی‌شوند. واقعیت این است که اختلاف‌نظرات پرشور و حتی سخنان بسیار تند، یکی از ریسک‌های ذاتی و چالش‌های همیشگی هر حکومت جمهوری دموکراتیکی است.

با توجه به این شرایط و تلاش‌های ادامه‌دار فرانسوی‌ها برای مداخله در امور سیاسی آمریکا بود که واشنگتن از سخنرانی خداحافظی‌اش در سال ۱۷۹۶ استفاده کرد تا در مورد مخاطرات مداخله خارجی هشدار بدهد. واشنگتن در این سخنرانی گفت: «جامعه آزاد باید همیشه هوشیار باشد؛ زیرا تاریخ و تجربه ثابت کرده که نفوذ خارجی یکی از مهلک‌ترین سم‌ها برای حکومت جمهوری است.» تاریخ‌نگاران گاهی هنگام ارزیابی مزایا و معایب مداخله بین‌المللی در جهان در مورد دلالت‌های ضمنی سخنرانی او بحث می‌کنند. اما خوب است به یاد داشته باشیم که واشنگتن بیشتر بر کشمکش آن لحظه و مداخله مستقیم خارجی در امور سیاسی آمریکا متمرکز بود و بی‌واسطه با ریسک‌های این مسئله دست‌وپنجه نرم می‌کرد.

البته در این چند قرنی که از سخنرانی واشنگتن می‌گذرد، تغییرات زیادی اتفاق افتاده است. در زمان او، افرادی که می‌خواستند روی نظر مردم تأثیر بگذارند، از روزنامه‌ها، بروشورها و کتاب‌ها استفاده می‌کردند. بعد تلگراف، رادیو، تلویزیون و اینترنت آمدند. امروز فردی در اتاقکی در سن‌پترزبورگ می‌تواند در عرض چند دقیقه با دروغ‌پراکنی هدفمند به تحولات سیاسی هر جای دنیا واکنش نشان دهد.

دولت ایالات متحده نیز از فناوری اطلاعات به‌منظور اطلاع‌رسانی و حتی متقاعد کردن مردم سایر کشورها برای پشتیبانی از برخی مواضع استفاده کرده است. البته بسیاری از این کارها پنهانی بوده‌اند. امروزه در ایالات متحده بسیاری از افراد فعالیت‌های سازمان «سیا» در اروپا و آمریکای لاتین در دهه ۱۹۵۰ را رد می‌کنند، اما

کارهای دیگر ایالات متحده در این زمینه از جمله رادیوی اروپای آزاد در طول جنگ سرد و صدای آمریکای امروز کاملاً آشکار هستند.

ایالات متحده با استفاده از فناوری جهت انتشار اطلاعات به‌منظور پرورش و ارتقای دموکراسی مشکلی نداشته است، اما اکنون از فناوری برای انتشار دروغ‌پراکنی و اختلال در دموکراسی استفاده می‌شود. از زاویه‌ای می‌توانیم بر اساس اصول مربوط به حقوق بنیادین بشر، این فعالیت‌ها را در طبقه‌بندی‌های متفاوتی قرار دهیم، اما از زاویه‌ای دیگر سیاست عملی از جنبه بسیار مهمی تغییر کرده است. تا همین اواخر به نظر می‌رسید فناوری‌های ارتباطاتی به نفع دموکراسی عمل می‌کنند و اقتدارگرایی را به حالت دفاعی می‌برند. حال باید بپرسیم آیا اینترنت ریسکی را به زیان دموکراسی‌ها ایجاد کرده که دولت‌های مستبد می‌توانند بسیار آسان‌تر از حکومت‌های جمهوری آن را خنثی کنند؛ همان حکومت جمهوری که فرانکلین به ما تأکید کرد «آن را حفظ کنیم».

پاسخ احتمالاً مثبت است. فناوری دیجیتال دنیایی متفاوت ایجاد کرده است؛ دنیایی که در تمام زمینه‌ها بهتر نیست. اینکه چطور می‌خواهیم به این مسئله رسیدگی کنیم، هنوز کاملاً روشن نیست، ولی رسیدگی به آن، مانند زمان جورج واشنگتن مستلزم همکاری همه ذی‌نفعان حکومت‌های جمهوری دموکراتیک، نه‌فقط احزاب سیاسی؛ بلکه بخش فناوری و همچنین دولت‌های سراسر جهان است.

فصل هشتم

دیپلماسی دیجیتال

ژئوپلیتیک فناوری

وقتی «کسپر کلینگ» در فوریه ۲۰۱۸ به مقر مایکروسافت در ردموند آمد، ممکن بود افراد از روی تیپ و قیافه‌اش به اشتباه فکر کنند کارآفرین حوزه فناوری است یا شاید با توجه به لباس شیک، حس‌وحال کالیفرنیایی و ته‌ریش‌اش فکر می‌کردند بازیگر یا نوازنده است. وقتی با او دست دادم، تازه یادم آمد با چه کسی دیدار می‌کنم.

کسپر از آن نوع سفیرانی نیست که معمولاً می‌بینیم. مأموریتش هم معمولی نیست. نخستین کسی است که به‌عنوان سفیر فناوری دانمارک انتخاب شده و مسئول برقراری ارتباط دولت دانمارک با شرکت‌های فناوری سراسر جهان است. «سفارت» او بیش از ۲۰ کارمند دارد که در سه قاره کار می‌کنند و در ایالات متحده، چین و دانمارک مستقر هستند.

وقتی بهار سال قبل با گروهی از سفیران اروپایی در کپنهاگ جلسه داشتم، شغل جدید کسپر ذهن افراد را به خود مشغول کرده بود. «اندرس ساموئلسن»، وزیر امور خارجه دانمارک این مسند را «نخستین در جهان» و جایگاهی ضروری خوانده و گفته بود شرکت‌های فناوری به اندازه کشورها بر دانمارک تأثیر می‌گذارند؛ «این شرکت‌ها به نوعی کشور جدید تبدیل شده‌اند و ما باید با این مسئله مواجه شویم.»

هرچند دانمارک نخستین کشوری بود که سفیری رسمی برای برقراری ارتباط با بخش فناوری منصوب می‌کرد، اما تصمیم این کشور در پی اقدام مشابهی در دولت بریتانیا انجام می‌شد. دیوید کامرون، نخست‌وزیر بریتانیا در سال ۲۰۱۴ جایگاهی را در دفترش برای نقش دیپلماتیک ویژه‌ای ایجاد کرد که ابتدا قرار بود به مسائل فناوری مجریان قانون رسیدگی کند و بعد قرار شد به‌عنوان «فرستاده ویژه به شرکت‌های فناوری ایالات متحده» خدمت کند. نخستین کسی که در این جایگاه جدید منصوب شد، «سر نایجل شینوالد»، سفیر سابق بریتانیا در ایالات متحده بود.

دولت‌های دیگر مثل استرالیا و فرانسه نیز اقدامات مشابهی انجام دادند. این تغییرات نشان می‌داد چقدر دنیا عوض شده است. از زمان ظهور امپراتوری‌های کسب‌وکار در عصر طلایی ایالات متحده، شرکت‌های بزرگ نقش مهمی در اقتصادها و جوامع ایفا کرده‌اند. هیچ صنعتی مانند راه‌آهن در نیمه دوم قرن نوزدهم، جامعه آمریکا و در نهایت قانون آمریکا را متحول نکرد. همان‌طور که «دستورالعمل پور برای

راه آهن‌های ایالات متحده» (Poor's Manual of the Railroads of the United States) در انتهای قرن نوزدهم ماهرانه بیان می‌کند: «هیچ سازمانی به اندازه راه‌آهن به واسطه نفوذی که اعمال می‌کند، قدرتی که می‌بخشد و امید کسب سودی که ایجاد می‌کند، وسوسه‌کننده نیست.»

راه‌آهن اولین کسب‌وکار بزرگ آمریکا بود که با هزاران مایل خط آهن از مرز ایالت‌ها می‌گذشت و محرک موجی از قانون‌گذاری در مورد تجارت، پتنت، املاک و نیروی کار شد. شاید وجود کتاب «راه‌آهن و قانون آمریکا» از «جیمز ایلای» (James Ely) در کتابخانه مدیر ارشدی که در حوزه نرم‌افزار فعالیت می‌کند عجیب به نظر برسد، اما یکی از کتاب‌هایی است که هرازگاهی به آن مراجعه می‌کنم تا در مورد این مسئله که «چطور فناوری دنیای اطرافش را تغییر می‌دهد» از آن بهره ببرم.

هرچند ممکن است برخی افراد راه‌آهن را اینترنت دوران خودش بدانند، اما فناوری دیجیتال امروز یک ویژگی بسیار متفاوت دارد. در دنیای کنونی محصولات و شرکت‌ها خیلی جهانی‌تر هستند و ماهیت فراگیر فناوری اطلاعات و ارتباطات بخش فناوری را به شکل فزاینده‌ای به قلب مسائل سیاست خارجی می‌کشد.

در سال ۲۰۱۶ این شعار که «بدون امنیت سایبری امنیت ملی وجود ندارد» در مایکروسافت فراگیر شد و به‌مرور به بحث‌های عمومی نفوذ کرد. در تشخیص این مسئله تنها نبودیم. به‌عنوان مثال شرکت خوشه‌ای زیمنس آلمان به‌طرز دقیقی پیش‌بینی کرده بود «امنیت سایبری مهم‌ترین مسئله امنیتی آینده خواهد بود». هر مسئله‌ای که نقشی اساسی در امنیت ملی داشته باشد، به‌وضوح بخش فناوری را جدی‌تر به سوی دنیای دیپلماسی بین‌المللی سوق می‌دهد.

این موضوع یکی از دلایلی بود که اهمیت ارائه توضیح شفاف به مردم درباره فعالیت‌هایمان حول این مسائل را افزایش داد. در حالی که تلاش‌هایمان در حوزه امنیت سایبری تکامل می‌یافت، متوجه لزوم اجرای سه استراتژی متمایز (و گفت‌وگو درباره آنها) شدیم. اولین و بدیهی‌ترین استراتژی، تقویت تدابیر دفاعی فنی بود. این کار به‌طور طبیعی از بخش فناوری شروع می‌شود، اما وقتی مشتریان این خدمات جدید را به کار می‌گیرند، بخشی از مسئولیت را هم می‌پذیرند. در مایکروسافت سالانه

بیش از یک میلیارد دلار برای توسعه قابلیت‌های امنیتی جدید هزینه می‌کردیم. این سرمایه‌گذاری شامل هزینه بیش از ۳۵۰۰ متخصص و مهندس امنیت اختصاصی می‌شد. این کار اولویتی بسیار مهم در بخش فناوری و فرایندی همیشگی است؛ زیرا پیوسته و با سرعتی فزاینده در حال ارائه قابلیت‌های امنیتی جدید هستیم.

رویکرد دوم که شامل امنیت عملیاتی می‌شود، از برخی جهات در مایکروسافت اولویت بیشتری نسبت به برخی شرکت‌های دیگر حوزه فناوری، دارد. این رویکرد شامل فعالیت‌های تیم‌های مرتبط با شناسایی تهدیدات، تمرکز مرکز عملیات‌های دفاع سایبری بر اشتراک‌گذاری این اطلاعات با مشتریان و فعالیت‌های واحد جرائم دیجیتال برای توقف حملات سایبری و اقدام علیه آنها می‌شود.

این فعالیت آخر، ما را بیش از پیش به حوزه‌ای وارد کرد که در گذشته دولت‌ها به‌تنهایی به آن رسیدگی می‌کردند. همچنین پرسش‌های پیچیده‌ای را مطرح کرد؛ از جمله اینکه شرکت‌ها چطور باید به برخی حملات پاسخ می‌دادند؟ بدیهی است که باید به مشتریان‌مان کمک می‌کردیم آسیب‌های ناشی از هک را برطرف کنند، اما چطور می‌توانستیم پیش از وقوع از حملات جلوگیری کنیم؟ آیا اجازه حمله متقابل داشتیم؟

وقتی در سال ۲۰۱۶ در جلسه‌ای در کاخ سفید این پرسش از گروهی از رهبران فناوری پرسیده شد، واکنش‌ها متفاوت بود. یکی از مدیران ارشد شرکت‌کننده از توانمند کردن شرکت‌ها برای انجام حمله متقابل استقبال کرد، اما نگران بودم که اجرای خودسرانه عدالت از سوی شرکت‌های فناوری، خطاها و حتی آشفتگی‌هایی در پی داشته باشد. به همین دلیل این حقیقت که معمولاً واحد جرائم دیجیتال را ملزم می‌کنیم مسائل، به‌ویژه پرونده‌های شامل مجریان قانون را در دادگاه حل کند، تا حدی مایه آسودگی خاطرم است. این کار باعث شده در چارچوب سیستمی قانونی عمل کنیم که در آن نهادهای مرجع عمومی نقش مناسب‌شان را ایفا می‌کنند و ما هم تابع آنها و به‌طور کلی قانون می‌مانیم. احساس می‌کردم پایبند ماندن به این رویکرد منطقی است.

با افزایش ملی‌گرایی از جمله در ایالات متحده، شرکت‌های جهانی باید از هوشمندی لازم برای جهانی عمل کردن برخوردار باشند. همتایان‌مان را به چالش کشیدیم تا نوعی

«سوئیس دیجیتال بی‌طرف» باشند که به دفاع از همه مشتریان در سراسر جهان متعهد است و خود را به رویکرد صد درصد دفاعی و صفر درصد تهاجمی ملزم کرده است. همه دولت‌ها از جمله آنهایی که دیدگاه‌های ملی‌گرایانه‌تری دارند باید بتوانند به فناوری اعتماد کنند. وقتی بخش فناوری، خود را به حفاظت از همه مشتریان، صرف‌نظر از ملیت‌شان، ملزم می‌کند و در حمله به شهروندان بی‌گناه به هیچ دولتی کمک نمی‌کند، این موضوع به نفع دولت‌ها هم هست.

وقتی این دو استراتژی را تلفیق کردیم، همچنان به نظر می‌رسید برای واکنش به حملات در حال گسترش کافی نیستند. باید رکن سوم و مهمی به مقوله امنیت سایبری اضافه می‌کردیم. این رکن سوم قوانین بین‌المللی قدرتمندتر و فعالیت دیپلماتیک هماهنگ برای مهار تهدیدات سایبری و کمک به ترغیب جامعه بین‌الملل به‌منظور فشار آوردن به دولت‌ها برای متوقف‌کردن حملات سایبری کور بود. فکر می‌کردیم تا وقتی پاسخگویی جهانی بیشتری وجود نداشته باشد، انکار هر گونه تخلفی برای دولت‌ها بسیار آسان خواهد بود.

در ژانویه ۲۰۱۷ از قضا یک هفته پیش از آنکه دانمارک تشکیل مسند آینده کسپر کلینگ را اعلام کند، در مایکروسافت در حال بحث در مورد راه‌هایی برای تلنگر زدن به بخش فناوری و متحد کردن جامعه بین‌الملل حول امنیت سایبری بودیم. یادم می‌آمد که کمیته بین‌المللی صلیب سرخ، دولت‌های جهان را در سال ۱۹۴۹ دور هم جمع کرده بود تا با پایه‌گذاری کنوانسیون چهارم ژنو در زمان جنگ، به نحو بهتری از غیرنظامیان محافظت کند. در آن جلسه پرسیدم: «تلخ و دور از انتظار نیست که اکنون، مثلاً در دوران صلح، شاهد این حملات علیه غیرنظامیان باشیم؟»

«دومینیک کار»، مدیر روابط عمومی‌مان، خیلی سریع پاسخ داد: «شاید زمان تصویب کنوانسیون دیجیتال ژنو فرا رسیده باشد.»

به هدف زده بود. همان‌طور که دولت‌ها در سال ۱۹۴۹ به محافظت از غیرنظامیان در زمان جنگ متعهد شده بودند، شاید کنوانسیون دیجیتال ژنو نیز می‌توانست در زمان صلح، تصور افراد از لزوم محافظت دولت‌ها از غیرنظامیان در اینترنت را به روی کاغذ بیاورد. این ایده می‌توانست از کارهای جاری دولت‌ها، دیپلمات‌ها و متخصصان فناوری

در برقراری هنجارهای امنیت سایبری بین کشورها بهره ببرد. اگر قرار بود این ایده به واقعیت بپیوندد، شاید مثال و برندی جذاب می‌توانست به ما کمک کند تا با مخاطبان غیرفنی که باید نظرشان را جلب می‌کردیم، ارتباط مؤثرتری برقرار کنیم.

خواستار تقویت پیوسته قوانین بین‌المللی برای جلوگیری از آن دسته از حملات سایبری شدیم که شهروندان عادی، نهادهای خصوصی یا زیرساخت‌های حیاتی را در زمان صلح هدف قرار می‌دادند. همچنین خواستار ممنوعیت گسترده استفاده از هک برای سرقت مالکیت معنوی شدیم. به همین ترتیب خواستار قوانین محکم‌تری شدیم که دولت‌ها را وادار می‌کند به تلاش‌های بخش خصوصی در شناسایی این نوع حملات و پاسخگویی به آنها کمک کنند. در نهایت خواستار ایجاد سازمان مستقلی شدیم که می‌تواند در مورد شواهدی که حملات دولتی را به کشوری خاص نسبت می‌دهند، تحقیق کند و آنها را با عموم به اشتراک بگذارد.

بعد از طرح ایده‌هایمان در همایش امنیتی RSA در سان‌فرانسیسکو در سال ۲۰۱۷، شماری از خبرنگاران به سراغ این مضمون رفتند و مشتاقانه به درخواست برای ایجاد کنوانسیون دیجیتال ژنو توجه کردند. هرچند رسانه‌ها سنگ محک و آزمون خوبی برای پذیرش ایده‌های جدید هستند، اما آزمون مهم‌تر این بود که این ایده‌ها باید می‌توانستند گفتمان سیاست‌مداران را تغییر دهند. راه خوبی برای اینکه بفهمیم حرف‌مان شنیده شده یا خیر، این بود که افرادی با آن مخالفت می‌کردند. به هر حال در دنیایی با مسائل بسیار زیاد و رسانه‌های چندپاره، ایده‌ها خیلی راحت به فراموشی سپرده می‌شوند. افراد پرمشغله و دارای جایگاه‌های مهم آن‌قدر وقت ندارند که به همه حرف‌هایی که دیگران در طول روز می‌زدند، واکنش نشان دهند.

در این آزمون قبول شدیم. در واشنگتن‌دی‌سی بیش از همه، مسئولانی از ایده کنوانسیون دیجیتال ژنو ناراحت شدند که در پرورش توانایی‌های سایبری تهاجمی کشور نقش پررنگی داشتند. استدلال می‌کردند که اعمال محدودیت‌های قانونی برای استفاده از توانایی‌های سایبری، دست‌وپای دولت‌هایی مثل ایالات متحده را می‌بندد. اشاره کردیم که دولت ایالات متحده همین حالا هم مخالف استفاده از حملات سایبری علیه غیرنظامیان در زمان صلح است و ما هم می‌خواستیم همین حوزه را محدود کنیم.

از دید کلی‌تر هم تاریخ فناوری تسلیحاتی نشان می‌داد که حتی اگر ایالات متحده اکنون در این زمینه پیشگام باشد، اما به‌زودی کشورهای دیگر به ما خواهند رسید.

این افراد می‌گفتند که اگر قوانین محکم‌تری وضع کنیم و ایالات متحده از آنها پیروی کند، دشمنان‌مان پیروی نخواهند کرد. اما معتقد بودیم در هر صورت قوانین بین‌المللی می‌توانند با ایجاد مبنای اخلاقی و هوشمندی مورد نیاز برای واکنش‌های بین‌المللی هماهنگ‌تر نسبت به حملات سایبری، به افزایش فشار بر همه کشورها کمک کنند. به هر حال اگر رفتاری، قانون را نقض نکند، محدود کردن آن دشوارتر می‌شود.

مثل همیشه درس‌های زیادی از این تبادل نظرات گرفتیم. برخی افراد اشاره می‌کردند که همین حالا هم هنجارهای بین‌المللی مهمی وجود دارند و این کار ممکن است این برداشت را ایجاد کند که قوانین موجود اهمیت ندارند. حق با آنها بود. از ابتدا به‌روشنی اعلام کردیم که کنوانسیون دیجیتال ژنو را هدفی بلندمدت و بخشی از چشم‌اندازی می‌بینیم که اجرای آن احتمالاً یک دهه طول می‌کشد. نمی‌خواستیم یکی از عوارض کارمان تضعیف هنجارهای موجود باشد. در مورد این جنبه‌ها گفت‌وگوهای مفصلی با دولت و متخصصان دانشگاهی سراسر جهان داشتیم و مشخص کردیم کدام قوانین شامل فضای سایبری می‌شوند و به تقویت کاربرد آنها و شناسایی خلأهای آنها نیاز داریم.

همچنین با واکنش منفی افرادی روبه‌رو شدیم که به این گزاره معترض بودند که شرکت‌های بین‌المللی به‌جای کمک به دولت محل استقرارشان برای حمله به سایر کشورها، از غیرنظامیان همه جهان محافظت کنند. در سفری که به واشنگتن‌دی‌سی داشتم، یکی از مشاوران ترامپ این‌طور من را به چالش کشید که «به‌عنوان شرکتی آمریکایی چرا نمی‌پذیرید که به دولت ایالات متحده برای جاسوسی از افرادی در کشورهای دیگر کمک کنید؟»

به این مسئله اشاره کردم که مجموعه هتل‌های زنجیره‌ای ترامپ به‌تازگی هتلی در خاورمیانه و همچنین هتلی در خیابان «پنسیلوانیا» در همین شهر افتتاح کرده است. پرسیدم: «آیا این هتل‌ها از میهمانان کشورهای دیگر جاسوسی می‌کنند؟ به نظر نمی‌رسد چنین کاری به نفع کسب‌وکار خانوادگی ترامپ باشد.» سرش را به نشانه

تأیید تکان داد.

دست‌کم موفق شده بودیم بحث جدیدی را آغاز کنیم. وقتی ساتیا و من در ژوئن ۲۰۱۷ به نشستی در حوزه فناوری در کاخ سفید رفتیم، در جلسه‌ای جانبی در مورد مسائل امنیت سایبری شرکت کردم. یکی از مسئولان کاخ سفید پیش از جلسه به من پیام داد: «لطفا به موضوع کنوانسیون دیجیتال ژنو اشاره نکنید. می‌خواهیم بحث فقط بر شیوه‌های برتر امنیتی برای دولت ایالات متحده متمرکز باشد و مسائل دیگر مطرح نشوند.»

در حالی که به سمت اتاق همایش پرنقش‌ونگاری می‌رفتیم که جلسه در آن برگزار می‌شد، به او اطمینان خاطر دادم که پیامش را گرفته‌ام، اما همان‌طور که بحث دنبال می‌شد، مدیرعامل شرکتی دیگر که اصلاً با او صحبت هم نکرده بودم، ناگهان روی میز خم شد و گفت: «ببینید، آنچه ما واقعاً نیاز داریم نوعی کنوانسیون دیجیتال ژنو است.»

نگاهی به آن کارمند کاخ سفید کردم و شانه‌هایم را بالا انداختم.

وقتی با افراد بیشتری در مورد ایده کنوانسیون دیجیتال ژنو حرف زدیم، متوجه شدیم که بسیاری از نکات مطرح‌شده مناسب هر گونه کنترل تسلیحاتی هستند. بحث‌های عمومی درباره قوانین حاکم بر تسلیحات سابقه زیادی داشتند و باید از آنها درس می‌گرفتیم.

در طول دهه‌های آخر جنگ سرد، در حالی که ابرقدرت‌های آن زمان، ایالات متحده و اتحاد جماهیر شوروی، در مورد پیمان‌هایی برای مدیریت تسلیحات هسته‌ای مذاکره می‌کردند، تمرکز ژئوپلیتیک بر کنترل تسلیحات بود. حلقه‌های سیاسی آن زمان، مسائل مربوط به کنترل تسلیحات را به‌خوبی درک می‌کردند و بحث‌های فراگیرتری هم در مورد این مسائل شکل می‌گرفت. وقتی در اوایل دهه ۱۹۸۰ احتمال وقوع آخرالزمان هسته‌ای به دست انسان، مدام در پس ذهن افراد تکرار شد، جایگاه مهمی در فرهنگ عامه پیدا کرد.

وقتی رئیس‌جمهور ریگان چهارم ژوئن ۱۹۸۳ با هلی‌کوپتر و با حجم زیادی از اسناد محرمانه کنترل تسلیحات به کمپ دیوید در مناطق روستایی ایالت مریلند می‌رفت،

این مخاطرات هسته‌ای بار سنگینی بر دوش او بودند. وقتی آن شب، توفانی رشته‌کوه «آپالاش» (Appalachians) در آن حوالی را درمی‌نوردید، ریگان و همسرش، نانسی در کلبه‌ای مستقر شدند و به تماشای فیلمی نشستند. این فیلم یکی از ۳۶۳ فیلمی بود که این ستاره سابق سینما در دو دوره ریاست‌جمهوری‌اش تماشا کرد. یکی از نویسندگان این فیلم جدید با عنوان «بازی‌های جنگی» (WarGames) نمایشی ویژه را ترتیب داده بود. اکران رسمی فیلم یک روز پیش شروع شده بود.

بازی‌های جنگی، فیلمی در ژانر ترسناک است و هکر نوجوانی را نشان می‌دهد که قصد دارد نمراتش را در کامپیوتر دبیرستان تغییر دهد که اتفاقی به ابرکامپیوتر «فرماندهی دفاع هوافضای آمریکای شمالی» وارد می‌شود و چیزی نمانده جنگ جهانی سوم را شروع کند. این داستان، ریگان را می‌ترساند. دو روز بعد در جلسه‌ای سطح بالا در کاخ سفید می‌پرسد کسی این فیلم را دیده است. وقتی هیچ‌کس پاسخی نمی‌دهد، شروع به تعریف داستان فیلم می‌کند و بعد از رئیس ستاد مشترک می‌پرسد آیا چنین داستانی امکان‌پذیر است. این گفت‌وگو موجب آغاز زنجیره‌ای از تصمیمات می‌شود که به اولین تلاش‌های دولت در زمینه امنیت سایبری منجر می‌شود. هنر برخاسته از زندگی واقعی تا اندازه‌ای باعث تصویب قانون «کلاهبرداری و سوءاستفاده کامپیوتری» شد که آن نوع هک تصویرشده در فیلم را غیرقانونی می‌کرد.

بازی‌های جنگی به دلهره مردم آن زمانه نسبت به تسلیحات و فناوری هسته‌ای دامن می‌زد. در دورانی که کامپیوترهای شخصی دستگاه‌های نوظهوری بودند که بیشتر در اتاق‌های پشتی افراد علاقه‌مند مشاهده می‌شدند، این فیلم با استقبال گسترده‌ای روبه‌رو شد. فیلمی که بیش از ۳۵ سال پیش تولید شده، اکنون پیشگویانه به نظر می‌رسد. این فیلم به نگرانی‌های مردم در مورد آسیب‌پذیری‌های کامپیوتر، تهدید جنگ و خارج‌شدن دستگاه‌ها از کنترل انسان می‌پردازد. همچنین از برتری دیپلماسی بر جنگ می‌گوید؛ آنجا که ابرکامپیوتر فیلم با درس‌گرفتن از تبعات یک جنگ هسته‌ای، در اوج فیلم بیان می‌کند: «بازی عجیبی است. تنها حرکت برنده، بازی‌نکردن است.»

پس از پایان جنگ سرد، موضوع کنترل تسلیحات تا حد زیادی از نگاه مردم دور شد. از این رو نسلی از متخصصان کنترل تسلیحات از عرصه خارج شدند و دیگر

درک عمومی فراگیری نسبت به این مسائل وجود ندارد. در سال ۲۰۱۸ دوباره داشتیم به آینده احتمالی فکر می‌کردیم. «مایکل مک‌فال»، سفیر سابق ایالات متحده در روسیه می‌گوید: «دیگر جنگ سردی در کار نیست، این بار با صلح داغ سروکار داریم.» بنابراین وقتش رسیده که برخی درس‌های گذشته را مرور کنیم.

از برخی جهات واکنش‌ها به جنگ جهانی دوم و دهه‌ها مذاکره در مورد تسلیحات اتمی، ایده‌هایی را حول امنیت سایبری فراهم می‌کند. هرچه نباشد دنیا بعد از بمباران اتمی ژاپن در سال ۱۹۴۵ تقریباً به مدت ۷۵ سال از هر گونه مناقشه اتمی اجتناب کرده است. از مسیرهای چالش‌برانگیز و گاهی پرپیچ‌وخم دولت‌ها در فاصله پایان جنگ جهانی دوم تا پایان جنگ سرد، می‌توان درس‌هایی گرفت.

منشاء یکی از این درس‌ها «حقوق بین‌المللی بشردوستانه» و فعالیت‌ها و همکاری دولت‌های جهان در سال ۱۹۴۹ برای ایجاد کنوانسیون چهارم ژنو است. نتیجه این کنوانسیون بیش از ممنوعیت یا محدودیت تسلیحات ویژه، محدود کردن دولت‌ها در ورود به مناقشه نظامی بود. بر اساس قوانین این کنوانسیون، دولت‌ها نمی‌توانند غیرنظامیان را هدف بگیرند، اقدامی انجام دهند که به تلفات نامتناسب غیرنظامیان منجر شود یا از تسلیحاتی استفاده کنند که آسیبی غیرضروری ورای ارزش نظامی‌شان ایجاد می‌کند. جالب است که نیروی پیشران کنوانسیون ۱۹۴۹ دولتی خاص نبود؛ بلکه کمیته بین‌المللی صلیب سرخ بود که همچنان تا امروز نقشی حیاتی در اجرای این کنوانسیون ایفا می‌کند.

کنوانسیون ژنو از زاویه مهمی درسی به ما می‌دهد که شامل کنترل تسلیحات می‌شود؛ واقع‌بینانه‌تر آن است که به جای ممنوعیت کامل تسلیحاتی خاص، مقدار یا ویژگی‌های آن را محدود یا نحوه استفاده از آن را کنترل کنیم. همان‌طور که نویسنده‌ای می‌گوید «اگر افراد سلاحی را وحشتناک و کم‌کاربرد بدانند، ممنوعیت ممکن است موفق شود، اما اگر سلاحی مزیت‌های بسیار مهمی در میدان نبرد داشته باشد، هر چقدر هم که وحشتناک به نظر برسد، بعید است ممنوعیت جواب بدهد.»

کنترل تسلیحات یکی از دشوارترین فعالیت‌ها در سطح جهان است. اما همان‌طور که مطالعه‌ای در انتهای جنگ سرد نتیجه‌گیری کرده بود، توافق‌نامه‌های کنترل

تسلیحاتی (که از به‌کارگیری آنها جلوگیری می‌کنند، نه اینکه آنها را کاملاً نابود کنند) «می‌توانند در نهایت بهتر باشند؛ چراکه احتمال موفقیت‌شان بیشتر است». این مفهوم شاید به اندازه مسائل دیگر به تلاش‌های متخصصان حقوق بین‌الملل برای تعریف هنجارهایی جهانی جان بخشیده باشد؛ هنجارهایی که نحوه استفاده از سلاح‌های سایبری را محدود می‌کنند.

درس تکراری دیگری از تاریخ کنترل تسلیحات نیز در این زمینه کاربرد دارد؛ اینکه دولت‌ها اگر بتوانند، گاهی اوقات سعی می‌کنند از عمل به توافق‌نامه‌های بین‌المللی سر باز بزنند، بنابراین باید راه‌های مؤثری برای نظارت بر پیروی کشورها از توافق‌نامه‌ها و پاسخگو کردن متخلفان وجود داشته باشد. این مسئله بیانگر یکی از بزرگ‌ترین چالش‌های کنترل تسلیحات سایبری است. این سلاح‌ها نه‌تنها برای دولت‌ها کاربردی هستند؛ بلکه دولت‌ها می‌توانند به‌نحوی از آنها استفاده کنند که شناسایی مهاجم ممکن نباشد. همان‌طور که «دیوید سانگر» (David Sanger) از نیویورک‌تایمز می‌نویسد متأسفانه این ویژگی برخی سلاح‌ها را به «سلاح بی‌نقص» تبدیل می‌کند.

این وضعیت اهمیت افزایش توانایی انتساب حملات سایبری به کشورهایی که این نوع حملات را انجام داده‌اند و ایجاد قابلیت واکنش جمعی به چنین حملاتی را نشان می‌دهد. ایالات متحده و دولت‌های دیگر بیش از پیش برای ایجاد چنین قابلیت‌هایی تلاش می‌کنند. این قابلیت‌ها طیف متنوعی از حملات واکنشی تا ابزارهای دیپلماتیک متعارف‌تر مثل تحریم‌ها را دربر می‌گیرند. اما این واکنش‌ها صرف‌نظر از نوع‌شان زمانی بیشترین فایده را برای پایداری سایبری خواهند داشت که بر اتفاق نظر در مورد قوانین بین‌المللی نقض‌شده و اجماع چندجانبه در مورد عامل حمله متکی باشند. علاوه بر این در عصری که این سلاح‌های جدید به مراکز داده، کابل‌ها و دستگاه‌های تحت مالکیت و مدیریت شرکت‌ها حمله می‌کنند، اطلاعات بخش خصوصی احتمالاً نقش گسترده‌تری در تعیین عامل حمله ایفا خواهد کرد.

همه این مسائل اهمیت همیشگی دیپلماسی بین‌المللی را برجسته می‌کند. در حالی که نسل جدید چالش‌های دیپلماتیک، ذهن‌مان را مشغول کرده، ابزارهای جدیدی هم به جعبه ابزار دیپلماسی اضافه شده است. وقتی وزیر امور خارجه

دانمارک گفت شرکت‌های فناوری به نوعی «کشور» تبدیل شده‌اند، در واقع به یکی از فرصت‌های جدید ما اشاره کرد. می‌دانستیم این مقایسه حداکثری نیست و حد و اندازه خودش را دارد، اما فرصتی کلیدی را نشان می‌داد. اگر شرکت‌های ما نوعی کشور محسوب می‌شدند، پس می‌توانستیم توافق‌نامه‌های بین‌المللی خودمان را تنظیم کنیم.

وقتی خواستار «سوئیس دیجیتال بی‌طرف» شدیم، در واقع سعی کردیم بخش فناوری را به این سمت هدایت کنیم. این خواسته را باید با همراه‌کردن شرکت‌ها با یکدیگر برای امضای پیمانی عملی می‌کردیم که بر اساس آن به دفاع از همه مشتریان قانونی‌مان در همه جای دنیا متعهد می‌شدیم. هرچند احساس می‌کردیم ایده‌های امنیت سایبری ما از پشتیبانی گسترده‌ای برخوردار هستند، اما می‌دانستیم کار آسانی در پیش نداریم. بخش فناوری مملو از افراد پرتلاشی است که برای سازمان‌های بلندپرواز کار می‌کنند. همراه‌کردن شرکت‌ها برای انجام کاری به‌صورت هماهنگ، روی کاغذ آسان‌تر از عمل است.

تیم دیپلماسی دیجیتال مایکروسافت به رهبری «کیت اوسالیوان» مناسب‌ترین گزینه برای تنظیم توافق‌نامه‌ای بود که بعداً با نام «پیمان امنیت سایبری شرکت‌های فناوری» شناخته شد. کیت تیمی از «دیپلمات‌های» مایکروسافت را رهبری می‌کند که با سیاست‌گذاران و شرکایمان در صنعت، در سراسر جهان همکاری می‌کنند تا اعتماد و امنیت در اینترنت را بهبود ببخشند. با توجه به مالکیت خصوصی فضای سایبری، خیلی وقت بود که متوجه شده بودیم حفاظت از این فضا مستلزم مشارکت چندجانبه و در عین حال چندذی‌نفعی است. ما هم مانند سفیران فناوری جدید که نماینده دولت‌ها بودند، به نمایندگانی معتقد به ارزش‌های دیپلماتیک نیاز داشتیم تا بر صلح دیجیتال تمرکز کنند و در این میدان جنگ جدید، از منافع و مشتریان‌مان حفاظت کنند.

پیش‌نویسی از اصول پیمان شرکت‌های فناوری تهیه کردیم و به تیم دیپلماسی دیجیتال مأموریت دادیم تا گرایش صنعت را بررسی کند. این پیمان ابتدا همه امضاکنندگان را به دو انگاره غالب متعهد می‌کرد؛ این انگاره‌ها حفاظت از کاربران و

مشتریان در همه جای دنیا و مخالفت با حمله به شهروندان و سازمان‌های بی‌گناه در سراسر جهان بودند. این انگاره‌ها زیربنایی اصولی ایجاد می‌کردند که فکر می‌کردیم بخش فناوری به آن نیاز دارد تا امنیت سایبری را در مقیاس جهانی ترویج و از آن حفاظت کند. این توافق‌نامه این دو اصل را با دو تکلیف عملی تکمیل می‌کرد؛ تکلیف اول برداشتن گام‌های تازه برای تقویت اکوسیستم فناوری با همکاری کاربران، مشتریان و توسعه‌دهندگان نرم‌افزار به‌منظور بهبود حفاظت امنیتی با استفاده از راه‌های عملی بود. تکلیف دوم نیز همکاری نزدیک‌تر با یکدیگر به‌منظور تقویت امنیت سایبری بود که از جمله شامل اشتراک‌گذاری اطلاعات بیشتر و کمک به یکدیگر در واکنش به حملات سایبری می‌شد.

تفاوت زیادی بین جلب موافقت افراد در مورد منطقی‌بودن این اصول و متعهد کردن آنها به این اصول نزد افکار عمومی وجود داشت. به‌سرعت گروه کوچکی دور هم جمع شدند. این گروه شامل فیس‌بوک هم می‌شد که در نتیجه رسیدگی به نگرانی‌های فزاینده نسبت به حریم خصوصی در این شرکت در این حوزه فعال‌تر شده بود. چند شرکت فناوری اطلاعات بزرگ و باتجربه دیگر مثل سیسکو، اوراکل، سیمانتک و اچ‌پی نیز به‌سرعت از این آرمان پشتیبانی کردند.

متقاعد کردن گوگل، آمازون و اپل دشوارتر بود. وقتی با آنها صحبت می‌کردیم، برخی می‌گفتند فکر می‌کنند در دوره‌ای که دولت‌های سراسر جهان فیس‌بوک را هدف گرفته‌اند، قرار گرفتن در کنار این شرکت بیش از حد بحث‌برانگیز است. از آنجایی که در دهه ۱۹۹۰ تجربه‌ای مشابه فیس‌بوک داشتیم، احتمالاً بیش از دیگران با این شرکت همدلی می‌کردم. همچنین درک می‌کردم که همه در مقطعی روزهای سخت را تجربه می‌کنند و اگر اصل اول‌مان این باشد که در سختی از افراد فاصله بگیریم، ممکن است خودمان را محکوم به انفعال حتی در مورد مسائلی کنیم که بیش از همه مستلزم تلاش‌های جمعی هستند.

شمار دیگری از افراد در این شرکت‌ها می‌گفتند واکنش منفی برخی افراد در دولت ایالات متحده را شنیده‌اند. نمی‌خواستند از مقوله‌ای پشتیبانی کنند که مورد انتقاد دولت بود. برخی دیگر هم گفتند نمی‌توانند افراد شرکت‌شان را به تصمیم‌گیری

متقاعد کنند، پس نمی‌توانند مجوز امضای پیمان را دریافت کنند. با وجود ایمیل‌ها و تماس‌های تلفنی مکرر نتوانستیم این شرکت‌ها را به امضای پیمان راضی کنیم.

خوشبختانه بقیه صنعت هم به‌مرور به ما پیوستند. در داخل مایکروسافت تصمیم گرفتیم که اگر بتوانیم امضای علنی دست‌کم ۲۰ شرکت را بگیریم، از پیمان شرکت‌های فناوری رونمایی می‌کنیم. در حالی که به همایش RSA سان‌فرانسیسکو در سال ۲۰۱۸ نزدیک می‌شدیم، مشهود بود که این هدف محقق خواهد شد.

در هفته‌های آخر پیش از رونمایی پیمان «امنیت سایبری شرکت‌های فناوری» برنامه‌هایمان را با کاخ سفید و مسئولان کلیدی بخش‌های دیگر ایالات متحده و سایر دولت‌ها در میان گذاشتیم. نمی‌خواستیم غافلگیر شوند. از کاخ سفید بازخورد مثبتی دریافت کردیم، اما شایعاتی شنیدیم مبنی بر اینکه برخی افراد در جامعه اطلاعاتی نگرانی‌هایی در مورد واژگان انتخابی در تعهد به کمک‌نکردن به دولت‌ها در انجام حمله سایبری علیه «شهروندان عادی و سازمان‌های خصوصی» دارند. نگران بودند که تروریست‌ها هم شامل عبارت «شهروندان عادی» شوند و اگر مورد اضطراری این‌چنینی وجود داشت، نتوانند به بخش فناوری مراجعه کنند. بازخورد مفیدی بود. عبارت را به «شهروندان بی‌گناه» تغییر دادیم که به نظر می‌رسید این تغییر، مشکل را برطرف می‌کند.

وقتی در آوریل ۲۰۱۸ از پیمان امنیت سایبری شرکت‌های فناوری رونمایی کردیم، ۳۴ شرکت آن را امضا کرده بودند. این رقم بیشتر از میزانی بود که برای ایجاد جنبش نیاز داشتیم. تا ماه می ۲۰۱۹ بیش از ۱۰۰ شرکت از بیش از ۲۰ کشور به عضویت این گروه درآمدند و با پشتیبانی از گام‌های عملی در راستای تقویت تدابیر حفاظتی امنیت سایبری، در حال اجرای پیمان بودند.

یکی از اتفاقات مهم این بود که نیاز به همکاری مؤثرتر بخش خصوصی، پشتیبانی بیشتری را از سراسر دنیا جلب کرد. زیمنس در یکی از اولین تلاش‌ها پیشگام شد و مقوله‌ای به نام «منشور اعتماد» ایجاد کرد تا بر حفاظت از دستگاه‌های کوچک فراگیر تشکیل‌دهنده اینترنت اشیا تمرکز کند. چند شرکت اروپایی مطرح شامل ایرباس، دویچه تلکام، آلیانز و توتال به‌سرعت به این منشور پیوستند.

در آسیا واکنشی از برخی جهات جالب‌تر در انتظار ما بود. وقتی جولای ۲۰۱۸ در توکیو بودیم، با مدیران ارشد هیتاچی ملاقات کردیم که می‌خواستند اولین امضاکننده بزرگ این پیمان در ژاپن باشند. وقتی به ساختمان مرکزی این شرکت رفتیم تا امضایشان را قطعی کنیم، همان ابتدای جلسه گفتند: «واناکرای به ما حمله کرد. یکی از گزینه‌هایمان سکوت بود، اما به این نتیجه رسیدیم که اگر در کنار هم نایستیم و کاری مثل این پیمان انجام ندهیم، هرگز نمی‌توانیم این مسئله را حل کنیم.»

در واقع نکته اصلی همین بود. تعجب کردم که یک شرکت فناوری ژاپنی قدیمی، حاضر است در این زمینه به پا خیزد، در حالی که شرکت‌هایی مثل گوگل، اپل و آمازون هیچ اقدامی نمی‌کردند. در توکیو در مورد نیاز بخش فناوری به کنشگرایی و تشکیل انواع جدیدی از ائتلاف‌های چندجانبه بحث کردیم.

ترجیح می‌دادیم دولت نقش فعال‌تری در رهبری داشته باشد؛ زیرا رویکرد چندجانبه به امنیت را پایدار می‌کرد؛ رویکردی که از انتهای جنگ جهانی دوم نقش اساسی داشت، اما در آن زمان در کاخ سفید یا پایتخت‌های دیگری که علاقه‌ای به همکاری نداشتند، چنین تفکری حاکم نبود.

عجیب و حتی معذب‌کننده بود که به‌عنوان یک شرکت، چندجانبه‌گرایی را به پیش ببریم؛ کاری که معمولاً نقش دولت‌ها بود. اما هرچه جلوتر رفتیم، بیش از انتقاد، با حمایت مواجه شدیم. هرچه پیشرفت کردیم، تعداد بیشتری از شرکت‌ها برای پیوستن به ما تمایل نشان دادند.

اما دیپلماسی نمی‌توانست با محدود بودن به بخش فناوری و جامعه کسب‌وکار، مؤثر واقع شود. دولت‌ها، شرکت‌ها و گروه‌های غیرانتفاعی باید راهی برای همکاری عملی پیدا می‌کردند. به‌دنبال فرصت مناسب بودیم و به این نتیجه رسیدیم که بهترین فرصت همایشی بین‌المللی است که در نوامبر ۲۰۱۸ در پاریس برگزار می‌شد. امانوئل مکرون، رئیس‌جمهور فرانسه، تصمیم گرفته بود این همایش را که «مجمع صلح پاریس» نام‌گذاری کرده بود، در یکصدمین سالگرد آتش‌بسی برگزار کند که به جنگ جهانی اول پایان داده بود. ویدئویی در یوتیوب بارگذاری کرده بود که ما چند بار آن را تماشا کردیم. در این ویدئو از تضعیف حکومت‌های دموکراسی و فروپاشی

چندجانبه‌گرایی در دو دهه بعد از این آتش‌بس صحبت می‌شد که به جنگ جهانی دوم منجر شد. مکرون خواستار ایده‌هایی برای پروژه‌هایی شده بود که دموکراسی و چندجانبه‌گرایی را در قرن بیست‌ویکم تقویت می‌کرد. به نظر می‌رسید بهترین دعوت‌نامه برای کاری است که می‌خواستیم انجام دهیم.

مسئولان در پاریس علاقه نشان دادند. «دیوید مارتینون»، سفیر فرانسه در حوزه دیپلماسی سایبری و اقتصاد دیجیتال در منصبی مشابه کسپر کلینگ در دانمارک قرار داشت. مسئول حکمرانی اینترنت، امنیت سایبری، آزادی بیان و حقوق بشر بود. مارتینون و سایر مسئولان فرانسه با رهبری «فیلیپ اتین»، مشاور دیپلماتیک رئیس‌جمهور بر طراحی آینده متمرکز شده بودند. با آنها در مورد فرصت تدوین اعلامیه و طرحی جدید برای رسیدگی به مسئله امنیت سایبری گفت‌وگو کردیم.

با رهبری قدرتمند فرانسه و بعد از ماه‌ها گفت‌وگوی حساب‌شده، سرانجام روز بعد از یکصدمین سالگرد آتش‌بس جنگ جهانی اول، رئیس‌جمهور مکرون از «فراخوان پاریس برای اعتماد و امنیت در فضای سایبری» رونمایی کرد که بر اهمیت هنجارهای بین‌المللی موجود در حفاظت از شهروندان و زیرساخت‌های غیرنظامی در برابر حملات سایبری سیستمی یا کور تأکید می‌کرد. این سند همچنین از دولت‌ها، شرکت‌های فناوری و سازمان‌های غیردولتی می‌خواهد که با همکاری یکدیگر از فرایندهای دموکراتیک و انتخاباتی در برابر تهدیدات سایبری دولتی محافظت کنند. معتقد بودیم این حوزه نیازمند حمایت شفاف‌تر تحت حقوق بین‌الملل است.

مسئله مهم‌تر، گستردگی حمایت از فراخوان پاریس بود. دولت فرانسه بعدازظهر روز سخنرانی مکرون اعلام کرد که فراخوان ۳۷۰ امضاکننده دارد. این فهرست شامل ۵۱ دولت از سراسر دنیا، از جمله همه ۲۸ عضو اتحادیه اروپا و ۲۷ عضو از ۲۹ عضو ناتو می‌شد. همچنین شامل دولت‌های کلیدی سایر نقاط دنیا از جمله ژاپن، کره جنوبی، مکزیک، کلمبیا و نیوزیلند می‌شد. تا اوایل سال ۲۰۱۹ تعداد امضاکنندگان به بیش از ۵۰۰ رسید و شامل ۶۵ دولت و بیشتر بازیگران حوزه فناوری از جمله گوگل و فیس‌بوک می‌شد. البته آمازون و اپل به این جمع ملحق نشدند.

به طرز دور از انتظار و از نظر ما تأسف‌آوری، فراخوان پاریس همه این حمایت‌ها را

بدون پشتیبانی دولت ایالات متحده به دست آورد که اعلامیه را در پاریس امضا نکرد. هرچند ابتدا امیدوار بودیم که دولت آمریکا هم به جمع ما بپیوندد، اما یک ماه پیش از جلسات پاریس مشخص شد که واشنگتن برای موضع‌گیری موافق یا مخالف آماده نیست. برخی اعضای کاخ سفید صرف‌نظر از اینکه پای چه مسئله‌ای در میان بود، تمایلی به طرح‌های چندجانبه نداشتند. این بی‌میلی ما را در موقعیتی غیرعادی قرار داده بود؛ چراکه به تیم‌های امور دولتی‌مان در سراسر جهان گفته بودیم از کشورهای دیگر بخواهند که از این تلاش پشتیبانی کنند.

در هر صورت فراخوان پاریس نوآوری مهمی به‌شمار می‌رود. این فراخوان رویکرد چندجانبه بسیار حیاتی را به کار می‌گیرد و آن را به نوعی رویکرد چندذی‌نفعی مورد نیاز برای رسیدگی به مسائل فناوری جهانی در دنیای امروز تبدیل می‌کند. این فراخوان اکثر حکومت‌های دموکراسی جهان را متحد و بین آنها و اغلب حوزه فناوری و گروه‌های غیردولتی سراسر جهان ارتباط برقرار می‌کند. با گذشت زمان نیز طرف‌های بیشتری می‌توانند به آن بپیوندند.

مدل تعبیه‌شده در فراخوان پاریس خیلی زود توجه جهانی بیشتری را جلب کرد. در جلسه‌ای که بعد از فاجعه کرایست‌چرچ در ماه مارس ۲۰۱۹ با «جاسیندا آردرن»، نخست‌وزیر و کابینه‌اش در نیوزیلند داشتیم، در مورد این مسئله بحث کردیم که چطور می‌توانیم از تکرار استفاده تروریست‌ها از اینترنت به‌عنوان صحنه نمایش حمله به مردم این کشور جلوگیری کنیم. بحث‌مان به‌سرعت به فراخوان پاریس و این موضوع کشیده شد که آیا می‌توانیم دولت‌ها، بخش فناوری و جامعه مدنی را به شکل مشابهی دور هم جمع کنیم. آن شب به این موضوع فکر کردیم و صبح روز بعد در جلسه‌ای با مسئولان دولتی، همه حاضران در مورد موضوع «فراخوان کرایست‌چرچ» بالقوه صحبت می‌کردند.

دولت نیوزیلند با رهبری آردرن ابتکار عمل را در دست گرفت. همان‌طور که در اولین جلسه‌مان به آردرن گفته بودم، او نوعی اعتبار اخلاقی به این مسئله اضافه می‌کرد. در پاسخ به این حرف به‌سرعت پاسخ داد که خشم دنیا سرانجام فروکش می‌کند. می‌خواست از این موقعیت نه برای بهبود جایگاهش نزد افکار عمومی؛ بلکه برای

دستیابی به هدفی مهم‌تر و ماندگارتر استفاده کند. «پل اش» (Paul Ash)، مسئول امنیت سایبری نیوزیلند را به اروپا فرستاد تا مشارکت با یکی از دولت‌های این قاره و گسترش فراخوان پاریس را بررسی کند. تیم مکرون با اشتیاق از این ایده استقبال کردند.

صنعت فناوری نقش مهمی داشت. چالش ما شناسایی گام‌هایی عملی بود که باید برمی‌داشتیم تا اجازه ندهیم افراد از خدمات‌مان برای تقویت خشونت افراطی استفاده کنند. در مایکروسافت از «دو اشتالکاف» (Dev Stahlkopf)، رئیس اداره حقوقی و «فرانک مارو»، رئیس کارکنانش، خواستم رهبری تلاش برای ایده‌پردازی را بر عهده بگیرند. هرچند ما با مسئله آپلود ویدئوی گسترده مواجه نیستیم که فیس‌بوک، توییتر و خدمت یوتیوب گوگل تجربه کرده بودند، اما کمی بعد به این جمع‌بندی رسیدیم که ۹ خدمت متمایز داریم که احتمالاً در برابر این نوع سوءاستفاده آسیب‌پذیر هستند. این آسیب‌پذیری‌ها از لینکدین و ایکس‌باکس لایو تا اشتراک‌گذاری ویدئو از طریق «وان‌درایو»، نتایج جست‌وجوی بینگ و استفاده از پلتفرم ابری «آژور» را دربر می‌گرفت.

سایر شرکت‌های فناوری آماده بودند که پیش‌قدم شوند و گام‌های بلندی بردارند. گوگل، فیس‌بوک و توییتر همگی پذیرفته بودند که استفاده از خدمات اشتراک‌گذاری محتوای آنها، توسط تروریست کرایست‌چرچ، برداشتن گام‌های بیشتر در این زمینه را برای آنها ضروری کرده است. تحسین‌برانگیز بود که آمازون متوجه شده بود که هرچند خدماتش در مشکل نقشی نداشتند، اما این شرکت می‌تواند در ارائه راه‌حل مثمر ثمر باشد.

مشهود بود که باید در انواع خدمات فناوری، طیفی از گام‌ها برداشته و موازنه‌های متفاوتی برقرار شود. باید همزمان نسبت به الزامات مهندسی و نگرانی‌های گسترده‌تر در مورد حقوق بشر و آزادی بیان حساسیت نشان می‌دادیم. مجموعه‌ای از تماس‌های گروهی به‌سرعت به جلب پشتیبانی شرکت‌ها از ۹ پیشنهاد ملموس برای رسیدگی به محتوای خشونت افراطی و تروریستی در محیط آنلاین منجر شد. این ۹ گام از جمله شامل ۵ گامی می‌شد که این خدمات می‌توانستند به‌صورت مجزا برای سخت‌گیرانه‌تر کردن شرایط و مقررات سرویس‌دهی، مدیریت بهتر ویدئوهای زنده، پاسخگویی به گزارش‌های سوءاستفاده کاربران، بهبود سیستم‌های کنترل فناوری و انتشار گزارش‌های

شفاف‌سازی بردارند. این گروه همچنین چهار گام برای اجرا در سطح صنعت تدوین کرد که شامل اجرای پروژه‌های تنظیم پروتکل واکنش به بحران، توسعه فناوری مبتنی بر رویکرد منبع‌باز، آموزش بهتر کاربران و پشتیبانی از پژوهش و تلاش‌های گسترده‌تر سازمان‌های غیردولتی برای ترویج تکثرگرایی و احترام در محیط آنلاین می‌شد.

آردرن اصرار داشت تا پیش از جلسه‌ای که یک ماه دیگر در پاریس برگزار می‌شد، تصمیمی اخذ شده و در آنجا اعلام شود. نمایندگان دولت‌های نیوزیلند و فرانسه در شمال کالیفرنیا با گروه‌های جامعه مدنی و شرکت‌های فناوری جلسه‌ای برگزار کردند تا در مورد مسائل ویژه مطرح‌شده به‌واسطه پیش‌نویس پیشنهادی فراخوان کرایست‌چرچ گفت‌وگو کنند. تیم دولت نیوزیلند تقریباً به‌صورت شبانه‌روزی مشغول کار بود و همزمان بازخوردهای رهبران دولتی و سایر ذی‌نفعان را مدیریت می‌کرد. در تماس دیروقتی که ساتیا و من با آردرن داشتیم، اشاره کردم که چقدر از سرعت دولتش شگفت‌زده شده‌ام. پاسخ داد: «وقتی کوچک هستید، باید چابک باشید!»

۱۵ ماه می، دو ماه بعد از حملات وحشتناک نیوزیلند، آردرن در پاریس به مکرون و هشت رهبر دولتی دیگر پیوست تا از «فراخوان کرایست‌چرچ برای اقدام» (Christchurch Call to Action) رونمایی کنند. در متن این سند به رسیدگی به محتوای تروریستی و خشونت افراطی در محیط آنلاین از طریق تعهد دولت‌ها و شرکت‌های فناوری به انجام اقدامات انفرادی و جمعی اشاره شده است. وقتی به جمع سایر رهبران فناوری و رؤسای دولت‌ها در پاریس پیوستم تا از طرف مایکروسافت فراخوان را امضا کنم، گروه پنج‌شرکتی ما در ضمن از ۹ گامی رونمایی کرد که قرار بود برای عملی‌کردن فراخوان کرایست‌چرچ، برداریم.

فراخوان‌های پاریس و کرایست‌چرچ که در فاصله تقریباً شش ماه از هم رونمایی شدند، نشان‌دهنده پیشرفتی هستند که جهان می‌تواند با توسل به اقدامی انجام دهد که کسپر کلینگ «تک‌پلوماسی» (از ترکیب کلمات تکنولوژی و دیپلماسی) می‌خواند. رویکرد جدید دیپلماسی چندذی‌نفعی به جای اتکای صرف به دولت‌ها؛ جامعه مدنی، شرکت‌های فناوری و دولت‌ها را دور هم جمع می‌کند.

این ایده از برخی جنبه‌ها کاملاً جدید نیست. همان‌طور که مطالعه‌ای به‌تازگی نتیجه

گرفته بود، طیفی از سازمان‌های غیردولتی شامل گروه‌های حامی، اندیشکده‌ها، جنبش‌های اجتماعی و گروه‌های آموزشی از دیرباز نقش مؤثری در مسائل کنترل تسلیحات ایفا کرده‌اند. یکی از موفق‌ترین طرح‌های اخیر که در دهه ۱۸۶۰ بنیان‌گذاران صلیب سرخ در ژنو کارزاری مشابه آن را رهبری کرده بودند، «کارزار بین‌المللی علیه مین‌های زمینی» (International Campaign to Ban Landmines) در دهه ۱۹۹۰ بود. این کارزار در سال ۱۹۹۲ با شش سازمان غیردولتی شروع شد و به‌تدریج رشد کرد و شامل تقریباً ۱۰۰۰ سازمان غیردولتی از ۶۰ کشور شد. این گروه «با موفقیت مین‌های زمینی را به جای مسئله‌ای صرفاً نظامی به مسئله‌ای انسان‌دوستانه و اخلاقی تبدیل کرد» و با پشتیبانی دولت کانادا کارزارش را به مجمعی ویژه برد که «معاهده ممنوعیت مین زمینی» را در دسامبر ۱۹۹۷ یعنی فقط پنج سال بعد از شروع کارزار تصویب کرد.

اگر با این دیدگاه بنگریم، شاید بدیع‌ترین جنبه فراخوان‌های پاریس و کرایست‌چرچ مشارکت شرکت‌ها، به‌عنوان نوع متفاوتی از سایر انواع نقش‌آفرینان غیردولتی، در نسل جدیدی از مسائل انسان‌دوستانه و محدودسازی تسلیحات باشد. بدون شک بدبینی برخی افراد به شرکت‌ها بیشتر از سازمان‌های غیردولتی خواهد بود، اما با توجه به سهم و نقش این شرکت‌ها در مالکیت و مدیریت فضای سایبری، به نظر می‌رسد نمی‌توان گفت که این شرکت‌ها هیچ نقشی ندارند.

فراخوان‌های پاریس و کرایست‌چرچ همچنین نوآوری دیگری را منعکس می‌کردند که احساس می‌کردیم در پیشگام‌بودن در عصر دیپلماسی دیجیتال مهم است. کنترل تسلیحات و حفاظت از حقوق انسانی همیشه نیازمند پشتیبانی گسترده افکار عمومی بوده است. در قرن بیستم گاهی اوقات ایده‌های جدید با موفقیت، از اندیشکده‌ها به گفت‌وگوهای مفصل با سازمان‌های غیردولتی و حلقه‌های سیاست‌گذاری دولتی راه می‌یافتند و در نهایت از طریق سخنرانی‌های مهم دولت‌مردان بین‌المللی در افکار عمومی نفوذ می‌کردند. اما در دوران چنددستگی رسانه‌های قدیمی و ظهور رسانه‌های اجتماعی، ارتباط با افکار عمومی با استفاده از روش‌های جدید همزمان به نیاز و فرصت تبدیل شده است.

این دیدگاه یکی از نتایجی است که از بحث‌های عمومی در مورد کنوانسیون

دیجیتال ژنو گرفتیم. هرچند برخی دیپلمات‌های سنتی ممکن است به نشانه مخالفت چشم‌غره بروند، اما این ایده توجه افکار عمومی را به‌شدت جلب کرد؛ اتفاقی که برای بحث تخصصی در مورد «راهنمای تالین ۲٫۰» نیفتاد. این راهنما حاصل مطالعه امنیت سایبری بین‌المللی بسیار مهم اما با عنوانی نه‌چندان جذاب بود. شبیه همان اتفاقی بود که در رویکرد نوآورانه و توییت‌های مکرر کسپر کلینگ مشاهده می‌کردم. همین رویکرد به افکار عمومی بود که باعث شد ما تلاش‌هایمان در زمینه فراخوان پاریس را با پشتیبانی دیپلماسی شهروندی همراه کنیم. یکی از کارهایمان در این زمینه فراخوان آنلاینی بود که برای پشتیبانی از کمپین «هم‌اکنون صلح دیجیتال»، بیش از ۱۰۰ هزار امضا از سراسر دنیا جمع کرده بود.

شاید دیپلماسی دیجیتال را به اندازه هر مسئله دیگری باید با اراده راسخی به پیش ببریم که مبنای آن نه‌فقط شرایط جدید و درس‌های امیدوارکننده گذشته؛ بلکه شکست‌های هشداردهنده تاریخ هم هست. وقتی در نوامبر ۲۰۱۷ برای سخنرانی به مقر اروپایی سازمان ملل در ژنو رفتیم، این درس به ما یادآوری شد. کاخ ملل (Palais des Nations) که اکنون میزبان سازمان ملل است، در دهه ۱۹۳۰ مقر جامعه ملل (League of Nations) بود. این ساختمان هنوز چند اتاق همایش کوچک با سبک معماری «آرت‌دکو» دارد که دوران پس از جنگ جهانی اول را به یاد می‌آورند.

این ساختمان به‌نوعی صحنه نمایش جهانی برخی از غم‌انگیزترین دوره‌های قرن بیستم بود. سال ۱۹۳۱ ژاپن به منطقه منچوری یورش برد و کمی بعد از آن رژیم نازی هیتلر به تهدیدی فزاینده در اروپا تبدیل شد. دولت‌هایی از ۳۱ کشور در این ساختمان دور هم جمع شدند تا در مجموعه‌جلساتی که بیش از پنج سال طول کشید، انباشت تسلیحات را محدود کنند. اما ایالات متحده از ایفای نقش رهبری مورد نیاز امتناع ورزید؛ چراکه فکر می‌کرد آن مسائل بیشتر مشکلات مربوط به اروپا هستند و هیتلر، آلمان را از مذاکرات و بعد جامعه ملل خارج کرد و ناقوس مرگ تلاش‌ها برای صلح جهانی را به صدا درآورد.

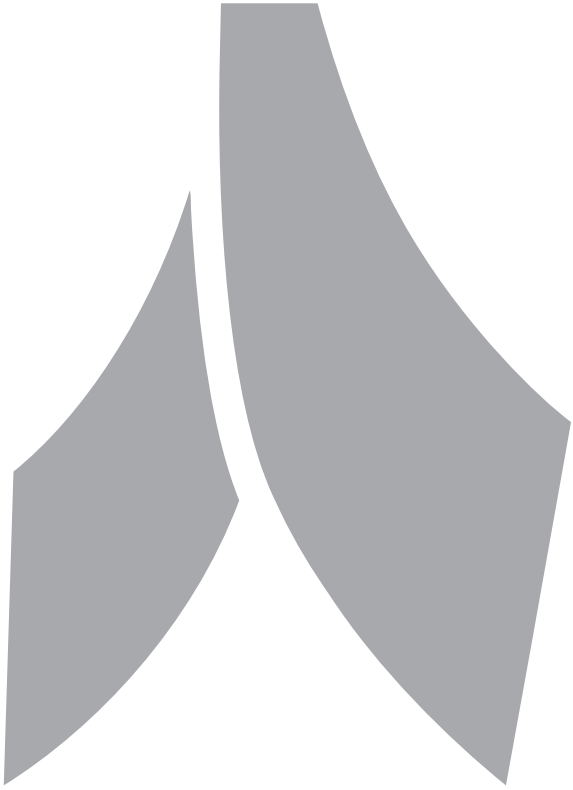
پیش از برگزاری کنفرانس ژنو در سال ۱۹۳۲ آلبرت اینشتین، بزرگ‌ترین دانشمند عصر خودش، هشداری داد که گوش شنوایی پیدا نکرد. اینشتین با دوراندیشی گفته بود پیشرفت‌های فناوری «می‌توانستند زندگی انسان را بی‌دغدغه و شاد کنند؛ البته به

شرطی که روند توسعه سازمان‌دهی قدرت، همگام با پیشرفت‌های فنی حرکت می‌کرد» اما «دستاوردهای عصر ماشین که با تلاش فراوان به دست آمده، در دستان نسل ما به اندازه تیغی در دستان کودکی سه‌ساله خطرناک است». کنفرانس ژنو با شکست به پایان رسید و پیش از پایان دهه، آن شکست به ویرانی جهانی غیرقابل تصوری تبدیل شد.

سخنان اینشتین اصل مطلب را در مورد چالش امروز بیان می‌کند. با تداوم پیشرفت فناوری آیا جهان می‌تواند آینده‌ای را که می‌سازد، کنترل نیز کند؟ جنگ‌ها در موارد زیادی نتیجه شکست انسان در همگام‌ماندن با نوآوری بوده، اینکه برای مدیریت فناوری جدید کارهای خیلی کمی را؛ آن هم خیلی دیر انجام دادیم. با قدرتمندتر شدن فناوری‌های نوظهور مثل تسلیحات سایبری و هوش مصنوعی، نسل ما هم دوباره در معرض این امتحان قرار خواهد گرفت.

اگر می‌خواهیم در امتحانی موفق شویم که افراد تقریباً یک قرن پیش ناکام ماندند، به رویکردی عملی به بازدارندگی به همراه انواع جدید دیپلماسی دیجیتال نیاز داریم. در آوریل ۲۰۱۹ در جلسه‌ای در سان‌فرانسیسکو به همراه کسپر کلینگ و همکارانش از بیش از ۲۰ دولت جهان شرکت کردیم. وقتی در آن جلسه همکاری نزدیک‌تر نسل جدیدی از دیپلمات‌های سایبری را مشاهده کردم، قوت قلب گرفتم.

نمی‌توان انکار کرد که دانمارک کشور کوچکی با جمعیت ۵٫۷ میلیون نفر است؛ یعنی جمعیتی کمتر از ایالت واشنگتن دارد. جمعیت نیوزیلند از این هم کمتر است. اما وزیر امور خارجه دانمارک درست می‌گفت. در قرن بیست‌ویکم بهترین راه برای رسیدگی به مسائل جهانی تشکیل تیمی است که می‌تواند علاوه بر سایر دولت‌ها با همه ذی‌نفعانی همکاری کند که آینده فناوری را تعیین می‌کنند. دست‌کم گرفتن کشوری کوچک با ایده‌ای خوب و رهبری ثابت‌قدم اشتباه است؛ دوران نوع جدیدی از دیپلماسی دیجیتال آغاز شده است.



فصل هشتم

حریم خصوصی مصرف‌کننده

«ورق برمی‌گردد»

در دسامبر ۲۰۱۳ که رهبران فناوری به جلسه‌ای در کاخ سفید آمده بودند تا رئیس‌جمهور اوباما را به اصلاح شیوه‌های نظارت الکترونیکی دولت ترغیب کنند، در مقطعی مسیر بحث عوض شد. رئیس‌جمهور مکثی کرد و گفت: «حدس می‌زنم در آینده ورق برمی‌گردد». این پیش‌بینی را با اشاره به این مسئله بیان کرد که بسیاری از شرکت‌های حاضر در آن جلسه بیشتر از هر دولتی در جهان، داده شخصی نگهداری می‌کردند. اوباما گفت زمانی می‌رسد که خواسته‌هایی که اکنون از دولت دارید، دیگران از بخش فناوری خواهند داشت.

از بسیاری ابعاد، عجیب به نظر می‌رسید که هنوز بخش فناوری هدف این خواسته‌ها قرار نگرفته بود. در اروپا این اتفاق خیلی وقت پیش افتاده بود. اتحادیه اروپا در سال ۱۹۹۵ دستورالعمل قدرتمندی در مورد حریم خصوصی داده تصویب کرد. این دستورالعمل زیربنای محکمی برای حفاظت از حریم خصوصی ایجاد کرد که از هر گونه قانونی در ایالات متحده پیشروتر بود. کمیسیون اروپا با بهره‌گیری از این دستورالعمل، در سال ۲۰۱۲ مقررات قدرتمندتری در زمینه حریم خصوصی پیشنهاد داد. بحث و بررسی چهار سال طول کشید، اما سرانجام اتحادیه اروپا در آوریل ۲۰۱۶ «مقررات عمومی حفاظت از داده» را تصویب کرد که مقرراتی فراگیر است. وقتی بریتانیا تنها دو ماه بعد و در پی رأی‌گیری برگزیت به خروج از اتحادیه اروپا رأی داد، مراجع حفاظت از داده این کشور به‌سرعت پشتیبانی‌شان را از تداوم اجرای این قوانین جدید در بریتانیا اعلام کردند؛ آنچنان که «ترزا می»، نخست‌وزیر، در جلسه‌ای در اوایل سال ۲۰۱۷ به مدیران ارشد فناوری گفت دولت متوجه بود که اقتصاد بریتانیا همچنان به جریان‌های داده در این قاره وابسته می‌ماند؛ بنابراین باید از مجموعه قوانین حریم خصوصی داده‌ای پیروی کند که با قوانین اتحادیه اروپا یکپارچه باشد.

شرایط در ایالات متحده چطور بود؟ در حالی که قوانین حریم خصوصی داده به سراسر دنیا گسترش یافته بودند، ایالات متحده خلاف مسیر دیگران پیش می‌رفت. مسئولان کشورهای مختلف اروپایی بیش از پیش در مورد حفاظت از حریم خصوصی شهروندان‌شان در دنیایی ابراز نگرانی می‌کردند که در آن داده‌ها از مرزها عبور می‌کنند و به مراکز داده ایالات متحده می‌روند، اما ایالات متحده در حفاظت گسترده‌تر از

حریم خصوصی در سطح ملی ناکام بود. به‌شخصه وقتی در سال ۲۰۰۵ در ساختمان کنگره سخنرانی کردم، خواستار تصویب قوانین ملی در زمینه حریم خصوصی شدم. اما به‌جز اچ‌پی و چند شرکت دیگر اکثریت فعالان صنعت فناوری با این ایده یا سرد برخورد کردند یا مخالفت کردند. کنگره نیز همچنان علاقه‌ای به این موضوع نشان نداد.

جرقه تغییر در ایالات متحده را تلاش‌های دو نفر زد که در ظاهر ربطی به این موضوع نداشتند. نفر اول که به نبرد در راه حریم خصوصی وارد شد، فردی به نام «مکس شرمس» (Max Schrems)، دانشجوی حقوق دانشگاه وین بود. در توقفی در اروپا در سال ۲۰۱۹ مکس، هم ما را با خوشمزگی گوشت گاو آب‌پز اتریشی آشنا کرد و هم داستان دور از انتظارش را برای ما تعریف کرد.

شرمس در اتریش تا حدی آدم معروفی است و اگر ماجرای حریم خصوصی اروپایی ـ آمریکایی را دنبال کرده باشید، بلافاصله او را می‌شناسید. یادم می‌آید با خنده می‌گفت: «به خاطر پرونده‌ای در مورد حریم خصوصی، حریم خصوصی خودم را از دست دادم.»

موضوع حریم خصوصی و از جمله خوانش آمریکایی از آن همیشه برای او کنجکاوی‌برانگیز بوده است. وقتی شرمس ۱۷ساله بود، به‌عنوان دانش‌آموز انتقالی دبیرستان به شهر «سبرینگ» (Sebring) یا به قول خودش «ناکجاآبادی» در فلوریدا آمده بود. شهر کوچک سبرینگ بدون شک شوکی فرهنگی به او وارد کرد، اما نه به دلایلی که احتمالاً انتظار دارید. شرمس را گردهمایی‌های مربوط به «کشاورزان آینده آمریکا» (Future Farmers of America) یا کلیسای باپتیست جنوبی حیرت‌زده نکردند؛ بلکه این روش‌های مدرسه برای دنبال‌کردن وضعیت دانش‌آموزان بود که او را به تعجب وامی‌داشتند.

شرمس می‌گوید: «مجموعه گسترده‌ای از روش‌های کنترلی وجود داشت. در مدرسه ایستگاه پلیس داشتیم و در همه راهروها دوربین نصب شده بود. همه کارهایمان رصد می‌شدند؛ از نمرات دروس، نمرات آزمون استاندارد ورود به دانشگاه و حضور و غیاب گرفته تا برچسب‌های کوچک روی کارت‌های دانش‌آموزی‌مان که به ما امکان استفاده

از اینترنت را می‌دادند.»

شرمس با افتخار به یاد می‌آورد که چطور به هم‌کلاسی‌های آمریکایی‌اش کمک کرده بود موانعی را دور بزنند که مدرسه برای جست‌وجوهای گوگل گذاشته بود. می‌گوید: «به آنها نشان دادم که Google.it وجود دارد که بدون مشکل کار می‌کند؛ چراکه مدرسه فقط نسخه دات‌کام وب‌سایت را مسدود کرده بود.» دانش‌آموز انتقالی، مدرسه را با دامنه‌های بین‌المللی برتر آشنا کرده بود!

شرمس به ما گفت بازگشت به وین مایه آسودگی خاطرش بوده؛ چراکه «اینجا آزادی بسیار زیادی دارد».

وقتی شرمس در سال ۲۰۱۱ و در ۲۴سالگی برای یک ترم تحصیلی در دانشکده حقوق دانشگاه «سانتا کلارا» به ایالات متحده برگشت، مسئله حریم خصوصی همچنان دغدغه ذهنی‌اش بود. روزی استاد میهمانی که یکی از وکلای فیس‌بوک هم بود، در کلاس حریم خصوصی شرمس سخنرانی می‌کند. وقتی شرمس از او در مورد تعهدات این شرکت بر اساس قوانین حریم خصوصی اروپا سؤال می‌کند، این وکیل پاسخ می‌دهد این قوانین اجرا نشده‌اند. شرمس می‌گوید: «به ما گفت هر کاری می‌توانید انجام دهید؛ زیرا جریمه‌ها آن‌قدر جزئی هستند که در عمل قانون اجرا نمی‌شود. مشخص بود که نمی‌داند فردی اروپایی در کلاس حضور دارد.»

این سخنان به شرمس انگیزه داد تا بررسی عمیق‌تری انجام دهد و مقاله ترمش را در مورد موضوعی بنویسد که خودش آن را «نقص‌های فیس‌بوک در ایفای تعهدات قانونی»اش در اروپا می‌دانست.

بیشتر دانشجویان بعد از این دیگر ماجرا را رها می‌کنند، اما شرمس مانند دیگران نبود. در عرض یک سال از آموخته‌هایش استفاده کرد و شکایتی را در نهاد مرجع حفاظت از داده ایرلند ثبت کرد. ایرلند کشوری بود که مرکز داده اروپایی فیس‌بوک در آنجا قرار داشت. شکایتش ساده و صریح بود، اما پیامدهای بالقوه دگرگون‌کننده‌ای برای اقتصاد جهان داشت. استدلال کرده بود که «اصول حریم خصوصی پناهگاه امن بین‌المللی» (International Safe Harbor Privacy Principles) که وضع شده بودند تا امکان انتقال داده‌های اروپایی به ایالات متحده را فراهم کنند، باید فسخ شوند. دلیل

او برای این تقاضا این بود که ایالات متحده برای حفاظت مناسب از داده‌های اروپایی مجراهای قانونی کافی ندارد.

اصول پناهگاه امن یکی از ارکان اساسی رابطه اقتصادی اروپا و آمریکا بود، اما به‌جز در میان متخصصان حریم خصوصی، در بین سایرین کمتر شناخته شده بود. این اصول یکی از نتایج دستورالعمل حریم خصوصی سال ۱۹۹۵ اتحادیه اروپا بود که اجازه می‌داد اطلاعات شخصی شهروندان اروپا به کشورهای دیگر منتقل شوند؛ البته به شرط آنکه قوانین و تمهیدات حفاظت از حریم خصوصی کافی در آن کشورها وجود داشته باشد. با توجه به نبود قانون حریم خصوصی ملی در ایالات متحده، مقداری خلاقیت سیاسی باید خرج می‌شد تا همچنان امکان انتقال داده‌ها از اروپا به آمریکا وجود داشته باشد. در سال ۲۰۰۰ برنامه‌ای داوطلبانه به‌عنوان راه‌حل تصویب شد. این برنامه به شرکت‌ها اجازه می‌داد خودشان گواهی دهند که از هفت اصل حریم خصوصی پیروی می‌کنند که وزارت بازرگانی ایالات متحده آنها را تأیید کرده بود. این اصول با قوانین اتحادیه اروپا مطابقت داشتند و به کمیسیون اروپا این امکان را دادند که نتیجه‌گیری کند ایالات متحده طبق الزامات دستورالعمل ۱۹۹۵ تمهیدات کافی برای حفاظت از حریم خصوصی را اندیشیده است. به این صورت اصول حریم خصوصی پناهگاه امن بین‌المللی به وجود آمدند.

طی ۱۵ سال، انتقال داده بین اروپا و آمریکا به‌شدت افزایش یافت. بیش از چهار هزار شرکت از اصول پناهگاه امن برای ارائه خدمات دیجیتالی با ارزش سالانه ۲۴۰ میلیارد دلار بهره می‌بردند. این خدمات شامل همه حوزه‌ها؛ از بیمه و خدمات مالی تا کتاب، موسیقی و فیلم می‌شد. اما ابعاد مالی بخش کوچکی از کل اطلاعات را دربر می‌گرفتند. شرکت‌های آمریکایی ۳٫۸ میلیون کارمند در اروپا داشتند که برای همه کارها؛ از دریافت حقوق تا بیمه سلامت و ارزشیابی عملکرد به انتقال داده‌ها طبق اصول پناهگاه امن وابسته بودند. مجموع فروش اروپایی شرکت‌های آمریکایی به رقم قابل توجه ۲٫۹ تریلیون دلار رسیده بود که بیشتر این فروش مستلزم انتقال داده‌های دیجیتال بود تا از رسیدن کالاها به مقصد و محاسبه دقیق درآمدها اطمینان حاصل شود. این مسئله شاخصی برای وابستگی فوق‌العاده زیاد جهان به داده بود.

در حالی که مسئولان دولتی و رهبران کسب‌وکار پناهگاه امن را یکی از ضرورت‌های دنیای مدرن می‌دانستند، مکس شرمس آن را کاملاً متفاوت می‌دید. وقتی شرمس به اصول پناهگاه امن نگاه می‌کرد، مانند بچه‌های داستان معروف «هانس کریستین اندرسن» با اطمینان می‌گفت: «پادشاه لخت است».

شرمس از سال ۲۰۰۸ کاربر فیس‌بوک بود و از این مستمسک در شکایتش نزد اداره حفاظت از داده ایرلند استفاده کرد. او سال ۲۰۱۲ به وین برگشته بود. شرمس بعد از «تبادل ۲۲ ایمیل» با فیس‌بوک یک سی‌دی دریافت کرده بود که حاوی یک فایل پی‌دی‌اف ۱۲۰۰صفحه‌ای از داده‌های شخصی‌اش بود. خودش می‌گوید: «فقط نصف یا یک‌سوم اطلاعاتی بود که از من داشتند، اما ۳۰۰ صفحه از این فایل اطلاعاتی بود که من حذف کرده بودم. در واقع همه این مطالب برچسب حذف‌شده خورده بودند.»

از نظر او توافق پناهگاه امنی که به فیس‌بوک اجازه می‌داد تا این اندازه داده را به این شکل جمع‌آوری و از آنها استفاده کند، امکان نداشت حفاظتی را فراهم کند که قوانین اروپا الزامی کرده بودند.

شرمس شکایتش را منتشر کرد و استدلالش مبنی بر «لزوم فسخ اصول پناهگاه امن» توجه محدود رسانه‌ها را به‌دنبال داشت. فیس‌بوک به‌سرعت دو مدیر ارشد اروپایی‌اش را به وین فرستاد تا او را متقاعد کنند که در دیدگاه‌هایش تجدیدنظر کند. شش ساعت را در اتاق همایش هتلی در کنار فرودگاه گذرانده بودند تا از شرمس بخواهند از شکایت‌هایش صرف‌نظر کند، اما او حاضر نبود شکایت‌هایش را پس بگیرد و پافشاری می‌کرد که می‌خواهد اداره حفاظت از داده ایرلند به نگرانی‌هایش رسیدگی کند.

افراد حاضر در بخش فناوری و جامعه حریم خصوصی این مسئله را با علاقه پیگیری می‌کردند، اما بیشتر افراد انتظار نداشتند پرونده شرمس به جایی برسد. در هر صورت شرمس بیش از آنکه برای تکمیل مقاله ترمش در سانتا کلارا وقت بگذارد، به نوشتن شکایت‌هایش پرداخته بود. دوره‌اش در این دانشگاه را هنوز تمام نکرده بود، اما از استادش وقت اضافه گرفته بود. کمی بعد به نظر می‌رسید این ماجرا به انتهای مسیر رسیده است. اداره حفاظت از داده ایرلند علیه شرمس حکم داد؛ زیرا به این

جمع‌بندی رسیده بود که کمیسیون اروپا در سال ۲۰۰۰ قید کرده است که پناهگاه امن کافی است. به نظر می‌رسید حالا دیگر شرمس باید این مسئله را رها کند و دوباره به سراغ مقاله دانشکده حقوقش برود، اما او قصد کوتاه‌آمدن نداشت.

سرانجام پرونده‌اش به دیوان دادگستری اروپا رسید و در ۶ اکتبر ۲۰۱۵ غوغایی به پا شد.

وقتی اول صبح آن روز تلفن زنگ زد، در فلوریدا بودم و برای رویدادی با حضور مشتریانی از آمریکای لاتین آماده می‌شدم. دیوان دادگستری اصول حریم خصوصی پناهگاه امن بین‌المللی را فسخ کرده بود. دادگاه نتیجه‌گیری کرده بود که مراجع حفاظت از داده ملی کشورهای اروپایی می‌توانند از انتقال داده بر اساس این توافق، ارزیابی خودشان را داشته باشند. دادگاه در عمل به رگولاتورهای مستقل کشورها اختیار بیشتری داده بود؛ رگولاتورهایی که در ارزیابی شیوه‌های حفاظت از حریم خصوصی در ایالات متحده سخت‌گیرانه‌تر عمل می‌کنند.

بلافاصله این سؤال برای افراد پیش آمد که آیا این تصمیم به معنی بازگشت به‌نوعی قرون وسطای دیجیتال است. آیا جریان داده بین اروپا و آمریکا متوقف خواهد شد؟ از آنجایی که دقیقاً برای چنین پیشامدی آماده شده بودیم، تدابیر قانونی دیگری اندیشیده بودیم تا مطمئن شویم که مشتریان می‌توانند به استفاده از خدمات‌مان برای انتقال بین‌المللی داده‌هایشان ادامه دهند. البته تلاش زیادی کردیم تا به مشتریان اطمینان خاطر بدهیم. در بخش فناوری همه سعی می‌کردند خودشان را آرام و مسئله را کم‌اهمیت نشان دهند، اما تصمیم دیوان دادگستری اروپا نگران‌کننده بود. یکی از وکلایی که در مذاکره در مورد پناهگاه امن کمک کرده بود، گفته بود: «اکنون هیچ سازوکاری در امان نیست. حکم دادگاه آن‌قدر گسترده است که می‌توان گفت هر سازوکاری که برای انتقال داده از اروپا استفاده می‌شود، در معرض خطر قرار دارد.»

این تصمیم به ماه‌ها مذاکره پرتب‌وتاب منجر شد. کمی شبیه این بود که ظرفی شکسته را دوباره کنار هم قرار دهیم. «پنی پریتزکر» (Penny Pritzker)، وزیر بازرگانی ایالات متحده و «ورا جوروا» (Věra Jourová)، از اعضای کمیسیون اروپا، در حال تدوین رویکردی بودند که احتمال بیشتری داشت که رضایت دادگاه و رگولاتورهای

گوناگون حریم خصوصی اروپا را جلب کند. وقتی در ژانویه ۲۰۱۶ به کمیسیون اروپا وارد شدم تا در مورد وضعیت موجود با جورووا گفت‌وگو کنم، در حالی که در ورودی طبقه پایین منتظر اجازه ورود بودم، به استقبالم آمد. از این کارش غافلگیر شدم. لبخندی زد و گفت برای استراحت چندلحظه‌ای از اتاقش خارج شده است. مردی که تاکنون ندیده بود، او را خارج از ساختمان شناخت و نزدیک شد و گفت: «ما باید با هم آشنا شویم. اسم من مکس شرمس است.»

در حالی که مذاکرات بین‌المللی ادامه داشت، بخش فناوری، خود را برای بدترین شرایط آماده می‌کرد. در مایکروسافت بررسی کردیم که ببینیم آیا می‌توانیم از نزدیکی سیاتل به کانادا استفاده کنیم و پشتیبانی کلیدی را به ساختمان‌هایمان در ونکوور انتقال دهیم یا خیر. با این کار برخی کارمندان ساختمان ردموند باید مدام در رفت‌وآمد می‌بودند، اما چون تصمیم دادگاه روی انتقال داده‌ها بین کانادا و اروپا تأثیری نمی‌گذاشت، می‌توانستیم فعالیت‌هایمان را بی‌دردسر انجام دهیم.

در نهایت انجام این کار لازم نشد. اوایل فوریه ۲۰۱۶ پریتزکر و جورووا از توافقی جدید رونمایی کردند. آنها اصول پناهگاه امن را با «سپر حریم خصوصی» جایگزین کردند که شامل الزامات شدیدتر در مورد حریم خصوصی و ارزیابی دوجانبه سالانه می‌شود. مایکروسافت اولین شرکت فناوری بود که به تطبیق با الزامات حفاظت از داده جدید متعهد شد.

از فاجعه داده‌ای جلوگیری شده بود، اما این موضوع روشن کرد که چقدر شرایط عوض شده است.

در وهله اول این اتفاق نشان داد که چیزی به نام جزیره حریم خصوصی وجود ندارد، دیگر کسی نمی‌توانست فرض کند که همه داده‌هایش درون مرزهای یک کشور باقی می‌ماند. این شرایط حتی در مورد قاره‌ای به بزرگی اروپا یا اقتصادی به بزرگی ایالات متحده نیز وجود دارد. اطلاعات شخصی برای انواع گوناگون تراکنش دیجیتال از کشوری به کشور دیگر می‌روند و افراد بیشتر اوقات از این موضوع آگاه نیستند.

این وضعیت اهرم سیاسی خارجی جدیدی را با پیامدهای عمیق بالقوه برای مسئله حریم خصوصی در ایالات متحده ایجاد کرده بود. اعضای دیوان دادگستری اروپا در

عمل به رگولاتورهای حفاظت از داده این قاره (که با تعهد سرسختانه‌شان به حریم خصوصی شناخته می‌شوند) این قدرت را داده بودند تا برای ایجاد استانداردهای حریم خصوصی سخت‌گیرانه‌تر در آمریکا مذاکره کنند.

اگر تردیدی هم در مورد این هدف وجود داشت، کمی بعد از تصمیم دادگاه در سال ۲۰۱۵، زمانی که گزارش‌های بی‌واسطه معتبری در سکوت، در حلقه‌های دولتی می‌چرخیدند، برطرف شد. یکی از اعضای دادگاه که نقشی محوری در رایزنی‌ها داشت، جلساتی حضوری با چند رگولاتور حریم خصوصی ملی برگزار کرده بود تا جزئیات تصمیم را برای آنها تشریح کند و پیشنهاد بدهد که چطور می‌توانند در مذاکره با کاخ سفید و وزارت بازرگانی بهترین بهره را از آن ببرند. از آن نوع کارها بود که اگر در ایالات متحده انجام می‌شد، در مغایرت با اصل تفکیک دادگاه‌ها و قوه مجریه بود. چنین حرکتی در اروپا غیرعادی بود، اما در بسیاری از نقاط دنیا سابقه داشت.

هرچند رهبران سیاسی آمریکا می‌توانند در سخنرانی‌هایشان نفوذ بیش از حد رگولاتورهای حریم خصوصی اروپا را محکوم کنند، اما یک موضوع را نمی‌توانند تغییر دهند؛ آن موضوع وابستگی حیاتی اقتصاد ایالات متحده به توانایی شرکت‌های آمریکایی در انتقال داده به کشورهای دیگر و دریافت داده از آن کشورهاست. در دنیای امروز می‌توان در مورد ساخت دیوار مرزی برای جلوگیری از ورود مهاجران بحث کرد، اما هیچ کشوری نمی‌تواند مانعی را که از جریان بین‌المللی داده‌ها جلوگیری می‌کند، تحمل کند. در واقع مذاکرات اروپایی-آمریکایی که روی شیوه‌های حفاظت از حریم خصوصی شرکت‌های آمریکایی تأثیر می‌گذارند، به یکی از واقعیت‌های اقتصادی امروز تبدیل شده‌اند.

حتی پیامدهای نهایی این بحث‌ها برای چین هم پراهمیت هستند. رویکرد اروپا در طول زمان می‌تواند به فشار فزاینده بر چین برای مواجهه با دوراهی مهمی منجر شود. این کشور می‌تواند بدون حفاظت از حریم خصوصی داده‌های داخل مرزهایش پیش برود یا می‌تواند ارتباطات اقتصادی‌اش با اروپا را با جریان‌های داده اجتناب‌ناپذیر مورد نیاز تقویت کند؛ اما انجام هر دو کار به‌صورت همزمان دشوار خواهد بود.

با این حال مانند واکنش به بسیاری از مواقعی که تا نزدیکی فاجعه می‌رسیم، واکنش

آنی به مذاکرات سپر حریم داده نشد. زنگ بیدارباش دیگری بود، اما افراد باز هم خواب خوش را ترجیح دادند. جریان‌های داده می‌توانستند تداوم داشته باشند و شرکت‌ها به کسب‌وکارشان ادامه دهند. بیشتر شرکت‌های فناوری و مسئولان دولتی تفکر عمیق‌تر در مورد پیامدهای ژئوپلیتیک بلندمدت‌تر را به فردایی دیگر موکول کردند.

از برخی جهات این اتفاق کاملاً قابل درک بود. در ادامه سال ۲۰۱۶ رأی‌گیری برای برگزیت و انتخابات ریاست‌جمهوری آمریکا توجه افراد را به خود جلب کردند. چند ماه بعد هم همه روی تحول دیگری در حوزه حریم خصوصی در اروپا متمرکز شدند. این تحول تاریخ اجرای نزدیک مقررات عمومی حفاظت از داده با سرواژه GDPR در اتحادیه اروپا بود.

این سرواژه به‌سرعت به سرواژه‌ای آشنا برای افراد شاغل در بخش فناوری تبدیل شد. هرچند غیرعادی نبود که بشنوید وکلا از سرواژه‌ها برای اشاره به مقررات دولتی استفاده می‌کنند، اما این سرواژه بر سر زبان مهندسان، بازاریابان و متصدیان فروش هم افتاد. این اتفاق بی‌دلیل نبود. این مقررات تغییر معماری بسیاری از پلتفرم‌های فناوری جهان را ضروری کرده بود؛ کاری که به هیچ‌وجه کار کوچکی نبود. هرچند اتحادیه اروپا لزوماً چنین نقشه‌ای نداشت، اما این مقررات ابزار دوم اروپا برای تأثیرگذاری بر استانداردهای حریم خصوصی در ایالات متحده و سراسر جهان شد.

مقررات عمومی حفاظت از داده با بسیاری از مقررات دولتی متفاوت است. مقررات در بیشتر موارد به شرکت‌ها می‌گوید چه کاری نمی‌توانند انجام دهند. برای مثال می‌گوید در تبلیغات‌تان عبارات گمراه‌کننده به کار نبرید یا در ساختمان‌هایتان از آزبست استفاده نکنید. فلسفه اساسی اقتصاد بازار از نوآوری در کسب‌وکار پشتیبانی می‌کند؛ در عین حال مقررات هم خط قرمزهای رفتاری ویژه‌ای تعیین می‌کند، اما در غیر از این موارد به شرکت‌ها آزادی گسترده‌ای برای تجربه‌کردن می‌دهد.

یکی از مهم‌ترین بخش‌های مقررات عمومی حفاظت از داده، منشور حقوق حریم خصوصی است. این مقررات با اعطای حقوق ویژه‌ای به مصرف‌کنندگان، شرکت‌ها را ملزم می‌کند که علاوه بر اجتناب از برخی شیوه‌ها، فرایندهای کسب‌وکار جدیدی ایجاد کنند. برای مثال شرکت‌هایی که اطلاعات شخصی نگهداری می‌کنند، ملزم شده‌اند

که امکان دسترسی به آنها را برای مصرف‌کنندگان فراهم کنند. مشتریان حق دارند بدانند هر شرکتی چه اطلاعاتی در مورد آنها دارد. حق دارند که اگر اطلاعات درست نیستند، آنها را تغییر بدهند. حق دارند اطلاعات را تحت شرایط گوناگونی حذف کنند و اگر ترجیح می‌دهند، حق دارند اطلاعات‌شان را به ارائه‌دهنده دیگری انتقال دهند.

این مقررات از ابعاد مهمی نوعی منشور کبیر برای حوزه داده است و موج دوم حفاظت از حریم خصوصی در اتحادیه اروپا محسوب می‌شود (منشور کبیر، منشوری است که پادشاه انگلستان پذیرفت و در آن به حفاظت از حقوق کلیسا، زندانی‌نکردن غیرقانونی بارون‌ها، دسترسی سریع به عدالت و محدود کردن خراج‌های فئودالی پرداختی به حکومت متعهد شد). موج اول در سال ۱۹۹۵ و با دستورالعملی در مورد حریم خصوصی آغاز شد که وب‌سایت‌ها را ملزم می‌کرد پیش از جمع‌آوری و استفاده از داده‌های مصرف‌کنندگان به آنها اطلاع بدهند و رضایت آنها را بگیرند. اما با رشد انفجاری اینترنت، افراد با سیلی از اعلان‌های حریم خصوصی مواجه شدند که برای خواندن آنها وقت نداشتند. مقررات عمومی حفاظت از داده با درک این مسئله شرکت‌ها را ملزم می‌کند که به مصرف‌کنندگان توانایی عملی مشاهده و کنترل همه داده‌هایی را بدهند که از آنها جمع‌آوری کرده‌اند.

جای تعجب ندارد که پیامدهای این مقررات برای فناوری بسیار فراگیر است. با این طرح شروع می‌کنیم که هر شرکتی با میلیون‌ها (یا حتی هزاران) مشتری باید فرایند کسب‌وکار تعریف‌شده‌ای برای مدیریت این حقوق جدید مشتریان داشته باشد. در غیر این صورت گرفتار کار ناکارآمد و تقریباً بدون شک ناقص کارمندان برای پیدا کردن داده‌های مشتریان می‌شود. اما فرایند باید خودکار باشد. شرکت‌ها برای تطبیق سریع و کم‌هزینه با این مقررات باید به‌صورت یکپارچه به داده‌های مشتریان در جزیره‌های مختلف داده دسترسی داشته باشند. در نتیجه ایجاد تغییرات در فناوری ضروری است.

تأثیر این مقررات بر شرکت فناوری مثل مایکروسافت که در حوزه‌های متنوعی فعالیت می‌کند بسیار شدید بود. بیش از ۲۰۰ محصول و خدمت داشتیم و به بسیاری از تیم‌های مهندسی این توانایی داده شده بود که زیرساخت‌های پشتیبانی داده

خودشان را ایجاد و مدیریت کنند. شباهت‌هایی بین این زیرساخت‌ها دیده می‌شد، اما تفاوت‌های مهمی هم در معماری اطلاعات مورد استفاده در بخش‌های متفاوت شرکت وجود داشت.

به‌سرعت متوجه شدیم که با اجرای مقررات عمومی حفاظت از داده، این تفاوت‌ها دردسرساز خواهند شد. مصرف‌کنندگان در اتحادیه اروپا انتظار داشتند فرایند واحدی وجود داشته باشد که همه اطلاعات‌شان را از همه خدمات‌مان استخراج کند تا بتوانند آنها را به‌صورت واحد و یکپارچه مشاهده کنند. تنها راه ما برای عملی‌کردن بهره‌ور این خواسته ایجاد معماری اطلاعات جدید و واحدی بود که به‌صورت سراسری شامل همه خدمات‌مان می‌شد. به عبارت دیگر یعنی باید آفیس ۳۶۵، اوت‌لوک، ایکس‌باکس لایو، بینگ، آژور، داینامیکس و همه خدمات دیگر را دربر می‌گرفت.

اوایل سال ۲۰۱۶ تیمی متشکل از بهترین معماران نرم‌افزارمان تشکیل دادیم. تا اجرای این مقررات در ۲۵ می ۲۰۱۸ دو سال مانده بود، اما آنها هیچ وقتی برای از دست دادن، نداشتند.

معماران ابتدا باید به وکلا مراجعه می‌کردند تا تعریفی از الزامات مقررات عمومی حفاظت از داده ارائه دهند. با کمک وکلا فهرستی از مشخصات تهیه کردند که همه قابلیت‌های فناوری که خدمات ما باید فراهم می‌کردند، مشخص می‌کرد. بعد معماران طرح اولیه جدیدی برای پردازش و ذخیره‌سازی اطلاعات تهیه کردند که شامل همه خدمات‌مان می‌شد و این قابلیت‌ها را عملی می‌کرد.

طرح تا آخرین هفته ماه آگوست برای ارزیابی در جلسه‌ای با ساتیا و تیم رهبری ارشد شرکت آماده شد. همه می‌دانستند که طرح اولیه نیازمند کار مهندسی بسیار زیادی است. باید بیش از ۳۰۰ مهندس را به مدت دست‌کم ۱۸ ماه به کار تمام‌وقت روی پروژه منتقل می‌کردیم و شش ماه پیش از تاریخ اجرای مقررات این رقم باید به هزاران نفر می‌رسید. چنین ارقامی به معنای تخصیص بودجه صدها میلیون دلاری بود. جلسه‌ای نبود که کسی بی‌دلیل آن را از دست بدهد. حتی برخی افراد تعطیلات‌شان را کوتاه کرده بودند تا در این جلسه حضور داشته باشند.

تیم‌های مهندسی و حقوقی طرح اولیه، زمان‌بندی‌ها و نحوه تخصیص منابع را

تشـریح کردند که تحسـین همه را واداشـت و در برخی جنبه‌هـا همـه را غافلگیر کرد. همین‌طور که جلسه پیش می‌رفت، ساتیا ناگهان با هیجان و با لبخندی بر لب گفت: «عالی نیسـت؟» بعد ادامـه داد: «سـال‌ها تقریباً غیرممکـن بود که همه مهندسـان شرکت در مورد یک معماری حریم خصوصی واحد به توافق برسند. حال که رگولاتورها و وکلا بـه مـا گفته‌اند چـه کار کنیم، مسـئولیت ایجـاد معماری واحد بسـیار آسـان‌تر شده است.»

نظر جالبی بود. مهندسی فرایندی خلاقانه است و مهندسان افراد خلاقی هستند. وقتـی دو تیم مهندسـی نرم‌افـزار با مسـئله‌ای یکسـان با روش‌هـای متفاوتـی برخورد می‌کنند، متقاعد کردن آنها برای رفع اختلاف‌نظرات و ایجاد رویکردی مشترک بسیار دشوار می‌شود. حتی اگر اختلافات به موضوعی محوری در قابلیتی بسیار مهم مربوط نشود، باز هم افراد تمایل دارند ساخته خودشان را حفظ کنند.

با توجه به سـاختار مهندسـی متنوع مایکروسـافت که برای تصمیم‌گیری مستقل توانمند شـده بود، گاهی اوقات این چالش در شـرکت ما دشـوارتر از سایر شرکت‌های فناوری بود. این شرایط باعث شده بود گاهی اوقات تا سال‌ها دو یا چند خدمت مشابه را حفظ کنیم؛ رویکردی که تقریباً هیچ‌وقت به نتیجه خوبی نرسیده بود. در مقابل اپل گاهی اوقات برای حل این مسئله به تمرکز محصول محدودترش و شیوه تصمیم‌گیری متمرکز اسـتیو جابز اتکا کرده اسـت. شـاید دور از انتظار بود، اما رگولاتورهـای اروپا با تعریف رویکردی واحد که مستلزم توافق و سازش گسـترده در مهندسی بود، در واقع به ما لطف کرده بودند.

سـاتیا بـا طـرح موافقـت کـرد. بعـد رو بـه همـه کـرد و الـزام جدیـدی را اضافـه کرد. سـاتیا گفت: «حال که می‌خواهیم پـول زیادی بـرای ایجاد این تغییـرات هزینه کنیم، می‌خواهم این کار را فقط بـرای خودمان انجام ندهیم. می‌خواهـم هر قابلیت جدیدی که برای اسـتفاده در دسـترس خودمان به‌عنوان شخص اول اسـت، در دسترس همه مشتریان‌مان به‌عنوان شخص ثالث هم باشد.»

به عبارت دیگر ساتیا می‌گفت فناوری را به نحوی بسازید که همه مشتریان بتوانند برای تطبیق با مقررات عمومی حفاظت از داده از آن اسـتفاده کننـد. این حرف به‌ویژه

در دنیای تحت تسلط داده، منطقی به نظر می‌رسید، اما در عین حال کار را هم بیشتر می‌کرد. آه همه مهندسان حاضر در اتاق درآمد؛ جلسه را با آگاهی از این موضوع ترک کردند که باید افراد بیشتری را برای این پروژه در نظر بگیرند.

الزامات فنی چشم‌گیر به توجیه وضعیت دومی کمک می‌کرد که به‌سرعت پدیدار شد؛ وضعیتی که پیامدهای ژئوپلیتیک مهمی داشت. وقتی کارهای مهندسی برای تطبیق با مقررات عمومی حفاظت از داده در مسیر درست قرار گرفت، ایجاد معماری فنی متفاوتی برای مکان‌های دیگر اشتیاق‌برانگیز نبود. هزینه‌ها و پیچیدگی‌های مهندسی برقراری سیستم‌های متفاوت، خیلی زیاد هستند.

این شرایط به گفت‌وگوی جالبی با «جاستین ترودو»، نخست‌وزیر کانادا، در اوایل سال ۲۰۱۸ منجر شد. در جلسه‌ای که ساتیا و من با او و شماری از مشاوران ارشدش داشتیم، به مسائل حریم خصوصی اشاره کردیم که همچنان برای مردم کانادا موضوع مهمی است. وقتی ترودو به احتمال ایجاد تغییرات در قانون حریم خصوصی کانادا اشاره کرد، ساتیا او را تشویق کرد که کارشان را راحت کنند و بندهای مقررات عمومی حفاظت از داده را به کار بگیرند. هرچند این پیشنهاد با کمی غافلگیری روبه‌رو شد، اما ساتیا توضیح داد که هزینه‌های برقراری یک فرایند یا معماری متفاوت برای کشوری واحد، احتمالاً از مزیت‌های بالقوه آن بیشتر خواهد بود؛ مگر در مورد برخی تفاوت‌ها که اهمیت اساسی دارند.

اشتیاق بیشتر ما نسبت به این مقررات، ما را در اردوگاه متفاوتی نسبت به برخی از شرکت‌های بخش فناوری قرار می‌داد که گاهی اوقات بیشتر بر بخش‌های دشوار این مقررات تمرکز می‌کردند. هرچند معتقد بودیم بخش‌هایی از این مقررات گیج‌کننده یا حتی بدتر هستند، اما باور داشتیم که یکی از کلیدهای موفقیت بلندمدت بخش فناوری حفظ اعتماد عمومی در مورد مسائل حریم خصوصی است. این رویکرد یکی دیگر از حوزه‌هایی بود که از تجربه ما در پرونده ضدانحصار در دهه ۱۹۹۰ و هزینه اعتباری زیادی که پرداخته بودیم، نشئت می‌گرفت. رویکردی متعادل‌تر به مسائل رگولاتوری بالقوه بحث‌برانگیز ممکن بود ما را نزد برخی همتایان‌مان در بخش فناوری یا حتی مهندسان خودمان بیش از حد دیپلمات جلوه دهد، اما احساس می‌کردم روزها

و مسائل زیادی وجود دارند که این رویکرد را هوشمندانه‌تر جلوه می‌دهند.

در هر صورت در بخش فناوری، دیگران اغلب به احساس متناقض مردم آمریکا نسبت به حریم خصوصی به‌عنوان دلیلی برای بی‌توجهی به فشارهای رگولاتوری ایالات متحده اشاره می‌کردند. می‌گفتند: «حریم خصوصی مُرده است. مردم باید با آن کنار بیایند.»

معتقد بودم مسئله حریم خصوصی آتش زیر خاکستر است، اما روزی می‌رسد که دیگر این‌طور نیست. آن وقت آتشی به پا خواهد شد، در حالی که زیربنای سیاسی محدودی برای اتخاذ رویکرد حساب‌شده‌تر وجود دارد. احساس متناقض مردم نسبت به حریم خصوصی تجربه صنعت انرژی هسته‌ای در چند دهه قبل را به من یادآوری می‌کرد.

در طول دهه ۱۹۷۰ صنعت انرژی هسته‌ای نتوانست به بحث عمومی مؤثری در مورد ریسک‌های ناشی از پیشرفت‌های فناورانه‌اش بپردازد. بنابراین وقتی در سال ۱۹۷۹ فاجعه‌ای در «نیروگاه هسته‌ای تری مایل آیلند» (Three Mile Island Nuclear Generating Station) در ایالت پنسیلوانیا رخ داد، مردم و سیاست‌مداران آماده نبودند. پیامدهای سیاسی حادثه «تری مایل آیلند» توسعه انرژی هسته‌ای را در آمریکا متوقف کرد؛ اتفاقی که در کشورهای دیگر نیفتاد. ۳۴ سال طول کشید تا ساخت نیروگاه هسته‌ای دیگری در ایالات متحده شروع شود.

احساس می‌کردم باید از این اتفاق تاریخی درس بگیریم و اجازه ندهیم تکرار شود.

در مارس ۲۰۱۸ معادل حادثه «تری مایل آیلند» برای حریم خصوصی اتفاق افتاد. این اتفاق جنجال کمبریج آنالتیکا بود. این شرکت مشاوره سیاسی با استفاده از داده‌های شخصی کاربران فیس‌بوک پایگاه داده‌ای ایجاد کرده و با بهره‌برداری از آن تبلیغات هدفمندی برای جلب پشتیبانی از کمپین ریاست‌جمهوری دونالد ترامپ طراحی کرده و با آنها رأی‌دهندگان آمریکایی را هدف قرار داده بود. هرچند این اقدام سیاست‌های فیس‌بوک را نقض کرده بود، اما سیستم‌های تطبیق این شرکت نتوانسته بودند آن را شناسایی کنند. در واقع از آن دست مشکلاتی بود که انتقادات زیادی را برمی‌انگیزد، اما شرکت را در موقعیتی غیرقابل دفاع قرار می‌دهد. در چنین شرایطی

تنها کاری که شرکت می‌تواند انجام دهد، عذرخواهی است؛ کاری که مارک زاکربرگ انجام داد.

در عرض چند هفته حال‌وهوای سیاسی در واشنگتن‌دی‌سی عوض شد. سرانجام سیاست‌مداران و رهبران فناوری به جای رد کردن مقررات، در مورد آن به‌عنوان امری اجتناب‌ناپذیر صحبت می‌کردند. اما نمی‌توانستند توضیح بدهند که به نظرشان این مقررات چه کاری باید انجام دهد.

پاسخ این پرسش در آن سوی کشور، در نزدیکی سیلیکون‌ولی، پیدا شد. این ماجرا هم نقش اول دور از انتظاری مانند مکس شرمس دارد.

این شخصیت مردی آمریکایی به نام «آلاستر مکتاگارت» بود. این توسعه‌دهنده املاک منطقه خلیج سان‌فرانسیسکو و پدر سه فرزند، در سال ۲۰۱۵ میزبان میهمانی شامی در منزلش در شهر «پیدمونت» ایالت کالیفرنیا بود. مقر غول‌های سیلیکون‌ولی در غرب خلیج و خانه او در شرق، در منطقه‌ای سرسبز قرار داشت. وقتی مکتاگارت از یکی از میهمانانش در مورد شغلش در گوگل پرسید، پاسخ‌هایش برای مکتاگارت نه‌تنها ناراضی‌کننده؛ بلکه ترسناک بود.

پرسیده بود شرکت‌های فناوری کدام داده‌های خصوصی را جمع‌آوری می‌کنند؟ با این داده‌ها چه کار می‌کنند؟ و چطور می‌توانم انتخاب کنم که نمی‌خواهم از داده‌هایم استفاده کنند؟ مهندس گوگل پاسخ داده بود اگر افراد می‌دانستند گوگل چه می‌داند، «وحشت‌زده می‌شدند».

گفت‌وگویی که هنگام صرف نوشیدنی شکل گرفت، آغازگر پیکار دوساله‌ای با بیش از سه میلیون دلار هزینه شد. تقریباً سه سال بعد وقتی در سان‌فرانسیسکو با مکتاگارت دیدار داشتیم، به ما گفت: «بسیار مهم به نظر می‌رسید. فکر می‌کردم فردی باید کاری در این مورد انجام دهد. با خودم گفتم چرا آن فردی که باید کاری انجام دهد، من نباشم؟»

مکتاگارت نمی‌خواست به جنگ صنعت فناوری برود. مدیر کسب‌وکار موفقی بود و اعتقاد راسخی به بازارهای آزاد و باز داشت. بالأخره درآمدش را از قیمت‌های سربه‌فلک‌کشیده املاک در همین منطقه‌ای به دست آورده بود که شرکت‌های فناوری

در آن حضور داشتند. اما مصمم بود تغییری ایجاد کند، به این امید که روزی به فرزندانش بگوید به حفاظت از موضوع ارزشمندی، یعنی داده‌های شخصی ما کمک کرده است.

در عصری که مکتاگارت و برخی دیگر آن را عصر «نظارت تجاری» می‌نامند، جست‌وجوهای آنلاین، ارتباطات، مکان دیجیتال، خریدها و فعالیت‌هایمان در رسانه‌های اجتماعی، اطلاعاتی بیشتر از آنچه احتمالاً می‌خواهیم به اشتراک بگذاریم، افشا می‌کنند. مکتاگارت به این نتیجه رسیده بود که این اطلاعات قدرت خارق‌العاده‌ای را به چند شرکت خاص داده است. با اشاره به ابزارهای آنلاین رایگانی که ندانسته با اطلاعات‌مان هزینه‌شان را می‌دهیم، گفت: «مجبورید شرایط حریم خصوصی آنها را بپذیرید؛ وگرنه نمی‌توانید از خدمات‌شان استفاده کنید، ولی ما برای زندگی‌کردن در جهان مدرن به این خدمات وابسته‌ایم. هیچ راهی وجود ندارد که از آنها استفاده نکنیم.»

عدم نظارت، او را به جذب حامیان هم‌فکر و تهیه پیش‌نویس قانون حریم خصوصی جدیدی برای کالیفرنیا ترغیب کرد. با اشاره به قوانین ساخت‌وساز پذیرفته‌شده حاکم بر حوزه املاک می‌گوید: «در فضایی به‌شدت رگوله‌شده کار می‌کنم. درستش همین است. قانون نباید از فناوری عقب بیفتد؛ وگرنه افراد مدام سعی می‌کنند محدودیت‌ها را کنار بزنند.»

مکتاگارت از تجربه‌اش در حوزه املاک درس‌های زیادی در مورد سازوکارهای دولت آموخته بود. با هوشمندی سیاسی‌اش درک می‌کرد که مخالفت سیلیکون‌ولی، تصویب قانون فدرال در واشنگتن‌دی‌سی را دشوار می‌کند. اما کالیفرنیا مانند برخی دیگر از ایالت‌های غربی آمریکا، راهکار سیاسی جایگزینی داشت. این ایالت‌ها که در میانه و اواخر قرن نوزدهم تأسیس شده‌اند، فرایندهایی را طبق قانون اساسی مقرر کرده‌اند که طبق آنها می‌توان با تعداد امضای کافی، پیشنهادی را برای تصویب به رأی مردم گذاشت.

فرایند تصویب پیشنهادهای شهروندی کالیفرنیا در گذشته مسیر تاریخ آمریکا را عوض کرده بود. چهار دهه قبل در سال ۱۹۷۸ رأی‌دهندگان این ایالت «پیشنهاد ۱۳»

را برای محدود کردن مالیات‌ها تصویب کرده بودند. این پیشنهاد مالیات املاک را در این ایالت کاهش می‌داد، اما در عین حال پیامدهای گسترده‌تری داشت. پیشنهاد ۱۳ به تقویت جنبشی مردمی در سراسر کشور کمک کرد که در موفقیت رونالد ریگان در انتخابات ریاست‌جمهوری سال ۱۹۸۰ و فشار ملی بیشتر برای کوچک‌کردن دولت و کاهش مالیات‌ها تأثیرگذار بود. این پیشنهاد نقطه‌عطفی سیاسی ایجاد کرد که از جهتی بازتاب این موضوع بود که از هر هشت آمریکایی یک نفر در کالیفرنیا زندگی می‌کند.

اگر کمبریج آنالتیکا می‌توانست به معادل حادثه «تری مایل آیلند» تبدیل شود، آیا آلاستر مکتاگارت می‌توانست معادل پیشنهاد ۱۳ را در مورد حریم خصوصی بیافریند؟

خیلی زود این احساس به وجود آمد که پاسخ این سؤال می‌تواند مثبت باشد. امضاهایی که مکتاگارت جمع کرد، بیش از دوبرابر تعداد مورد نیاز برای به رأی گذاشتن پیشنهاد بود. نظرسنجی اولیه نشان می‌داد که ۸۰ درصد از رأی‌دهندگان از پیشنهاد او پشتیبانی می‌کنند. مکتاگارت از اینکه ۲۰ درصد رأی‌دهندگان موافق این پیشنهاد نبودند، ناراحت شده بود؛ تا اینکه مسئولان نظرسنجی توضیح دادند که تاکنون شاهد چنین ارقام بالایی نبوده‌اند. در حالی که کمپین‌های طرح‌هایی با منابع مالی مناسب تقریباً همیشه در رأی‌گیری موفق می‌شدند، مشخص بود که اگر مکتاگارت حاضر باشد بیش از میلیون‌ها دلار درآمدش از املاک را برای کمپینی مؤثر هزینه کند، شانس بسیار زیادی برای موفقیت پای صندوق‌های رأی در ماه نوامبر خواهد داشت.

ما در مایکروسافت نسبت به طرح مکتاگارت احساسات ضدونقیضی داشتیم. از طرفی خیلی وقت بود که از قانون‌گذاری در مورد حریم خصوصی در ایالات متحده و از جمله در سطح فدرال پشتیبانی می‌کردیم. با رهبری «جولی بریل»، رئیس سابق کمیسیون فدرال تجارت که اکنون مدیریت امور حریم خصوصی و رگولاتوری مایکروسافت را بر عهده دارد، تصمیم گرفته بودیم وقتی مقررات عمومی حفاظت از داده در می ۲۰۱۸ اجرایی می‌شود، رویکرد متفاوتی نسبت به سایر بخش‌های فناوری اتخاذ کنیم؛ به جای آنکه حقوق مصرف‌کننده مندرج در این مقررات را فقط در دسترس

افراد ساکن در اتحادیه اروپا قرار دهیم، این حقوق را به همه مشتریان‌مان در همه جای دنیا اختصاص دادیم. خیلی زود متوجه شدیم که مصرف‌کنندگان آمریکایی بسیار بیشتر از اروپایی‌ها به اجرایی‌شدن این حقوق علاقه دارند؛ اتفاقی که مُهر تأییدی بر این احساس ما بود که آمریکا سرانجام به سمت تصویب حقوق حریم خصوصی حرکت خواهد کرد.

اما از نظر ما متن پیش‌نویس پیشنهاد مکتاگارت پیچیده و در برخی موارد، گیج‌کننده بود. نگران بودیم که به اعمال الزاماتی فنی در برخی نقاط منجر شود که به دلایل نه‌چندان مفیدی با مقررات عمومی حفاظت از داده تفاوت داشته باشد. این مشکلات از نوعی بودند که می‌شد آنها را با قانون‌گذاری در مجلس و فرایند مفصل تهیه پیش‌نویس، برطرف کرد، اما با پیشنهادی با دو گزینه آری یا نه در صندوق رأی‌گیری نمی‌شد. مسئله این بود که چطور همه را متقاعد کنیم تا تلاش‌هایشان را به جای صندوق رأی از طریق مجلس ایالتی پیگیری کنند و در عین حال تلاش‌ها را به‌کلی ضایع نکنیم.

سایر شرکت‌های فناوری، کمپین جذب اعانه‌ای را راه‌اندازی کردند تا علیه این پیشنهاد فعالیت کنند. سیلیکون‌ولی می‌دانست که برای رسیدن به موفقیت، احتمالاً باید بیش از ۵۰ میلیون دلار کمک جذب کند. ما ۱۵۰ هزار دلار کمک کردیم. به اندازه‌ای بود که ارتباط ما را با سایر فعالان صنعت برقرار نگه دارد، اما آن‌قدر نبود که به تلاش‌های مخالفان شتاب ببخشد.

در نهایت نیاز به منابع مالی زیاد برای ایجاد کمپین در مورد این پیشنهاد، به هر دو طرف برای مذاکره انگیزه داد. مکتاگارت حاضر بود با مسئولان کلیدی منتخب مردم جلسه بگذارد تا در مورد جزئیات قانون به نتیجه برسند. برای برخی از سایر شرکت‌های فناوری، تصمیم‌گیری در مورد اینکه چه کاری می‌خواهند انجام بدهند، دشوار بود، ولی ما دو نفر از متخصصان حریم خصوصی مایکروسافت را به ساکرامنتو فرستادیم. این متخصصان تقریباً به‌صورت شبانه‌روزی کار کردند و با رهبران قانون‌گذاری ایالت و تیم مکتاگارت به بررسی جزئیات پرداختند.

مجلس در آخرین لحظات ممکن «قانون حریم خصوصی مصرف‌کننده کالیفرنیا

۲۰۱۸» را تصویب و «جری براون»، فرماندار، به‌سرعت آن را امضا کرد. قانون مذکور، قدرتمندترین قانون حریم خصوصی در تاریخ ایالات متحده بود. این قانون مانند مقررات عمومی حفاظت از داده به ساکنان ایالت کالیفرنیا این حق را می‌دهد که بدانند شرکت‌ها چه داده‌هایی از آنها جمع‌آوری می‌کنند، همچنین با فروش داده‌هایشان مخالفت کنند و اگر شرکت‌ها از داده‌های شخصی‌شان حفاظت نکردند، از آنها توضیح بخواهند.

تقریباً بلافاصله تأثیر تصویب این قانون در سطح ملی احساس شد. در عرض چند هفته حتی مخالفانی در واشنگتن‌دی‌سی که مدت‌ها در برابر قانون‌گذاری جامع در مورد حریم خصوصی مقاومت می‌کردند، به باوری روی آوردند که برای آنها شبیه دینی جدید بود. با پیشگام‌شدن کالیفرنیا واضح بود که سایر ایالات هم احتمالاً از آن پیروی خواهند کرد. گروه‌های کسب‌وکاری که ترجیح می‌دادند با ملغمه‌ای از قوانین ایالتی گوناگون مواجه نشوند، شروع به لابی‌گری در کنگره کردند تا این نهاد، قانونی ملی را در مورد حریم خصوصی به تصویب برساند که بر قانون کالیفرنیا و مصوبات سایر ایالت‌ها تقدم یا در عمل تسلط پیدا کند. هرچند هنوز راه طولانی در پیش بود، اما مکتاگارت با موفقیت نگاه کشور به مسائل حریم خصوصی را عوض کرده بود؛ دستاورد بسیار مهمی بود.

وقتی با مکتاگارت در سان‌فرانسیسکو دیدار کردیم، نمی‌شد تحت تأثیر قرار نگیریم. به‌راحتی ممکن بود او را تهدید ببینیم؛ کنشگری که به‌دنبال مهار صنعتی است که بیش از حد قدرتمند شده است. در عوض او را عمل‌گرایی دوست‌داشتنی دیدیم که با دیدی باز به آینده فکر می‌کرد.

مکتاگارت می‌گفت: «کار تمام نشده است. تا صدها سال همچنان در مورد فناوری و حریم خصوصی صحبت خواهیم کرد؛ همان‌طور که با گذشت بیش از یک قرن از پرونده «استاندارد اویل» همچنان در مورد قانون ضدانحصار حرف می‌زنیم.»

شرکتی بودیم که ۸۰ سال بعد از پیروزی وزارت دادگستری در برابر شرکت استاندارد اویل، از تلاطم پرونده ضدانحصار به سلامت عبور کرده بودیم، پس به‌خوبی مقایسه او را درک می‌کردیم. در مجموع مقایسه تاریخی مکتاگارت چند خوراک فکری بسیار

مهم برای ما فراهم می‌کند.

ترکیب تلاش‌های مکس شرمس و آلاستر مکتاگارت برای آینده چند درس مهم دارد.

اول اینکه سخت می‌توان باور کرد که حریم خصوصی (آن‌طور که برخی افراد بخش فناوری یک یا دو دهه قبل پیش‌بینی کرده بودند)، در سکوت از یاد برود. افراد آگاه شده‌اند که تقریباً همه ابعاد زندگی‌شان نوعی ردپای دیجیتال از خود بر جای می‌گذارد. حریم خصوصی باید حفاظت شود و قوانین حریم خصوصی قدرتمندتر اجتناب‌ناپذیر شده‌اند. قطعاً روزی می‌رسد که ایالات متحده در اجرای قانونی شبیه مقررات عمومی حفاظت از داده به اتحادیه اروپا و سایر کشورها بپیوندد.

همچنین محتمل است که در چند سال آینده، به‌ویژه در اروپا، شاهد ظهور موج سوم حفاظت از حریم خصوصی باشیم. همان‌طور که مقررات عمومی حفاظت از داده واکنشی به انبوه اعلان‌های حریم خصوصی بود که افراد برای خواندن‌شان وقت نداشتند، اکنون نیز نگرانی‌هایی را می‌شنویم که افراد به اندازه کافی زمان ندارند تا همه داده‌هایی را که طبق این مقررات در فضای آنلاین در دسترس قرار می‌گیرند، بازبینی کنند. این نگرانی‌ها احتمالاً موج جدیدی از قوانین دولتی را برای رگوله‌کردن نحوه جمع‌آوری و استفاده از داده‌ها به وجود می‌آورد.

بنابراین بخش فناوری باید در مورد نوآوری‌هایی که از حریم خصوصی حفاظت کرده و در عین حال امکان استفاده مناسب از داده‌ها را فراهم می‌کنند، خلاقیت بیشتری از خود بروز دهد. همین حالا هم چند رویکرد فنی جدید ظهور کرده‌اند، برای مثال توانایی پیشبرد پیشرفت‌های هوش مصنوعی با استفاده از داده‌هایی که رمزنگاری‌شده می‌مانند و در نتیجه حریم خصوصی بهتر حفاظت می‌شود؛ اما تازه در ابتدای راهیم.

دست آخر اینکه تجربیات شرمس و مکتاگارت بیانگر نقاط قوت و فرصت‌های مهمی برای دموکراسی‌های جهان هستند. ممکن است توانایی غیرقابل پیش‌بینی یک دانشجوی حقوق و توسعه‌دهنده املاک در متحول‌کردن قوانین حاکم بر شماری از قدرتمندترین فناوری‌های دوران ما، برای رهبران دولتی یکه‌تاز هشداردهنده باشد، اما دیدگاه دیگری هم وجود دارد که با در نظر گرفتن همه عوامل به نظر می‌رسد دیدگاه بهتری است؛ شرمس و مکتاگارت از فرایندهای قضایی و قانونی موجود برای اصلاح

اشتباهات موجود از نظر خودشان استفاده کردند. همچنین موفقیت آنها نشان‌دهنده توانایی بالقوه جوامع دموکراتیک برای سازگار شدن با نیازهای متغیر افراد و قرار دادن قوانین کشور در مسیر درست با ایجاد کمترین اختلال است.

ماهیت درهم‌تنیده اقتصاد جهانی و نفوذ فراوان قوانین حریم خصوصی اروپا، حتی بر کشورهایی مثل چین نیز فشار وارد می‌کند تا قوانین محکمی برای حفاظت از حریم خصوصی تصویب کنند. به عبارت دیگر اروپا فقط زادگاه دموکراسی و مهد حفاظت از حریم خصوصی نیست؛ بلکه به احتمال زیاد تنها امید دنیا برای آینده حریم خصوصی است.

۹

فصل نهم
اینترنت پرسرعت روستایی
الکتریسیته قرن بیست‌ویکم

وقتی به رستوران و کافه «ناتی پاین» (Knotty Pine Restaurant & Lounge) در خیابان اصلی شهر ریپابلیک (Republic) در ایالت واشنگتن نزدیک می‌شوید، از ظاهر شهر می‌فهمید که در یکی از شهرهای پررونق سابق غرب وحشی قرار دارید. نمای چوب سرو رستوران نشانه عصری است که در آن شهرک‌های موقت معدن‌کاوی و چوب‌بری با عجله ساخته می‌شدند. اما پلاکارد زرد روشن آویزان از در که روی آن نوشته شده «پذیرای موتورسواران»، به شما یادآوری می‌کند که این شهر کوچک کاملاً در عصری جدید قرار دارد.

آن روز صبح وقتی جی‌پی‌اس می‌گفت به چپ بپیچید، باید به راست می‌پیچیدیم و وقتی می‌گفت به راست بپیچید، باید به چپ می‌پیچیدیم و با ماشین اجاره‌ای مسیری پرپیچ‌وخم را در جاده‌های روستایی می‌راندیم. جای زیبایی است، پس از بیراهه‌رفتن بدمان نمی‌آمد. اما قراری داشتیم که باید به آن می‌رسیدیم و جی‌پی‌اس در این گوشه شمال شرقی ایالت کار نمی‌کرد. سرانجام بی‌خیال تلفن‌های هوشمندمان شدیم و از روی نقشه‌ای کاغذی در مسیر شاهراه ۲۰ به سمت شهرستان «فری» (Ferry) و شهر ریپابلیک حرکت کردیم؛ جایی که گروه کوچکی از افراد محلی پیش از ناهار منتظرمان بودند.

شهرستان فری مدت‌هاست بیشترین نرخ بیکاری را در ایالت دارد که با سرد شدن هوا در زمستان و کاهش کارهای کشاورزی به بیش از ۱۶ درصد می‌رسد. از شهرستان کینگ (King)، خانه مایکروسافت، آمازون، استارباکس، کاستکو و بوئینگ می‌آمدیم. شهرستان کینگ با نرخ بیکاری کمتر از چهار درصد، بیشترین رشد را در ایالت با دوبرابر میانگین کشوری دارد. به این فکر می‌کردیم که شهرستان فری چطور می‌تواند از رونق قرن بیست‌ویکمی آن طرف رشته کوه «کسکید» (Cascade) یعنی شهرستان کینگ بهره ببرد.

رستوران ناتی پاین تمام روز صبحانه سرو می‌کرد، پس ما هم با ۵٫۹۵ دلار تخم مرغ هم‌زده، بیکن و پنکیک‌های بسیار بزرگ غرق‌شده در شیره افرا سفارش دادیم. بعد از رانندگی طولانی، غذا می‌چسبید، اما در برابر میهمان‌نوازی میهمانان حرفی برای گفتن نداشت.

کاوشگرانی که در انتهای قرن نوزدهم این شهر کوچک را بنیان‌گذاری کرده بودند، نام آن را «یوریکا گالچ» (Eureka Gulch) گذاشتند. ریپابلیک در دره‌ای بین منطقه پوشیده از درخت کاج به نام «واکاندا» (Wauconda) و گردنه «شرمن» در شمال شرقی ایالت واشنگتن قرار دارد. گردنه شرمن به احترام ژنرال مشهور جنگ داخلی «ویلیام تکامسه شرمن» نام‌گذاری شده که در سال ۱۸۸۳ از آن عبور کرده بود؛ ناحیه‌ای تماشایی که رویای هر طبیعت‌دوستی است.

گذشته شهر با رگه‌های طلایی تعریف می‌شد که در سنگ‌های گرانیت آن منطقه وجود داشتند و تا دره‌های گود و باریک رودخانه کشیده می‌شدند. بانکداری، حمل‌ونقل و سایر خدمات پشتیبان خیلی زود پشت سر معدن‌کاوان و بعد چوب‌بران به شهر آمدند. حال که معادن بسته شده‌اند، این منطقه در بازتعریف خود برای آینده با چالش روبه‌رو شده است.

وقتی قرار جلسه را می‌گذاشتیم، «البرت کونتز»، چوب‌بر سابق و شهردار کنونی این شهر به ما گفت که «بهترین شلوار ورزشی‌اش» را برای ناهار با ما می‌پوشد. وقتی با شلوار پارچه‌ای اتوکشیده آمد، ذوقم کور شد. البرت سخاوتمندانه دانشش را در اختیار دیگران می‌گذاشت و آدم شوخ و بذله‌گویی بود، اما وقتی در مورد وضعیت اینترنت پرسرعت در شهرستان فری پرسیدم، نخندید، فقط ابروهایش را بالا انداخت.

گفت: «این حوالی تقریباً هیچ‌کس اینترنت پرسرعت ندارد. سال‌هاست که قول‌هایی داده می‌شود، اما کاری انجام نشده است.» اما داده‌های کمیسیون ارتباطات فدرال نشان می‌داد که در شهرستان فری همه به اینترنت پرسرعت دسترسی دارند.

به لطف کابل فیبر نوری عبوری از گردنه شرمن مرکز این شهر کوچک با حدود هزار نفر جمعیت تا حدودی به اینترنت پرسرعت دسترسی داشت، اما واضح بود که سایر ساکنان این منطقه دسترسی ندارند. البرت به ما گفت: «مشکل این است که ما اینجا در جنگل زندگی می‌کنیم. یعنی وقتی از شهر خارج می‌شویم، دسترسی‌ها کاملاً قطع می‌شوند.»

وقتی جمعیت به نشانه تأیید سر تکان دادند و داستان گرفتاری‌هایشان با اینترنت پرسرعت را بازگو کردند، حال‌وهوا عوض شد. برخی افراد از ارتباطات ماهواره‌ای استفاده می‌کردند که زیاد قطع می‌شد. دیگران حتی برای دانلود به‌روزرسانی‌های نرم‌افزاری

لپ‌تاپ‌هایشان به شهر می‌آمدند تا از نقاط اتصال داخل شهر استفاده کنند. برخی دیگر امیدوار بودند اینترنت نسل پنجم به دادشان برسد، اما حاضران اتفاق‌نظر داشتند که بیشتر مناطق شهرستان فری به اینترنت پرسرعت قابل اطمینان دسترسی ندارد.

فردی با ریشخند گفت: «این را به کمیسیون ارتباطات فدرال بگویید.»

ما هم همین کار را کردیم.

چند ماه بعد در باران و ترافیک خیابان دوازدهم به سمت ساختمان مرکزی کمیسیون ارتباطات فدرال در واشنگتن‌دی‌سی رفتیم. آمده بودیم با «آجیت پای» (Ajit Pai)، رئیس این کمیسیون دیدار کنیم. بعد از ورود و عبور از بازرسی به سمت دفترش راهنمایی شدیم. آجیت پای با لبخند از ما استقبال کرد و گفت: «ممنون که تشریف آوردید. چه کاری از دست من برمی‌آید؟»

عکس‌های خانوادگی‌اش روی طاقچه‌ها بودند و از پنجره‌های دفترش می‌شد پایتخت باران‌زده را از بالا نگاه کرد. «پای» یک آمریکایی هندی‌تبار و بزرگ‌شده در کانزاس است. والدینش پزشکانی هستند که دو سال قبل از به دنیا آمدن او به آمریکا مهاجرت کردند.

از سفرمان به شهرستان فری و شرایط میدانی آنجا گفتم. نقشه ملی کمیسیون ارتباطات فدرال نشان می‌دهد که در شهرستان فری همه به اینترنت پرسرعت دسترسی دارند. در واقع کمیسیون ارتباطات فدرال می‌خواهد دسترسی به اینترنت پرسرعت را برای همه آمریکایی‌ها امکان‌پذیر کند، اما مسئله دشوار و پرهزینه‌ای است؛ به‌ویژه وقتی کاملاً درک نمی‌کنید مسئله چقدر بزرگ است. با اشاره به داده‌های نادرست گفتم: «شما آن رئیس کمیسیون ارتباطات فدرالی نیستید که این مشکل را به وجود آورده، اما می‌توانید رئیسی باشید که آن را برطرف می‌کند.» این مسئله را باید اولویت ملی بدانیم.

همان‌طور که شهردار ریپابلیک به ما گفته بود، بخش زیادی از داده‌های دولت فدرال در مورد شهرستان فری و به همین ترتیب کل مناطق روستایی آمریکا اشتباه است. ساکنان شهرستان فری این مسئله را می‌دانستند و باعث سلب اعتمادشان از دولت می‌شد. از نظر این افراد داده‌های نادرست مسئله کوچکی نبود. این داده‌ها روی تخصیص بودجه فدرال برای اینترنت پرسرعت تأثیر می‌گذاشت. وقتی دولت معتقد باشد منطقه‌ای دسترسی دارد، دیگر بودجه‌ای را برای این کار به آنجا اختصاص نمی‌دهد. در سطح

گسترده‌تر هم این عدم دسترسی به سایر منابع عمومی حیاتی ضربه می‌زند. برای مثال آن منابعی که برای مقابله با آتش‌سوزی‌های تابستان هرساله غرب کشور مورد نیاز هستند.

البرت می‌گفت: «اینجا واقعاً غرب وحشی است. اداره کلانتری بزرگی نداریم، اداره آتش‌نشانی بزرگی نداریم، هیچ‌کدام از اینها را نداریم. همه آتش‌نشانان ما داوطلب هستند. وقتی آتش به جان طبیعت می‌افتد، این داوطلبان در شرایط پرخطری قرار می‌گیرند.»

در سال ۲۰۱۶ وقتی بادهای سوزان آگوست یکی از خطوط برق فشار قوی را خراب کردند و شعله‌های آتش برخاسته از آن را به شمال شهرستان فری آوردند، آتشی ایجاد شد که به‌سرعت گسترش می‌یافت. آتش‌سوزی مهارنشدنی در عرض پنج ساعت بیش از ۲۵۰۰ هکتار را سوزاند و همچنان در حال گسترش بود. برای بخش‌هایی از مناطق آسیب‌دیده هشدار تخلیه سطح ۳ صادر شد که در واقع یعنی «همین حالا تخلیه کنید».

زیرساخت ناقص شبکه موبایل و نبود اینترنت پرسرعت مخابره داده‌های حیاتی به محل آتش‌سوزی و از آن و آگاه‌کردن مسئولان از مسیر آتش و محل‌های نیازمند تخلیه را غیرممکن می‌کرد. تنها راه انتقال اطلاعات حیاتی بین آتش‌نشانان، جنگلبانی و مجریان قانون این بود که داده‌ها روی حافظه فلش بارگذاری شود، حافظه به راننده یک خودروی پیکاپ سپرده شود و او از مکان آتش‌سوزی ۴۰ دقیقه تا ریپابلیک رانندگی کند که مسئولان بتوانند از اینترنت پرسرعت و ارتباطات رادیویی استفاده کنند.

البرت می‌گفت وقتی آتش می‌تواند در عرض یک دقیقه بادی با سرعت ۲۰ مایل را به تندبادی با سرعت ۵۰ مایل تبدیل کند، «چنین کاری بدون شک خطرناک است».

آمریکایی‌هایی که در دوران دایال‌آپ گیر افتاده‌اند، به شهرستان فری محدود نمی‌شوند. چنین مناطقی در همه ایالت‌های کشور وجود دارد. گزارش اینترنت پرسرعت سال ۲۰۱۸ کمیسیون ارتباطات فدرال نشان می‌دهد که بیش از ۲۴ میلیون آمریکایی که بیش از ۱۹ میلیون نفر آنها در مناطق روستایی زندگی می‌کنند، به اینترنت پرسرعت ثابت دسترسی ندارند. این رقم تقریباً معادل جمعیت ایالت نیویورک است.

مسئله این نیست که افراد در این مناطق به‌دلیل نداشتن توانایی مالی به اینترنت

پرسرعت دسترسی ندارند، بلکه مسئله این است که اگر توانایی مالی هم داشته باشند، نمی‌توانند این خدمات را تهیه کنند. بسیاری از افراد در این مناطق از فناوری دایال‌آپ برای انتقال داده در سیم‌های مسی استفاده می‌کنند و نمی‌توانند به خدمات آنلاینی دسترسی داشته باشند که بیشتر ما با سرعت دانلود و آپلود عادی به‌راحتی به آنها دسترسی داریم. به عبارت دیگر بخش قابل توجهی از مناطق روستایی به اینترنت پرسرعتی دسترسی ندارند که بیش از یک دهه پیش در مناطق شهری در دسترس بود.

هرچند همین رقم هم هشداردهنده است، اما شواهد محکمی وجود دارد که درصد آمریکایی‌هایی که به اینترنت پرسرعت دسترسی ندارند، بسیار بیشتر از ارقامی است که کمیسیون ارتباطات فدرال اعلام می‌کند. با تحلیل این داده‌ها به این نتیجه رسیدیم که مبنای آنها روشی معیوب است. اگر یک شرکت ارائه‌دهنده خدمات محلی گزارش بدهد که می‌تواند خدمات اینترنت پرسرعت را «بدون تخصیص منابع بسیار زیاد» به فردی ارائه کند، کمیسیون ارتباطات فدرال نتیجه می‌گیرد که آن فرد به اینترنت پرسرعت دسترسی دارد. اما بسیاری از این‌گونه شرکت‌ها در عمل این خدمات را ارائه نمی‌کنند. مثل این است که رستورانی محلی بگوید اگر بخواهد می‌تواند به فردی ناهار رایگان بدهد و شما فرض کنید آن فرد به ناهار رایگان دسترسی دارد. در حالی که بیان این موضوع از سوی آن رستوران به این معنی نیست که این کار را انجام می‌دهد.

در واقع سایر داده‌ها تصویر بسیار متفاوتی از کشور ترسیم می‌کنند. به‌عنوان مثال مرکز تحقیقات «پیو» (Pew Research Center) از سال ۲۰۰۰ با نظرسنجی‌های منظم استفاده از اینترنت را بررسی و پیگیری کرده است. طبق آخرین داده‌های این مرکز ۳۵ درصد از آمریکایی‌ها یا تقریباً ۱۱۳ میلیون نفر گزارش داده‌اند که در خانه از اینترنت پرسرعت استفاده نمی‌کنند. حتی داده‌های کمیسیون ارتباطات فدرال نیز نشان می‌دهد که ۴۶ درصد از خانوارهای آمریکایی اشتراک خدمات اینترنت پرسرعت ندارند.

هرچند دسترسی به اینترنت پرسرعت با استفاده از آن فرق دارد، اما تفاوت بین ارقام آن‌قدر زیاد است که این تردید به وجود می‌آید که احتمالاً یکی از این ارقام اشتباه است. از تیم علوم داده خودمان خواستیم که بررسی مفصل‌تری را بر اساس منابع داده عمومی و مایکروسافت انجام دهد. تحقیقات آنها نشان داد که آمار پیو در مقایسه با برآورد

کمیسیون ارتباطات فدرال، به ارقام واقعی بسیار نزدیک‌تر است. اما علاوه بر این به نتیجه اجتناب‌ناپذیری می‌رسیم؛ اینکه در حال حاضر هیچ برآورد کاملاً دقیقی از دسترسی به اینترنت پرسرعت در هیچ جای ایالات متحده وجود ندارد.

آیا اهمیتی دارد؟ حتماً و بسیار زیاد.

اینترنت پرسرعت به الکتریسیته قرن بیست‌ویکم تبدیل شده است. در کار، زندگی و آموزش افراد نقشی اساسی دارد. آینده پزشکی، پزشکی از راه دور است. آینده آموزش، آموزش آنلاین است و آینده کشاورزی، کشاورزی دقیق (Precision agriculture) است. حتی با آینده‌ای که در آن «رایانش لبه‌ای» بیشتری وجود دارد (منظور دستگاه‌های کوچک و قدرتمند فراگیری است که خودشان داده بیشتری را پردازش می‌کنند)، باز هم باید دسترسی پرسرعت به ابر وجود داشته باشد که مستلزم وجود اینترنت پرسرعت است.

در حال حاضر مناطق روستایی که به اینترنت پرسرعت دسترسی ندارند، هنوز در قرن بیستم زندگی می‌کنند. این را می‌توان تقریباً در همه شاخص‌های اقتصادی مشاهده کرد. تیم علوم داده ما بر این یافته دانشگاه‌ها و مؤسسات پژوهشی سراسر جهان مهر تأیید زد که بیشترین نرخ‌های بیکاری کشور اغلب مربوط به شهرستان‌هایی است که کمترین دسترسی را به اینترنت پرسرعت دارند. این یافته ارتباط تنگاتنگ دسترسی به اینترنت پرسرعت و رشد اقتصادی را برجسته می‌کند.

وقتی به رهبران کسب‌وکارها می‌گویید ممکن است کجا فعالیت‌هایشان را گسترش دهند و شغل جدید ایجاد کنند، تقریباً بلافاصله این شرط مطرح می‌شود. اینکه از آنها بخواهید در جایی بدون اینترنت پرسرعت ساختمان جدیدی افتتاح کنند، مانند این است که بخواهید در مرکز بیابان موهاوی کسب‌وکاری ایجاد کنند. در دنیای وابسته به دسترسی پرسرعت به داده، منطقه‌ای بدون اینترنت پرسرعت، در واقع بیابان ارتباطات است.

رکود در رشد اشتغال روی تمام بخش‌های جامعه محلی تأثیر می‌گذارد. تعجبی نداشت که در نوامبر ۲۰۱۶، بعد از انتخابات ریاست‌جمهوری ایالات متحده متوجه شدیم که جوامع روستایی احساس می‌کردند فراموش شده‌اند. از دید بسیاری از مردم این مناطق، رفاه اقتصادی کشور در مرز مناطق شهری و حومه شهری متوقف شده بود.

مناطق روستایی سراسر کشور مثل شهرستان فری به انتخاب فردی پوپولیست برای مسند ریاست‌جمهوری کمک کرده بودند. سفرمان را از شهرستان کینگ شروع کرده بودیم که سیاتل در آن قرار دارد و فقط ۲۲ درصد به دونالد ترامپ رأی داده بودند. در مقابل در شهرستان فری فقط ۳۰ درصد به هیلاری کلینتون رأی داده بودند. این دو شهرستان از لحاظ گرایش‌های سیاسی کاملاً معکوس یکدیگر هستند. تقسیم یک روز کاری در این دو منطقه فرصت خوبی فراهم کرد تا درک شفاف‌تری از ملتی به دست آوریم که دچار تفرقه و دودستگی شده است.

این مسئله همچنین دست‌کم بخشی از مسیری را نشان داد که باید طی کنیم تا آینده‌ای روشن‌تر برای مناطق روستایی بسازیم.

مرکز امور روستایی (The Center for Rural Affairs) این چالش را کاملاً لمس کرده است. این مرکز که سه دفتر در آیووا و نبراسکا دارد، با لحن رک و بی‌ریای مردم مناطق مرکزی کشور حرف می‌زند. این گروه می‌گوید: «ما بدون شرمندگی روستایی هستیم و از خانواده‌های کشاورزی و دامداری کوچک، صاحبان کسب‌وکارهای جدید و جوامع روستایی پشتیبانی می‌کنیم.»

از قرار معلوم مرکز امور روستایی جزئیات و آماری دارد که توجیهی اقتصادی برای اینترنت پرسرعت ارائه می‌کنند. گزارش سال ۲۰۱۸ این مرکز با عنوان «نقشه راه رفاه» (Map to Prosperity) نشان می‌دهد که به ازای هر هزار مشترک جدید اینترنت پرسرعت، ۸۰ شغل جدید ایجاد می‌شود. افزایش چهار مگابایت بر ثانیه‌ای سرعت اینترنت خانگی باعث افزایش ۲۱۰۰ دلاری درآمد سالانه خانوار می‌شود و کارجویان از طریق جست‌وجوی آنلاین ۲۵ درصد سریع‌تر از رویکردهای قدیمی کار پیدا می‌کنند.

وضعیت ناراحت‌کننده کنونی اینترنت پرسرعت روستایی در آمریکا چند دلیل دارد؛ اولین و مهم‌ترین دلیل هزینه زیاد نصب زیرساخت مرسوم اینترنت پرسرعت و جایگزین‌های آن است. برآوردهای صنعت نشان می‌دهد که نصب کابل فیبر نوری (معیار مرسوم برای ارائه خدمات اینترنت پرسرعت) می‌تواند ۳۰ هزار دلار در هر مایل هزینه داشته باشد. در نتیجه ارائه اینترنت پرسرعت کافی به بخش‌های دورافتاده کشور میلیاردها دلار هزینه دارد؛ هزینه‌ای که بخش خصوصی تاکنون تمایلی به پرداخت

آن نداشته است. با این حال مکانیسم خدمات فراگیر و برنامه‌های موروثی کمیسیون ارتباطات فدرال هشت‌برابر بودجه‌ای را که از طریق صندوق پویایی (Mobility Fund) و برنامه‌های موروثی به اپراتورهای بی‌سیم ارائه می‌دهد، به اپراتورهای تلفن ثابت اختصاص می‌دهد.

مسئله دوم این است که تا همین اواخر روند توسعه راهکارهای جایگزین کابل فیبر نوری آهسته و نامتعادل بود. هرچند فناوری‌های مخابراتی موبایلی مثل اینترنت نسل چهارم از طریق تلفن‌های هوشمند و سایر دستگاه‌های موبایل به مشتریان سرعتی مشابه اینترنت پرسرعت ارائه داده‌اند، اما این فناوری بیشتر برای مناطقی با تراکم جمعیت زیاد مناسب است. اینترنت پرسرعت ماهواره‌ای می‌تواند راه‌حل مناسبی برای مناطق بسیار کم‌تراکم باشد، اما اغلب دچار مشکلاتی مثل تأخیر زیاد، پهنای باند ناکافی و هزینه بالای داده است.

مسئله سوم این است که عدم قطعیت رگولاتوری در چالش‌های ارائه اینترنت پرسرعت به مناطق روستایی آمریکا مؤثر بوده است. برای مثال ارائه‌دهندگانی که می‌خواهند حق عبور را کسب کنند (که برای تأسیسات شبکه حیاتی است)، اغلب با قوانین اعطای مجوز فدرال، ایالتی و محلی سردرگم‌کننده‌ای روبه‌رو می‌شوند که زمان و هزینه پروژه‌ها را افزایش می‌دهند.

مسئله آخر وجود این نگاه است که تقاضای کم برای اینترنت پرسرعت در مناطق روستایی سرمایه‌گذاری خصوصی را توجیه‌ناپذیر می‌کند. اگر پیشرفت مستلزم کسب بازده از سرمایه‌گذاری ۳۰ هزار دلاری به ازای هر مایل کابل فیبر نوری باشد، چنین نگاهی درست است، اما این نگاه نکته مهمی را نادیده می‌گیرد. تقاضای روستایی واقعاً وجود دارد و بازار می‌تواند با رویکردی کم‌هزینه‌تر به این تقاضا پاسخ بدهد.

اینجا محل تلاقی تاریخ و فناوری است که بینش مهمی برای آینده دارد.

تاریخ نشان می‌دهد که همیشه ورود فناوری‌های سیمی مثل تلویزیون کابلی، برق و تلفن ثابت به مناطق روستایی بسیار بیشتر از فناوری‌های بی‌سیم مثل رادیو، تلویزیون و تلفن موبایل طول می‌کشد. ۴۰ سال طول کشید تا تلفن ثابت به نرخ نفوذ ۹۰ درصدی برسد، در حالی که موبایل فقط در یک دهه به این رقم رسید. هیچ‌وقت در مورد نیاز به حل

مسئله شکاف رادیو یا تلویزیون نمی‌شنویم؛ این دستگاه‌های بی‌سیم که برای کار کردن کافی بود به فرکانس درست متصل شوند، به‌سرعت پذیرفته شدند و به‌راحتی نصب و راه‌اندازی می‌شدند. درسی که از این موضوع می‌توان گرفت، مشهود است. اگر در مورد اینترنت پرسرعت بتوانیم به جای کابل‌های فیبر نوری از فناوری بی‌سیم استفاده کنیم، می‌توانیم پوشش اینترنت پرسرعت را بیشتر و سریع‌تر و با هزینه کمتر، نه فقط در ایالات متحده؛ بلکه در تمام دنیا گسترش دهیم.

در طول دهه گذشته فناوری بی‌سیم جدیدی برای پر کردن این شکاف ظهور کرده است. این فناوری فضاهای سفید فرکانس تلویزیونی (TV white spaces) خوانده می‌شود و از کانال‌های خالی در باندی از فرکانس تلویزیونی استفاده می‌کند که سیگنال‌ها مسافت زیادی را طی می‌کنند. اگر پیش از ظهور تلویزیون کابلی بزرگ شده باشید، برای تماشای تلویزیون یا از آنتنی بزرگ روی سقف استفاده می‌کردید یا زمانی را صرف تنظیم «آنتن‌های داخلی» تلویزیون می‌کردید تا سیگنال VHF یا UHF را دریافت کنید؛ این سینگال‌های زمینی می‌توانند مایل‌ها مسافت را از دور تپه‌ها، میان درخت‌ها و دیوار خانه‌های ما طی کنند. در حال حاضر بسیاری از کانال‌های VHF و UHF بی‌استفاده هستند و می‌توان آنها را به اهداف دیگری اختصاص داد. با فناوری پایگاه داده، آنتن‌ها و دستگاه‌های پایانه تازه توسعه‌یافته می‌توانیم با اتصال برج فضای سفید فرکانس تلویزیونی به یک کابل فیبر نوری از این فضای خالی استفاده کنیم و این سیگنال‌های بی‌سیم را به شهرها، خانه‌ها و مزرعه‌هایی در فاصله بیش از ۱۰ مایلی ارسال کنیم.

به‌طور اتفاقی نقش مؤثری در اولین تجربه عملی با فناوری فضاهای سفید فرکانس تلویزیونی در آفریقا داشتم. سال ۲۰۱۱ در همایش سازمان ملل در نایروبی، پایتخت کنیا بودیم و برای شرکت‌کنندگان امکان استفاده از ایکس‌باکس با اینترنت پرسرعت تأمین‌شده از طریق سیگنال‌های فضاهای سفید فرکانس تلویزیونی را فراهم کردیم که حدود یک مایل را طی کرده بودند. مسئولان دولت کنیا از اولین افرادی بودند که پتانسیل این فناوری را درک کردند و ما به همکاری با آنها و چند دولت دیگر در این زمینه ادامه دادیم. سال ۲۰۱۵ به روستایی کوچک در کنیا و روی خط استوا رفتم که فقط ۱۲ درصد از جمعیتش به برق دسترسی داشتند، اما با استارت‌آپی مشارکت کرده بودیم تا با استفاده

از فضاهای سفید فرکانس تلویزیونی به افراد اینترنت پرسرعت ارائه کنیم. با معلمانی دیدار کردم که از افزایش نمرات دانش‌آموزان و ایجاد شغل‌هایی برای افراد می‌گفتند که تا همین یک سال پیش در این منطقه غیرقابل تصور بودند.

سال ۲۰۱۷ به این جمع‌بندی رسیدیم که فناوری فضاهای سفید فرکانس تلویزیونی برای پذیرش گسترده‌تر و در مقیاس بیشتر از جمله در مناطق روستایی ایالات متحده آماده است. بعد از چند ماه برنامه‌ریزی، در ماه جولای در هتل ویلارد اینترکانتیننتال (Willard InterContinental) در واشنگتن دی‌سی از طرح باند هوایی روستایی مایکروسافت (Microsoft Rural Airband Initiative) رونمایی کردیم.

متعهد شدیم در عرض پنج سال یعنی تا ۴ جولای ۲۰۲۲ برای دو میلیون آمریکایی دیگر در مناطق روستایی پوشش اینترنت پرسرعت ایجاد کنیم. قرار نبود به کسب‌وکار مخابرات وارد شویم، اما با ارائه‌دهندگان خدمات مخابراتی مشارکت می‌کردیم و ترکیبی از فناوری‌های بی‌سیم شامل دستگاه‌های بی‌سیم جدیدی را مستقر می‌کردیم که از فضاهای سفید طیف فرکانس تلویزیونی استفاده می‌کردند. متعهد شدیم که تا پنج سال همه سودهای به‌دست‌آمده از این تلاش‌ها را به سرمایه‌گذاری مجدد برای گسترش بیشتر پوشش اختصاص دهیم. خواستار سیاست‌گذاری ملی مناسب برای افزایش دسترسی به اینترنت پرسرعت در مناطق روستایی شدیم و اعلام کردیم که در عرض ۱۲ ماه ۱۲ پروژه را در ۱۲ ایالت راه‌اندازی خواهیم کرد و سپس آن پروژه‌ها را گسترش می‌دهیم.

انتخاب هتل ویلارد بی‌دلیل نبود. علاوه بر اینکه می‌خواستیم توجه قانون‌گذاران فدرال را جلب کنیم، این مکان را برای اشاره به رویداد ویژه‌ای انتخاب کردیم که در ۷ مارس ۱۹۱۶ در همین مکان اتفاق افتاده بود. الکساندر گراهام بل، رهبران بخش تلفن و تلگراف آمریکا و شخصیت‌های برجسته‌ای از سراسر کشور برای ضیافت مجللی در این هتل بزرگ جمع شده بودند که انجمن «نشنال جئوگرافیک» به‌منظور بزرگداشت چهلمین سالگرد اختراع تلفن توسط گراهام بل برگزار کرده بود. البته رهبران AT&T می‌خواستند کاری بیشتر از صرف بزرگداشت انجام دهند. بنابراین برنامه‌ای ترتیب داده بودند تا از این رویداد برای ترسیم چشم‌اندازی جسورانه برای آینده استفاده کنند.

«تئودور ویل»، رئیس AT&T می‌خواست با چشم‌انداز بردن تلفن‌های راه دور به

گوشه‌گوشه کشور حتی در دورافتاده‌ترین نقاط الهام‌بخش کشور باشد. مردم آمریکا با اشتیاق از این هدف استقبال کردند. تا آن روز افراد فکر می‌کردند خدمات تلفن تجاری به خطوط بین‌شهری بزرگ‌ترین شهرهای کشور و چند تلفن‌خانه کوچک دیگر محدود است. ویل در آن میهمانی از جماعت حاضر پرسید: «آیا امکان ندارد زمانی برسد که هر کسی در هر جایی بتواند بلافاصله با هر کسی در هر جای دیگری از دنیا ارتباط برقرار کند؟»

همان‌طور که امروز می‌دانیم این رویا به واقعیت تبدیل شد. در واقع کشور ما در گذشته بر این چالش فائق آمده است و اطمینان داشتیم باز هم می‌تواند این کار را انجام دهد.

هرچند برنامه باند هوایی را به ارائه اینترنت پرسرعت به دو میلیون نفر اختصاص دادیم، اما به‌وضوح می‌دانستیم که هدف واقعی‌مان بسیار بزرگ‌تر است. می‌خواستیم از فناوری برای بهره‌برداری از قدرت اقتصاد آزاد استفاده کنیم و شرایط جدیدی را در بازار برقرار کنیم که شکاف اینترنت پرسرعت مناطق روستایی را با سرعت بیشتری برای همه پر کند. در این راستا باید بخشی از منابع مالی‌مان را برای سرعت‌بخشیدن به نوآوری سخت‌افزاری سازندگان تراشه و تولیدکنندگان دستگاه‌های پایانه‌ای استفاده می‌کردیم که این سیگنال‌ها را به خانه‌ها، دفاتر کار و مزرعه‌ها می‌بردند. بعد این سیگنال‌ها در آن نقاط به سیگنال‌های وای‌فای تبدیل می‌شدند. همچنین باید ارائه‌دهندگان کوچک خدمات مخابراتی را در کنسرسیوم خریداران دور هم جمع می‌کردیم تا این دستگاه‌ها را بخرند و تخفیفات ناشی از خرید پرحجمی را به دست آورند که فقط در دسترس خریداران بزرگ‌تر است.

فهمیدیم می‌توانیم هدفمندتر و سریع‌تر از هر دولتی عمل کنیم و زودتر از پیش‌بینی‌هایمان پیشرفت کنیم. در ۱۷ ماه بعد از رونمایی از طرح باند هوایی، در ۱۶ ایالت قراردادهای مشارکت تجاری امضا کردیم. این مشارکت‌ها پوشش اینترنت پرسرعت را برای بیش از یک میلیون نفری فراهم می‌کردند که تا پیش از شروع این طرح به اینترنت پرسرعت دسترسی نداشتند. پیشرفت آن‌قدر سریع بود که در انتهای سال ۲۰۱۸ اهداف‌مان را ارتقا دادیم و اعلام کردیم پوشش را تا سال ۲۰۲۲ نه برای دو میلیون؛ بلکه برای سه میلیون نفر فراهم می‌کنیم. اگر گام‌های دیگری هم برداشته می‌شد، باز هم امکان

افزایش سرعت پیشرفت این فناوری وجود داشت.

شاید تعجب‌برانگیز نبود که بیانیه‌های مایکروسافت توجه زیادی را به خود جلب کنند. برنامه‌های گفت‌وگومحور رادیو و سرمقاله‌های روزنامه‌ها در مناطق روستایی سراسر کشور پشتیبانی زیادی از ما کردند. تماس‌های فراوانی از فرمانداران و اعضای کنگره دریافت می‌کردیم که می‌خواستند ایالت‌ها و ناحیه‌هایشان را به فهرست‌مان اضافه کنیم.

یکی از نکات کلیدی در اجرای این استراتژی استفاده از فناوری مناسب در مکان مناسب است. انتظار داریم فناوری فضاهای سفید فرکانس تلویزیونی و سایر فناوری‌های بی‌سیم ثابت در نهایت بهترین رویکرد برای دسترسی به تقریباً ۸۰ درصد از جمعیت روستایی کمتر برخوردار باشند؛ به‌ویژه در مناطقی که تراکم جمعیت بین ۲ تا ۲۰۰ نفر در هر مایل مربع است. اما در سایر مناطق به فناوری‌های دیگر از جمله فناوری‌های کابلی و ماهواره‌ای نیاز داریم. معتقدیم این رویکرد چندگانه می‌تواند سرمایه اولیه و هزینه‌های عملیاتی کشور را در مقایسه با صرفاً استفاده از کابل‌های فیبر نوری حدود ۸۰ درصد و در مقایسه با استفاده از فناوری بی‌سیم ثابت LTE تقریباً ۵۰ درصد کاهش دهد.

گاهی اوقات که افراد می‌شنوند در طرح باند هوایی به جای کسب سود، درآمد حاصل از مشارکت‌های مخابراتی دوباره سرمایه‌گذاری می‌شود، با شگفتی و ابهام به ما می‌نگرند. می‌پرسند چرا شرکتی باید پولش را این‌طور خرج کند؟ همان‌طور که گفتیم تمام بخش فناوری و از جمله مایکروسافت از اتصال افراد بیشتر به ابر بهره می‌برند. علاوه بر این در حال ساخت اپلیکیشن‌هایی هستیم که افراد در مناطق روستایی می‌توانند بعد از اتصال به اینترنت پرسرعت از آنها استفاده کنند. یکی از اپلیکیشن‌های محبوب‌مان از این مجموعه «فارم‌بیتس» (FarmBeats) است که از فضاهای سفید فرکانس تلویزیونی برای اتصال حسگرهای کوچک در زمین‌های کشاورزی استفاده می‌کند تا امکان بهره‌برداری از روش‌های دقیقی را فراهم کند که بهره‌وری کشاورزی را افزایش و فاضلاب مضر برای محیط زیست را کاهش می‌دهند. اگر بتوانیم راه‌های جدیدی را برای تلفیق کار خیر با عملکرد خوب پیدا کنیم، فرصت‌هایی برای سرمایه‌گذاری‌های بیشتر فراهم می‌کنیم که می‌تواند دوباره موتور محرک رشد اقتصادی را در مناطق روستایی روشن کند.

با این حال حتی با این شرایط بازار باز هم باید نقش مهم بخش عمومی در پر کردن

شکاف اینترنت پرسرعت را به رسمیت بشناسیم. اول از همه به قطعیت رگولاتوری نیاز داریم تا مطمئن شویم فضاهای سفید طیف فرکانس تلویزیونی در دسترس می‌مانند. هرچند بخشی از باند تلویزیونی به مزایده گذاشته و مجوز استفاده از آن به اپراتورهای موبایل داده شده است، اما باید اطمینان حاصل کنیم که در همه بازارها دست‌کم دو کانال قابل استفاده و در مناطق روستایی تعداد بیشتری کانال برای فناوری فضاهای سفید فرکانس تلویزیونی در دسترس عموم قرار می‌گیرد. خوشبختانه بخش زیادی از کارهای مورد نیاز در این زمینه انجام شده و همچنان ادامه دارد.

همچنین در تأمین مالی بخش عمومی باید به نحوی عمل کنیم که هر چه بهتر بر فناوری‌های جدید متمرکز باشیم و صرفاً به‌دنبال کشیدن کابل‌های فیبر نوری گران‌قیمت نباشیم. تأمین مالی دولتی می‌تواند بیشترین تأثیرگذاری را با کمترین هزینه داشته باشد، به شرط اینکه شامل فرصتی برای تأمین مالی هدفمند باشد تا دولت متناسب با سرمایه‌گذاری‌های شرکت‌های مخابراتی در کارها مشارکت کند. این منابع مالی به این فعالیت‌ها سرعت می‌بخشند و به نفوذ به بخش‌هایی از کشور کمک می‌کنند که بخش خصوصی ممکن است به‌تنهایی نتواند با سرعت مناسبی به آنها نفوذ کند.

در نهایت به نهضتی ملی نیاز داریم که بر شکاف اینترنت پرسرعت متمرکز شود و آن را پر کند. باید درک کنیم که درست مانند برق، در کشوری که دسترسی برابر به اینترنت پرسرعت وجود ندارد، از اتحاد و یکپارچگی مردم کاسته می‌شد. در واقع می‌توان از اقدامات کشور در گسترش برق به خارج از مراکز شهری و سراسر کشور درس‌های زیادی گرفت. فرانکلین دی روزولت که با گرفتاری‌های کشاورزان روستایی همدردی می‌کرد، در سال ۱۹۳۵ متعهد شد که برق را به همه نقاط کشور برساند. متوجه شده بود که کشور نمی‌تواند به عصر فناوری جدیدی وارد شود، اما مناطق روستایی را در همان عصر گذشته رها کند.

روزولت در بخشی از برنامه‌اش برای خارج‌کردن ایالات متحده از شرایط رکود بزرگ، فرمانی صادر کرد و بر اساس آن اداره برق‌رسانی روستایی را به‌عنوان بخشی از برنامه «نیو دیل» (New Deal) ایجاد کرد. این اداره به جوامع کشاورزی کمک می‌کرد تعاونی‌های برق محلی تشکیل دهند (این مفهوم برای کشاورزانی که همان زمان هم بذر و تجهیزات

را از طریق تعاونی‌ها تهیه می‌کردند، مفهوم آشنایی بود) تا هزینه احداث مایل‌های آخر شبکه برق را پرداخت کنند. وام‌های کم‌بهره اداره برق‌رسانی روستایی هزینه ساخت سیستم‌های برق محلی را تأمین می‌کردند. تعاونی‌ها صاحب این سیستم‌ها بودند و بر آنها نظارت می‌کردند.

این برنامه در واشنگتن‌دی‌سی شروع شد، اما موفقیت آن مستلزم وجود افرادی بود که امکان استفاده از برق را به تمام نقاط کشور ببرند. آن زمان هم مانند اکنون افرادی که می‌خواستند کشور را تغییر دهند، باید به ایالت آیووا سفر می‌کردند، البته این کار را نه مثل اکنون برای نامزد شدن در انتخابات ریاست‌جمهوری (اشاره به این موضوع دارد که آیووا اولین ایالتی است که انتخابات مقدماتی ریاست‌جمهوری در آن برگزار می‌شود و از این جهت اهمیت دارد)، بلکه برای گسترش فرصت فناوری جدید باید انجام می‌دادند.

بیش از ۸۰ سال پیش کشاورزان درمانده شهرستان «جونز» (Jones) در ایالت آیووا مشکلی مشابه مشکل دوستان ما در رستوران ناتی پاین داشتند. اما در تابستان ۱۹۳۸ امید در افق دید آنها ظاهر شد. ساکنان مناطق روستایی آیووا برای افتتاحیه سیرکی در شهر کوچک «آنوموسا» (Anamosa) در شرق این ایالت جمع شده بودند؛ تفریح خوشایندی بعد از روزی سخت و تقریباً ۱۰ سال تنگنای اقتصادی.

این نمایش دلقک، بندباز یا حیوان دست‌آموز نداشت، اما سیرک برقی سیار اداره برق‌رسانی روستایی مایه شادی و لذت مخاطبان شد. در این نمایش «لوئیزن ممر» (Louisan Mamer)، بانوی اول اداره برق‌رسانی روستایی، عجایب عصر مدرن مثل لامپ، اجاق‌گاز، یخچال، ماشین جوجه‌کشی و دستگاه شیردوش را به نمایش می‌گذاشت.

لوئیزن با فشردن یک دکمه یا چرخاندن یک دستگیره اتاق‌ها را روشن می‌کرد، لباس‌ها را می‌شست و اتو می‌کرد، موسیقی می‌نواخت، گردوخاک را می‌زدود و مواد غذایی را سرد و منجمد می‌کرد. در دورانی که آشپزی بدون برق کاری بسیار پرزحمت بود، کار کردن در آشپزخانه را آسان جلوه می‌داد. وقتی روی اجاق‌گاز «وستینگ‌هاوس» تاس‌کباب، بوقلمون کبابی و پیراشکی آماده کرد، شگفتی جمعیت را برانگیخت. نمایش را با برگزاری مسابقه آشپزی هیجان‌انگیزی بین دو مرد از تماشاچیان به پایان رساند.

وقتی لوئیزن به اداره برق‌رسانی روستایی پیوست، ۹۰ درصد از آمریکایی‌های شهرنشین و فقط ۱۰ درصد از روستانشینان برق داشتند. چنین شکافی در سایر کشورهای غربی مشاهده نمی‌شد. در آن زمان خانه‌ها و انبارهای تقریباً ۹۵ درصد از مناطق روستایی فرانسه به برق دسترسی داشتند.

شرکت‌های برق خصوصی ایالات متحده مانند شرکت‌های مخابراتی بزرگ امروز شهرهای کنار بزرگراه‌های اصلی را به شبکه متصل کرده بودند، اما به مناطق کم‌جمعیت‌تر که بیشتر مزرعه بودند، توجهی نکرده بودند. این شرکت‌ها به این نتیجه رسیده بودند که نمی‌توانند هزینه گسترش خطوط‌شان به راه‌های فرعی دورافتاده مناطق روستایی آمریکا را جبران کنند. علاوه بر این شرکت‌های برق حدس می‌زدند حتی اگر این مناطق روستایی به شبکه متصل شوند، باز هم کشاورزان آمریکایی که از رکود بزرگ آسیب زیادی دیده بودند، به هیچ‌وجه نمی‌توانند هزینه خدمات ماهانه را پرداخت کنند.

نبود برق نه‌تنها آسایش و راحتی عصر مدرن را از کشاورزان دریغ کرده بود؛ بلکه آنها را از مزایای بهبود شرایط اقتصادی کشور هم محروم کرده بود. افرادی که می‌خواستند با اقتصاد جدید کشور ارتباط برقرار کنند، باید هزینه‌های گزافی به شرکت‌های برق خصوصی پرداخت می‌کردند تا خطوط برق را تا زمین آنها بکشند. در پنسیلوانیا، به «جان ارل جورج» (John Earl George) گفته بودند باید به شرکت برق پنسیلوانیا ۴۷۱ دلار پرداخت کند تا شبکه برق را ۱۱۰۰ فوت بیشتر تا خانه‌اش در منطقه روستایی شهرستان «دری» (Derry) گسترش دهند. در سال ۱۹۳۹ در مناطق روستایی پنسیلوانیا ۴۷۱ دلار معادل میانگین دستمزد سالانه افراد بود.

در نهایت اداره برق‌رسانی روستایی از ۴۱۷ تعاونی در سراسر کشور پشتیبانی کرد که به ۲۸۸ هزار خانوار خدمت‌رسانی می‌کردند. همچنین لوئیزن و سیرک برقی را به توری چهارساله در سراسر کشور فرستاد تا به کشاورزان آموزش بدهند چطور بیشترین بهره را از این فناوری جدید ببرند. تعاونی برق روستایی دره «ماکوئوکتا» (Maquoketa) در آیووا اولین تعاونی‌ای بود که از این سیرک میزبانی کرد. این سیرک تا سال چهارم به جایی رسید که جمعیت‌های بیش از ۱۰ هزار نفری را از مناطق روستایی جذب می‌کرد.

تا انتهای دهه ۱۹۳۰ یک‌چهارم خانوارها به شبکه برق متصل شدند. جان ارل جورج

در پنسیلوانیا برای پیوستن به شرکت تعاونی برق روستایی مرکزی جنوب غربی، حق عضویت پنج دلاری پرداخت کرد. اولین قبض برقش فقط ۳٫۴۰ دلار بود. وقتی رئیس‌جمهور روزولت در سال ۱۹۴۵ درگذشت، ۹ مزرعه از هر ۱۰ مزرعه مناطق روستایی آمریکا دارای برق بودند. ایالات متحده از طریق مشارکت‌های عمومی و خصوصی، پشتکار و کمی ابتکار توانسته بود در عرض ۱۰ سال شکاف برق روستایی را ۸۰ درصد کاهش دهد و همه این موفقیت‌ها همزمان با بهبود اقتصادی دشوار و جنگ جهانی دوم به دست آمدند.

از نگاه لوئیزن گسترش فناوری مدرن به مزارع نه‌فقط ضرورتی اقتصادی؛ بلکه آرمانی اجتماعی بود. او که در مناطق روستایی ایالت ایلینوی بدون آب لوله‌کشی و برق بزرگ شده بود، بی‌واسطه زندگی طاقت‌فرسای روستایی را درک می‌کرد. عدم دسترسی به برق نه‌فقط به معیشت خانواده‌های روستایی؛ بلکه به زندگی‌شان نیز آسیب می‌زد. در مصاحبه‌ای در هشتادوچندسالگی گفته بود: «فکر می‌کنم شاید تقریباً در همه خانه‌های روستایی این اعتقاد وجود داشت که بار سنگین خانه‌داری در مناطق روستایی باید سبک شود. بار سنگین دستی‌بودن همه کارها و به دنیا آوردن فرزندان زیاد باعث می‌شد زنان بسیار کمتر عمر کنند.»

داستان او بار دیگر نشان می‌دهد که باید بپذیریم گسترش فناوری جدید صرفاً ضرورتی اقتصادی نیست و باید با آن به‌عنوان آرمانی اجتماعی برخورد کرد.

وقتی شهرستان فری در ایالت واشنگتن را ترک می‌کردیم، در مورد چیزهایی که دیده و فهمیده بودیم، حرف‌های زیادی داشتیم. بیش از همه در مورد این سؤال حرف زدیم که آیا می‌توانیم کار معنی‌داری انجام دهیم؟

نمی‌خواستیم ساکنان روستا را با وعده‌های توخالی ترک کنیم؛ کاری که قبلاً افراد زیادی انجام داده بودند. می‌دانستیم طرح باند هوایی ما می‌تواند کمک کند فناوری قرن بیست‌ویکمی را در دسترس افرادی مثل البرت کونتز و همسایگانش در شهرستان فری قرار دهیم. از «پل گارنت» (Paul Garnett)، مدیر طرح باند هوایی مایکروسافت خواستیم شریک مناسب را برای این کار پیدا کند.

پل و تیمش موفق شدند و تا انتهای سال با «دکلریشن نتورکس گروپ» (Declaration

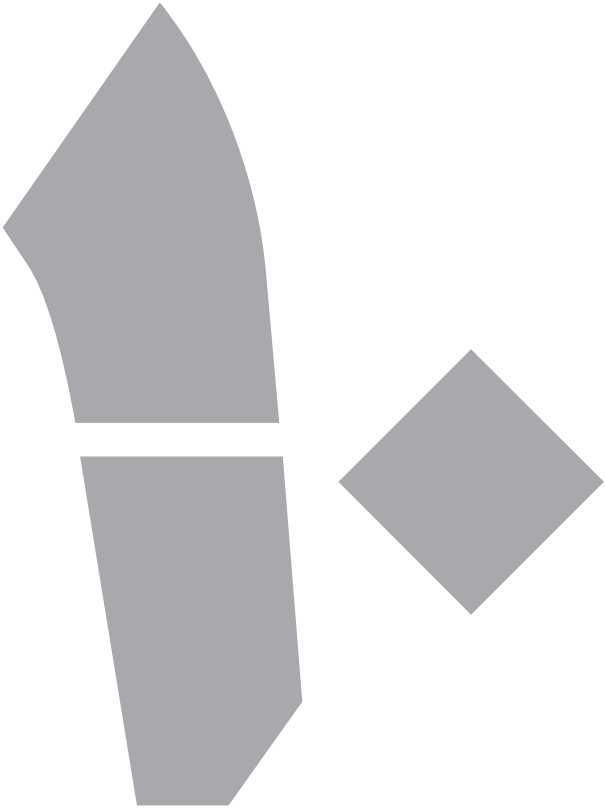
Networks Group) به توافق رسیدیم تا در طول سه سال آینده با استفاده از فضاهای سفید فرکانس تلویزیونی و فناوری‌های بی‌سیم دیگر دسترسی به اینترنت پرسرعت را برای ۴۷ هزار نفر در شرق شهرستان فری و شهرستان استیونز (Stevens) در همسایگی آن فراهم کند. در ابتدای مسیر بودیم، ولی واقعاً حرکت را شروع کرده بودیم.

در تابستان ۲۰۱۹، تقریباً یک سال بعد از اولین بازدیدمان از شهرستان فری به ریپابلیک برگشتیم تا پیشرفت مشارکت با دکلریشن نتورکس و مشارکت‌های جدید دیگر را بررسی کنیم. این بار خودمان مسیر را می‌دانستیم.

آن شب پیش از خروج از شهر در خیابان اصلی جلوی کافه ریپابلیک متوقف شدیم. اینجا محل اجتماعات شهر هم محسوب می‌شود. ورودی کافه در خیلی بزرگی دارد. وقتی آفتاب می‌تابد، در کاملاً باز می‌شود تا میز و صندلی‌ها به بیرون و پیاده‌رو آورده شوند.

سال گذشته که از شهر بازدید کرده بودیم، یکی از صاحبان کافه کار پیشخدمتی را انجام می‌داد. وقتی شنید از مایکروسافت آمده‌ایم، تعجب کرد. گفت‌وگو با او فرصت و چالشی را پیش روی ما قرار داد. متفکرانه گفته بود: «از نظر من هیچ شکی وجود ندارد که در پنج سال آینده وضعیت دسترسی به اینترنت در این منطقه کاملاً با الان فرق خواهد کرد. افراد باهوش زیادی در این منطقه زندگی می‌کنند. وقتی دسترسی بهتری به اینترنت داشته باشند، متوجه همه کارهای متنوعی می‌شوند که می‌توانند در زندگی‌شان انجام دهند.»

این چالشی بود که تا چند ماه دغدغه هر روز صبح‌مان بود و چالشی است که باید دغدغه هر روز صبح همه کشور در سال‌های پیش رو باشد.



فصل دهم

خلاء استعداد

ضلع سرمایه انسانی فناوری

بیشتر افراد فناوری را کسب‌وکار محصول می‌دانند. محصولات صنعت فناوری توجه مردم را جلب می‌کنند و در شیوه زندگی‌شان تأثیر می‌گذارند. اما در دنیایی که محصولات پرفروش امروز خاطرات فردا هستند، هر شرکت فناوری فقط به اندازه محصول بعدی‌اش خوب است و محصول بعدی‌اش فقط به اندازه افرادی که آن را می‌سازند خوب است. خلاصه فناوری اساساً کسب‌وکار افراد است.

انقلاب صنعتی چهارم با تحول دیجیتال تعریف می‌شود. هر شرکتی تا اندازه‌ای در حال تبدیل‌شدن به یک شرکت فناوری است. همین موضوع در مورد دولت‌ها و گروه‌های غیرانتفاعی هم درست است. در نتیجه ضلع سرمایه انسانی فناوری برای همه بخش‌های اقتصاد مهم شده است.

پیامدهای این مسئله چندوجهی و عمیق است. شرکت‌ها برای موفقیت در عصر دیجیتال باید برترین استعدادها را از داخل کشورشان و هر جای دیگری جذب کنند. جوامع محلی باید اطمینان حاصل کنند که شهروندان‌شان به مهارت‌های فناوری‌محور جدید مجهز شده‌اند. کشورها باید سیاست‌هایی را در زمینه مهاجرت وضع کنند که استعدادهای برتر جهان را در دسترس‌شان قرار دهد. کارفرمایان باید نیروی کاری پرورش دهند که تنوع مشتریان و شهروندانی را منعکس و درک کند که به آن خدمات ارائه می‌دهند. بدین منظور باید علاوه بر کنار هم قرار دادن افراد متنوع‌تر، فرهنگ و فرایندهایی ایجاد کنید که به کارمندان این امکان را بدهد که پیوسته از یکدیگر یاد بگیرند. دست‌آخر اینکه با توجه به افزایش سرعت رشد فناوری در مراکز شهری، این مناطق باید چالش‌های ناشی از این رشد را نه‌تنها برای هر نهاد؛ بلکه برای کلیت جامعه مدیریت کنند.

شرکت‌های فناوری در همه این حوزه‌ها به پشتیبانی یک جامعه و اغلب حتی یک ملت وابسته هستند. در عین حال در همه این حوزه‌ها شرکت‌های فناوری فرصت و مسئولیت دارند که خودشان کارهای بیشتری انجام دهند؛ این چالشی دشوار شبیه مکعب روبیک است که تنها با حرکت همزمان چندین بخش حل می‌شود.

چگونه می‌توانیم به بهترین شکل ضلع سرمایه انسانی فناوری را بهبود ببخشیم؟ وقتی در سال ۲۰۱۸ به جشنواره علمی سالانه شرکت برای توسعه‌دهندگان نرم‌افزار

رفتیم، فرصت یادگیری مناسبی در این زمینه به دست آوردیم. مرکز همایش‌های مایکروسافت به «تک‌فست» (TechFest) سالانه ما تبدیل شده بود که واحد تحقیقات مایکروسافت (Microsoft Research) برگزار می‌کند.

واحد تحقیقات مایکروسافت یکی از بزرگ‌ترین سازمان‌های دنیا در زمینه پژوهش بنیادی است. به هیچ‌وجه مکانی عادی نیست؛ زیرا سازندگان فناوری گلچینی از نخبگان هستند. اما نگاه به این واحد چشم‌انداز اولیه مهمی برای دنیای فناوری فراهم می‌کند.

واحد تحقیقات مایکروسافت بیش از ۱۲۰۰ کارمند دارای مدرک دکتری دارد که ۸۰۰ نفر از آنها در حوزه علوم کامپیوتر مدرک گرفته‌اند. برای اینکه این رقم را ملموس‌تر درک کنید، باید بگویم گروه‌های علوم کامپیوتر دانشگاه‌های بزرگ معمولاً ۶۰ تا ۱۰۰ نفر را با مدرک دکتری و به‌عنوان عضو هیئت‌علمی و دانشجوی فوق دکتری استخدام می‌کنند. از لحاظ کیفیت نیز واحد تحقیقات مایکروسافت معمولاً معادل دانشگاه‌های برتر به‌شمار می‌رود. یکی از بهترین گروه‌های علوم کامپیوتر دانشگاه‌های جهان را در نظر بگیرید و آن را ۱۰ برابر کنید، به واحد تحقیقات مایکروسافت می‌رسید. مترادف امروزی مجموعه‌ای است که AT&T دهه‌ها پیش در آزمایشگاه‌های «بل» (Bell Labs) جمع‌آوری کرده بود.

تک‌فست سالانه واحد تحقیقات مانند نمایشگاهی تجاری است، اما در بیشتر موارد فقط کارمندان مایکروسافت می‌توانند در آن شرکت کنند. تیم‌های پژوهشی غرفه‌هایی ایجاد می‌کنند تا تازه‌ترین پروژه‌هایشان را به نمایش بگذارند. هدف این است که مهندسان گروه‌های مختلف شرکت پیشرفت‌ها را ببینند و با بیشترین سرعت ممکن آنها را در محصولات‌شان به کار بگیرند.

یکی از غرفه‌هایی که می‌خواستیم حتماً ببینیم، هوش مصنوعی خصوصی بود؛ پیشرفت شگرف تازه‌ای که با ایجاد توانایی فنی آموزش الگوریتم‌های هوش مصنوعی با مجموعه‌های داده‌ای که رمزنگاری‌شده می‌مانند، بهتر از حریم خصوصی افراد حفاظت می‌کند. تیم هوش مصنوعی خصوصی اطراف غرفه‌شان جمع شده بودند و با اشتیاق به پرسش‌های ما پاسخ می‌دادند. می‌شد دید که این مردان و زنان گروهی

صمیمی هستند و همدیگر را خوب می‌شناسند، اما با اتمام گفت‌وگو متوجه موضوع برجسته دیگری شدیم. این تیم هشت‌نفره اهل هفت کشور متفاوت بودند. در این تیم دو نفر از آمریکا و از هر کدام از کشورهای فنلاند، رژیم صهیونیستی، ارمنستان، هند، ایران و چین یک نفر حضور داشت. اکنون همه این هشت نفر در ناحیه سیاتل زندگی می‌کردند و با هم در ساختمان ردموند مشغول کار بودند.

این گروه پژوهشگران نماد پدیده‌ای بسیار بزرگ‌تر از خودش بود. تیمی بودند که روی یکی از بزرگ‌ترین چالش‌های امروز فناوری کار می‌کردند که نیازمند تیمی منتخب از برترین‌های جهان بود؛ تیمی که سیستم مهاجرت آمریکا به ما این امکان را داده بود تا دور هم جمع کنیم.

مسئله مهاجرت همیشه یکی از چالش‌های دشوار بخش فناوری در ایالات متحده بوده است. مهاجرت از جهتی برای رهبری آمریکا در زمینه فناوری در جهان ضروری بوده است. اگر ایالات متحده بسیاری از بهترین و بااستعدادترین افراد جهان را برای کار در دانشگاه‌های برتر یا زندگی در مراکز فناوری سراسر کشور جذب نکرده بود، امکان نداشت بتواند به رهبر جهانی فناوری اطلاعات تبدیل شود.

وقتی هنوز کشاورزی نیروی غالب اقتصاد ساحل غربی ایالات متحده بود و سیلیکون هنوز فقط شن را به یادمان می‌آورد، نقش مهاجرت در نوآوری برای ایالات متحده مهم بود. توانایی کشور در جذب آلبرت اینشتین از آلمان در اوج رکود بزرگ نقشی حیاتی در آگاه‌کردن رئیس‌جمهور فرانکلین روزولت از نیاز به ایجاد پروژه منهتن ایفا کرد. درهای باز کشور برای دانشمندان موشکی آلمان بعد از جنگ جهانی دوم در فرستادن اولین انسان به ماه حیاتی بود. ایالات متحده با کمک سرمایه‌گذاری‌های فدرال در پژوهش‌های بنیادی در دانشگاه‌های بزرگ کشور و پشتیبانی رئیس‌جمهور آیزنهاور از ریاضیات و علوم در مدارس دولتی رویکرد خود را به پژوهش، آموزش و مهاجرت تغییر داد که به دهه‌ها رهبری اقتصادی و فکری در جهان منجر شد.

سایر کشورهای دنیا به مطالعه این مدل پرداختند و بیش از پیش از آن دنباله‌روی کردند. اما آمریکایی‌ها بیش از پیش فراموش کردند که عامل موفقیت این مدل چه بود و به‌مرور پشتیبانی سیاسی از بخش‌های گوناگون آن برداشته شد.

شروع چالش‌های مهاجرت کمی بعد از آغاز قرن بیست‌ویکم، بخش فناوری را به مواجهه با این اختلافات فزاینده واداشت. جمهوری‌خواهان هرساله از ورود مهاجران بسیار ماهر پشتیبانی می‌کردند، اما از اصلاحات گسترده‌تر در سیستم مهاجرت پشتیبانی نمی‌کردند. دموکرات‌ها نیز از ورود مهاجران بسیار ماهر تنها به‌عنوان بخشی از اصلاحات گسترده‌تر در سیستم مهاجرت پشتیبانی می‌کردند. سال‌ها گفت‌وگو با رهبران هر دو حزب تقریباً همیشه با این جمع‌بندی به پایان می‌رسید که هیچ کاری انجام نخواهد شد. بعد از انتخابات ریاست‌جمهوری سال ۲۰۱۶ شرایط از این هم بدتر شد.

در دسامبر ۲۰۱۶ که با ساتیا به نیویورک پرواز می‌کردیم تا در جلسه رئیس‌جمهور منتخب با رهبران فناوری در برج ترامپ شرکت کنیم، تصمیم گرفتیم راهی برای طرح مسئله مهاجرت در مقطعی از گفت‌وگو پیدا کنیم. ساتیا در اوایل بحث به اهمیت مسئله مهاجرت در زندگی شخصی‌اش و تداوم اهمیت آن تا امروز اشاره کرد. دیگر کسی به این مسئله اشاره نکرد تا اینکه ترامپ از گروه خواست اگر مایل هستید، در مورد دیدگاه‌هایمان صحبت کنیم. در مورد جزئیات مهم این مسئله بحث کردیم. ترامپ هنگام بحث اشاره کرد که هیچ جای نگرانی نیست. گفت: «فقط آدم‌های بد باید کشور را ترک کنند. همه آدم‌های خوب می‌توانند بمانند و همچنان به کشور وارد شوند.» مگر می‌شود با چنین سخنی مخالفت کرد؟ اما کسی نمی‌دانست واقعاً منظور از این حرف چیست.

در حاشیه جلسه با اعضای ستاد جدید کاخ سفید در مورد مسائل مهاجرت و آموزش صحبت کردیم. این گفت‌وگوها کمی امیدوارکننده بود، اما فوریه ۲۰۱۷ یعنی یک ماه بعد از مراسم تحلیف ترامپ این امید بر باد رفت. رئیس‌جمهور جدید ممنوعیت کاملی بر همه افرادی وضع کرد که از هفت کشور مسلمان می‌آمدند. در نقاط مختلف کشور مردم در فرودگاه‌ها تجمع کردند تا به هدف‌گرفتن کشورها بر مبنای دین و مذهب‌شان اعتراض کنند. این ممنوعیت در مایکروسافت روی ۱۴۰ کارمند و اعضای خانواده‌شان تأثیر گذاشت، از جمله چند نفر که خارج از کشور بودند و نمی‌توانستند برگردند.

در بخش فناوری هیچ تردیدی نداشتیم که کدام طرف این معادله می‌ایستیم؛ در کنار افرادمان می‌ایستادیم. کارمندان و خانواده‌هایی داشتیم که در معرض خطر بودند و در این بحران از آنها پشتیبانی می‌کردیم.

«باب فرگوسن»، دادستان کل ایالت واشنگتن، تنها چند ساعت بعد از صدور فرمان تصمیم گرفت شکایت کند. در روزهای اول که به‌دنبال تعریف مسیر استراتژیک بودیم، «دیوید زاپولسکی»، رئیس بادرایت اداره حقوقی آمازون، نقش بسیار مهمی ایفا کرد. بعدازظهر یکشنبه بعد، تماسی را ترتیب دادم و با اپل، آمازون، فیس‌بوک و گوگل تصمیم گرفتیم همکاری کنیم تا پشتیبانی گسترده بخش فناوری را در یک دعوی حقوقی سازمان‌دهی کنیم.

با وجود جنجالی که به واسطه فرمان ممنوعیت سفر به پا شد، امیدوار بودیم اوضاع آرام شده و فضایی برای چانه‌زنی و توافق فراهم شود. ژوئن ۲۰۱۷ به همراه ساتیا برای جلسه دیگری با حضور رهبران فناوری به کاخ سفید رفتیم. «کریس لیدل»، مدیر ارشد مالی سابق مایکروسافت که با هدایت «جرد کوشنر» مجموعه‌ای از طرح‌های مدرن‌سازی دولت فدرال را رهبری می‌کرد، سلسله‌جلسات جامعی را برنامه‌ریزی کرده بود. در بحث جانبی صریح و متنوعی شرکت کردم که امکان تدوین بسته پیشنهادی مهاجرت گسترده‌تری را بررسی می‌کرد. هرچند اختلاف سلیقه آشکاری بین بخش‌های مختلف ستاد کاخ سفید وجود داشت، اما دوباره کمی امیدوار شدیم.

در ابتدای سپتامبر مشخص شد که کاخ سفید (و کشور) به چالشی تاریخی در زمینه مهاجرت نزدیک می‌شود. مسئله این بود که آیا رئیس‌جمهور برنامه «تعویق اخراج مهاجران که در کودکی وارد آمریکا شدند» (Deferred Action for Childhood Arrivals) یا داکا را لغو می‌کند و زندگی بیش از ۸۰۰ هزار جوان مهاجر واجد شرایط تحت قانون دریم (DREAM Act) از جمله برخی کارمندان‌مان را در بلاتکلیفی محض قرار می‌دهد یا خیر؟ (قانون دریم یا «قانون توسعه، امداد و آموزش برای افراد نابالغ خارجی» به مهاجران واجد شرایطی که پیش از رسیدن به سن قانونی به ایالات متحده آمده‌اند، اقامت مشروط و حق کار می‌دهد.) خواستار توافقی بینابین شدیم که به مسئله امنیت مرزی رسیدگی کند و در عین حال داکا و سایر طرح‌های مهاجرتی کلیدی را

لغو نکند.

به نتیجه‌ای نرسیدیم. وقتی در ساعات پایانی پیش از اعلام تصمیم در این زمینه با افرادی در کاخ سفید صحبت می‌کردم، موقعیت بیش از پیش ناخوشایند به نظر می‌رسید. با «ایمی هود»، مدیر ارشد مالی مایکروسافت گفت‌وگو کردم تا ببینیم در مورد کارمندان تحت قانون داکای شرکت چه کارهایی می‌توانیم انجام دهیم. برنامه‌ای تدوین کردیم و ساتیا با آن موافقت کرد. وقتی رئیس‌جمهور تصمیم‌گیری مبنی بر لغو داکا را اعلام کرد، آماده بودیم. مایکروسافت اولین شرکتی بود که متعهد شد در دادگاه از کارمندانی دفاع کند که تحت تأثیر این تصمیم قرار گرفته‌اند. چنانچه به خبرنگار رادیوی عمومی ملی (NPR) گفتم اگر دولت فدرال می‌خواست هر کدام از کارمندان تحت برنامه داکای ما را از کشور اخراج کند، «اول باید با ما مواجه می‌شد». بعد به دانشگاه پرینستون و یکی از دانشجویانش پیوستیم تا شکایتی را برای به چالش‌کشیدن لغو داکا ثبت کنیم.

لغو داکا از بسیاری جهات شرایط همه بحث‌های بعدی مربوط به مهاجرت را تعیین کرد. گاهی اوقات حرف‌هایی از توافق زده می‌شد، اما بعد به نتیجه نمی‌رسید. در هر صورت بخشی از الگویی بود که از یک دهه پیش وجود داشت. رئیس‌جمهور جرج دبلیو بوش در دوره دومش تلاش کرد با قانون‌گذاری جامع مسئله مهاجرت را از بن‌بست خارج کند. اوباما هم در دوره دومش تلاش مشابهی انجام داد و سنا در سال ۲۰۱۳ لایحه‌ای جامع تصویب کرد، اما باز هم همه‌چیز به بن‌بست رسید.

البته اکنون مذاکرات تند و تیزتر بودند. همه طرف‌ها پایبندی مطلقی به افکار حزبی خودشان در این زمینه داشتند. همه به‌سختی تلاش می‌کردند نظر پایگاه طرفداران‌شان را جلب کنند و این وسط فرصت برداشتن هر گونه گام مثبت از دست می‌رفت.

گاهی اوقات دور از بازی‌های سیاسی ما هم با وضعیت مشابهی روبه‌رو می‌شدیم. در دنیای کسب‌وکار یا رگولیشن هم کشمکشی بر سر مسئله‌ای واحد شکل می‌گیرد. رقابتی ایجاد می‌شود که در نهایت یک برنده و یک بازنده از آن بیرون می‌آید. این رویکرد در واقع دستورالعمل ایجاد بن‌بست همیشگی و انجام‌نشدن هیچ کاری است.

دور از انتظار است، اما گاهی اوقات پاسخ چنین مسائلی گسترده‌تر کردن چالش است. یکی از اصولی که همیشه در مذاکرات به کار می‌بردم، اصلی ساده بود؛ اینکه هرگز اجازه ندهید مذاکره به یک مسئله محدود شود که در نهایت فقط یک برنده داشته باشد، حتی اگر به معنی باز کردن بحث‌های دیگری باشد که ممکن است توافق در موردشان در دسترس به نظر برسد. بحث را گسترش دهید تا مذاکره مسائل بیشتری را شامل شود. فرصت بده‌بستان بیشتر و سازش‌هایی را فراهم کنید تا امکان رسیدن به سناریویی وجود داشته باشد که در آن همه در نهایت بتوانند اعلام کنند پیروز شده‌اند. وقتی می‌خواستیم مشاجرات دشوار مربوط به پرونده‌های ضدانحصار و مالکیت معنوی را با دولت‌ها و شرکت‌های سراسر دنیا حل کنیم، به این نتیجه رسیدیم که اتخاذ این رویکرد ضروری است.

باعث شد باور کنیم که این اصل می‌تواند در پرداختن به مسائل مهاجرت هم نقش داشته باشد. در هر صورت باید تعادلی واقعی و منصفانه بین پر کردن شغل‌های جدید در حوزه فناوری ایالات متحده با مهاجران و ایجاد شغل‌هایی حتی بیشتر از آن برای شهروندان آمریکا وجود داشت.

این مسئله مبتنی بر اصول و سیاست عملی بود. آن‌قدر روی مسئله مهاجرت کار کرده بودیم که درک می‌کردیم بزرگ‌ترین چالش سیاسی تهدیدی است که افراد فکر می‌کردند مهاجرت برای فرصت‌های شغلی شهروندان آمریکا ایجاد می‌کند. این مسئله را در بسیاری از کشورهای دیگری که کارمند داشتیم هم مشاهده می‌کردیم. مانند تجارت، به افزایش مهاجرت هم می‌توان به دید تهدیدی برای فرصت‌های شغلی جمعیت داخلی نگاه کرد. اما مهاجرت اغلب بیشتر از لحاظ سیاسی بحث‌برانگیز است؛ زیرا با توجه به ورود افراد و رسوم و سنن کشورهای دیگر می‌توان به آن به دید عامل ایجاد آشفتگی در فرهنگ داخلی نگاه کرد.

در سال ۲۰۱۰ «استراتژی استعداد ملی» برای ایالات متحده را ارائه کردیم که فکر می‌کردیم بهترین ایده‌مان در آن زمان است. می‌خواستیم مسئله را گسترش دهیم و مهاجرت را به نحوی بهبود ببخشیم که برای آمریکایی‌ها فرصت بیشتری ایجاد کند. ایده کلی این بود که در کنار افزایش محدود تعداد ویزاها و گرین‌کارت‌ها هزینه‌های

مهاجرت را هم افزایش دهیم و از درآمد اضافه آن در تأمین مالی فرصت‌های آموزشی و کارآموزی مهارت‌های پرتقاضا برای شغل‌های جدید استفاده کنیم.

طبیعی بود که باید به جزئیات بسیار زیادی توجه می‌کردیم. در سال ۲۰۱۳ گروهی از سناتورها این چالش را پذیرفتند. «اورین هچ» (Orrin Hatch) و «ایمی کلوبشار» (Amy Klobuchar) تلاشی دوحزبی را رهبری کردند که به ارائه قانون نوآوری مهاجرت (Immigration Innovation Act) منجر شد. این طرح که با نام «آی-اسکوئرد» (I-Squared) هم شناخته می‌شود، از همان فرمول ابتدایی پیشنهادی ما استفاده می‌کرد و در عین حال به کمبود شدید گرین‌کارت برای برخی کشورهای کلیدی می‌پرداخت و اصلاحات دیگری را هم انجام می‌داد که پیش از اینها باید اجرا می‌شدند. بیشتر بندهای این قانون در طرح مهاجرت جامع مصوب سال ۲۰۱۳ سنا وجود داشتند، اما در مجلس نمایندگان تضعیف شدند. وقتی در دسامبر ۲۰۱۶ در برج ترامپ در مورد مهاجرت بحث می‌کردیم، دوباره این رویکرد را مطرح کردم. بیشتر رهبران فناوری موافق آن بودند، اما در این زمینه اختلاف سلیقه آشکاری بین اعضای ستاد رئیس‌جمهور منتخب وجود داشت.

بخشی از جذابیت آی-اسکوئرد این بود که برای هدفی پول جذب می‌کرد که به‌وضوح اهمیتش افزایش یافته بود. همه کشورها با این ضرورت جدید مواجه هستند که پرورش مهارت‌های مورد نیاز برای فرصت‌های شغلی بهتر در اقتصاد مبتنی بر هوش مصنوعی و فناوری را برای افراد آسان‌تر کنند. چون یک شرکت فناوری هستیم، باید در بخشی از فرایند استخدام‌مان به این مسئله رسیدگی کنیم. مشکلات حقوقی پرونده‌های ضدانحصار که در دهه ۱۹۹۰ تجربه کردیم، باعث شدند مشارکت بیشتری در این مسائل داشته باشیم، به نحوی که بینش‌مان نسبت به این مسائل بهبود یافت.

یکی از نقاط عطف خود ما در اوایل ژانویه ۲۰۰۳ یعنی درست زمانی اتفاق افتاد که همه بعد از تعطیلات سال نو در حال بازگشت به کار بودند. تیم دادخواهی ما موافقتی اصولی را چکش‌کاری و تدوین کرده بود تا در مورد بزرگ‌ترین شکایت جمعی ناشی از شکست‌مان در پرونده ضدانحصار در دادگاه تجدیدنظر فدرال واشنگتن دی‌سی به توافق برسیم. این پرونده شامل همه مصرف‌کنندگان در ایالت کالیفرنیا می‌شد.

جریمه‌ای که باید پرداخت می‌کردیم، مبلغ هنگفت ۱٫۱ میلیارد دلار بود. در صورت اجرا، بزرگ‌ترین توافق قضایی در تاریخ مایکروسافت می‌شد. به «استیو بالمر»، مدیرعامل وقت مایکروسافت ایمیلی فرستادم و گفتم می‌خواهم موافقتم را با این توافق اعلام کنم و بعد با اضطراب منتظر واکنش او ماندم.

استیو صبح همان روز به دفترم آمده بود تا در مورد توافق پیشنهادی صحبت کند. مانند تقریباً همه مدیران ارشد کسب‌وکار درک می‌کرد که وکلایی که شکایت‌های جمعی را مطرح می‌کنند، همیشه مطمئن می‌شوند که این توافقات برای خودشان هم منافع قابل توجهی دارند. اما استیو می‌خواست بداند این شکایت شامل چه چیزهای دیگری می‌شود. دور اتاق من قدم می‌زد؛ کاری که اغلب انجام می‌داد. بعد نشست، اما نه روی صندلی؛ بلکه روی میز من نشست و پاهایش را روی هم انداخت. تابه‌حال ندیده بودم چنین کاری انجام دهد. مستقیم در چشمانم نگاه کرد و گفت: «اگر قرار است چنین مبلغی را هزینه کنیم، می‌خواهم اطمینان حاصل کنی که این پول فقط به وکلا و دیگران نمی‌رسد و منفعتی واقعی به آدم‌های واقعی می‌رسد.» قول دادم که این کار را انجام می‌دهم.

توافق نهایی خواسته استیو را برآورده می‌کرد. مایکروسافت موافقت کرده بود بن‌هایی را به مدارس بدهد تا بتوانند فناوری کامپیوتری جدید بخرند. فقط هم محدود به فناوری ما نبود، می‌توانستند از هر شرکتی، از جمله رقبای ما نرم‌افزار، سخت‌افزار و خدمات خریداری کنند. از این مدل در نقاط دیگر کشور هم پیروی کردیم و در مجموع بیش از سه میلیارد دلار بن به مدارس سراسر کشور دادیم.

با این حال این توافق بینش بی‌واسطه‌ای به ما داد که بقیه کشور هم یاد گرفت؛ اینکه با وجود صرف میلیاردها دلار، بزرگ‌ترین چالش فناوری مدارس اختصاص کامپیوترهای بیشتر به کلاس‌ها نبود؛ بلکه تجهیز معلمان با مهارت‌های مورد نیاز برای استفاده مناسب از این فناوری بود. نمی‌دانستیم که هنوز با بزرگ‌ترین چالش مهارتی معلمان مواجه نشده‌ایم. این چالش فراهم‌کردن فرصت یادگیری علوم کامپیوتر برای معلمان بود؛ رشته‌ای که وقتی بسیاری از این معلمان به دبیرستان یا دانشگاه می‌رفتند، هنوز نوپا بود. تنها پس از یادگیری علوم کامپیوتر بود که می‌توانستند دوره‌های

کدنویسی و علوم کامپیوتری را آموزش بدهند که آینده نسل جدیدی از دانش‌آموزان را تعیین می‌کرد.

علوم کامپیوتر به‌سرعت به یکی از حوزه‌های تعیین‌کننده قرن بیست‌ویکم تبدیل شده است. محتوای شغل‌ها به شکل فزاینده‌ای دیجیتال شده و همان‌طور که مطالعه مؤسسه بروکینگز در سال ۲۰۱۷ نشان می‌دهد، شغل‌هایی با محتوای دیجیتال بیشتر، درآمد بیشتری از شغل‌هایی با محتوای دیجیتال کمتر دارند. همان‌طور که «اد لازوسکا» (Ed Lazowska)، استاد برجسته در دانشگاه واشنگتن گفته است، علوم کامپیوتر «در همه‌چیز نقش محوری» پیدا کرده است. او توضیح می‌دهد که «علوم کامپیوتر نه‌فقط در نرم‌افزار، در زیست‌شناسی و هر حوزه دیگری که نام ببرید، نقش محوری دارد.»

اما با کمبود شدید معلمانی مواجه هستیم که بتوانند علوم کامپیوتر را تدریس کنند. کمتر از ۲۰ درصد از دبیرستان‌های کشور دوره کارآموزی پیشرفته را در این حوزه ارائه می‌دهند. در سال ۲۰۱۷ تعداد جوانانی که این دوره را گذراندند، کمتر از تعداد افرادی بودند که دوره ۱۵ موضوع دیگر از جمله تاریخ اروپا را گذرانده بودند. البته یکی از چالش‌ها هزینه بالای تربیت معلمان برای آموزش علوم کامپیوتر است.

دولت‌ها در رسیدگی به این مشکل کُند عمل کرده‌اند، اما کارهای بشردوستانه سرعت بیشتری داشته‌اند. یکی از افرادی که تغییر مثبتی ایجاد کرده، «کوین وانگ» است. کوین همزمان مدرک علوم کامپیوتر و آموزش دارد و پیش از اینکه مهندس نرم‌افزار شود، در دبیرستان تدریس کرده است. سه سال بعد از استخدام در مایکروسافت، دبیرستانی در سیاتل از پیشینه‌اش آگاه شد و از او خواست به‌صورت داوطلبانه به یک کلاس علوم کامپیوتر آموزش بدهد. این کار را کرد و کمی بعد مدارس محلی دیگر هم از او خواستند در آن مدارس هم تدریس کند.

کوین توضیح داد که شغل ثابت دارد و بدیهی است که همزمان نمی‌تواند در پنج نقطه تدریس کند، اما اگر علاقه‌مند باشند توسعه‌دهندگان دیگری را در مایکروسافت می‌شناسد که می‌توانند به همراه فردی مثل معلم ریاضی مدرسه به‌صورت تیمی آموزش بدهند. در این سناریو داوطلب تخصصش در علوم کامپیوتر را ارائه می‌کند

و معلم ریاضی هم کـه می‌داند چطور آموزش دهـد، کلاس را مدیریت و بـا موفقیت با دانش‌آموزان تمرین می‌کند. معلم ریاضی با گذشت زمان علوم کامپیوتر را در همکاری با داوطلـب یاد می‌گیـرد و خودش معلم علـوم کامپیوتر هم می‌شـود. با این پیشـنهاد رویکردی جدید به تربیت معلم به وجود آمد.

واحد «بشردوستانه» مایکروسافت، این برنامه جدید با نام آموزش و سواد فناوری در مـدارس (Technology Education and Literacy in Schools) را بـه یکـی از ارکان اساسـی مأموریت آموزشی‌اش تبدیل کرد. این برنامه هر سـال ۱۴۵۰ داوطلب را از مایکروسـافت و ۵۰۰ شـرکت و سـازمان دیگر ثبت‌نام می‌کند تا علـوم کامپیوتر را در تقریباً ۵۰۰ دبیرسـتان در ۲۷ ایالت آمریکا، ناحیـه کلمبیا و اسـتان بریتیش کلمبیای کانادا آموزش دهند.

بعد فرد دیگـری در این زمینه پیش‌قدم شـد و تأثیر بیشـتری هم گذاشـت. «هادی پرتوی» با موفقیت طیفی از شرکت‌های فناوری را در نقاط مختلف ساحل غربی آمریکا تأمین مالی و بنیان‌گذاری کرده بود. او فرزند والدینی ایرانی است که در پی انقلاب ایران از کشورشان مهاجرت کرده و به ایالات متحده آمدند. با وجود موفقیت‌هایی که هادی به دست آورده بود، پدرش دوست داشت دستاوردی مهم‌تر از اینها کسب کند. واکنش هادی این بود که با بخشی از پول خودش گروه جدیدی به نام Code.org را بنیان‌گذاری کرد که آموزش علوم کامپیوتر را متحول ساخت.

نفوذ Code.org در مقایسه با سازمان‌های غیرانتفاعی مرسوم شگفت‌انگیز است. هادی برای آشنا کردن نسل جدید با کدنویسی برنامه‌ای سالانه به نام ساعت کدنویسی ایجاد کرد که دانش‌آموزان را از طریق کلاس‌های آنلاین یک‌ساعته به کدنویسی ترغیب می‌کند. هادی بـرای ایـن کار از مهارت‌هـای بازاریابی وایرالش اسـتفاده کـرد و تا امروز صدها میلیون دانش‌آموز در سطح جهان در این برنامه شرکت کرده‌اند. مایکروسافت بزرگ‌ترین تأمین‌کننده مالی Code.org شـد و همواره با گسترش برنامه تربیت معلم و پشتیبانی این سازمان در سراسر کشور آنها را تشویق کرده است.

مسـئله این اسـت که برای دسترسـی بهتر به دانش‌آموزانـی با همـه پیش‌زمینه‌ها همچنـان به پشـتیبانی بیشـتر نیـاز داریـم. هرچند عقیـده عمومـی بر این اسـت که

همه دانش‌آموزان باید دوره‌های علوم کامپیوتر را بگذرانند، اما می‌توان گفت همه دانش‌آموزان سزاوار این فرصت هستند. برای جامه عمل پوشاندن به این حرف، باید علوم کامپیوتر را به همه دبیرستان‌ها و همچنین به مقاطع پایین‌تر برد. تنها راه رسیدن به این مقیاس در تربیت معلمان این است که منابع مالی فدرال به پر کردن این خلأ کمک کنند.

بعد از سال‌ها لابی‌گری سرانجام در سال ۲۰۱۶ پیشرفتی در علاقه دولت فدرال به این موضوع حاصل شد. رئیس‌جمهور اوباما در ماه ژانویه پیشنهاد جسورانه‌ای اعلام کرد که بر اساس آن چهار میلیارد دلار از منابع مالی فدرال به‌منظور گسترش آموزش علوم کامپیوتر در مدارس کشور سرمایه‌گذاری می‌شد. هرچند این پیشنهاد با استقبال پرشوری مواجه شد، اما باعث نشد کنگره منابع مالی جدیدی را به این موضوع اختصاص دهد.

ایوانکا ترامپ سال بعد موفقیت بیشتری در این زمینه کسب کرد. حتی پیش از ورود پدرش به کاخ سفید به سرمایه‌گذاری‌های فدرال در گسترش علوم کامپیوتر در مدارس علاقه‌مند بود. اطمینان خاطر داشت که می‌تواند رئیس‌جمهور را به پشتیبانی از این ایده متقاعد کند، اما در عین حال بر این باور بود که کلید جذب منابع مالی عمومی تأمین منابع مالی قابل توجه از شرکت‌های فناوری بزرگ است. گفته بود تلاش می‌کند در عرض پنج سال یک میلیارد دلار از منابع مالی فدرال تأمین کند، به شرط آنکه بخش فناوری هم متعهد به تأمین ۳۰۰ میلیون دلار در همین دوره شود.

مثل همیشه مسئله این بود که ابتدا باید شرکتی پیش‌قدم می‌شد. کاخ سفید به‌دنبال شرکتی بود که با تعهد به تأمین ۵۰ میلیون دلار در طول پنج سال برنامه را شروع کند. با توجه به مشارکت دیرین، پشتیبانی مالی و طرفداری قبلی مایکروسافت در دوره اوباما، یکی از انتخاب‌های طبیعی ما بودیم. با دادن این تعهد موافقت کردیم و شرکت‌های دیگر هم مسیر ما را در پیش گرفتند و در سپتامبر ۲۰۱۷ «مری اسنپ» (Mary Snapp)، رئیس واحد بشردوستانه مایکروسافت در شهر دیترویت به ایوانکا پیوست تا با هم خبر این برنامه را اعلام کنند.

گسترش علوم کامپیوتر در مدارس کشور عاملی اساسی در ایجاد فرصت برای نسل

جدید در اقتصاد در حال تحول است. اما فقط بخشی از معادله است. گروه‌های غیرانتفاعی و مدیران ایالتی بیش از پیش در حال تدوین برنامه‌های نوآورانه‌ای هستند که به تقویت مدارس محلی، سرمایه‌گذاری در دانشکده‌های علمی کاربردی، بهبود یادگیری همیشگی و بررسی مسیرهای شغلی جدید برای افرادی می‌پردازند که با افزایش سن‌شان باید شغل یا مسیر شغلی‌شان را تغییر دهند. گروه‌هایی از سراسر کشور به خارج سفر می‌کنند تا ببینند آیا مدل کارآموزی سوئیس یا یادگیری مادام‌العمر سنگاپور را می‌توان در ایالات متحده اجرا کرد یا خیر. این چالشی ملی است و به دور از بن‌بست واشنگتن، پیشرفت فوق‌العاده‌ای در سراسر کشور مشاهده می‌شود.

بخش فناوری همچنین در حال سرمایه‌گذاری در ابزارهای کاریابی است. برای مثال ما در مایکروسافت لینکدین را داریم. این شبکه اجتماعی گراف اقتصادی (Economic Graph) را ایجاد کرده که انواع شغل‌هایی که شرکت‌ها در هر منطقه و کشور ایجاد می‌کنند و انواع مهارت‌های مورد نیاز برای انجام‌دادن آن شغل‌ها را شناسایی می‌کند. گراف اقتصادی با استفاده از داده‌های بیش از ۶۰۰ میلیون عضو از سراسر جهان ابزاری را ارائه می‌کند تا به برنامه‌ریزهای دولتی کمک کند که برنامه‌های آموزشی و مهارت‌آموزی بر مقوله‌های مناسب متمرکز کنند. سازمان‌های دولتی و غیرانتفاعی؛ از ایالت کلرادو گرفته تا استرالیا و بانک جهانی در حال استفاده از این ابزار هستند.

همان‌طور که داده‌های لینکدین نشان می‌دهد، مهارت‌های مبتنی بر کامپیوتر و علوم داده بیش از پیش برای کارجویان جدید مهم شده‌اند. در ماه می ۲۰۱۹ چهار مهارتی که فارغ‌التحصیلان جدید دانشگاه بیش از همه در لینکدین لرنینگ (LinkedIn Learning) دنبال کرده بودند، یعنی مصورسازی داده؛ مدل‌سازی داده؛ زبان‌های برنامه‌نویسی و آنالیتیکس وب، نشان‌دهنده این اهمیت بودند. «ژان فیلیپ کورتوا» (Jean-Philippe Courtois) و «جادسون آلتوف» (Judson Althoff)، دو رهبر ارشد فروش مایکروسافت به این نتیجه رسیدند که کاربرد فناوری جدید بیش از پیش مستلزم این است که در برنامه‌های پرورش استعداد نه‌تنها برای کارمندان خودمان؛ بلکه برای کارمندان مشتریان‌مان نیز سرمایه‌گذاری کنیم. بنابراین برنامه‌ای ایجاد

کردیم که فرصت پرورش مهارت‌های هوش مصنوعی و سایر فناوری‌ها را برای مشتریان در سراسر دنیا فراهم می‌کند.

همین‌طور که پیش می‌رویم، درس‌ها و چالش‌های جدیدی پیش روی ما قرار می‌گیرد. یکی از چالش‌های همیشگی این است که اطمینان حاصل کنیم افراد توانایی مالی کسب مهارت‌های جدید را از جمله با رفتن از کلاس‌های علوم کامپیوتر دبیرستان به کالج یا سایر دوره‌های آموزش عالی دارند. بخش فناوری و دولت‌ها می‌توانند با مشارکت در قالب‌های جدید این چالش را برطرف کنند.

در ایالت واشنگتن راه‌حلی را در این زمینه تجربه کرده‌ایم. برنامه «کمک‌هزینه فرصت ایالت واشنگتن» (Washington State Opportunity Scholarship) که نهاد قانون‌گذار ایالت ایجاد کرده، منابع مالی عمومی و خصوصی را ترکیب می‌کند تا به دانش‌آموزان این ایالت کمک کند در رشته‌های مراقبت سلامت، علوم تجربی، فناوری، مهندسی و ریاضی مدرک کالج بگیرند. از سال ۲۰۱۱ تاکنون در این ترکیب تقریباً ۲۰۰ میلیون دلار جذب شده و در هر سال از حدود پنج هزار دانشجوی کالج پشتیبانی می‌شود که هر کدام تا ۲۲٫۵۰۰ دلار کمک‌هزینه تحصیلی دریافت می‌کنند. این برنامه دسترسی به کالج را گسترش داده است. تقریباً دوسوم دریافت‌کنندگان این کمک‌هزینه‌ها اولین فرد در خانواده‌شان هستند که به کالج می‌روند و بیشتر دانشجویان هم زن و رنگین‌پوست هستند.

هرچند همه این اتفاقات برای تأمین‌کنندگان مالی و کارفرمایان بزرگ بخش خصوصی مثل مایکروسافت و بوئینگ خبر خوشی بوده، اما اتفاق دلگرم‌کننده‌تر، رویکرد فراگیرتر و نتایج این برنامه است. وقتی «ناریا سانتا لوسیا» (Naria Santa Lucia) پنج سال پیش به این تلاش‌های انسان‌دوستانه اضافه شد، بر فراهم‌ساختن منتور، کارآموزی و ارتباط با کارفرمایان بالقوه برای دانشجویان تمرکز کرد. این اقدام نقش‌هایی را برای کسب‌وکارها و افراد در جامعه به وجود آورده است. این ترکیب نه‌تنها باعث افزایش میزان فارغ‌التحصیلی دانشجویان شده، بلکه مسیر روشنی را نیز به سمت شغل‌هایی با درآمد مناسب فراهم کرده است. ارزیابی تازه‌ای نشان می‌دهد که متوسط درآمد شرکت‌کنندگان تنها پنج سال بعد از فارغ‌التحصیلی

حدود ۵۰ درصد بیشتر از درآمد کل خانواده‌شان در زمان شروع دوره کالج بوده است. این اتفاق در دورانی می‌افتد که در کل کشور احتمال اینکه آمریکایی‌های ۳۰ساله بیشتر از والدین‌شان در همان سن درآمد کسب کنند «از ۸۶ درصد در ۴۰ سال پیش به ۵۱ درصد در زمان حال کاهش یافته است».

این موفقیت به ما انگیزه می‌دهد که تلاش گسترده‌تری را در سطح ایالت دنبال کنیم تا دسترسی به مهارت‌های جدید و آموزش عالی را گسترش دهیم. در اوایل سال ۲۰۱۹ رهبران محلی از من خواستند که در کنار «آنا ماری کاس» (Ana Mari Cauce)، رئیس دانشگاه واشنگتن در پیشبرد موضوع ایجاد صندوق آموزش جدیدی قرار بگیرم که منابع آن از طریق افزایش مالیات بر گروهی از کسب‌وکارها تأمین می‌شود که به نظام آموزش عالی وابسته هستند.

هرچند این ایده جذاب بود، اما چالش‌هایی را هم به همراه داشت. می‌خواستم اطمینان حاصل کنم که منابع نه‌تنها به افرادی می‌رسد که می‌خواهند در دوره‌های کارشناسی چهارساله شرکت کنند؛ بلکه به دانشجویانی هم که به دانشکده‌های فنی و حرفه‌ای و علمی کاربردی می‌روند، کمک می‌کند. همچنین می‌خواستم اطمینان حاصل کنم که شورای مستقلی ایجاد می‌شود که بر هزینه‌کرد مسئولانه منابع مالی نظارت کند و بندهایی اضافه شود که از انحراف منابع در زمان رکود اقتصادی جلوگیری کنند.

هرچند پرداختن به این مسائل تقریباً آسان بود، ولی باز هم حمایت از دریافت مالیاتِ بیشتر از کسب‌وکارهای دیگر، کار راحت و خوشایندی نبود. با ایمی هود جلسه گذاشتیم تا آثار مالی و سیاسی حمایت‌مان از این برنامه بر شرکت را بررسی کنیم. به این جمع‌بندی رسیدیم که اگر می‌خواهیم با حمایت از وضع مالیات بیشتر بر کسب‌وکارهای ایالت، از اعتبار شرکت خرج کنیم، باید ساختاری را پیشنهاد بدهیم که مایکروسافت و آمازون، یعنی بزرگ‌ترین شرکت‌های فناوری ایالت را به پرداخت نرخ مالیات بیشتری از سایر شرکت‌ها ملزم کند.

این پیشنهاد ما بود و به همان صورت هم تصویب شد. حمایت عمومی‌مان را با مقاله ویژه‌ای در روزنامه سیاتل‌تایمز شروع کردیم و پیشنهاد دادیم مالیات ایالتی کسب‌وکار

و اشتغال بر بخش خدمات افزایش یابد. در مقاله نوشته بودیم: «بیایید از بزرگ‌ترین شرکت‌های بخش فناوری که بزرگ‌ترین کارفرمایان استعدادهای بسیار ماهر هستند، بخواهیم کمی بیشتر کمک کنند.» هرچند ابتدا این پیشنهاد با مخالفت‌هایی از طرف شرکت‌های دیگر مواجه شد، ولی قانون‌گذاران راهی برای رسیدن به توافق پیدا کردند که بر اساس آن حداکثر افزایش مالیات برای هر شرکت در هر سال هفت میلیون دلار تعیین شد. تنها شش هفته بعد، نهاد قانون‌گذار بودجه جدیدی را با صندوقی اختصاصی تصویب کرد که تقریباً ۲۵۰ میلیون دلار در سال برای آموزش عالی جذب می‌کند. قانون جدید «سرمایه‌گذاری آموزشی برای نیروی کار» (Workforce Education Investment Act) ایالت واشنگتن در سطح محلی و ملی به خاطر تعهد به رایگان یا ارزان‌کردن شهریه دانشگاه برای دانشجویان دارای درآمد کم و متوسط که در دوره‌های دانشکده‌های علمی کاربردی و مؤسسات عمومی شرکت می‌کنند، تأمین منابع مالی جدید برای دانشکده‌های علمی کاربردی که دچار مشکل مالی هستند و حذف فهرست انتظار دریافت کمک مالی از سال ۲۰۲۰ تحسین شد. همان‌طور که یکی از استادان دانشگاه تمپل (Temple University) می‌گوید، این قانون «پیشروترین طرح تأمین مالی آموزش عالی ایالتی» بود که در چند سال گذشته تصویب شده بود. از نظر من این قانون ثابت می‌کرد که اگر بخش فناوری رویکردی جامعه‌محورتر را بپذیرد و شاید کمی بیشتر از سهمش برای جامعه هزینه کند، می‌توانیم شاهد آثار واقعی و مثبتی باشیم.

متأسفانه این نوع پیشرفت همچنان فقط یک آبادی در کویر است. در ایالات متحده دسترسی به مهارت‌های فناوری به هیچ‌وجه برابر توزیع نشده‌اند. شکاف مهارتی مانند شکاف اینترنت پرسرعت برای برخی گروه‌ها بیشتر است. این شکاف تقریباً همه اختلافات دامن‌گیر آمریکا را تشدید می‌کند.

وقتی به دانشجویان علوم کامپیوتر نگاه می‌کنید، اثر ناهمگون این شکاف را به‌وضوح می‌بینید. در دورانی که بخش فناوری با کمبود نیروی کار زن مواجه است، فقط ۲۸ درصد از دانش‌آموزان شرکت‌کننده در آزمون کارآموزی پیشرفته علوم کامپیوتر سال ۲۰۱۸ دختر بودند. همین روند را در مورد اقلیت‌های نژادی به‌حاشیه‌رفته هم مشاهده

می‌کنیم. در حالی که این گروه‌ها ۴۳ درصد از کشور را تشکیل می‌دهند، فقط ۲۱ درصد از دانش‌آموزان شرکت‌کننده در این آزمون‌ها از این گروه‌ها هستند. علاوه بر این در دورانی که کشور نگران فرصت‌های اقتصادی مناطق روستایی است، فقط ۱۰ درصد از شرکت‌کنندگان آزمون‌های کارآموزی پیشرفته علوم کامپیوتر در سال ۲۰۱۸ از این مناطق بودند.

خلاصه اینکه دانشجویان شرکت‌کننده در کلاس‌های علوم کامپیوتر بیشتر از میانگین کشور مرد، سفید، مرفه و شهرنشین هستند. این مسئله چند دلیل دارد، اما بخش فناوری باید سهمش از مسئولیت را بپذیرد. بخش فناوری جای مناسب و راحتی برای کار کردن زنان و اقلیت‌ها نبوده است.

از دیرباز زنان پیشگام و برجسته‌ای در حوزه علم و فناوری وجود داشته، از جمله «ماری کوری» که همچنان تنها فردی است که دو بار برنده جایزه نوبل شده و «برتا بنز» (Bertha Benz)، اولین کسی که پتانسیل خودرو را به جهان نشان داد. هرچند مردان دستاوردهای این زنان را به‌صورت فردی به رسمیت می‌شناسند، اما دنیای فناوری در پذیرش زنان و ایجاد فرصت برای آنها همیشه کُند عمل کرده است. در بیشتر شرکت‌های فناوری زنان همچنان کمتر از ۳۰ درصد نیروی کار را تشکیل می‌دهند و حتی درصد کمتری از شغل‌های فنی را به خود اختصاص داده‌اند. به همین ترتیب سهم آمریکایی‌های آفریقایی‌تبار، هیسپانیک و لاتین در نیروی کار شرکت‌های فناوری معمولاً کمتر از نیمی از مقداری است که با توجه به درصد جمعیت‌شان در آمریکا انتظار می‌رود.

خوشبختانه در چند سال گذشته سرانجام شاهد تغییراتی در این دیدگاه بودیم. در بخش فناوری، شرکت‌ها برنامه‌های جدیدی را شروع کرده‌اند تا استخدام را متنوع‌تر کنند و فرهنگ فراگیرتری را در محل کار ترویج کنند. برخی پیشرفت‌های جدید ناشی از کاربرد آن دسته از شیوه‌های کسب‌وکار ابتدایی بوده که بسیاری از بخش‌های اقتصادی دیگر از دیرباز به کار گرفته‌اند. برای مثال اینکه مقداری از حقوق و مزایای مدیران ارشد را به این موضوع وابسته کنیم که آیا پیشرفتی واقعی در پیشبرد تنوع‌بخشی حاصل شده یا فقط به لفاظی در مورد مسئله بسنده شده است یا گروهی از استعدادیاب‌ها

را برای کمک به شناسایی نامزدهای متنوع قدرتمند و افزایش تلاش‌ها برای بازدید از کالج‌هایی اختصاص دهیم که از گذشته بیشتر دانشجوی سیاه‌پوست داشته‌اند و دانشگاه‌هایی که جمعیت هیسپانیک زیاد و موفق دارند.

آنچنان سخت و پیچیده نیست. در واقع اصلاً پیچیده نیست. بیشتر عقل سلیم است. خوشبختانه سرانجام تحول آغاز شده است. با این حال بدون تردید بخش فناوری در زمینه شمول بسیار بیشتر از آنچه تاکنون انجام داده، کار در پیش دارد.

شاید برون‌نگری بیشتر بتواند به شرکت‌های فناوری کمک کند متغیر نهایی معادله سرمایه انسانی را با دیدگاهی فراگیرتر بررسی کنند. این متغیر تأثیری است که این شرکت‌ها روی جوامعی می‌گذارند که با سرعت زیاد در حال رشد در آنها هستند.

شرکت‌های فناوری پرشتاب شغل‌های پردرآمد را به جوامع می‌آورند. مگر می‌شود منطقه‌ای چنین مزیتی را نخواهد؟ رقابت برای جذب ساختمان دوم آمازون این بُعد را بیش از پیش آشکار کرد. شهرها از یکدیگر سبقت می‌گرفتند تا با برآورده‌کردن خواسته‌های آمازون در مورد معافیت مالیاتی و سایر مشوق‌ها این شرکت را متقاعد کنند ساختمان دومش را در آن شهر بنا کند.

اما رشد چالش‌هایی را هم به همراه دارد. هرچند مشکل رده‌بالایی است، اما در هر صورت باید آن را برطرف کرد. در این زمینه شرایط در بسیاری از مناطق بدتر شده است.

اولین نمود این مشکل را در بزرگراه‌ها می‌بینیم. ترافیک گند می‌شود، مدت‌زمان سفرهای درون‌شهری افزایش می‌یابد و شرکت‌های فناوری شروع به ارائه سرویس‌های اتوبوس به کارمندان‌شان می‌کنند. در سیلیکون‌ولی بسیاری از روزهای غیرتعطیل بزرگراه‌ها بیشتر شبیه پارکینگ هستند، البته در پارکینگ می‌توان کمی سریع‌تر رانندگی کرد. شلوغی بزرگراه‌ها در واقع بخش مشهود مشکل است. راحت‌تر دیده می‌شود، اما رشد همین بار بیشتر را به همه بخش‌های زیرساخت یک منطقه از سیستم‌های حمل‌ونقل تا مدارس تحمیل می‌کند.

در طول چند سال گذشته مسئله بسیار عمیق‌تر شده است. هرچند شغل‌ها افزایش یافته‌اند، اما تأمین مسکن با رشد همگام نبوده است. در این زمینه اصول اولیه اقتصاد حاکم است. وقتی افراد به مناطقی نقل مکان می‌کنند تا شغل‌های پردرآمدتری

به دست آورند و مسکن‌سازی همگام با این روند رشد نمی‌کند، قیمت مسکن افزایش می‌یابد و افراد دارای درآمد کم و متوسط مجبور می‌شوند از آن مناطق بروند. معلمان، پرستاران و نیروهای امداد و نجات آن جامعه (همچنین نیروهای پشتیبانی شرکت‌های فناوری) اغلب مجبور می‌شوند به مناطق دورتر بروند و در نتیجه برای رفت‌وآمد به محل کارشان مسافت بیشتری را طی کنند.

در ژوئن ۲۰۱۸ به همراه ساتیا در جلسه‌ای کوچک در سیاتل در مورد این مسئله گفت‌وگو می‌کردیم. سال‌ها بود که مدیران کسب‌وکارهای ایالت را به تمرکز بر آموزش و حمل‌ونقل به‌عنوان مسائل بنیادی تمام منطقه ترغیب می‌کردیم. حال در حال صرف صبحانه‌ای کاری با ۱۰ مدیر محلی دیگر به‌عنوان بخشی از یک گروه شهری و کسب‌وکاری محلی به نام «چلنج سیاتل» بودیم که به بنیان‌گذاری آن کمک کرده بودیم و «کریستین گرگوا» (Christine Gregoire)، فرماندار سابق واشنگتن مدیرعامل آن بود. آن روز صبح در مورد اولویت‌های گروه برای آینده بحث می‌کردیم.

این صبحانه کاری جرقه‌ای در ذهنم زد. همین‌طور که افراد دور میز به‌ترتیب صحبت می‌کردند، همه شرکت‌کنندگان به این موضوع پرداختند که ابعادی از منطقه در حال تغییر است که همگی مثبت نیستند. در سیاتل به گذشته افتخار می‌کردیم که در زمینه مسکن به اندازه سان‌فرانسیسکو و شمال کالیفرنیا با چالش روبه‌رو نشده‌ایم. تا اینکه فهمیدیم دیگر این‌طور نیست. با تداوم رشد شرکت‌هایی مثل آمازون و مایکروسافت، پایگاه‌های مهندسی پررونقی از بیش از ۸۰ شرکت مستقر در سیلیکون‌ولی به شهر ما آمده بودند. سیاتل ناگهان از شهر زمردین به شهر ابر تبدیل شده بود. در فاصله سال‌های ۲۰۱۱ تا ۲۰۱۸ میانه قیمت مسکن در سیاتل ۹۶ درصد افزایش یافته، در حالی که میانه درآمد خانوار فقط ۳۴ درصد افزایش یافته است.

آثار این مشکلات اوایل همان سال در مرکز شهر سیاتل مشاهده شد. شورای شهر سیاتل که از تداوم و افزایش بی‌خانمان‌ها به ستوه آمده بود، تلاش کرد با پیشنهاد افزایش ۷۵ میلیون دلاری سالانه مالیات سرانه بر مشاغل به این مسئله رسیدگی کند. جامعه کسب‌وکار با درماندگی واکنش پرسروصدایی نشان داد و آمازون همراه با متوقف‌کردن برنامه‌ریزی ساخت‌وساز برای برجی جدید در سیاتل تهدید کرد که

اگر تصمیم لغو نشود، سرعت رشد اشتغال را کاهش خواهد داد. ما روند تحولات این مسئله را از آن طرف دریاچه واشنگتن مشاهده می‌کردیم که سیاتل را از بسیاری از شهرهای دیگر منطقه از جمله ردموند، محل استقرار مایکروسافت جدا می‌کند. هرچند در بحث‌های سیاتل مشارکتی نداشتیم، ولی با احساسات ضدونقیض تحولات را دنبال می‌کردیم. ما هم نسبت به وضع مالیات شغلی بدبین بودیم، اما احساس می‌کردیم جامعه کسب‌وکار باید کاری بیشتر از انتقاد به این مصوبه انجام دهد؛ باید گام‌های بلندتر روبه‌جلویی بردارد. شهردار و شورای شهر سیاتل مالیات سرانه را لغو کردند، اما جایگزین مؤثری برای آن ارائه نشد.

در آن صبحانه کاری ساتیا نگرانی‌ها نسبت به مسئله مسکن را مطرح کرد و دیگران هم به‌سرعت با او همراه شدند. اشاره کردم که صبح شنبه‌ای در همین اواخر با «استیو مایلت»، رئیس پلیس «بلویو» (Bellevue)، بزرگ‌ترین شهر اطراف سیاتل جلسه داشتم. درخواست ملاقات داده بودم تا نگرانی‌هایی را با او در میان بگذارم که شماری از کارمندان‌مان در مورد چالش‌های نژادی مطرح کرده بودند که از جمله شامل نگاه‌شان به پلیس محلی می‌شد. با نگاه باز پذیرای دیدگاه‌هایم بود و موضوعی را با من در میان گذاشت که برایم تازگی داشت. گفت افزایش قیمت مسکن باعث شده مأموران جدید پلیس بلویو دیگر نتوانند در شهر محل خدمت‌شان خانه بخرند. حتی رئیس پلیس هم هر روز مسیری یک‌ساعته را برای رفتن به سر کار طی می‌کرد. بین دو نکته‌ای که مطرح کردیم، ارتباط مهمی وجود داشت. وقتی مأموران پلیس محلی توانایی مالی لازم برای زندگی‌کردن در حوالی یک منطقه را ندارند، ایجاد رابطه مستحکم‌تر بین آن جامعه و نیروی پلیس دشوار می‌شود.

این داستان را با گروه چلنج سیاتل در میان گذاشتم و اشاره کردم که از تیم‌مان در مایکروسافت خواسته‌ام ایده‌هایی را برای طرحی جدید پرورش دهند. در حالی که با ساتیا از محل جلسه خارج می‌شدیم، این ایده‌ها را با جزئیات بیشتر تشریح کردم. تا وقتی به آسانسور رسیدیم، تصمیم گرفتیم این طرح را در اولویت قرار دهیم.

در ردموند از یک تیم علوم داده کمک گرفتیم تا این مشکل را بهتر درک کنیم. این تیم با شرکت «زیلو»، پایگاه داده آنلاین املاک همکاری کرد تا با استفاده از داده‌های

املاک مجموعه داده‌ای بزرگ‌تر از مجموعه موجود ایجاد کند. بینش‌ها دور از انتظار و نه‌فقط برای ما؛ بلکه در نهایت برای کل منطقه روشنگر بودند. داده‌ها نشان می‌دادند که نه‌تنها دچار مشکل بی‌خانمانی هستیم؛ بلکه در سطح گسترده‌تر با بحران به‌سرعت در حال گسترشی در زمینه مسکن مقرون‌به‌صرفه مواجهیم. اشتغال در این منطقه ۲۱ درصد افزایش یافته بود، اما ساخت‌وساز مسکن عقب مانده بود و فقط ۱۳ درصد رشد کرده بود. این فاصله در شهرهای کوچک‌تر اطراف سیاتل بیشتر بود. در این شهرها ساخت‌وساز مسکن برای افراد دارای درآمد کم و متوسط راکد بود. خانواده‌های دارای درآمد کم و متوسط بیش از پیش مجبور می‌شدند به شهرک‌ها و حومه شهرهایی بروند که فاصله بسیار زیادی با محل کارشان داشت. اکنون این منطقه به یکی از بدترین مناطق کشور از لحاظ درصد افرادی تبدیل شده بود که روزانه بیش از ۹۰ دقیقه برای رفتن به محل کار سفر می‌کردند.

به این نتیجه رسیدیم که باید کاری انجام شود تا تأمین مسکن افراد دارای درآمد کم و متوسط افزایش یابد. ماه‌ها با افراد و گروه‌هایی در منطقه مشورت کردیم و اطلاعات در دسترس را از سراسر کشور و دنیا به دست آوردیم. ایمی هود و من با حمایت ساتیا تصمیم گرفتیم از پروژه‌ای در داخل شرکت حمایت کنیم و ایمی به تیم مالی‌اش مأموریت داد گزینه‌های جایگزینی را تدوین کنند. به‌سرعت متوجه شدیم که خوشبختانه مایکروسافت مثل برخی دیگر از شرکت‌های فناوری ترازنامه بسیار مثبت و دارایی‌های نقدی زیادی دارد که می‌توانیم از آنها بهره ببریم. ایمی و من در ژانویه ۲۰۱۹ اعلام کردیم که مایکروسافت ۵۰۰ میلیون دلار را به‌صورت ترکیبی از وام، سرمایه‌گذاری و کمک انسان‌دوستانه به حل این مسئله اختصاص می‌دهد.

از تلاش‌هایمان دو بینش به دست آوردیم که بسیار مهم به نظر می‌رسیدند؛ اول اینکه روشن شد که پول هرگز نمی‌تواند به‌تنهایی مسئله را حل کند. با مطالعه این مسئله در نقاط مختلف دنیا به این نتیجه رسیدیم که تنها مسیر مؤثر برای پیشرفت، تلفیق سرمایه بیشتر با طرح‌های سیاست عمومی است. اعلامیه همزمان شهرداران ۹ شهر منطقه برای بررسی اصلاحاتی به‌منظور رشد تأمین مسکن افراد دارای درآمد کم و متوسط، به همان اندازه برنامه تأمین مالی ما مهم بود. در آستانه اعلام این برنامه،

کریستین گرگوا به همراه این شهرداران مجموعه‌ای از پیشنهادهای ویژه برای اهدای زمین‌های عمومی، اصلاح الزامات ناحیه‌بندی و ایجاد تغییرات دیگر به‌منظور افزایش سرعت ساخت‌وساز را بررسی کرده بود. این مسائل پردردسر بودند و برداشتن این گام‌ها مستلزم جسارت سیاسی زیادی بود. امیدوار بودیم منابع مالی ما به اندازه مسائل دیگر تسهیلگر تلاش گسترده‌تر مورد نیاز برای نزدیک‌کردن جامعه به هم باشد.

بینش دوم با توجه به واکنش‌ها به برنامه تأمین مالی‌مان به دست آمد. خیلی زود فهمیدیم که این مسئله نه‌فقط در سطح منطقه؛ بلکه در سطح ملی و جهانی هم برای افراد بسیار مهم است. نتایج انتخابات ریاست‌جمهوری ۲۰۱۶ حاکی از این نگرانی در حال گسترش در بسیاری از مناطق روستایی بود که در عصر رفاه ناشی از فناوری، افراد این مناطق رها و فراموش شده‌اند. اما اکنون این نگرانی از راه‌های جدیدی در حال گسترش به مناطق شهری هم بود. افراد ممکن است در خیابانی در سایه برج‌های جدید و درخشنده محل زندگی کارمندان بخش فناوری راه بروند، اما دیگر خودشان توان مالی زندگی‌کردن در آن حوالی را نداشته باشند.

این مسئله احساس درماندگی قابل درکی به وجود آورده بود که می‌توانست بُعد جدیدی را به مسائل سیاسی آمریکا اضافه کند. پیامدهای این بُعد جدید را خیلی زود در شهر نیویورک دیدیم. برخی سیاست‌مداران این شهر از موفقیت‌شان در متقاعد کردن آمازون برای احداث ساختمان دومش در این شهر از طریق یارانه و معافیت مالیاتی پشیمان شده بودند. با توجه به تأثیر رشد این شرکت بر نیازهای مسکن منطقه سیاتل به‌خوبی این مسئله را درک می‌کردیم.

مسئله مسکن مقرون‌به‌صرفه از برخی جهات ماهیت به‌هم‌پیوسته همه مسائل سرمایه انسانی مربوط به بخش فناوری را برجسته می‌کند. برای ایجاد کسب‌وکار سالم داشتن مجموعه کارمندان متنوع و قرار داشتن در جامعه‌ای شکوفا حیاتی است. هرچند منطقی است که شرکت‌های فناوری بپرسند جوامع‌شان برای آنها چه کار می‌کنند، اما صنعت فناوری به نقطه‌ای رسیده که باید پرسش بزرگ‌تری را بپرسد. موفقیت علاوه بر مقیاس، مسئولیت را هم افزایش می‌دهد. بخش فناوری بیش از

پیش باید از خود بپرسد برای کمک به جوامعی که در آنها قرار دارد، چه کار بیشتری انجام می‌دهد. ما باید به استعدادهای برتر، نه‌فقط از شهر و منطقه خودمان؛ بلکه از سراسر جهان دسترسی داشته باشیم، اما باید بیشتر تلاش کنیم تا برای افراد پیرامون‌مان فرصت بسازیم.

حل همه این چالش‌ها در گرو اقدام عملی است؛ همان‌طور که گاهی در مایکروسافت می‌گویم وقتی پروژه جدیدی را شروع می‌کنیم، در درجه اول باید کاری بزرگ انجام دهیم، اما همین که کاری انجام دهیم، هم کافی است.

موفقیت به‌ندرت به خانه کسی می‌رود که هیچ کاری نمی‌کند.

فصل یازدهم

هوش مصنوعی و اخلاقیات

وقتی در ژانویه ۲۰۱۷ برای شـرکت در مجمع جهانی اقتصاد به شهر داووس سوئیس رفتم تـا در این رویداد سـالانه آینده‌نگرانه در مـورد روندهای جهانی بحـث کنیم، هوش مصنوعی موضوع روز بود. همه شـرکت‌های فناوری خودشـان را به‌عنوان شرکت هوش مصنوعی مطـرح می‌کردند. شـبی بعد از شـام به یـاد دوران کودکی‌ام در شـمال شـرقی ویسکانسین، به دل برف و یخ زدم و مسـافت دو مایلی بلوار اصلی داووس را پیاده رفتم. بیشتر شبیه خیابان اصلی لاس‌وگاس بود تا روستایی که در دامنه کوه آلپ قرار دارد. به‌جز چند بانک، این شهرِ محل اسکی، مملو از لوگوهای پرنور و تابلوهای جذاب شرکت‌های فناوری بود که هر کدام (و از جمله مایکروسافت) استراتژی هوش مصنوعی خود را برای کسب‌وکارها، رهبران فکری و دولت‌هایی تبلیغ می‌کردند که آن هفته را در دامنه کوه آلپ در سوئیس می‌گذراندند. دو موضوع بسیار مشهود بود، هوش مصنوعی مد جدید است و شرکت‌های فناوری بودجه بازاریابی فراوانی دارند.

بعد از شرکت در بحث‌های بی‌شمار در مورد مزیت‌های هوش مصنوعی متوجه شدم هیچ‌کس توضیح نمی‌دهـد هوش مصنوعی دقیقاً چیسـت و چطـور کار می‌کند. فرض کرده بودند همه حاضـران این چیزهـا را می‌دانند. با توجـه به گفت‌وگوهایـم در داووس می‌دانستم که این‌طور نیست، اما افراد تمایلی نداشتند دست‌شان را بالا ببرند و در مورد اصول اولیه این فناوری سؤال بپرسند که البته قابل درک بود. هیچ‌کس نمی‌خواست اولین نفری باشد که اعتراف می‌کند او (و به احتمال زیاد نصف مخاطبان) کاملاً درک نمی‌کنند که نصف دیگر مخاطبان در مورد چه چیزی حرف می‌زنند.

علاوه بر ابهام فراگیری که حول هوش مصنوعی وجود داشت، متوجه مسئله دیگری هم شدم؛ هیچ‌کس نمی‌خواست در مورد این موضوع صحبت کند که آیا لازم است این فناوری جدید رگوله شود یا خیر.

در وبکسـتی به میزبانی «دیوید کرکپتریـک» (David Kirkpatrick) از «تکونومی» (Techonomy) از من پرسیدند آیا مایکروسـافت فکر می‌کند رگولیشن دولتی در مورد هوش مصنوعی وجود خواهد داشت یا خیر. گفتم احتمالاً پنج سال بعد در حال بحث در مورد پیشـنهادهای دولتی متمرکز بر رگولیشـن‌های جدید هوش مصنوعی خواهیم بود. یکی از مدیران ارشد IBM مخالفت کرد و گفت: «نمی‌توان آینده را پیش‌بینی کرد.

معلوم نیست بتوانیم سیاست دقیقی داشته باشیم. نگرانم چنین کاری آثار نامطلوبی داشته باشد.»

آن هفته در داووس بازتاب‌دهنده موضوعات فراگیری در بخش فناوری بود که لزوماً همه مثبت نیستند. صنعت فناوری مانند بیشتر صنایع بدون اینکه به افراد کمک کند ماهیت یا سازوکار نوآوری جدیدی را کاملاً درک کنند، آن نوآوری را به‌سرعت به پیش می‌برد. در کنار این رویکرد این باور هم وجود دارد که همه فناوری‌های جدید کاملاً مفید خواهند بود؛ باوری که تا مدت‌های زیادی تقریباً مقدس شمرده می‌شد. در سیلیکون‌ولی بسیاری از افراد از دیرباز بر این باور بودند که رگولاتورهای دولتی نمی‌توانند همگام با فناوری پیش بروند.

این نگاه ایده‌آل‌گرا به فناوری اغلب در نیت خوبی ریشه دارد، اما واقع‌بینانه نیست. بهترین فناوری‌ها هم پیامدهای ناخواسته‌ای دارند و مزیت‌ها هم به‌ندرت یکنواخت توزیع می‌شوند. تازه این موارد مربوط به قبل از زمانی است که از فناوری برای اهداف زیان‌بخش سوءاستفاده شود؛ اتفاقی که اجتناب‌ناپذیر است.

در قرن هجدهم کمی بعد از اینکه بنجامین فرانکلین اداره پست را در ایالات متحده راه‌اندازی کرد، مجرمان کلاهبرداری پستی را ابداع کردند. در قرن نوزدهم مجرمان با تلگراف و تلفن کلاهبرداری تلگرافی و تلفنی را ابداع کردند. در قرن بیستم که متخصصان فناوری، اینترنت را اختراع کردند، برای همه افراد آگاه از تاریخ روشن بود که ابداع انواع جدیدی از کلاهبرداری گریزناپذیر است.

چالش این بود که بخش فناوری همیشه به آینده نگاه می‌کرد که البته شایسته تحسین هم هست. مشکل این بود که افراد کمی وقت می‌گذاشتند یا حتی می‌پذیرفتند که به اندازه کافی به پشت سر توجه کنند تا از دانش گذشته برای پیش‌بینی مشکلات پیش رو استفاده کنند.

در عرض یک سال پس از میهمانی هوش مصنوعی در داووس، این فناوری به‌مرور پرسش‌های گسترده‌تری را برای جامعه ایجاد کرد. در گذشته محور مبحث اعتماد مردم به فناوری حریم خصوصی و امنیت بود، اما اکنون هوش مصنوعی هم افراد را نگران کرده و به‌سرعت به موضوعی محوری در بحث‌های عمومی تبدیل شده بود.

قرار بود به کامپیوترها توانایی یادگیری و تصمیم‌گیری داده شود و بیش از پیش از مداخله انسانی بی‌نیاز شوند. اما چطور این تصمیمات را می‌گرفتند؟ بهترین ویژگی‌های انسان را بازتاب می‌دادند یا ویژگی‌های کمتر دلگرم‌کننده؟ بیش از پیش روشن شده بود که اگر فناوری‌های هوش مصنوعی بخواهند برای جامعه مفید باشند، حتماً باید با اصول اخلاقی قدرتمند هدایت شوند.

از مدت‌ها قبل می‌شد آمدن این روز را پیش‌بینی کرد. چند سال پیش از اینکه پژوهشگران کالج دارتموث مطالعه‌ای تابستانی را در سال ۱۹۵۶ انجام دهند تا توسعه کامپیوترهایی را بررسی کنند که می‌توانند یاد بگیرند (برخی افراد این مطالعه را آغاز بحث‌های دانشگاهی درباره هوش مصنوعی می‌دانند)، «آیزاک آسیموف» قوانین سه‌گانه روباتیک را در داستان کوتاه «دور باطل» نوشته بود. این داستان روایتی علمی-تخیلی بود در مورد تلاش انسان برای ایجاد قوانینی اخلاقی که سیستم تصمیم‌گیری خودران مبتنی بر هوش مصنوعی روبات‌ها را هدایت کنند. همان‌طور که در فیلم جذاب «من، روبات» (I, Robot) محصول سال ۲۰۰۴ و با هنرنمایی ویل اسمیت نشان داده می‌شود، این تلاش فرجام خوبی پیدا نمی‌کند.

هوش مصنوعی از اواخر دهه ۱۹۵۰ کم‌وبیش و با فرازونشیب توسعه یافته بود. یکی از دوره‌های برجسته در این مسیر دوره کوتاهی در میانه دهه ۱۹۸۰ با رگباری از هیاهو، سرمایه‌گذاری، استارت‌آپ و توجه رسانه‌ای در مورد «سیستم‌های خبره» بود، اما چه شد که هوش مصنوعی ۶۰ سال بعد در سال ۲۰۱۷ اینچنین مطرح شد؟ هوش مصنوعی دوباره مدی زودگذر نشده بود. اتفاقاً برعکس بازتاب‌دهنده روندها و مسائلی بود که بسیار گسترده‌تر بودند و از مدت‌ها قبل به سوی همگرایی پیش می‌رفتند.

هیچ تعریف همگانی پذیرفته‌شده‌ای برای هوش مصنوعی در بخش فناوری وجود ندارد و متخصصان فناوری به شکل قابل درکی دیدگاه خودشان را با قدرت به پیش می‌برند. در سال ۲۰۱۶ مدتی را در مورد ظهور مسائل جدید هوش مصنوعی با «دیو هاینر» (Dave Heiner) از مایکروسافت سپری کردم که در آن زمان با «اریک هورویتز» (Eric Horvitz) کار می‌کرد که مدت زیادی بود بسیاری از پژوهش‌های بنیادی ما در این حوزه را رهبری می‌کرد. وقتی با اصرار از دیو خواستم، تعریفی به من ارائه داد که همچنان فکر می‌کنم

روش مفیدی برای نگاه‌کردن به مقوله هوش مصنوعی است. دیو گفت: «هوش مصنوعی سیستمی کامپیوتری است که می‌تواند با تشخیص الگوهای داده‌های تزریق‌شده به آن از تجربه‌ها یاد بگیرد و در نتیجه تصمیم‌گیری کند». اریک از تعریفی تا حدی گسترده‌تر استفاده می‌کند و می‌گوید: «هوش مصنوعی مطالعه مکانیسم‌های محاسباتی زیربنایی در تفکر و رفتار هوشمندانه است». هرچند تفکر و رفتار هوشمندانه اغلب شامل داده می‌شود، اما می‌تواند مبتنی بر تجربه‌هایی مثل بازی‌کردن، درک زبان‌های طبیعی و مانند آن هم باشد. توانایی یک کامپیوتر در یادگیری از داده‌ها و تجربه و بعد تصمیم‌گیری (یعنی جوهره این تعریف‌های هوش مصنوعی) مبتنی بر دو قابلیت فناورانه بنیادی یعنی ادراک انسانی و شناخت انسانی است.

توانایی کامپیوترها برای ادراک آنچه در دنیا اتفاق می‌افتد، به نحوی که انسان‌ها از طریق بینایی و شنوایی ادراک می‌کنند، ادراک انسانی خوانده می‌شود. از زاویه‌ای دستگاه‌ها از زمان اختراع دوربین در دهه ۱۸۳۰ قادر به «دیدن» دنیا بودند، اما همیشه باید انسانی حضور داشته باشد تا درک کند در تصویر چه چیزی ثبت شده است. به همین ترتیب دستگاه‌ها از زمانی که توماس ادیسون در سال ۱۸۷۷ گرامافون را اختراع کرد، قادر به «شنیدن» بودند، اما هیچ دستگاهی نمی‌توانست گفتار را با دقت انسان درک و به متن تبدیل کند.

تشخیص تصویر و گفتار از دیرباز از آرزوهای دست‌نیافتنی پژوهشگران حوزه علوم کامپیوتر بوده است. در سال ۱۹۹۵ که بیل گیتس واحد تحقیقات مایکروسافت را بنیان‌گذاری کرد، یکی از اولین اهداف «ناتان مروالد» (Nathan Myhrvold)، رهبر این واحد جذب پژوهشگران ارشد تشخیص تصویر و گفتار بود. هنوز آن زمانی را در دهه ۱۹۹۰ به یاد دارم که تیم پژوهش‌های بنیادی مایکروسافت خوش‌بینانه پیش‌بینی کرد که کامپیوترها به‌زودی می‌توانند گفتار را به‌خوبی انسان درک کنند.

متخصصان دانشگاه و بخش فناوری نیز با پژوهشگران مایکروسافت هم‌عقیده بودند. واقعیت این بود که بهبود تشخیص گفتار بیشتر از آنچه متخصصان پیش‌بینی می‌کردند طول کشید. هدف تشخیص تصویر و گفتار این بود که کامپیوترها را قادر به ادراک جهان با نرخ دقتی مشابه دقت انسان کنیم که البته کمتر از ۱۰۰ درصد است.

همه اشتباه می‌کنیم، از جمله در تشخیص آنچه دیگران به ما می‌گویند. متخصصان برآورد می‌کنند که نرخ دقت ما در درک گفتار تقریباً ۹۶ درصد است و ذهن ما آن‌قدر سریع جاهای خالی را پر می‌کند که ما به آن چهار درصد فکر نمی‌کنیم. اما تا زمانی که سیستم‌های هوش مصنوعی به این سطح نرسند، احتمالاً اشتباهات کامپیوترها بیشتر ما را اذیت می‌کنند تا اینکه تحت تأثیر عددی مثل نرخ موفقیت ۹۰ درصد قرار بگیریم.

تا سال ۲۰۰۰ کامپیوترها به آستانه ۹۰ درصدی در تشخیص تصویر و گفتار رسیدند، اما پیشرفت یک دهه متوقف شد. بعد از سال ۲۰۱۰ پیشرفت از سر گرفته شد. وقتی انسان‌های صد سال بعد به تاریخ قرن بیست‌ویکم نگاه کنند، احتمالاً به این جمع‌بندی می‌رسند که دهه ۲۰۱۰ تا ۲۰۲۰ زمانی بود که هوش مصنوعی به اثربخشی رسید.

سه پیشرفت اخیر فناوری، سکوی پرتابی را فراهم کردند که اوج‌گرفتن هوش مصنوعی را امکان‌پذیر ساخت. اول اینکه قدرت رایانش سرانجام به مقدار لازم برای انجام محاسبات بسیار زیاد مورد نیاز رسید. دوم اینکه رایانش ابری مقادیر زیادی از این قدرت رایانش و ظرفیت ذخیره‌سازی را بدون نیاز به سرمایه‌گذاری زیاد در تعداد بسیار زیادی سخت‌افزار در دسترس افراد و سازمان‌ها قرار داد. سوم اینکه رشد انفجاری داده‌های دیجیتال امکان ایجاد مجموعه‌های داده بسیار بزرگ‌تر برای آموزش سیستم‌های مبتنی بر هوش مصنوعی را فراهم کرد. معلوم نبود بدون این عناصر، هوش مصنوعی بتواند با این سرعت پیشرفت کند.

اما عنصر اساسی چهارمی لازم بود که در کمک به متخصصان کامپیوتر و داده برای اثربخش کردن هوش مصنوعی نقشی حیاتی داشته است. این عنصر به قابلیت فناورانه دوم و حتی اساسی‌تر مورد نیاز هوش مصنوعی یعنی شناخت مربوط است. شناخت در واقع توانایی کامپیوتر در استدلال و یادگیری است.

به مدت چند دهه بحث‌های پرحرارتی درباره بهترین رویکرد فناورانه برای ایجاد توانایی فکر کردن در کامپیوترها وجود داشت. یکی از رویکردها مبتنی بر «سیستم‌های خبره» بود. سیستم‌های خبره که در اواخر دهه‌های ۱۹۷۰ و ۱۹۸۰ بسیار پرطرفدار بودند، شامل جمع‌آوری مقادیر زیادی از واقعیت‌ها و ایجاد قواعدی می‌شد که کامپیوترها می‌توانستند در زنجیره‌های استدلال منطقی برای تصمیم‌گیری به کار بگیرند. همان‌طور

که یک متخصص فناوری می‌گوید، این رویکرد مبتنی بر قاعده نمی‌توانست متناسب با پیچیدگی مسائل دنیای واقعی افزایش مقیاس پیدا کند. «در حیطه‌های پیچیده تعداد قواعد فوق‌العاده زیاد هستند و از آنجایی که واقعیت‌های جدید غیرخودکار اضافه می‌شوند، پیگیری استثناها نسبت به سایر قواعد و تعاملات با آنها غیرممکن می‌شود.» ما در زندگی انسانی در بسیاری از ابعاد نه از استدلال از طریق قواعد؛ بلکه از تشخیص الگوها بر اساس تجربه استفاده می‌کنیم. با نگاه به گذشته شاید بتوان گفت سیستم مبتنی بر قواعد پرجزئیات رویکردی بود که فقط به مذاق وکلا خوش می‌آمد.

از دهه ۱۹۸۰ به بعد رویکرد دیگری به هوش مصنوعی، برتری خود را اثبات کرد. در این رویکرد از روش‌های آماری برای تشخیص الگو، پیش‌بینی و استدلال استفاده می‌کنیم و در عمل سیستم‌ها را از طریق الگوریتم‌هایی می‌سازیم که از داده‌ها یاد می‌گیرند. در طول یک دهه گذشته جهش‌هایی در علوم کامپیوتر و داده، به استفاده گسترده از مقوله به‌اصطلاح یادگیری عمیق یا شبکه‌های عصبی منجر شده است. مغز ما انسان‌ها دارای نورون‌هایی با ارتباطات سیناپسی هستند که به ما توانایی تشخیص الگوها در دنیای اطراف‌مان را می‌دهند. شبکه‌های عصبی کامپیوتری دارای واحدهای رایانشی هستند که آنها را نورون می‌خوانیم و به‌صورت مصنوعی با هم در ارتباط هستند تا سیستم‌های هوش مصنوعی بتوانند استدلال کنند. در واقع رویکرد یادگیری عمیق با استفاده از لایه‌های زیادی از این نورون‌های مصنوعی مقادیر بسیار زیادی از داده‌های مربوط را به کامپیوتر تزریق می‌کند تا آن را برای تشخیص الگو آموزش دهد. این فرایند به قدرت رایانش و داده‌های فراوانی نیاز دارد. به همین دلیل پیشرفت در آن نیازمند پیشرفت‌های دیگری بود که قبلاً ذکر شدند. همچنین نیازمند پیشرفت‌های شگرف جدیدی در روش‌های مورد نیاز برای آموزش شبکه‌های عصبی چندلایه‌ای بود که از حدود ۱۰ سال قبل به‌مرور به ثمر نشسته بودند.

تأثیر جمعی این تغییرات به پیشرفت‌های سریع و تحسین‌برانگیزی در سیستم‌های مبتنی بر هوش مصنوعی منجر شد. در سال ۲۰۱۶ تیم سیستم تشخیص تصویر واحد تحقیقات مایکروسافت در چالشی ویژه برای شناسایی تعداد زیادی از اشیا در کتابخانه‌ای به نام «ایمیج‌نت» (ImageNet) عملکردی مشابه انسان داشت. این تیم

سپس کار مشابهی را در مورد تشخیص گفتار انجام داد و در چالشی ویژه به نام مجموعه داده «سوئیچ‌بورد» (Switchboard) به نرخ دقت ۹۴٫۱ درصد رسید. به عبارت دیگر کامپیوترها به‌مرور داشتند دنیا را به‌خوبی انسان‌ها درک می‌کردند. همین پدیده در مورد ترجمه زبان‌ها نیز اتفاق افتاد که مستلزم این است که کامپیوترها معنی واژه‌های متفاوت و از جمله تفاوت‌های ظریف و عبارت‌های عامیانه را درک کنند.

به‌سرعت مقالاتی منتشر شدند که می‌پرسیدند اگر کامپیوتری مبتنی بر هوش مصنوعی بتواند به‌تنهایی فکر کند و با سرعت ابرانسانی استدلال کند، آیا دستگاه‌هایی ساخته خواهند شد که بتوانند بر دنیا مسلط شوند. این مقالات نگرانی مردم را در پی داشتند. این حالت را متخصصان فناوری ابرهوش یا به عبارت دیگر «تکینگی» می‌خوانند. همان‌طور که وقتی در سال ۲۰۱۶ بر این مسئله متمرکز شدیم، دیو هاینر استدلال کرد این مسئله بیش از اندازه زمان و توجه را به خود جلب کرده و حواس را از مسائل مهم‌تر و فوری‌تر پرت کرده بود. دیو می‌گفت: «در حال حاضر این مسئله کاملاً به داستان‌های علمی-تخیلی تعلق دارد و مسائل فوری‌تر ناشی از هوش مصنوعی را به حاشیه برده است.»

آن مسائل فوری‌تر همان سال در همایشی با پشتیبانی مالی کاخ سفید مطرح شده بودند. بحث اصلی همایش در مورد مقاله‌ای از پروپابلیکا (ProPublica) با عنوان «سوگیری ماشین» بود. عنوان فرعی این مقاله حرف اصلی را زده بود: «در نقاط مختلف کشور از نرم‌افزاری برای پیش‌بینی مجرمان آینده استفاده می‌شود که علیه سیاه‌پوستان سوگیری دارد.» از هوش مصنوعی بیش از پیش برای پیش‌بینی در طیف گسترده‌ای از محیط‌ها و شرایط استفاده می‌شد و این نگرانی ایجاد شده بود که این سیستم‌ها ممکن است در سناریوهای گوناگون نسبت به برخی گروه‌ها از جمله افراد رنگین‌پوست سوگیری منفی داشته باشند.

مسئله سوگیری که در سال ۲۰۱۶ در پروپابلیکا مطرح شد، مسئله‌ای جدی بود. این مسئله دو عامل را بازتاب می‌داد که اگر قرار بود هوش مصنوعی همان عملکردی را داشته باشد که مردم به‌درستی انتظار دارند، باید به آنها رسیدگی می‌کردیم. عامل اول شامل پروژه‌هایی می‌شود که از مجموعه داده‌های جهت‌دار استفاده می‌کنند. برای مثال

مجموعه داده تشخیص چهره‌ای که عکس‌هایی از چهره‌های افراد دارد، ممکن است به اندازه کافی عکس از مردان سفیدپوست داشته باشد تا چهره مردان سفیدپوست را با نرخ دقت زیادی پیش‌بینی کند. اما اگر مجموعه‌های داده کوچک‌تری از عکس‌های زنان یا رنگین‌پوستان داشته باشد، آن وقت احتمالاً نرخ خطا در تشخیص این گروه‌ها زیاد می‌شود.

اتفاقاً دو دانشجوی دکتری در پژوهش‌شان در مورد پروژه‌ای به نام «طیف‌های جنسیت» دقیقاً به همین نتیجه رسیدند. «جوی بولامووینی»، پژوهشگر ام‌آی‌تی؛ دارای بورسیه رودز (Rhodes Scholarship) دانشگاه آکسفورد و «تیمنت گبرو» (Timnet Gebru)، پژوهشگر دانشگاه استنفورد تلاش کردند با مقایسه نرخ دقت تشخیص چهره برای جنسیت‌ها و نژادهای متفاوت درک عمومی را از سوگیری هوش مصنوعی بهبود ببخشند. برای مثال این زنان مشاهده کردند نرخ خطای تشخیص جنسیت برای چهره سیاست‌مداران سیاه‌پوست در آفریقا بیشتر از سیاست‌مداران سفیدپوست در شمال اروپاست. حتی بولامووینی که زن آمریکایی آفریقایی‌تباری است، مشاهده کرد که برخی از سیستم‌ها او را مرد شناسایی می‌کنند.

پژوهش بولامووینی و گبرو جنبه دومی از سوگیری را مشخص کرد که باید آن را در نظر بگیریم. سخت است فناوری مناسبی برای جهان بسازیم؛ بدون اینکه اول تیمی تشکیل بدهیم که از تنوع جهانی برخوردار است. همان‌طور که یافته‌های آنها نشان می‌دهد، گروهی متنوع‌تر از پژوهشگران و مهندسان احتمالاً مشکلات سوگیری را بیشتر درک می‌کنند و فقط مشکلاتی را نمی‌بینند که روی خودشان تأثیر می‌گذارند.

اگر هوش مصنوعی به کامپیوترها توانایی گسترده‌ای برای یادگیری از تجربه‌ها و تصمیم‌گیری بدهد، می‌خواهیم چه نوع تجربه‌هایی داشته باشند و در واگذاری چه تصمیماتی به آنها مشکلی نداریم؟

اریک هورویتز در اواخر سال ۲۰۱۵ این نگرانی‌ها را با جامعه علوم کامپیوتر در میان گذاشت. اریک در مقاله‌ای که به همراه فرد دیگری در مجله‌ای پژوهشی نوشته بود، اعلام کرد که بیشتر دانشمندان علوم کامپیوتر ریسک‌های آخرالزمانی، تکینگی را در بهترین حالت بعید در نظر می‌گیرند، اما زمان آن رسیده که با جدیت بیشتری به طیف فزاینده‌ای

از سایر مسائل توجه کنیم. سال بعد ساتیا مشعل را در دست گرفت و در مجله آنلاین «اسلیت» مقاله‌ای نوشت و پیشنهاد داد که «بحث باید در مورد ارزش‌های نهادینه‌شده در افراد و مؤسساتی باشد که این فناوری را می‌سازند». ساتیا در ضمن چند ارزش اولیه مثل حریم خصوصی، شفافیت و پاسخگویی را مطرح کرد که باید نهادینه شوند.

اواخر سال ۲۰۱۷ به این جمع‌بندی رسیدیم که در واقع حرف‌مان این است که به رویکردی توسعه‌یافته به اخلاقیات در هوش مصنوعی نیاز داریم. به هیچ‌وجه حرف ساده‌ای نبود. دستیابی کامپیوترها به توانایی اتخاذ تصمیماتی که در گذشته فقط در اختیار انسان‌ها بود، همه پرسش‌های اخلاقی برای انسان را به پرسش‌های اخلاقی برای کامپیوترها تبدیل می‌کرد. اگر هزاران سال بحث بین فیلسوف‌ها به شکل‌گیری پاسخ‌های روشن و جهان‌شمولی منجر نشده بود، آن وقت بعید بود صرفاً به این خاطر که نیاز داشتیم این پرسش‌ها را در کامپیوترها به کار ببریم، یک‌شبه به اجماع دست یابیم.

سال ۲۰۱۸ شرکت‌هایی مثل مایکروسافت و گوگل که طلایه‌دار هوش مصنوعی بودند، رسیدگی جدی به این چالش را شروع کردند. همراه با متخصصان دانشگاهی و غیردانشگاهی متوجه شدیم که به مجموعه‌ای از اصول اخلاقی نیاز داریم تا سرلوحه توسعه هوش مصنوعی قرار دهیم. در مایکروسافت سرانجام در مورد شش اصل اخلاقی برای این حوزه به توافق رسیدیم.

اصل اول از ما می‌خواست به نیاز به انصاف یا همان مسئله سوگیری پاسخ بدهیم. بعد به سراغ دو حوزه دیگر رفتیم که دست‌کم تا حدی در موردشان اجماع عمومی وجود داشت. این دو حوزه اهمیت قابلیت اعتماد و ایمنی و نیاز به حریم خصوصی و امنیت بودند. جنبه‌های مهمی از این مفاهیم از طریق قانون و رگولیشن و در واکنش به تحولات فناورانه قبلی پیشرفت کرده بودند. قانون مسئولیت کالا و قوانین مشابه استانداردهای قابلیت اعتماد و ایمنی را در پاسخ به نیازهای حوزه راه‌آهن و خودرو تعیین کرده بودند. به همین ترتیب هنجارهای حریم خصوصی و امنیت در پاسخ به تحولات فناوری اطلاعات و ارتباطات پدیدار شده بودند. هرچند هوش مصنوعی چالش‌های جدیدی را در این حوزه‌ها به وجود آورده بود، اما می‌توانستیم به مفاهیم قانون قبلی اتکا و از آنها بهره‌برداری کنیم.

اصل چهارم ما به مسئله‌ای می‌پرداخت که کارمندان‌مان از سال ۲۰۱۴ که ساتیا مدیرعامل شده بود، پشت آن بسیج شده بودند. این اصل اهمیت ایجاد فناوری فراگیری بود که به نیازهای افراد کم‌توان پاسخ می‌داد. طبیعی بود که تمرکز شرکت بر فناوری فراگیر شامل هوش مصنوعی هم می‌شد. تصور کنید اگر کامپیوترها بتوانند ببینند، چقدر می‌توانند برای افراد نابینا مفید باشند و اگر بتوانند بشنوند، چقدر می‌توانند برای افراد ناشنوا مفید باشند. علاوه بر این برای دنبال‌کردن این فرصت‌ها لزوماً نیازی نبود دستگاه‌های کاملاً جدیدی ابداع و توزیع کنیم. تلفن‌های هوشمند افراد همین حالا هم دوربین‌هایی داشتند که می‌توانستند ببینند و میکروفن‌هایی داشتند که می‌توانستند بشنوند. با تعیین شمول به‌عنوان اصل اخلاقی چهارم به‌تدریج مسیر پیشرفت در این حوزه مشخص می‌شد.

اگرچه هر چهار اصل مهم بودند، اما متوجه شدیم که همه بر دو اصل دیگر استوارند که در موفقیت اصول دیگر نقش اساسی دارند. اصل اول شفافیت بود. شفافیت برای ما به این معنی بود که اطمینان حاصل کنیم اطلاعات مربوط به نحوه اتخاذ تصمیمات مهم توسط هوش مصنوعی در دسترس عموم و قابل درک هستند. هرچه نباشد اگر سازوکارهای داخلی هوش مصنوعی پنهان نگه داشته شوند، مردم چطور می‌توانند به هوش مصنوعی اعتماد کنند و رگولاتورهای آینده چطور می‌توانند پیروی آن از چهار اصل اول را ارزیابی کنند؟

برخی افراد استدلال می‌کنند که توسعه‌دهندگان هوش مصنوعی باید الگوریتم‌های مورد استفاده خود را منتشر کنند، اما جمع‌بندی ما این بود که این کار احتمالاً در بیشتر شرایط روشنگر نخواهد بود یا اسرار تجاری ارزشمندی را افشا خواهد کرد که رقابت در بخش فناوری را تضعیف می‌کند. پیش از این در ائتلاف مشارکت در هوش مصنوعی (Partnership on AI) در حال همکاری با پژوهشگران و سایر شرکت‌های فناوری بودیم تا رویکردهای بهتری را توسعه دهیم. تمرکز تازه بر توضیح‌پذیر کردن هوش مصنوعی در حقیقت همان توصیف عناصر کلیدی مورد استفاده در تصمیم‌گیری بود.

آخرین اصل اخلاقی هوش مصنوعی، پاسخگویی، سنگ بنای همه اصول دیگر است. آیا جهان آینده‌ای را می‌سازد که در آن کامپیوترها به افراد پاسخگو می‌مانند و افرادی که

این دستگاه‌ها را طراحی می‌کنند، به بقیه پاسخگو می‌مانند؟ این پرسش شاید یکی از پرسش‌های تعیین‌کننده نسل ما باشد.

برای عملی‌شدن این اصل نهایی انسان‌ها باید در حلقه تصمیم‌گیری بمانند تا سیستم‌های مبتنی بر هوش مصنوعی خودسرانه و بدون ارزیابی، قضاوت و دخالت انسان عمل نکنند. به عبارت دیگر تصمیمات مبتنی بر هوش مصنوعی که تأثیر قابل توجهی بر حقوق افراد می‌گذارند، باید مشمول ارزیابی و کنترل انسانی معنی‌دار بمانند. در نتیجه باید افرادی وجود داشته باشند که برای ارزیابی تصمیمات هوش مصنوعی آموزش دیده باشند.

همچنین به این جمع‌بندی رسیدیم که در این راستا فرایندهای حکمرانی گسترده‌تر حیاتی هستند. هر نهادی که هوش مصنوعی را توسعه می‌دهد یا به کار می‌گیرد، به سیاست‌ها، فرایندها، برنامه‌های آموزشی، سیستم‌های تطبیق و افراد جدیدی نیاز دارد تا توسعه و پیاده‌سازی سیستم‌های هوش مصنوعی را ارزیابی کنند و در این مورد مشاوره ارائه دهند.

اصول‌مان را در ژانویه ۲۰۱۸ منتشر کردیم و متوجه شدیم روی مسئله حساسی دست گذاشته‌ایم. مشتریان خواستار گزارش‌هایی درباره فناوری هوش مصنوعی ما و همچنین رویکردمان به مسائل و روش‌های اخلاقی شدند. البته امری منطقی بود. استراتژی کلی شرکت «دموکراتیک‌کردن هوش مصنوعی» با فراهم‌کردن دسترسی به عناصر سازنده این فناوری (برای مثال ابزارهای تشخیص تصویر و گفتار و یادگیری ماشین) بود تا مشتریان بتوانند خدمات هوش مصنوعی سفارشی خودشان را ایجاد کنند. اما در این راستا باید رویکرد پیشرفته‌ای به اخلاقیات در هوش مصنوعی توسعه داده می‌شد و به اندازه خود این فناوری گسترش می‌یافت.

این فراگیری هوش مصنوعی همچنین به این معنی بود که رگولیشن این فناوری نه‌تنها محتمل؛ بلکه ضروری است. درک عمومی از اخلاقیات در هوش مصنوعی می‌توانست کمک کند افراد اخلاق‌مدار به داشتن عملکرد اخلاقی ترغیب شوند. اما در مورد افرادی که علاقه‌ای ندارند اخلاقی عمل کنند، چه کار باید انجام دهیم؟ تنها راه برای اطمینان از اینکه همه سیستم‌های هوش مصنوعی طبق استانداردهای اخلاقی ویژه‌ای عمل می‌کنند، این

بود که آنها را ملزم به این کار کنیم و برای رسیدن به این هدف باید نیروی قانون و رگولیشن را پشتیبان استانداردهایی می‌کردیم که جوامع پذیرفته‌اند.

شواهد نشان می‌داد که تلاش‌های رگولاتوری با سرعتی بیشتر از آن چارچوب زمانی پنج‌ساله‌ای پیش می‌روند که سال قبل در داووس پیش‌بینی کرده بودم. این موضوع زمانی برایمان روشن‌تر شد که در آوریل ۲۰۱۸ در سنگاپور بودیم و با مقامات دولتی مسئول در زمینه مسائل هوش مصنوعی دیدار کردیم. این مسئولان به ما گفتند: «در مورد این مسائل صبر جایز نیست. باید جلوتر از فناوری باشیم. می‌خواهیم اولین پیشنهادهایمان را نه در عرض چند سال؛ بلکه در عرض چند ماه منتشر کنیم.»

وقتش که برسد، مسائل اخلاقی هوش مصنوعی از گفت‌وگوهایی کلی به مباحثی ملموس تبدیل می‌شوند. به احتمال زیاد این مباحث شامل مسائل بحث‌برانگیز منحصربه‌فردی می‌شوند. هرچند هم‌اکنون نمی‌توان پیش‌بینی کرد که در ۵ یا ۱۰ سال آینده در مورد چه مسائلی بحث خواهیم کرد، ولی می‌توانیم از مسائلی که تاکنون مطرح شده‌اند، بینش‌هایی را بیرون بکشیم.

یکی از اولین موارد از این دست مسائل بحث‌برانگیز که در سال ۲۰۱۸ مطرح شد، استفاده قریب‌الوقوع از هوش مصنوعی در تسلیحات نظامی بود. این مسئله در بحث‌های عمومی با عبارت «روبات‌های قاتل» مطرح شد؛ عبارتی که تصاویری را از داستان‌های علمی‌ـتخیلی به یاد می‌آورد. تصویری است که افراد به‌راحتی درک می‌کنند، شاید دلیلش هم این باشد که مجموعه فیلم‌های ترمیناتور از زمان اکران اولش در سال ۱۹۸۴ به بعد، در هر دهه دست‌کم یک فیلم عرضه کرده است. به عبارت دیگر اگر شما نوجوان یا بزرگ‌تر باشید، به احتمال زیاد خطرات تسلیحات خودکار را در سینما مشاهده کرده‌اید.

یکی از درس‌های اولیه این بحث در حوزه سیاست عمومی نیاز به ایجاد درک یا طبقه‌بندی ظریف‌تر و دقیق‌تر از انواع فناوری‌های دخیل است. در گفت‌وگو با رهبران نظامی سراسر دنیا به یک وجه مشترک‌شان پی بردم؛ هیچ‌کدام نمی‌خواهند صبح بیدار شوند و بفهمند وقتی آنها خواب بودند، دستگاه‌ها خودشان جنگی را شروع کرده‌اند. تصمیم‌گیری در مورد جنگ و صلح فقط باید در اختیار انسان‌ها باشد.

اما منظور این نیست که مسئولان نظامی جهان در مورد سایر مسائل هم اتفاق‌نظر دارند. تمایزات اینجا خود را نشان می‌دهند. «پل شاره» (Paul Scharre)، یکی از مسئولان دفاعی سابق ایالات متحده که در اندیشکده‌ای کار می‌کند، پرسش‌های بجایی را در کتابش با عنوان «ارتش بی‌نفر: تسلیحات خودکار و آینده جنگ» مطرح می‌کند. همان‌طور که او نشان می‌دهد یکی از پرسش‌های محوری این است که کامپیوترها نه‌فقط چه زمانی؛ بلکه چگونه باید توانمند شوند تا بدون ارزیابی انسانی با سلاحی شلیک کنند؟ از طرفی هرچند پهپادی با بینایی کامپیوتر و تشخیص چهره ممکن است در شناسایی تروریستی در صحنه نبرد دقیق‌تر از انسان عمل کند، اما نمی‌توان نتیجه گرفت که مسئولان نظامی باید- یا بهتر است- نفرات یا منطق انسانی را از حلقه تصمیم‌گیری خارج کنند. از طرف دیگر اگر ده‌ها موشک به سمت ناوی پرتاب شد، سامانه‌های دفاع ضدموشکی سیستم یورشی «آگیس» (Aegis) باید بر اساس تصمیم‌گیری مبتنی بر کامپیوتر واکنش نشان دهند. اما در این حالت هم سناریوهای متنوعی وجود دارد و کاربرد سیستم تسلیحات را می‌توان سفارشی‌سازی کرد. معمولاً انسان باید اولین تصمیم را در مورد شلیک بگیرد، اما برای اینکه انسان‌ها همه اهداف مجزا را تأیید کنند، وقت نیست.

با توجه به نگرانی‌های احتمالی نسبت به تسلیحات خودکار، برخی استدلال کرده‌اند که شرکت‌های فناوری باید هر گونه همکاری با ارتش در مورد فناوری‌های مبتنی بر هوش مصنوعی را رد کنند. برای مثال گوگل بعد از اعتراض کارمندانش از قراردادی در زمینه هوش مصنوعی با پنتاگون خارج شد. وقتی شماری از کارمندان ما نگرانی‌های مشابهی را مطرح کردند، ما هم با همین مسئله روبه‌رو شدیم. از دیرباز برای ارتش ایالات متحده و سایر ارتش‌ها کار انجام داده بودیم؛ واقعیتی که وقتی دوباره یادآوری شد که چند سال پیش از ناو هواپیمابر «یواس‌اس نیمیتز» (USS Nimitz) در بندرگاه دائمش در شهر «اورت» (Everett) ایالت واشنگتن در نزدیکی شمال سیاتل بازدید کردم. این ناو هواپیمابر بیش از چهار هزار کامپیوتر داشت که از سیستم‌عامل ویندوز سرور ما بهره می‌بردند و طیف گسترده‌ای از کارکردهای کشتی را مدیریت می‌کردند.

اما بسیاری از افراد نظر قابل درکی دارند و می‌گویند سیستم‌های مبتنی بر هوش

مصنوعی در طبقه‌بندی متفاوتی نسبت به این فناوری‌های پلتفرمی قرار می‌گیرند. می‌دانستیم که این فناوری جدید نسل جدیدی از مسائل پیچیده را مطرح کرده و وقتی در حال بررسی قراردادی احتمالی برای ارائه فناوری واقعیت افزوده و دستگاه‌های «هولولنز» (HoloLens) به سربازان ارتش ایالات متحده بودیم، در مورد کارهایی که باید انجام بدهیم بحث مفصلی کردیم.

بر خلاف گوگل به این جمع‌بندی رسیدیم که باید همچنان بهترین فناوری‌هایمان را به ارتش ایالات متحده و همچنین سایر دولت‌ها و کشورهای متحد خود ارائه بدهیم که در آنها به فرایندهای دموکراتیک و حساسیت‌های بنیادین در مورد حقوق بشر اطمینان داریم. سامانه‌های دفاعی-نظامی آمریکا و ناتو از گذشته به دسترسی به پیشرفته‌ترین فناوری‌ها وابسته بوده‌اند. همان‌طور که به‌صورت خصوصی و علنی گفتیم «به اقتدار قدرت دفاعی ایالات متحده باور داریم و می‌خواهیم افرادی که از این کشور دفاع می‌کنند به بهترین فناوری‌های کشور از جمله فناوری‌های مایکروسافت دسترسی داشته باشند.»

همزمان متوجه بودیم که برخی کارمندان‌مان به کار کردن در قراردادهای دفاعی برای ایالات متحده یا سایر سازمان‌های نظامی تمایلی ندارند. برخی از این کارمندان شهروندان کشورهای دیگر بودند، برخی دیدگاه‌های اخلاقی متفاوتی داشتند یا صلح‌طلب بودند و برخی دیگر صرفاً می‌خواستند انرژی‌شان را وقف کاربردهای دیگر فناوری کنند. به این دیدگاه‌ها احترام گذاشتیم و به‌سرعت اعلام کردیم امکانی را برای این افراد فراهم می‌کنیم تا روی سایر پروژه‌ها کار کنند. با توجه به اندازه و تنوع فناوری‌های موجود در مایکروسافت، احساس می‌کردیم به احتمال زیاد می‌توانیم این درخواست‌ها را برآورده کنیم.

اما در عین حال فکر نمی‌کردیم هیچ‌کدام از این کارها ما را از نیاز به بررسی کامل و پرداختن به مسائل اخلاقی پیچیده ناشی از تلفیق هوش مصنوعی و تسلیحات مبرا کند. وقتی در مورد این جنبه در جمع مدیران ارشد بحث می‌کردیم، اشاره کردم که از قرن نوزدهم که فشنگ توخالی و بعد دینامیت به میدان نبرد وارد شد، مسائل اخلاقی در توسعه تسلیحات مهم بوده‌اند. ساتیا به من یادآوری کرد که تاریخ مسائل اخلاقی مربوط به جنگ، به نوشته‌های «سیسرون»، فیلسوف و سیاست‌مدار رومی برمی‌گردد. بعد همان شب ایمیلی برای من فرستاد که در آن نوشته بود مادرش از او راضی نیست که

سیسرون را به یاد داشته، اما حماسه هندی مهابهاراتا را فراموش کرده باشد (خوشبختانه در ایمیلش لینکی از مدخل این اثر در ویکی‌پدیا را هم گذاشته بود تا بیشتر در مورد آن یاد بگیرم).

این نوع بحث‌ها باعث شد به این نتیجه برسیم که به‌عنوان شهروندان شرکتی کنشگر نباید پرداختن به مسائل اخلاقی را متوقف کنیم. به‌علاوه باور داشتیم که حضور ما می‌تواند در شکل‌گیری مسائل سیاست عمومی در حال ظهور کمک کند. همان‌طور که به کارمندان‌مان گفتیم، معتقد بودیم هیچ‌کدام از شرکت‌های فناوری در پرداختن به مسائل سیاست‌گذاری ناشی از فناوری‌های جدید، به‌ویژه در مورد نظارت الکترونیکی دولت و تسلیحات سایبری، بیشتر از ما فعالیت نکرده‌اند. احساس می‌کردیم در این مورد هم بهترین رویکرد حمایت از سیاست‌ها و قوانین مسئولانه در مورد هوش مصنوعی و ارتش است. آستین‌ها را بالا زدیم تا بیشتر یاد بگیریم و دیدگاه‌های تصفیه‌شده‌تری به دست آوریم. این کار باعث شد دوباره به سراغ شش اصل اخلاقی‌مان برویم که به مسائل اخلاقی مربوط به هوش مصنوعی و تسلیحات شکل داده بودند. به این جمع‌بندی رسیدیم که سه اصل قابلیت اعتماد و ایمنی، شفافیت و مهم‌تر از همه پاسخگویی بیش از همه در معرض خطر هستند. تنها با پرداختن به هر سه اصل می‌توان اعتماد عمومی را به این موضوع حفظ کرد که هوش مصنوعی به نحوی پیاده‌سازی خواهد شد که کنترل آن در دست انسان‌ها بماند.

همچنین به این نتیجه رسیدیم که شباهت‌های مهمی بین این مسائل و مسائلی وجود دارد که در قالب امنیت و حملات سایبری دولتی به آنها پرداخته بودیم. در آن حوزه قوانین داخلی و بین‌المللی گوناگونی وجود دارند که همین حالا هم شامل انواع جدید فناوری مثل تسلیحات خودکار مرگبار می‌شوند.

بسیاری از شرایط دیگر نیز مشابه مسائل امنیتی مربوط به تسلیحات سایبری به نظر می‌رسند. وقتی «آنتونیو گوترش»، دبیرکل سازمان ملل در سال ۲۰۱۸ خواستار ممنوعیت «روبات‌های قاتل» شد، ملاحظه را کنار گذاشت و گفت: «بیایید بی‌پرده بگوییم؛ این دورنما که دستگاه‌ها اختیار و قدرتِ گرفتن جان انسان‌ها را داشته باشند، از لحاظ اخلاقی مشمئزکننده است.» اما درست مانند تسلیحات سایبری قدرت‌های نظامی برتر دنیا در

برابر قوانین بین‌المللی جدیدی که توسعه فناوری‌شان را محدود کند مقاومت کرده‌اند.

در نتیجه با امید به شکستن بن‌بست، بحث‌هایی در مورد سناریوهای ویژه‌ای شکل گرفت که به محور نگرانی‌های بالقوه می‌پردازند. برای مثال دیدبان حقوق بشر از دولت‌ها خواسته است؛ «آن دسته از سیستم‌های تسلیحاتی را ممنوع کنند که می‌توانند بدون کنترل انسانی معنی‌دار اهدافی را انتخاب و با آنها درگیر شوند.» هرچند احتمالاً ریزه‌کاری‌های دیگری نیز وجود خواهد داشت که باید به آنها بپردازیم، اما این نوع رایزنی‌های بین‌المللی با تمرکز بر عبارت‌های ویژه‌ای مثل «کنترل انسانی معنی‌دار» یکی از عناصر ضروری در رسیدگی به نسل جدید چالش‌های اخلاقی است.

اتکای این تلاش‌ها بر عرف‌های اخلاقی و حقوق بشری اهمیت دارد. توجه بسیار زیاد و پرسابقه ارتش ایالات متحده به تصمیم‌گیری اخلاقی من را تحت تأثیر قرار داده است. این توجه باعث نشده نیروهای مسلح دچار لغزش‌های اخلاقی نشوند، حتی در مواردی اشتباهات بسیار بزرگی مرتکب شده‌اند، اما آن‌طور که از افراد گوناگونی؛ از ژنرال‌های ارشد تا یک دانشجوی دانشکده نظامی «وست پوینت» شنیدم، نمی‌توان بدون گذراندن دوره‌ای در رشته اخلاق از دانشکده نظامی ایالات متحده فارغ‌التحصیل شد. چنین موضوعی را در مورد رشته‌های علوم کامپیوتر در بسیاری از دانشگاه‌های آمریکا مشاهده نمی‌کنیم.

در بحث با رهبران سایر کشورها در مورد این مسائل و مسائل نوظهور مشابه، به این نتیجه رسیدیم که دیدگاه‌های اخلاقی در نهایت به حقوق بشر و مبانی فلسفی کلی‌تر اتکا دارند. بنابراین باید بین این موضوعات با درکی از فرهنگ‌های متنوع جهان و همچنین قوانین و رویکردهای گوناگون ناشی از این تنوع ارتباط برقرار کنیم.

هوش مصنوعی مانند تمام مجموعه فناوری اطلاعات، در ذات خود به صورت جهانی طراحی شده است. متخصصان هوش مصنوعی می‌خواهند این فناوری همه جا کارکرد مشابهی داشته باشد، اما قوانین و مقررات در کشورهای مختلف تفاوت‌هایی با هم دارند که چالش‌هایی را برای دیپلمات‌های دولتی و متخصصان فناوری ایجاد می‌کنند. این چندگانگی‌ها را ابتدا در مورد قوانین مالکیت فکری، بعد در مورد قوانین رقابت و به‌تازگی در مورد قوانین حریم خصوصی تجربه کردیم، اما از برخی جهات این تفاوت‌ها

در مقایسه با پیچیدگی بالقوه قوانین مربوط به مسائل اخلاقی که اساساً بر فلسفه اتکا دارند، ساده به‌شمار می‌آیند.

حال هوش مصنوعی به طرز بی‌سابقه‌ای جهان را وادار کرده با شباهت‌ها و تفاوت‌های میان این قوانین و سنت‌های فلسفی دیگر مواجه شود. این مسائل از برخورد هوش مصنوعی با مباحثی مثل نقش پاسخگویی شخصی، اهمیت شفافیت عمومی، مفاهیم حریم خصوصی فردی و انگاره‌های انصاف بنیادین ناشی می‌شوند. چطور جهان می‌تواند در مورد رویکردی واحد به اخلاقیات برای کامپیوترها به همگرایی برسد، در حالی که نمی‌تواند در مورد مسائل فلسفی مربوط به افراد به توافق دست پیدا کنند؟ این مسئله معمایی پیچیده و بنیادین برای آینده است.

برای حل این مسئله باید افرادی که فناوری را می‌سازند، بیش از گذشته (نه‌فقط از رشته‌هایی مثل علوم کامپیوتر و داده؛ بلکه از علوم اجتماعی، طبیعی و انسانی) به میدان بیایند. اگر می‌خواهیم اطمینان حاصل کنیم که مبنای تصمیم‌گیری هوش مصنوعی بهترین ویژگی‌های انسانی است، توسعه آن باید نتیجه فرایندی چندرشته‌ای باشد. به‌علاوه در حالی که به آینده آموزش عالی فکر می‌کنیم، باید مطمئن شویم که همه متخصصان کامپیوتر و داده با علوم انسانی آشنا می‌شوند؛ همان‌طور که همه دانشجویان رشته‌های علوم انسانی باید کمی با علوم کامپیوتر و داده آشنا شوند.

همچنین باید شاهد تمرکز بیشتر بر اخلاقیات در دوره‌های علوم کامپیوتر و داده باشیم. نمود این تمرکز ممکن است در دوره‌ای ویژه یا عنصری در همه دوره‌ها یا هر دو باشد.

می‌توانیم خوش‌بین باشیم که نسل جدیدی از دانشجویان این هدف را با اشتیاق بپذیرند. در اوایل سال ۲۰۱۸ همراه با «هری شوم» (Harry Shum) پرسشی را به‌صورت عمومی مطرح کردم. هری از معاونان مایکروسافت و مسئول بسیاری از فعالیت‌هایمان در زمینه هوش مصنوعی است که دکترای روباتیک دارد. پرسش این بود: «آیا می‌توانیم برای کدنویسان هم مانند پزشکان شاهد سوگندنامه‌ای بقراطی باشیم؟» همراه با دیگران اعلام کردیم که وجود چنین سوگندنامه‌ای منطقی است. در عرض چند هفته استاد علوم کامپیوتر در دانشگاه واشنگتن تلاش کرد با ویرایش سوگندنامه بقراط منشور جدیدی را برای سازندگان هوش مصنوعی پیشنهاد دهد. در سخنرانی‌هایی که هری و من در

پردیس‌های دانشگاهی سراسر دنیا داشتیم، متوجه شدیم که نسل بعدی به این مسئله اهمیت می‌دهد.

در نهایت، گفت‌وگوی جهانی درباره اصول اخلاقی برای هوش مصنوعی نیازمند حضور ذی‌نفعان بیشتری است. علاوه بر متخصصان فناوری، دولت‌ها، سازمان‌های مردم‌نهاد و مسئولان آموزشی؛ فیلسوفان و نمایندگان ادیان مختلف جهان هم باید در این گفت‌وگوها حاضر باشند. نیاز به این گفت‌وگوهای جهانی باعث شد به واتیکان برویم؛ جایی که اصلاً انتظار نداشتم روزی در آنجا در مورد فناوری صحبت کنیم.

این بازدید نکات جالبی داشت. در فوریه ۲۰۱۹ به رم رسیدیم؛ درست چند روز قبل از آنکه برای شرکت در کنفرانس امنیتی مونیخ به سمت آلمان حرکت کنیم؛ جایی که اطراف‌مان پر از رهبران نظامی جهان بود. به رم رفته بودیم تا در مورد اخلاقیات برای کامپیوترها با رهبران واتیکان گفت‌وگو کنیم؛ آن هم درست یک هفته قبل از آن بود که رهبران واتیکان جلسه خودشان را برای رسیدگی به مسائل اخلاقی کشیش‌ها و سوءاستفاده از کودکان در کلیساها برگزار کنند. این زمان‌بندی بلندپروازی‌ها و چالش‌های انسان را برجسته می‌کرد.

وقتی به واتیکان رسیدیم، «وینچنزو پاگلیا» (Vincenzo Paglia)، مونسینیور خوشرو و اسقف اعظم خنده‌روی کلیسای کاتولیک ایتالیا به استقبال ما آمد. وینچنزو پاگلیا که نویسنده چند کتاب است، رهبری کارهای واتیکان در پرداختن به طیفی از مسائل اخلاقی شامل چالش‌های جدید مربوط به هوش مصنوعی را بر عهده دارد. مایکروسافت و واتیکان تصمیم گرفته بودند که در کنار هم از اهدای جایزه رساله دکترایی برای بررسی تلاقی این فناوری نوظهور با پرسش‌های اخلاقی دیرینه حمایت مالی کنند.

این برنامه یادآور خوبی برای برخوردهای تاریخی فناوری و علم از یک طرف با فلسفه و از طرف دیگر با دین بود. وقتی در واتیکان بودیم، مونسینیور پاگلیا کتابخانه «سیستین» (Sistine) را به ما نشان داد. در آنجا با احتیاط یکی از اولین انجیل‌هایی را ورق زدیم که «یوهانس گوتنبرگ» با دستگاه چاپ فلزی متحرکی چاپ کرده بود که در دهه ۱۴۵۰ اختراع و شروع به استفاده از آن کرده بود؛ پیشرفتی فناورانه که ارتباطات را متحول کرد و بر همه بخش‌های جامعه اروپا از جمله کلیسا تأثیر گذاشت.

بعد به سـراغ طوماری از نامه‌ها رفتیم که ۱۵۰ سال بعد نوشته شده بودند. این نامه‌ها ارتباطات گالیله با پاپ را نشـان می‌دادند که محور مناقشه گالیله و نهاد کلیسا در مورد مکان نسبی زمین و خورشید در آسمان‌ها بودند. همان‌طور که این طومار نشان می‌داد، گالیله در اوایـل قرن هفدهم از تلسـکوپش برای ثبت وضعیت مکانی متغیر خورشـید استفاده کرده بود که نشان می‌داد خورشید در حال گردش است؛ بخشی از مناقشه‌ای تلخ در مورد تفسیر انجیل که به دادگاه تفتیش عقاید گالیله در رم و حبس خانگی‌اش تا زمان مرگ منجر شد.

این دو کتاب در کنار هم نشـان می‌دادند که چطور علم و فناوری می‌توانند با مسـائل مربوط به ایمان، دین و فلسفه ارتباط برقرار کرده یا برخورد کنند. مانند اختراعاتی از جمله دستگاه چاپ و تلسـکوپ، غیرممکن به نظر می‌رسد که هوش مصنوعی به این حوزه‌ها کاری نداشته باشد. مسئله این است که چطور می‌توانیم گفت‌وگوی جهانی حساب‌شده، محترمانه و فراگیر را ترویج کنیم.

در جلسه با پاپ فرانسیس و مونسـینیور پاگلیا در مورد این موضوع بحث کردیم. در مورد توسعه فناوری در این بستر صحبت کردیم که کشورها بیش از پیش به منافع داخلی خودشـان توجه می‌کنند و گاهی اوقات همسایه‌ها و سایر کشـورهای نیازمند را به حال خود رها می‌کنند. به هشـدارهای شـدید آلبرت اینشـتین در مورد مخاطرات فناوری در دهه ۱۹۳۰ اشاره کردم. بعد پاپ سخن اینشتین بعد از جنگ جهانی دوم را به من یادآور شد؛ اینشـتین گفته بود: «نمی‌دانم تسلیحات جنگ جهانی سـوم چه خواهد بود، اما تسلیحات جنگ جهانی چهارم چوب و سنگ خواهد بود.» منظور اینشتین این بود که فناوری؛ به‌ویژه فناوری اتمی آن‌قدر پیشـرفت کرده بود که می‌توانسـت همه‌چیز را نابود کند. هنگام ترک جلسه پاپ فرانسیس دستم را با دست راستش فشرد و مچم را با دست چپش گرفت و با تأکید گفت: «انسانیت‌تان را حفظ کنید.»

خوب اسـت در فکـر کـردن به آینـده هـوش مصنوعـی، همـه، ایـن نصیحـت را آویزه گوش‌مان کنیم.

۱۲

فصل دوازدهم

هوش مصنوعی و تشخیص چهره

«استیون اسپیلبرگ» در ژوئن ۲۰۰۲ فیلم «گزارش اقلیت» (Minority Report) را ساخت که بر اساس داستان کوتاه معروفی از «فیلیپ کی دیک» (Philip K. Dick)، نویسنده داستان‌های علمی-تخیلی، بود. ستاره این فیلم که واشنگتن دی‌سی عاری از جرم و جنایت در سال ۲۰۵۴ را نشان می‌دهد، «تام کروز» است که رئیس واحد پیش‌جرم، واحد ویژه‌ای در نیروی پلیس است که قاتلان را پیش از ارتکاب جرم دستگیر می‌کند. این تیم اختیار دارد که افراد را بر اساس رویاهای سه فرد غیب‌گو دستگیر کند که می‌توانند آینده را ببینند. اما وقتی این غیب‌گوها پیش‌بینی می‌کنند که تام کروز در آستانه ارتکاب قتل است، حالا اوست که باید در شهری که همه کس و همه چیز تحت نظر هستند، از واحد خودش بگریزد.

خوشبختانه با گذشت بیش از ۱۵ سال این رویکرد به اجرای قانون، هنوز بسیار دور از دسترس می‌نماید، اما به نظر می‌رسد یکی از جنبه‌های گزارش اقلیت بسیار زودتر از سال ۲۰۵۴ از راه برسد. کروز هنگام فرار به یکی از فروشگاه‌های پوشاک گپ وارد می‌شود. این خرده‌فروشی فناوری‌ای دارد که همه مشتریان ورودی را تشخیص می‌دهد و بلافاصله روی یک باجه تصاویر لباس‌هایی را به نمایش می‌گذارد که معتقد است مشتری دوست خواهد داشت. شاید از نظر برخی افراد این پیشنهادها جذاب به نظر برسند، اما دیگران ممکن است آنها را آزاردهنده یا حتی چندش‌آور بدانند. خلاصه اینکه ورود به فروشگاه می‌تواند تا حدی همان احساسی را به ما بدهد که گاهی اوقات بعد از مرور وب و ورود به فیدمان در رسانه‌های اجتماعی احساس می‌کنیم؛ اینکه می‌بینیم تبلیغات جدیدی برایمان به نمایش گذاشته می‌شوند که در رابطه با همان چیزهایی است که پیش‌تر مشاهده کرده بودیم.

اسپیلبرگ در گزارش اقلیت از تماشاگران می‌خواهد به این فکر کنند که چطور می‌توان از فناوری هم استفاده و هم سوءاستفاده کرد، هم از جرم و جنایت پیش از وقوع جلوگیری کرد و هم حقوق افراد را زیر پا گذاشت. فناوری‌ای که کروز را در فروشگاه گپ شناسایی می‌کند، از اطلاعات تراشه‌ای بهره می‌برد که درون بدنش جاسازی شده است، اما پیشرفت‌های فناوری در دو دهه اول قرن بیست‌ویکم از تصورات اسپیلبرگ هم فراتر رفته است؛ چراکه امروزه برای این کار به چنین تراشه‌ای نیاز نداریم. فناوری تشخیص چهره

که از بینایی کامپیوتر مبتنی بر هوش مصنوعی به همراه دوربین‌ها و داده‌های موجود در فضای ابری بهره می‌برد، می‌تواند هنگام ورود مشتریان به فروشگاه چهره آنها را بر اساس بازدید هفته قبل یا یک ساعت قبل‌شان شناسایی کند. این فناوری یکی از اولین فرصت‌ها را برای بخش فناوری و دولت‌ها فراهم کرده تا با تصمیم‌گیری در مورد اینکه تشخیص چهره چطور باید رگوله شود، به مسائل اخلاقی و حقوق بشری هوش مصنوعی به‌صورت متمرکز و ملموس بپردازند.

مقوله‌ای که برای بیشتر افراد با سناریویی ساده مثل فهرست‌بندی و جست‌وجوی تصاویر شروع شد، خیلی سریع به مقوله‌ای بسیار پیچیده‌تر تبدیل شد. همین حالا هم بسیاری از افراد برای باز کردن قفل آیفون یا لپ‌تاپ ویندوزی‌شان ترجیح می‌دهند به‌جای رمز عبور از تشخیص چهره استفاده کنند. علاوه بر این، استفاده از این فناوری به همین موارد خلاصه نخواهد شد.

کامپیوترها اکنون می‌توانند کاری را انجام دهند که کم‌وبیش همه ما انسان‌ها می‌توانیم از تقریباً بدو تولد انجام دهیم، یعنی تشخیص چهره افراد. در مورد بیشتر ما احتمالاً این کار با توانایی تشخیص مادرمان شروع شده است. یکی از لذت‌های پدر یا مادر بودن زمانی است که کودک نوپا با برگشتن آنها به خانه ذوق می‌کند. این واکنش که تا ابتدای دوران نوجوانی ادامه دارد، به توانایی‌های ذاتی تشخیص چهره انسان‌ها وابسته است. هرچند این توانایی در زندگی روزمره ما نقشی اساسی دارد، اما تقریباً هیچ‌وقت به این فکر نمی‌کنیم که چطور امکان‌پذیر می‌شود.

از قرار معلوم چهره ما به اندازه اثر انگشت‌مان منحصربه‌فرد است. ویژگی‌های چهره شامل فاصله مردمک‌های چشم از یکدیگر، اندازه بینی، حالت لبخند و فک می‌شود. وقتی کامپیوترها از عکس‌ها برای ترسیم نمودار این ویژگی‌ها و همبسته‌کردن آنها استفاده می‌کنند، زیربنای معادله‌ای ریاضیاتی را ایجاد می‌کنند که الگوریتم‌ها می‌توانند به آنها دسترسی پیدا کنند.

افراد در سراسر دنیا از این فناوری بهره می‌برند تا زندگی را بهتر کنند. در برخی موارد هدف افزایش راحتی مصرف‌کننده است. بانک ملی استرالیا با استفاده از فناوری تشخیص چهره مایکروسافت، در حال توسعه توانایی مراجعه به خودپرداز بدون کارت

بانکی و برداشت پول به‌صورت امن است. خودپرداز چهره فرد را تشخیص می‌دهد و فرد می‌تواند رمزش را وارد کند و تراکنشش را انجام دهد.

در سناریوهای دیگر مزیت‌ها بسیار فراگیرتر هستند. در واشنگتن دی‌سی، مؤسسه ملی تحقیقات ژنوم انسان (National Human Genome Research Institute) از تشخیص چهره برای کمک به پزشکان در تشخیص بیماری‌ای به نام «سندروم دی‌جرج» یا سندرم حذف 22q11.2 استفاده می‌کند. این بیماری اغلب افرادی از آفریقا، آسیا یا آمریکای لاتین را مبتلا می‌کند و می‌تواند به طیفی از مشکلات سلامتی شدید مثل آسیب به قلب و کلیه‌ها منجر شود. در عین حال اغلب خود را با نشانه‌های ظریفی در صورت نشان می‌دهد که می‌توان آنها را با سیستم‌های تشخیص چهره شناسایی کرد. این سیستم‌ها به پزشکان کمک می‌کنند بیماران نیازمند درمان را شناسایی کنند.

این سناریوها روش‌های مهم و ملموسی را ترسیم می‌کنند که از آنها می‌توان برای منفعت‌رساندن به جامعه استفاده کرد. تشخیص چهره ابزار جدیدی برای قرن بیست‌ویکم است.

با این حال مانند بسیاری از ابزارهای دیگر می‌توان آن را به سلاح هم تبدیل کرد. دولت‌ها ممکن است از تشخیص چهره برای شناسایی افراد شرکت‌کننده در تظاهرات مسالمت‌آمیز استفاده کنند و با این کار آزادی بیان و توانایی تشکیل تجمعات را سرکوب کنند. حتی در جوامع دموکراتیک نیز پلیس ممکن است با درک‌نکردن این مسئله که تشخیص چهره مانند هر فناوری دیگری همیشه بی‌نقص کار نمی‌کند، برای شناسایی مظنونان بیش از حد به این ابزار اتکا کند.

به همین دلایل تشخیص چهره به‌راحتی با مسائل سیاسی و اجتماعی گسترده‌تر گره خورده است و پرسشی حیاتی را مطرح می‌کند؛ می‌خواهیم این شکل از هوش مصنوعی چه نقشی در جامعه ما ایفا کند؟

در تابستان ۲۰۱۸ نمایی کلی از آنچه در پیش داریم در ارتباط با یکی از پرحرارت‌ترین مباحث سیاسی آن ایام پدیدار شد. در ماه ژوئن مردی از ویرجینیا که خود را «همه‌فن‌حریف نرم‌افزار رایگان» توصیف می‌کرد و به‌وضوح علاقه زیادی به مسائل سیاسی کلی‌تر داشت، بر اساس گزارشی که در ماه ژانویه در بلاگ بازاریابی شرکت ارسال

شده بود، رشته توییتی را درباره قراردادی بین مایکروسافت و سازمان اعمال مهاجرت و گمرک (Immigration and Customs Enforcement) ایالات متحده یا «آیس» منتشر کرد. از آن دست گزارش‌هایی بود که همه افراد شرکت فراموش کرده بودند. اما در آن آمده بود که فناوری مایکروسافت امتیازی بالاتر از حدنصاب امنیتی بالای آیس کسب کرده و این سازمان از این فناوری استفاده خواهد کرد. همچنین گفته شده بود که شرکت به پشتیبانی از کار این سازمان افتخار می‌کند. به‌علاوه گزارش شامل جمله‌ای درباره پتانسیل نهایی استفاده از تشخیص چهره برای آیس می‌شد.

در ژوئن ۲۰۱۸ تصمیم دولت ترامپ مبنی بر جداسازی کودکان از والدین در مرز جنوبی ایالات متحده به مسئله‌ای جنجال‌برانگیز تبدیل شد. بیانیه بازاریابی که چند ماه پیش منتشر شده بود، اکنون بسیار متفاوت به نظر می‌رسید. استفاده از فناوری تشخیص چهره نیز در این مورد متفاوت به نظر می‌رسید. افراد نگران بودند که آیس و سایر نهادهای مسئول مهاجرت از فناوری‌ای مثل تشخیص چهره استفاده کنند. آیا ممکن بود از دوربین‌های متصل به ابر برای شناسایی مهاجران در خیابان‌ها استفاده شود؟ آیا با توجه به ریسک سوگیری این فناوری، امکان داشت افراد را به اشتباه شناسایی کند و به بازداشت افراد نادرست منجر شود؟ این پرسش‌ها فقط دو مورد از پرسش‌های پرشمار بودند.

تا زمان شام در سیاتل توییت‌های مربوط به بلاگ بازاریابی در اینترنت جنجالی به پا کرده بود و تیم ارتباطات ما در حال کار روی پاسخ مناسب بود. برخی کارمندان تیم‌های مهندسی و بازاریابی پیشنهاد دادند آن مطلب را حذف کنیم و بگوییم «این مطلب بسیار قدیمی است و در حال حاضر اهمیت تجاری ندارد».

«فرانک شاو» (Frank Shaw)، مدیر ارتباطات مایکروسافت سه بار به آنها توصیه کرد که مطلب را حذف نکنند. می‌گفت: «این کار فقط شرایط را بدتر می‌کند.» در هر صورت فردی تسلیم این وسوسه شد و بخشی از پست را پاک کرد. همان‌طور که می‌شد حدس زد، شرایط بدتر شد و در پی این اتفاق دور دیگری از پوشش رسانه‌ای منفی ایجاد شد. تا صبح روز بعد افراد متوجه اشتباه بدیهی‌شان شدند و مطلب را دوباره به همان صورت اولیه درآوردند.

باید مثل بسیاری از موارد دیگر ابتدا می‌فهمیدیم قرارداد شرکت با آیس دقیقاً چه مواردی را پوشش می‌دهد.

وقتی همه ابعاد مسئله را بررسی کردیم، فهمیدیم که از قرارداد اصلاً برای تشخیص چهره استفاده نمی‌شود. علاوه بر این خوشبختانه مایکروسافت در پروژه جداسازی کودکان از خانواده‌هایشان در مرز کار نمی‌کرد. این قرارداد به آیس کمک می‌کرد فعالیت‌های مدیریت ایمیل، تقویم، پیام‌رسانی و اسناد را به ابر منتقل کند. مشابه پروژه‌هایی بود که در آنها با مشتریان از جمله سایر سازمان‌های دولتی در ایالات متحده و نقاط مختلف جهان همکاری می‌کردیم.

در هر صورت جنجال تازه‌ای برپا شده بود.

برخی افراد پیشنهاد دادند مایکروسافت قرارداد با آیس را فسخ و همه همکاری‌ها با این سازمان را متوقف کند. در تابستان آن سال این نوع برخورد با استفاده دولت از فناوری به‌دفعات تکرار شد. گروهی از کارمندان در حال جمع‌آوری امضا برای طوماری با درخواست توقف قرارداد با آیس بودند. این مسئله به‌مرور کل بخش فناوری را درگیر کرد. کارمندان شرکت نرم‌افزاری مبتنی بر ابر «سلزفورس» (Salesforce) نیز کنشگری مشابهی را در مورد قرارداد این شرکت با اداره گمرک و حفاظت مرزی ایالات متحده شروع کرده بودند. بعد از این اتفاق کنشگری کارمندان گوگل اتفاق افتاد که باعث شد این شرکت پروژه‌ای در مورد توسعه هوش مصنوعی برای ارتش ایالات متحده را لغو کند. اتحادیه آزادی‌های مدنی آمریکا (American Civil Liberties Union) نیز آمازون را هدف گرفت و از کارمندانی پشتیبانی کرد که نگرانی‌شان در مورد «ریکاگنیشن» (Rekognition)، خدمت تشخیص چهره این شرکت را علنی کرده بودند.

این نوع کنشگری کارمندی برای بخش فناوری و در سطح گسترده‌تر جامعه کسب‌وکار، تازگی داشت. برخی افراد ارتباطی بین این کنشگری‌ها و نقشی می‌دیدند که اتحادیه‌های کارگری بیش از یک قرن در برخی صنایع ایفا کرده بودند. اما اتحادیه‌ها بیشتر بر شرایط اقتصادی و کاری اعضایشان متمرکز بودند. کنشگری کارمندی در تابستان ۲۰۱۸ مقوله متفاوتی بود. در این کنشگری‌ها از کارفرمایان خواسته می‌شد در مورد مسائل اجتماعی

ویژه‌ای مواضعی را اتخاذ کنند. کارمندان به‌صورت مستقیم یا حتی غیرمستقیم منفعتی به دست نمی‌آوردند؛ بلکه از کارفرمایان‌شان می‌خواستند از آن دسته ارزش‌ها و مواضع اجتماعی پشتیبانی کنند که از نظرشان مهم بودند.

ارزیابی واکنش‌های مختلف به این موج جدید کنشگری کارمندی برای ما مفید بود. فقط چند مایل آن‌طرف‌تر؛ در سیاتل، به نظر می‌رسید رهبران آمازون برای تعامل با کارمندان به‌منظور بحث در مورد این نوع مسائل تلاش کمی می‌کنند. به نظر می‌رسید این واکنش تا حدی تمایل کارمندان به طرح مسائل را کاهش می‌دهد و در عمل افراد را ترغیب می‌کند که در این‌گونه مسائل دخالت نکنند و بر کار خودشان متمرکز بمانند. در سیلیکون‌ولی، رهبران گوگل رویکرد بسیار متفاوتی را در پیش گرفتند و گاهی اوقات به‌سرعت با تجدیدنظر در تصمیم‌شان از جمله با فسخ قراردادی نظامی در زمینه هوش مصنوعی، به شکایت‌های کارمندان واکنش نشان می‌دادند. همان ابتدا مشخص شد که هیچ رویکرد واحدی وجود ندارد و هر شرکتی باید فرهنگ خودش و خواسته‌اش از ارتباط با کارمندانش را در نظر بگیرد. وقتی به فرهنگ‌مان فکر می‌کردیم، تصمیم گرفتیم با توجه به رویکردهایی که در شرکت‌های دیگر می‌دیدیم، رویکردی بینابین و متعادل را در پیش بگیریم.

به نظر می‌رسید این اتفاقات چند تحول مهم را منعکس می‌کنند. اولین و شاید مهم‌ترین تحول انتظار فزاینده‌ای بود که کارمندان از کارفرمایان‌شان داشتند. چند ماه پیش شاخص سالانه اعتماد ادلمن (Edelman Trust Barometer) این تحول را به‌خوبی تجسم کرده بود. شرکت ارتباطات ادلمن از سال ۲۰۰۱ شاخص اعتماد را منتشر می‌کند و نشان می‌دهد که با افزایش و کاهش اعتماد افراد به نهادها چه تغییراتی در نگاه و حال‌وهوای مردم اتفاق می‌افتد. گزارش این شرکت در اوایل سال ۲۰۱۸ نشان می‌داد که هرچند اعتماد به بسیاری از نهادها کمتر شده، اما اعتماد کارمندان به کارفرمایان از این قاعده مستثنی است. این شاخص نشان می‌داد که در سطح جهان ۷۲ درصد از افراد به کارفرمایشان اعتماد دارند که «کار درست را انجام می‌دهد». این در حالی بود که این رقم برای ایالات متحده ۷۹ درصد بود. در مقابل فقط یک‌سوم آمریکایی‌ها به دولت‌شان چنین احساسی داشتند.

تجربه ما هم بازتاب‌دهنده این دیدگاه و فراتر از آن بود. در بخش فناوری، برخی کارمندان می‌خواستند در شکل‌دادن به تصمیمات شرکت و مشارکت در مسائل روز نقش فعالی داشته باشند. شاید تعجب‌آور نبود که این دیدگاه در دورانی برجسته‌تر شده بود که افراد کمتر به دولت‌ها اعتماد داشتند. کارمندان به نهاد دیگری مراجعه می‌کردند که امیدوار بودند کار درست را انجام دهد و تا حدی روی پیامدهای عمومی کارها تأثیر بگذارد.

این تغییر، رهبران کسب‌وکار را به قلمروی جدیدی وارد می‌کرد. در میهمانی شام کوچکی در سیاتل، مدیرعامل یکی از شرکت‌های فناوری در سخنانی، نگرانی جمع را خلاصه کرد. با تشریح اینکه چطور سلسله‌مراتب را طی کرده تا به این مقام برسد، گفت: «برای بیشتر بخش‌های شغلم کاملاً آماده‌ام، اما اکنون به قلمرویی کاملاً متفاوت کشیده شده‌ام. واقعاً نمی‌دانم چطور به کارمندانی واکنش نشان دهم که از من می‌خواهند به نگرانی‌هایشان در مورد مهاجرت، مسائل محیط زیست و بسیاری از مسائل دیگر رسیدگی کنم.»

احتمالاً جای تعجب نداشت که این پدیده را در جدیدترین نسل از کارمندان‌مان به‌طور برجسته‌تر مشاهده می‌کردیم. هرچه نباشد رسم تثبیت‌شده‌ای وجود دارد که دانشجویان در پردیس‌های دانشگاهی برای تغییر اجتماعی اعتراض می‌کنند و در مواردی دانشگاه‌هایشان را مجبور می‌کنند که با تغییر سیاست‌هایشان، در کنشگری پیشگام شوند. چون تابستان بود، حدود سه هزار کارآموز در ساختمان اصلی مایکروسافت داشتیم و همان‌طور که انتظار می‌رفت، علاقه زیادی به این مسئله نشان می‌دادند. برخی از آنها می‌خواستند حتی اگر فقط همین تابستان را با ما هستند، اثر مستقیمی بر موضع شرکت بگذارند.

گفت‌وگو کردیم که چطور تمام ابعاد این موضوع را بررسی کنیم و واکنش نشان دهیم. وقتی با ساتیا تبادل نظر می‌کردم، به مسائلی اشاره کردم که هنگام حضور در هیئت امنای دانشگاه پرینستون یاد گرفته بودم. گفتم: «فکر می‌کنم رهبری یک شرکت فناوری در حال شبیه‌شدن به رهبری یک دانشگاه است. پژوهشگرانی با مدرک دکترا داریم که شبیه هیئت علمی هستند. کارآموزان و کارمندان جوانی داریم که گاهی اوقات دیدگاه‌هایی

مشابه دانشجویان دارند. همه می‌خواهند صدایشان شنیده شود و برخی همان‌طور که از دانشگاه می‌خواهند خرید سهام شرکتی را تحریم کند که کار نامناسبی انجام داده، از ما هم می‌خواهند سازمانی دولتی را تحریم کنیم.»

تجربه‌ام در جایگاه عضو هیئت امنا چند نکته کلیدی به من یاد داده بود. احتمالاً مهم‌ترین نکته این بود که دانشجویان ممکن است نیت درستی داشته باشند و پرسش‌های درستی بپرسند، اما پاسخ و راه‌حل درستی نداشته باشند. این پرسش‌ها ممکن است به مسیر بهتری منجر شوند که از دید متخصصان و رهبران ارشد دور مانده‌اند؛ چنانچه به تیم‌هایمان در شرکت می‌گویم بهترین واکنش به ایده‌ای خام حذف آن نیست؛ بلکه پختن آن است. برخی از بهترین طرح‌های ما با پیروی از همین روش با موفقیت ایجاد شده‌اند. به‌علاوه این روش مبتنی بر ذهنیت رشد و یادگیری پیوسته و متکی بر فرهنگی است که ساتیا در مایکروسافت ترویج کرده بود. خلاصه اینکه اگر عصر جدیدی از کنشگری کارمندی آغاز شده بود، باید راه‌های جدیدی برای تعامل با کارمندان‌مان، درک نگرانی‌هایشان و تلاش برای رسیدن به پاسخی سنجیده پیدا می‌کردیم.

علاوه بر این از تجربه‌ام در دانشگاه پرینستون یاد گرفته بودم که دانشگاه‌ها فرایندهای معقولی را برای برطرف‌کردن این نیاز توسعه داده‌اند. فرصت‌هایی را برای همه ایجاد کرده بودند تا نظرشان را بگویند و بحث‌های مشارکتی‌تری داشته باشند. این رویکرد به گروه کمک می‌کرد همه جوانب را بسنجد و تصمیمی دشوار را در زمان مورد نظر بگیرد، اجازه می‌داد احساسات فروکش کنند و منطق مسلط شود. این مسیر را در پیش گرفتیم و اریک هورویتز، فرانک شاو و «ریچ زاو» (Rich Sauer)، وکیل ارشد مسئول مسائل اخلاقی هوش مصنوعی شروع به برگزاری مجموعه‌ای از میزگردها کردند که کارمندان می‌توانستند در آنها شرکت کنند.

بیش از پیش ضروری بود که توضیح بدهیم چه زمانی فکر می‌کنیم برای شرکت منطقی است که در مورد مسئله‌ای عمومی موضع بگیریم و چه زمانی نباید موضع بگیریم. معتقد نبودیم رهبری شرکتی، مجوزی برای استفاده از نام شرکت برای پرداختن به هر مسئله‌ای است. مسئله مورد نظر باید ارتباطی مهم با ما می‌داشت. فکر می‌کردیم اساساً

مسئولیت داریم به آن دسته از مسائل عمومی بپردازیم که مشتریان‌مان و استفاده آنها از فناوری، کارمندان‌مان در محل کار و زندگی و کسب‌وکارمان و نیازهای سهام‌داران و شرکایمان را تحت تأثیر قرار می‌دهند. این طبقه‌بندی به همه پرسش‌ها پاسخ نمی‌داد، اما چارچوب مفیدی برای بحث با کارمندان‌مان فراهم می‌کرد.

پرسش‌های کارمندان همچنین اثر سازنده دیگری داشت و ما را ترغیب کرد که در مورد رابطه‌مان با دولت و چالش‌های ناشی از فناوری‌های جدیدی مثل تشخیص چهره بیشتر فکر کنیم.

از طرفی با این پیشنهاد موافق نبودیم که با تحریم سازمان‌های دولتی به رخدادهای روز واکنش نشان دهیم، به‌ویژه در جوامع دموکراتیک که قانون حاکم است. این واکنش از جهتی اصولی بود. همان‌طور که اغلب سعی می‌کردم به افراد یادآوری کنم که کسی ما را در رأی‌گیری انتخاب نکرده است. نه‌فقط عجیب؛ بلکه غیردموکراتیک به نظر می‌رسید که شرکت‌های فناوری بر دولت نظارت کنند. به‌عنوان اصلی کلی، منطقی‌تر به نظر می‌رسید که از دولت منتخب مردم بخواهیم شرکت‌ها را رگوله کند تا اینکه از شرکت‌هایی که پشتوانه رأی مردم را نداشتند، بخواهیم چنین دولتی را رگوله کنند. با ساتیا زیاد در مورد این موضوع گفت‌وگو می‌کردیم و معتقد بودیم اهمیت دارد.

جنبه عمل‌گرایانه‌ای هم وجود داشت. وابستگی شدید سازمان‌ها و افراد به فناوری‌مان را درک می‌کردیم. اگر صرفاً به خاطر اعتراض به کاری که یک سازمان دولتی انجام می‌داد، فناوری را قطع می‌کردیم، راه بسیار راحت را انتخاب کرده بودیم که آشفتگی و پیامدهای ناخواسته‌ای به‌دنبال داشت.

این جنبه عمل‌گرایی در آگوست ۲۰۱۸ بسیار روشن شد. صبح جمعه‌ای در حال رانندگی به سمت محل کار بودم و به روایتی از پادکست دیلی (Daily) نیویورک‌تایمز گوش می‌دادم که به ابعاد اصلی مسئله‌ای مهم می‌پرداخت. مسئله روز ناتوانی دولت در عمل به مهلت دادگاه برای بازگرداندن کودکان مهاجر به خانواده‌هایشان بود. وقتی گوش می‌دادم، صدای «وندی یانگ» (Wendy Young) را شناختم. وندی رهبری سازمان خیریه کودکان نیازمند دفاع قانونی (Kids in Need of Defense) یا «کایند» را بر عهده دارد که بیش از یک دهه رئیس هیئت‌مدیره آن بودم. همان‌طور که وندی توضیح می‌داد،

دولت سیاست جداسازی اعضای خانواده‌ها را اجرا کرده بود، بدون آنکه فکر کند بعداً چطور می‌خواهد آنها را پیش هم بازگرداند. هرچند به‌واسطه چند گفت‌وگو با وندی با این وضعیت آشنا بودم، اما جزئیات بیشتر گزارش «کیتلین دیکرسون» (Caitlin Dickerson) و «انی کوریل» (Annie Correal)، خبرنگاران نیویورک‌تایمز حیرت‌زده‌ام کرد. توضیح می‌دادند که وقتی افراد ابتدا از مرز عبور می‌کردند، کارمندان اداره گمرک و حفاظت مرزی از سیستمی کامپیوتری با منوی آبشاری استفاده می‌کردند. مأموران افراد را در دسته‌های نابالغ بدون همراه، بزرگسال تنها یا بزرگسال با کودک یعنی خانواده طبقه‌بندی می‌کردند. بعد وقتی کودکان از والدین‌شان جدا می‌شدند، طراحی این سیستم کامپیوتری مأموران را مجبور می‌کرد که این مشخصات را تغییر دهند، برای مثال نام کودک را به‌عنوان نابالغ بدون همراه و نام پدر یا مادر را به‌عنوان بزرگسال تنها وارد کنند. موضوع حیاتی این بود که این کار داده‌های جدید را جایگزین داده‌های قبلی می‌کرد، یعنی سیستم دیگر وضعیت قبلی افراد به‌صورت خانواده را حفظ نمی‌کرد. در نتیجه دولت دیگر هیچ سابقه‌ای در دست نداشت که اعضای خانواده را به هم متصل کند.

موضوع فقط مهاجرت و خانواده‌ها نبود و به فناوری هم مربوط می‌شد. دولت از پایگاه داده ساختاریافته‌ای استفاده می‌کرد که برای یک فرایند مناسب بود، اما برای یک فرایند دیگر مفید نبود. دولت به جای به‌روزرسانی سیستم فناوری اطلاعات به‌منظور پشتیبانی از گام‌های جدید مربوط به جداسازی اعضای خانواده‌ها، بدون فکر کردن به معماری کامپیوتری مورد نیاز با عجله کار را شروع کرده بود. با توجه به اینکه در بازدیدی به همراه وندی در چند ماه گذشته، سیستم‌های اداره گمرک و حفاظت مرزی را در یک مرکز فرماندهی نزدیک مرز مکزیک دیده بودم، از منسوخ‌بودن این سیستم‌ها تعجب نکردم. با این حال وحشتناک بود که دولت به زیرساخت فناوری ابتدایی مورد نیاز فکر نکرده بود.

وقتی آن روز صبح به اتاق همایشی وارد شدم که تیم رهبری ارشد ساتیا برای جلسه روز جمعه جمع شده بودند، شنیده‌هایم را بازگو کردم. در حین صحبت در مورد این موضوع متوجه شدیم که به نگرانی‌های گسترده‌تر ما در مورد پیشنهاد برخی افراد مربوط است. پیشنهاد این افراد این بود؛ شرکت‌های فناوری ارائه تمام خدمات به دولت را که مبتنی بر سیاست‌هایی هستند که به آنها اعتراض دارند، متوقف کنند. فناوری به

یکی از زیرساخت‌های کلیدی زندگی ما تبدیل شده و نارسایی در به‌روزرسانی آن یا بدتر، تصمیم برای قطع آن، می‌تواند پیامدهای ناخواسته و پیش‌بینی‌نشده فراوانی داشته باشد. همان‌طور که ساتیا در گفت‌وگوهای داخل شرکت چند بار اشاره کرده بود، دولت از ایمیل به‌عنوان یکی از ابزارهای برگرداندن خانواده‌ها پیش هم استفاده می‌کرد. اگر این خدمات را قطع می‌کردیم، معلوم نبود چه اتفاقی می‌افتد.

بنابراین به این جمع‌بندی رسیدیم که تحریم سازمانی دولتی در ایالات متحده رویکرد اشتباهی است، اما مدافعان این پیشنهاد، از جمله شماری از کارمندان خودمان، پرسش‌های درستی را مطرح می‌کردند. برای مثال فناوری تشخیص چهره چالش‌هایی را ایجاد کرده بود که توجه بیشتری را می‌طلبید.

با بررسی‌های جامع نتیجه گرفتیم که باید قوانین و رگولیشن جدیدی بر این فناوری جدید حاکم شود. تنها راه برای پاسخگویی به نیاز مردم به حفظ حریم خصوصی و برطرف‌کردن ریسک‌های سوگیری و تبعیض و در عین حال فراهم‌کردن امکان استمرار نوآوری همین بود.

از نظر بسیاری از افراد عجیب بود که شرکتی از دولت بخواهد محصولاتش را رگوله کند. «جان تامپسون» (John Thompson)، رئیس هیئت‌مدیره ما می‌گفت برخی افراد در سیلیکون‌ولی به او گفته‌اند که فکر می‌کنند ما در بازار از شرکت‌های دیگر عقب هستیم و می‌خواهیم رگولیشن، سرعت رقبایمان را کاهش دهد. با حرفش مو به تنم سیخ شد. اتفاقاً برعکس، مؤسسه ملی استانداردها و فناوری، سال ۲۰۱۸ دور دیگری از آزمایش‌های تشخیص چهره را تکمیل کرد و به این نتیجه رسید که الگوریتم‌های ما در همه بخش‌ها بهترین یا نزدیک به بهترین هستند. ۴۴ شرکت دیگر نیز فناوری‌شان را برای آزمایش ارائه داده بودند، البته بسیاری از شرکت‌های دیگر از جمله آمازون این کار را نکرده بودند.

تمایل ما به رگولیشن ناشی از احساس تازه‌ای نسبت به مسیر پیش‌روی بازار بود. چند ماه قبل یکی از تیم‌های فروش‌مان خواسته بود راه‌حل هوش مصنوعی محوری شامل خدمات تشخیص چهره را به دولت کشوری بفروشد که نظام قضایی مستقلی نداشت و سابقه‌اش در احترام به حقوق بشر آنچنان درخشان نبود. این دولت می‌خواست این راه‌حل را در دوربین‌های پایتخت این کشور پیاده‌سازی کند. نگران بودیم دولتی که حقوق

بشـر را زیر پا می‌گذارد، از این فناوری برای دنبال‌کردن هر کسی در هر جا یا همه کس در همه جا استفاده کند.

با توصیـه کمیتـه اخلاق هـوش مصنوعـی داخلی‌مـان تصمیـم گرفتیـم این قـرارداد پیشـنهادی را کنـار بگذاریم. کمیته پیشـنهاد داد که خدمات تشـخیص چهـره را برای اسـتفاده فراگیر در کشـورهایی که سـازمان خانه آزادی (Freedom House) آنها را آزاد نمی‌دانسـت، در دسـترس قرار ندهیم. خانه آزادی دیدبان مستقلی است که وضعیت آزادی و دموکراسی را در سراسر دنیا بررسـی و پیگیری می‌کند. آن تیم محلی از تصمیم ما ناراضی بود. به‌عنوان مسئول تصمیم نهایی ایمیلی پراحساس از رئیس تیم فروشی دریافت کردم کـه روی این قـرارداد کار کرده بود. نوشـته بود: «به‌عنوان یک مادر شـاغل احساس امنیت بیشتری می‌کردم اگر این خدمت را برای مقابله با ریسک‌های خشونت و فعالیت‌های تروریستی در دسترس قرار می‌دادیم.»

منظورش را درک می‌کردم. حرف‌هایش بده‌بستان‌های دشواری را برجسته می‌کرد که ویژگی بارز تنش‌های دیرین میان امنیت عمومی و حقوق بشر بودند. همچنین ماهیت سـلیقه‌ای بسـیاری از تصمیمـات اخلاقی جدیـدی را نشـان مـی‌داد که در مـورد هوش مصنوعی گرفته خواهد شد و البته همان‌طور که او و دیگران گفتند، همچنان نگران بودیم که اگر ما این خدمت را ارائه نکنیم، ممکن است شرکت دیگری این کار را انجام دهد. اگر این اتفاق می‌افتاد، هم قرارداد را از دست می‌دادیم و هم از کنار گود تماشا می‌کردیم که با وجود موضع ما، شرکتی دیگر کاربرد زیان‌بار این فناوری را تسهیل می‌کند، اما با مقایسه همه این عوامل به این جمع‌بندی رسـیده بودیم که باید تلاش کنیم توسـعه این فناوری جدید را به سمت نوعی مبنای اخلاقی هدایت کنیم. تنها راه برای رسیدن به این هدف هم نپذیرفتن برخی استفاده‌ها و تلاش برای ترویج بحث عمومی گسترده‌تر بود.

این نیاز به رویکرد اصولی زمانی بیشتر قوت گرفت که نیروی پلیس محلی در کالیفرنیا با ما تماس گرفت و گفت می‌خواهد همه دوربین‌های خودرو و لباس پلیس را با قابلیتی تجهیز کند که از افراد متوقف‌شـده توسـط پلیس، حتی در موارد روزمـره، عکس بگیرد تا ببیند با موردی در پایگاه داده مظنونان سـایر جرائم مطابقـت دارد یا خیر. منطق این کاربرد را می‌فهمیدیم، اما گفتیم فناوری تشخیص چهره هنوز برای استفاده در این نوع

سناریوها آماده نیست. کاربردی با این ماهیت، دست‌کم در سال ۲۰۱۸ به مثبت‌های کاذب بسیار زیاد و نشان‌دار کردن افرادی منجر می‌شد که به اشتباه شناسایی شده‌اند، به‌ویژه اگر آن افراد رنگین‌پوست یا زن بودند که نرخ خطا در موردشان همچنان بیشتر بود. این پیشنهاد را نپذیرفتیم و نیروی پلیس را متقاعد کردیم که از تشخیص چهره برای این هدف استفاده نکند.

این تجربه‌ها به‌مرور بینش‌هایی را در مورد اصولی فراهم کرد که می‌توانستیم در مورد تشخیص چهره به کار بگیریم. اما نگران بودیم که اگر مسیر اخلاقی را انتخاب کنیم و شرکت‌های دیگری که هیچ محافظت یا محدودیتی قائل نمی‌شدند، این‌گونه قراردادها را از دست‌مان دربیاورند، تأثیر عملی چندانی مشاهده نخواهیم کرد. فرقی هم نمی‌کرد آن شرکت‌ها همین نزدیکی در آن‌طرف سیاتل یا آن‌طرف اقیانوس آرام قرار داشته باشند. تشخیص چهره مانند بسیاری از فناوری‌های مبتنی بر هوش مصنوعی، با حجم بیشتر داده‌ها بهبود می‌یابد. این وضعیت به ذی‌نفعان مختلف این انگیزه را می‌دهد که تا حد امکان بیشترین قراردادهای زودهنگام را امضا کنند که در نتیجه ریسک رقابت برای مقررات‌زدایی را به همراه دارد. این اقدام شرکت‌های فناوری را نیز مجبور می‌کند بین مسئولیت اجتماعی و موفقیت در بازار یکی را انتخاب کنند.

تنها راه برای جلوگیری از این رقابت برای مقررات‌زدایی، ایجاد حداقل‌های مسئولیت‌پذیری است که از رقابت سالم در بازار پشتیبانی کند. بدین منظور باید اطمینان حاصل کنیم که قانون بر این فناوری و سازمان‌های توسعه‌دهنده و کاربر آن حاکم است.

از تاریخچه رگولیشن فناوری‌های دیگر، بینش‌هایی را استنباط کردیم. بازارهای زیادی وجود دارند که در آنها رویکرد متوازن به رگولیشن شرایط سالم‌تری را همزمان برای مصرف‌کنندگان و تولیدکنندگان فراهم کرده است. در قرن بیستم صنعت خودروسازی دهه‌ها در برابر مطالبه رگولیشن مقاومت می‌کرد، اما امروزه درکی همگانی از نقش اساسی قوانین در فراگیر شدن کمربند ایمنی و کیسه هوا و افزایش بهره‌وری مصرف سوخت وجود دارد. همین وضعیت در ایمنی هوایی، مواد غذایی و داروسازی هم برقرار بود.

البته بین حرف‌زدن از نیاز به رگولیشن و تعریف منطقی‌ترین نوع رگولیشن تفاوت

زیادی وجود دارد. در جولای ۲۰۱۸ فهرستی از پرسش‌ها را منتشر کردیم که معتقد بودیم باید در نظر گرفته شوند و از افراد خواستیم در مورد پاسخ‌های احتمالی به ما مشاوره بدهند. این بحث‌ها با کارمندان و متخصصان فناوری شروع شد، اما خیلی زود به سراسر کشور و جهان و از جمله گروه‌های آزادی‌های مدنی از جمله اتحادیه آزادی‌های مدنی آمریکا گسترش یافت که نقش فعالی در این مسئله ایفا می‌کرد.

واکنش قانون‌گذارانی که با آنها در مجمع ملی (National Assembly) فرانسه ملاقات کردم، به‌طور ویژه توجه من را جلب کرد. یکی از اعضا گفت: «هیچ شرکت فناوری دیگری این پرسش‌ها را از ما نمی‌پرسد. چرا شما متفاوت هستید؟» در برخی زمینه‌های تشخیص چهره با سایر شرکت‌های بخش فناوری اختلاف سلیقه داشتیم. این مسئله شاید بیش از هر چیزی بازتاب‌دهنده درس‌هایی بود که از پرونده‌های ضدانحصار در دهه ۱۹۹۰ گرفته بودیم. آن زمان مانند بسیاری از شرکت‌ها و صنایع استدلال کرده بودیم که رگولیشن غیرضروری و احتمالاً زیان‌آور است. اما یکی از درس‌هایی که از این تجربه گرفتیم، این بود که چنین رویکردی در مورد محصولاتی که تأثیر فراگیری روی جامعه دارند یا کاربردهای مفید و بالقوه دردسرساز را ترکیب می‌کنند، لزوماً نتیجه‌بخش نیست (یا غیرقابل قبول در نظر گرفته می‌شود).

دیگر مانند اغلب شرکت‌های فناوری که از گذشته در برابر مداخله دولت مقاومت می‌کردند، مقاومت نشان نمی‌دادیم. پیش از این در این نبرد جنگیده بودیم. در عوض حامی رویکردی شده بودیم که فکر می‌کردیم رویکردی فعال‌تر اما متوازن به رگولیشن است. یکی از دلایلی نیز که خیلی زود یعنی از سال ۲۰۰۵ خواستار قانون‌گذاری فدرال در مورد حریم خصوصی شدیم، همین بود. می‌دانستیم روزهایی پیش می‌آید که دولت در جزئیات اشتباه کند و شاید از حمایت‌مان از مداخله دولت پشیمان شویم. اما بر این باور بودیم که در مجموع این رویکرد بیشتر از شیوه‌ای که در مدیریت همه مسائل، صرفاً به بخش فناوری متکی است، برای فناوری و جامعه مفید است.

نکته کلیدی فهمیدن جزئیات بود. مقاله‌ای از «نیتاشا تیکو» (Nitasha Tiku) در وایرد اهمیت این شرایط را به‌خوبی تشریح کرده بود. همان‌طور که او در انتهای سال ۲۰۱۸ نوشته بود: «پس از سالی جهنمی از رسوایی‌های فناوری، حتی مدیران ارشد ضددولتی هم

به‌مرور اعلام می‌کنند که پذیرای قانون‌گذاری هستند.» اما همان‌طور که او اذعان داشت هدف ما این بود که با ارائه پیشنهادی ویژه برای رگوله‌کردن فناوری تشخیص چهره توسط دولت «گامی بلندتر برداریم».

تا دسامبر به این نتیجه رسیدیم که آن‌قدر آموخته‌ایم که قانون جدیدی را پیشنهاد دهیم. می‌دانستیم پاسخ همه پرسش‌های بالقوه را نداریم، اما معتقد بودیم به اندازه کافی پاسخ وجود دارد تا قانون‌گذاری اولیه خوبی در این حوزه انجام شود که همزمان استمرار پیشرفت فناوری و حفاظت از منافع عمومی را ممکن کند. فکر می‌کردیم دولت‌ها باید با پیشرفت فناوری همگام باشند و رویکرد تدریجی امکان یادگیری سریع‌تر و بهتر بخش فناوری را فراهم کنند.

در واقع مفهومی را به امانت گرفته بودیم که حامیان زیادی در شرکت‌های استارت‌آپی و توسعه نرم‌افزار داشت. این مفهوم «کمینه محصول پذیرفتنی» بود. طبق تعریف «اریک ریس» (Eric Ries)، کارآفرین و نویسنده، این مفهوم از ایجاد «نسخه‌ای اولیه از محصول جدید» پشتیبانی می‌کند که «امکان کسب بیشترین دانش اعتبارسنجی‌شده (دانش مبتنی بر جمع‌آوری داده‌های واقعی، نه حدس‌زدن درباره آینده) در مورد مشتریان را می‌دهد». به عبارت دیگر طبق این مفهوم نباید تا رسیدن به پاسخ کامل همه پرسش‌های ممکن، منتظر بمانید. اگر مطمئنید پاسخ‌های قابل اطمینانی برای پرسش‌های حیاتی دارید، دست به عمل بزنید، محصول‌تان را بسازید و به بازار عرضه کنید تا بتوانید از بازخوردهای مشتریان واقعی یاد بگیرید. این رویکرد پیشروی سریع‌تر و موفق‌تر را برای کسب‌وکارها و همچنین فناوری ممکن کرده است.

وقتی سریع پیش می‌رویم، باز هم بسیار مهم است که سنجیده عمل کنیم و مطمئن باشیم که گام‌های اولیه مثبت خواهند بود. در این مورد باور داشتیم که برای پرداختن به مسئله تشخیص چهره مجموعه منسجمی از ایده‌ها داریم. در مؤسسه بروکینگز در واشنگتن دی‌سی نظر و استدلال‌مان برای قانون‌گذاری جدید را ارائه دادم و جزئیات بیشتری از پیشنهادمان منتشر کردم. سپس در طول شش ماه آینده با شرکت در رویدادهای عمومی و جلسات استماع قانونی در سراسر ایالات متحده و هشت کشور دیگر در اقصی نقاط جهان پیشنهادمان را ارائه کردیم.

معتقد بودیم قانون‌گذاری می‌تواند به سه مسئله کلیدی «ریسک سوگیری»، «حریم خصوصی» و «حفاظت از آزادی‌های دموکراتیک»، رسیدگی کند و بازاری کارآمد می‌تواند به پیشرفت در مسیر کاهش سوگیری شتاب ببخشد. هیچ‌کدام از مشتریانی که با آنها برخورد می‌کردیم، علاقه‌ای به خرید خدمت تشخیص چهره‌ای نداشتند که نرخ خطای بالایی دارد و به تبعیض منجر می‌شود. اما اگر مشتریان اطلاعات نداشتند، بازار نمی‌توانست کارکرد مناسبی داشته باشد. معتقد بودیم همان‌طور که گروه‌هایی مثل گزارش‌های مصرف‌کننده (Consumer Reports) مردم را از مسائلی مثل ایمنی خودرو آگاه کرده بودند، گروه‌های پژوهشی و سایر گروه‌ها می‌توانند آزمایش انجام دهند و در مورد دقت خدمات تشخیص چهره رقیب اطلاعات ارائه کنند. چنین کارهایی به پژوهشگرانی مثل جوی بولامووینی در ام‌آی‌تی قدرت بیشتری می‌داد تا پژوهش‌هایی را دنبال کنند که به ما کمک می‌کرد. موضوع کلیدی این بود که شرکت‌های حاضر در بازار ملزم به فراهم‌کردن امکان آزمایش محصولات‌شان شوند. پیشنهاد ما این بود و در عمل باعث می‌شد استفاده از رگولیشن بازار را تقویت کند.

معتقد بودیم برای کمک به کاهش ریسک تبعیض، قانون جدید باید سازمان‌هایی که فناوری تشخیص چهره را پیاده‌سازی می‌کنند، ملزم به آموزش کارمندان برای ارزیابی نتایج پیش از اتخاذ تصمیمات کلیدی کند، نه اینکه اجازه دهد تصمیم‌گیری را کاملاً به کامپیوترها واگذار کنند. در کنار مسائل دیگر نگران بودیم که ریسک‌های سوگیری زمانی تشدید شود که سازمان‌ها، تشخیص چهره را به نحوی پیاده‌سازی کنند که با نیت اولیه در زمان طراحی متفاوت باشد. کارمندان آموزش‌دیده می‌توانستند به برطرف‌کردن این مسئله کمک کنند.

از برخی جهات پرسش پیچیده‌تر این بود که مجریان قانون چه زمانی باید اجازه داشته باشند از تشخیص چهره برای انجام نظارت پیوسته بر افرادی خاص در زندگی روزمره استفاده کنند.

دموکراسی همواره به توانایی افراد در گفت‌وگو با یکدیگر و بحث در مورد دیدگاه‌هایشان به‌صورت خصوصی و عمومی وابسته بوده است. برای تحقق این شرایط افراد باید همواره بتوانند آزادانه و بدون نظارت دولتی رفت‌وآمد کنند.

کاربردهای دولتی بسیاری برای فناوری تشخیص چهره وجود دارد که از امنیت مردم حفاظت می‌کند و ارائه خدمات بهتر به مردم بدون ایجاد این نوع نگرانی‌ها را تقویت می‌کند. اما وقتی فناوری تشخیص چهره با دوربین‌های فراگیر و قدرت رایانش کلان و ذخیره‌سازی در ابر ترکیب می‌شود، دولت‌ها می‌توانند از آن برای نظارت همیشگی بر افراد خاصی استفاده کنند. می‌توانند این کار را در هر زمانی یا حتی همیشه انجام دهند. استفاده از این فناوری به این شکل می‌تواند نظارت انبوه را در مقیاسی بی‌سابقه ممکن کند.

همان‌طور که جرج اورول در رمان ۱۹۸۴ توصیف می‌کند، در یکی از چشم‌اندازهای آینده شهروندان باید مخفیانه راهی را به سمت اتاقی سیاه پیدا کنند تا کدها را روی بازوهای یکدیگر ثبت کنند؛ چراکه در غیر این صورت دوربین‌ها و میکروفن‌ها؛ چهره‌ها، صداها و همه کلمات‌شان را ثبت و ضبط خواهند کرد. اورول تقریباً ۷۰ سال پیش این تصویر را ترسیم کرده است. نگران بودیم که اکنون فناوری این نوع آینده را ممکن کند.

از نظر ما پاسخ این بود که قانون به سازمان‌های مجری قانون اجازه می‌داد فقط زمانی از تشخیص چهره برای نظارت پیوسته بر افرادی خاص استفاده کنند که برای این نظارت حکم دادگاهی مثل حکم تفتیش گرفته باشند یا موردی اضطراری مثل خطر برای جان انسان وجود داشته باشد. با این کار قوانینی برای خدمات تشخیص چهره وضع می‌شد که شبیه قوانین کنونی ایالات متحده برای ردیابی افراد از طریق اطلاعات جی‌پی‌اس تلفن‌های همراه‌شان بود. همان‌طور که دیوان عالی در سال ۲۰۱۸ تصمیم گرفته بود، پلیس نمی‌تواند بدون حکم تفتیش سوابق تلفن همراهی را به دست آورد که مکان آن و در نتیجه مکان فیزیکی فردی را نشان می‌دهد. پرسیده بودیم «آیا چهره‌ها به‌اندازه تلفن‌های همراه درخور حفاظت هستند؟ از نظر ما پاسخ کاملاً مثبت است».

در نهایت واضح بود که رگولیشن تشخیص چهره باید حریم خصوصی را در بستر تجاری هم حفظ کند. به‌سرعت به عصری نزدیک می‌شویم که در آن همه فروشگاه‌ها می‌توانند دوربین‌های متصل به ابر با خدمات تشخیص چهره آنی را نصب کنند. از لحظه‌ای که به مرکز خریدی وارد می‌شوید، این امکان وجود خواهد داشت که نه‌تنها از شما عکس گرفته شود؛ بلکه هر جا می‌روید کامپیوتری شما را شناسایی کند. صاحب

مرکز خرید می‌تواند این اطلاعات را با همه فروشگاه‌ها به اشتراک بگذارد. صاحبان فروشگاه‌ها با این داده‌ها می‌توانند بفهمند آخرین بار چه زمانی به فروشگاه آنها آمده‌اید و چه محصولی را مشاهده یا خریداری کرده‌اید و با به اشتراک گذاشتن این داده‌ها با سایر فروشگاه‌ها پیش‌بینی کنند دفعه بعد قصد خرید چه محصولی را دارید.

منظورمان این نبود که رگولیشن جدید باید همه این نوع فناوری‌ها را ممنوع کند. برعکس خودمان از شرکت‌هایی هستیم که به فروشگاه‌ها کمک می‌کنیم با استفاده مسئولانه از فناوری، تجربه خرید را بهبود ببخشند. معتقدیم بسیاری از مصرف‌کنندگان از خدمات مشتریان ناشی از این همکاری‌ها استقبال خواهند کرد. اما در عین حال احساس می‌کنیم افراد حق دارند بدانند چه زمانی از تشخیص چهره استفاده می‌شود، در مورد آن سؤال بپرسند و واقعاً حق انتخاب داشته باشند.

پیشنهاد دادیم قوانین جدید، سازمان‌هایی که از تشخیص چهره استفاده می‌کنند را به «اطلاع‌رسانی مشهود» ملزم کنند تا افراد از آن آگاه باشند. در ضمن گفتیم باید قوانین جدیدی تدوین شوند تا مشخص کنند افراد چه زمانی و چگونه می‌توانند از کنترل معنی‌دار بهره ببرند و رضایت خود را اعلام کنند. این مسئله دوم به‌وضوح نیازمند تلاش بیشتر برای تعریف رویکرد قانونی مناسب در طول سال‌های آتی است، به‌ویژه در ایالات متحده که قوانین حریم خصوصی کمتر از اروپا توسعه یافته‌اند.

بررسی نفوذ قوانین جدید نیز مفید بود. در مورد برخی جنبه‌ها نیاز نبود همه جا از تصویب قانون پشتیبانی کنیم. برای مثال اگر ایالت یا کشور مهمی شرکت‌ها را به در دسترس قرار دادن خدمات تشخیص چهره‌شان برای آزمایش عمومی و پژوهشی ملزم می‌کرد، آن‌وقت نتایج همه جا منتشر و پخش می‌شد. با این باور قانون‌گذاران ایالتی را ترغیب کردیم در حالی که برای تشکیل جلسات‌شان در ابتدای سال ۲۰۱۹ آماده می‌شوند، قانون‌گذاری جدید را در نظر بگیرند.

اما در مورد حفاظت از حریم خصوصی مصرف‌کننده و حفاظت از آزادی‌های دموکراتیک در همه حوزه‌های استحفاظی به قوانین جدید نیاز داریم. متوجه بودیم که با توجه به دیدگاه‌های متفاوت دولت‌های سراسر دنیا چنین هدفی واقع‌بینانه نیست. به همین دلیل صرفاً درخواست از دولت برای اقدام‌کردن، کافی نخواهد بود. حتی اگر

دولت ایالات متحده همراه می‌شد، همچنان سایر کشورها همراهی نمی‌کردند. افراد هرگز نمی‌توانستند مطمئن باشند که همه دولت‌های جهان از این فناوری مطابق اصول حفاظت از حقوق بشر استفاده خواهند کرد.

نیاز به رهبری دولت، شرکت‌های فناوری را از مسئولیت‌های اخلاقی‌شان معاف نمی‌کند. تشخیص چهره باید مطابق با ارزش‌های اجتماعی فراگیر توسعه یابد و استفاده شود. متناظر با پیشنهادهایمان برای قانون‌گذاری، شش اصل را منتشر کردیم که در ادامه در فناوری تشخیص چهره خودمان به کار بردیم. سیستم‌ها و ابزارهایی را هم برای اجرای این اصول ایجاد کرده‌ایم. سایر شرکت‌های فناوری و گروه‌های حامی و مدافع نیز رویکردهای مشابهی را در پیش گرفته‌اند.

مسئله تشخیص چهره نمایی کلی از سیر تکامل احتمالی چالش‌های اخلاقی دیگر هوش مصنوعی فراهم می‌کند. هرچند دیگران هم مانند ما می‌توانند کار را با اصولی کلی و عمومی شروع کنند، اما زمانی این اصول آزمایش می‌شوند که در عمل از آنها در فناوری‌های هوش مصنوعی ملموس و سناریوهای مشخص استفاده کنیم. با این اتفاق کاربردهای احتمالاً بحث‌برانگیز هوش مصنوعی نیز ظهور خواهند کرد.

مسائل بیشتری وجود خواهند داشت و هر کدام باید مانند تشخیص چهره با دقت بررسی شوند تا کاربردهای بالقوه این فناوری آشکار شود. در مورد بسیاری از این کاربردها به ترکیبی از رگولیشن جدید و خودتنظیمی شرکت‌های فناوری نیاز داریم. بسیاری از این کاربردها به طرح دیدگاه‌های مهم و متفاوتی در کشورها و فرهنگ‌های گوناگون منجر خواهند شد. بنابراین باید توانایی بهتری را برای کشورها توسعه دهیم تا در رسیدگی تکرارشونده به این مسائل سرعت و همکاری بیشتری داشته باشند. تنها از این طریق می‌توانیم مطمئن شویم که دستگاه‌ها نسبت به افراد پاسخگو می‌مانند.

۱۳

فصل سیزدهم

هوش مصنوعی و نیروی کار

بیستم دسامبر ۱۹۲۲ اسب‌های ایستگاه آتش‌نشانی ۲۰۵ به افسارهای کهنه‌شان فشار می‌آوردند و برای تاختن در این صبح سرد زمستانی مشتاق بودند. صدای سم اسب‌ها در خیابان‌های بروکلین هایتس (Brooklyn Heights) پژواک می‌شد. معاون ایستگاه، مارتین ملقب به «اسموکی جو» (Smokey Joe) زنگ ایستگاه را به صدا درآورد. نشانه اولین مأموریت گروه بود و اسب‌های مشتاق آتش‌نشان باید پای به خیابان‌های نیویورک می‌گذاشتند.

اما جایی آتش نگرفته بود. موتور بخار اسبی به سمت سالن «بروکلین بارو» (Brooklyn Borough Hall) حرکت می‌کرد؛ جایی که قرار بود زمام کار را به یگان موتوری واگذار کند.

هنگام خروج موتور بخار اسبی و تجهیزات آب‌پاش از ایستگاه آتش‌نشانی، مردم نیویورک در پیاده‌روها صف کشیده بودند تا این گروه را تشویق و در شهر همراهی کنند. شهروندان، مسئولان محلی و آتش‌نشانان از جمله سگ دالماسیان دوست‌داشتنی ایستگاه جمع شده بودند تا به آخرین اسب‌های آتش‌نشان باوفای ایستگاه ۲۰۵ ادای احترام کنند.

وقتی اسب‌ها نفس‌زنان و خیس عرق به سالن رسیدند، سگ دالماسیان شروع به چرخیدن دور درشکه آتش‌نشانی کرد تا آتش‌نشانان را به وصل‌کردن شیلنگ به شیر آتش‌نشانی تشویق کند. اما آتش‌نشانان اسب‌ها را با تاج‌های گل مزین کردند. آخرین مأموریت این تیم و آخرین مأموریت همه درشکه‌های آتش‌نشانی شهر نیویورک بود.

بازنشست‌کردن اسب‌های افسانه‌ای آتش‌نشان تصمیمی واقع‌بینانه بود، اما همان‌طور که روزنامه «بروکلین ایگل» (Brooklyn Eagle) نوشته بود، پیشرفت تأثیر عمیقی بر فرهنگ شهر گذاشت: «اسب آتش‌نشان باعث شادی و شعف پسران کوچک سه نسل شده بود؛ چراکه آتش‌نشانان همواره الهام‌بخش بوده‌اند. امروز اسب‌های آتش‌نشان احتمالاً برای همیشه از شهر نیویورک می‌روند.»

اسب آتش‌نشان پس از ۵۰ سال خدمت شغلش را از دست می‌داد. این اتفاق داستانی درباره تغییر فناوری و تأثیر آن بر کار است. در گذشته اسب‌های آتش‌نشان در جابه‌جایی درشکه‌های آتش‌نشانی جایگزین افراد شده بودند. ابتدا تیم‌هایی از مردان

و پسران داوطلب این درشکه‌ها را می‌کشیدند، اما در سال ۱۸۳۲ که همه‌گیری وبا در نیویورک بخش زیادی از نیروی اداره آتش‌نشانی این شهر را بیمار و ناتوان کرد، نیروی اسب به کمک آمد. «افراد کافی وجود نداشتند تا درشکه‌ها را تا محل آتش‌سوزی حمل کنند.» ضرورت، همان منشاء نوآوری، اداره آتش‌نشانی نیویورک را مجبور کرد که مبلغ هنگفت ۸۶۴ دلار را برای خرید ناوگانی از اسب‌ها صرف کند تا جایگزین آتش‌نشانان بیمار و در حال مرگ شوند.

تازه در دهه ۱۸۶۰ بود که نیروی انسانی رسماً جایش را در ایستگاه‌های آتش‌نشانی به نیروی اسب داد، اما این تغییر آسان نبود. یکی از موانع افتخار آتش‌نشانان به شغل کشندگی بود. در سال ۱۸۸۷ «آبراهام پردی» (Abraham Purdy)، یکی از مسن‌ترین آتش‌نشانان زنده آن زمان گفته بود که ورود اسب‌ها آن‌قدر در اداره آتش‌نشانی مشاجره به پا کرده که باعث شده شماری از اعضا استعفا کنند.

اما هیچ چیز نمی‌توانست سد راه جریان پیشرفت شود. پیشرفت‌های ادامه‌دار تجهیزات مثل افسارهای اسب بهتر در نهایت داوطلبان را از وظیفه کشیدن شیلنگ‌های آتش‌نشانی با دست خلاص کرد. سال ۱۸۶۹ اسب‌ها و آتش‌نشانان آموزش‌دیده می‌توانستند در کمتر از یک دقیقه از ایستگاه خارج شوند. اما در قرن بیستم اسب‌ها نیز با همان سرنوشت انسان‌ها در قرن قبلی روبه‌رو شدند. آنها هم شغل‌شان را از دست دادند. این بار ماشین‌های دارای موتور احتراقی جایگزین اسب‌ها شدند.

این تغییر بخش کوچکی از کل اقتصاد را نشان می‌داد. تغییرات فناوری در تقریباً سه قرن پی‌درپی ماهیت کار را عوض کرده و بدون شک استانداردهای زندگی را افزایش داده بود. اما حقیقت اجتناب‌ناپذیر این است که همیشه برنده‌ها و بازنده‌هایی وجود دارند. گاهی اوقات این برنده‌ها یا بازنده‌ها افراد و خانواده‌ها هستند، اما اغلب جوامع، ایالت‌ها و حتی کشورها هستند.

همان‌طور که قابل درک است، دنیای امروز هم به هوش مصنوعی با ترکیبی از امید و نگرانی نگاه می‌کند. آیا کامپیوترها همان کاری را با ما می‌کنند که ماشین‌ها با اسب‌ها کردند؟ شغل‌های ما تا چه حد در معرض خطر هستند؟

هر جا سفر می‌کنیم، افراد این پرسش‌ها را از ما می‌پرسند. وقتی در بعدازظهر یکشنبه‌ای توفانی با هواپیما به سمت باند فرودگاه بیابانی شهر «ال پاسو» (El Paso) در غرب تگزاس و مجاور مرز مکزیک می‌رفتیم، این پرسش‌ها ذهنم را مشغول کرده بودند. هواپیما در باد مخالف تکان می‌خورد و هنگام فرود سخت بالا و پایین شد. این شهر در شکافی در کوهستان پرصخره فرانکلین قرار دارد و به‌نوعی تقاطع دو ایالت و دو کشور در امتداد رود «ریو گرانده» (Rio Grande) است. بخش زیادی از این چشم‌انداز را از پنجره هواپیما تماشا کرده بودیم.

فرود نامساعدمان خیلی زود با استقبال گرم میزبانان خنثی شد. ال پاسو شهر دوزبانی و دوفرهنگی سرزنده و بخشی از جامعه بین‌المللی منحصربه‌فردی است که شامل شهر بزرگ‌تر خوارس (Juarez) در آن طرف مرز مکزیک می‌شود.

این سفر بخشی از برنامه «تک‌اسپارک» (TechSpark) مایکروسافت بود. این طرح را سال ۲۰۱۷ تدوین کردیم تا با چند جامعه در نقاط مختلف ایالات متحده مشارکت کنیم. هدف‌مان این بود که با استفاده از روش‌های جدیدی با رهبران کسب‌وکارها، دولت و سازمان‌های غیرانتفاعی محلی همکاری کنیم تا تأثیر فناوری بر جوامع خارج از شهرهای بزرگ کشور را بهتر ارزیابی کنیم. این برنامه شامل مشارکت فناوری‌محور با باشگاه فوتبال آمریکایی «گرین بی پکرز» (Green Bay Packers) می‌شد که در نزدیکی محل زندگی‌ام در کودکی قرار داشت. این طرح در سراسر کشور فرصتی را فراهم کرده بود تا از چالش‌های جدید ناشی از فناوری و چشم‌اندازهای روشن‌تری آگاه شویم که زمانی پدیدار می‌شوند که بتوانیم با روش‌های جدید از فناوری بهره‌برداری کنیم.

در حالی که در مسیر بزرگراه میان‌ایالتی ۱۰ رانندگی می‌کردیم، ضمیمه جدید اقتصاد ال پاسو توجه‌مان را جلب کرد. مراکز تماس بسیار بزرگی در بیابان پدیدار شده بودند، این مراکز، نماینده صنعت به‌سرعت در حال رشدی هستند که از توانایی این منطقه برای جذب کارمندان مسلط به هر دو زبان انگلیسی و اسپانیایی استفاده می‌کند. این مراکز تماس که هزاران نفر از اهالی ال پاسو را استخدام کرده‌اند، می‌توانند به جمعیتی تقریباً یک میلیارد نفری در نیم‌کره غربی خدمات ارائه کنند. اما در بازدید از این منطقه فکری آزاردهنده در ذهن‌مان سنگینی می‌کرد. تا یک دهه دیگر یا حتی زودتر، هوش

مصنوعی جایگزین بسیاری از شغل‌ها در مراکز تماس خواهد شد.

در جلسه‌ای که با رهبران این منطقه برای گفت‌وگو در مورد نحوه تأثیرگذاری احتمالی هوش مصنوعی بر اقتصاد محلی داشتیم، به نظرمان رسید بهتر است جلسه را با هشدار شروع کنیم. هیچ گوی بلورین آینده‌بینی وجود ندارد. اتفاقاً خیلی راحت است که رهبری در حوزه فناوری مدعی شود «آینده‌بین» بزرگی است و پیش‌بینی‌های در ظاهر مطمئن و حتی باشکوهی از جهان در یک یا دو دهه بعد ارائه دهد. افراد بدون شک گوش می‌دهند و اگر این رویکرد را دنبال کنید، خبر خوب برای شما این است که ۱۰ سال بعد احتمالاً افراد کمی به یاد می‌آورند شما چه گفتید و حتی اگر کاملاً اشتباه کنید، زمان زیادی برای اصلاح مسیرتان دارید.

اما صرف‌نظر از این هشدار، فرصت مهمی برای استنباط بینش‌های واقعی وجود دارد که به پیش‌بینی مسیر آینده کمک می‌کند. در دیدار با افراد در ال پاسو و بحث در مورد تأثیرگذاری هوش مصنوعی بر شغل‌ها در این منطقه، در مورد دو موضوع صحبت کردیم که می‌توانیم برای کسب بینش به آنها نگاه کنیم.

اولین موضوع این است که درک کنیم هوش مصنوعی توانایی انجام چه کارهایی را دارد و ندارد و ببینیم این توانایی‌ها چه تأثیری روی شغل‌ها و کار می‌گذارد. با نگاه منطقی باید به پیشرفت‌های تازه‌ای توجه کنیم که به هوش مصنوعی این امکان را داده که گفتار انسان را درک کند، تصاویر را تشخیص دهد، زبان‌ها را ترجمه کند و بر اساس توانایی‌اش در تشخیص الگوها به نتیجه‌گیری‌های جدید برسد. اگر بخش زیادی از یک شغل شامل کارهایی شود که هوش مصنوعی می‌تواند (با سرعت بیشتری) انجام دهد، آن‌وقت آن شغل در معرض ریسک جایگزین‌شدن با کامپیوتر قرار خواهد گرفت.

اگر بخواهم شغلی را پیش‌بینی کنم که هوش مصنوعی احتمالاً زودتر از سایر شغل‌ها آن را حذف خواهد کرد، جایگاه پذیرش سفارش از مشتریان در کیوسک رستوران‌های فست‌فود خودرویی را انتخاب می‌کنم. در حال حاضر فردی وجود دارد که به حرف ما گوش می‌دهد و سفارش‌مان را در کامپیوتر وارد می‌کند، اما هوش مصنوعی با وجود میکروفن‌های خارجی بهتر می‌تواند حرف‌ها را به‌خوبی انسان ثبت و درک کند. در نتیجه به‌زودی این کار را دستگاه انجام خواهد داد. طولی نمی‌کشد که به رستورانی

خودرویی برویم و به جای انسان با کامپیوتر حرف بزنیم. شاید کامپیوتر ۱۰۰ درصد دقیق نباشد، اما انسان هم این‌طور نیست. به همین دلیل است که فرصتی برای تأیید و اصلاح سفارش وجود خواهد داشت.

به همین دلیل به صنعت پررونق مرکز تماس در ال پاسو با ترکیبی از تحسین و نگرانی نگاه می‌کردیم. بخش زیادی از گفت‌وگوی تلفنی با مشتریان شامل درک خواسته‌ها و حل مسائل‌شان می‌شود. اما همین حالا هم کامپیوترها در حال پاسخگویی به درخواست‌های پشتیبانی ساده مشتریان هستند. اغلب وقتی با پشتیبانی مشتریان تماس می‌گیریم، احساس می‌کنیم سخت‌ترین کار این است که به فردی واقعی متصل شویم. دلیلش این است که کامپیوترها جواب تلفن را می‌دهند، از ما می‌خواهند شماره‌ای را وارد کنیم تا دستوری اجرا شود و از حرف‌های ما در قالب جمله‌های ساده رمزگشایی می‌کنند. با استمرار پیشرفت هوش مصنوعی بخش بیشتری از این کارها خودکار خواهد شد.

این شرایط همچنین دسته‌بندی‌های شغلی دیگری را نشان می‌دهد که ممکن است در خطر باشند. بخش زیادی از رانندگی شامل تشخیص بصری تصاویر از طریق شیشه‌های خودرو، تحلیل این اطلاعات و تصمیم‌گیری می‌شود. با پیشرفت کامپیوترها در این حوزه‌ها هوش مصنوعی می‌تواند عملیات رانندگی ماشین‌ها یا کامیون‌ها را بر عهده بگیرد. در میانه قرن بیستم افرادی حقوق می‌گرفتند تا در آسانسورهای ساختمان‌های بلند بنشینند و آن را راهبری کنند. امروزه چنین کاری نه‌تنها غیرعادی؛ بلکه بی‌مورد به نظر می‌رسد. آیا در میانه قرن بیست‌ویکم افراد همین احساس را در مورد رانندگان تاکسی یا اوبر خواهند داشت؟

پدیده مشابهی نیز روی بررسی و کنترل دستگاه‌ها تأثیر گذاشته است. در ساختمان مرکزی ردموند مایکروسافت بیش از ۳۵۰۰ کپسول آتش‌نشانی وجود دارد. در گذشته افرادی را به کار می‌گرفتیم تا هر ماه فشار هر کدام از کپسول‌های آتش‌نشانی را بررسی کنند و مطمئن شوند که از آستانه پذیرفته‌شده کمتر نیست. امروزه همه این کپسول‌ها با حسگرهای کوچکی به شبکه شرکت متصل هستند. هر وقت فشار از مقداری مشخص کمتر شود، داشبوردی مرکزی بلافاصله آن را نشان‌دار می‌کند تا فردی آن را

پر کند. امنیت، بهبود و هزینه کاهش یافته است، اما دیگر افرادی استخدام نمی‌شوند تا هر ماه این ۳۵۰۰ کپسول آتش‌نشانی را بررسی کنند.

مدت زیادی است که دستگاه‌ها و اتوماسیون جایگزین کارهای غیرفکری یا کارهای دستی تکراری می‌شوند، اما توانایی کامپیوترها برای فکر کردن شغل‌هایی را در معرض خطر قرار می‌دهد که علاوه بر زور بازو، شامل نیروی ذهنی هم می‌شوند. برای مثال با توجه به توانایی هوش مصنوعی در ترجمه زبان‌های انسانی که به‌سرعت بهبود می‌یابد، حذف شغل مترجمان شفاهی اجتناب‌ناپذیر به نظر می‌رسد.

به همین ترتیب کار دستیارهای وکیل را در نظر بگیرید. سال‌هاست که خدمات مبتنی بر فناوری روی این حوزه تأثیر گذاشته‌اند. ۱۵ سال پیش در مایکروسافت به ازای هر وکیل تقریباً یک دستیار وکیل استخدام می‌کردیم، اما توانایی ارائه دستیاری سلف‌سرویس در شبکه داخلی باعث شده اکنون به ازای هر چهار وکیل به یک دستیار وکیل نیاز داشته باشیم. با توجه به توانایی روبه‌رشد سیستم‌های مبتنی بر هوش مصنوعی در تشخیص الگو از طریق یادگیری ماشین، می‌توان انتظار داشت که فناوری علاوه بر کارهای دستیارهای وکیل، تحقیقات قانونی وکیل‌های کم‌سابقه را هم بر عهده بگیرد.

حتی تحصیلات تکمیلی یا مجموعه‌ای از مهارت‌های پیچیده باعث نمی‌شود کارمندان شغل‌شان را از دست ندهند. هوش مصنوعی روی همه طبقات درآمدی تأثیر می‌گذارد. متخصصان رادیولوژی را در نظر بگیرید که میانگین درآمدشان ۴۰۰ هزار دلار در سال است. این افراد بیشتر روز را صرف مشاهده و بررسی تصاویر سی‌تی‌اسکن و ام‌آرآی برای شناسایی ناهنجاری‌ها می‌کنند. با تزریق تعداد کافی تصویر به یک دستگاه متکی بر هوش مصنوعی، می‌توان آن را آموزش داد تا تصاویر ایکس‌ری بهنجار و ناهنجار را در تصاویر استخوان‌های شکسته، خون‌ریزی یا تومورهای سرطانی شناسایی کند.

از زاویه‌ای نابودی برخی شغل‌ها با هوش مصنوعی واقعاً ترسناک است، اما روزنه‌های امیدی هم وجود دارد. از آنجایی که خودم کارم را به‌عنوان وکیل دون‌پایه شروع کرده‌ام، درک می‌کنم که چرا ممکن است بسیاری از فارغ‌التحصیلان دانشکده حقوق از این

گزاره حمایت کنند که انجام کارهای حقوقی اولیه بسیار زیاد، در ابتدای مسیر کاری، به‌شدت ملال‌آور است. هنوز به یاد دارم وقتی در سال ۱۹۸۶ یکی از اولین کارهایم در شرکت حقوقی بزرگی شامل مطالعه و دیکته‌کردن خلاصه‌های بیش از ۱۰۰ هزار صفحه سند می‌شد، چه واکنشی نشان دادم. چنین کاری همین حالا هم خودکار شده است. لحظات مهیج کار معمولاً نه در جست‌وجوی پاسخ در حجم زیادی از اسناد یا پرونده‌های حقوقی؛ بلکه در طراحی پرسش‌های خلاقانه برای پرسیدن اتفاق می‌افتاد. هوش مصنوعی در برخی موارد جایگزین فعالیت‌های پیش‌پاافتاده و کارهای دشوار می‌شود. این‌گونه می‌توانیم تفکرمان را ارتقا ببخشیم و روی کارهایی تمرکز کنیم که کمال‌آفرین‌تر هستند.

انسان‌ها از بسیاری جهات در ایجاد کارهای جدیدی که نیازمند زمان و توجه بیشتری هستند، بسیار سرسخت بوده‌اند. در طول چند دهه ظهور خودرو، ماشین حساب، پست صوتی، پردازش واژگان و نرم‌افزارهای طراحی گرافیکی، بسیاری از شغل‌ها را حذف کرده یا تغییر داده‌اند، اما هنوز کارهای زیادی برای انجام‌دادن وجود دارد. گفته می‌شود شغل‌ها ترکیبی از وظایف هستند. برخی وظایف خودکار می‌شوند و برخی نمی‌شوند.

با عبور از موج‌های صنعتی‌سازی و اتوماسیون گوناگون، اکنون چه کاری خیلی زمان ما را می‌گیرد؟ همان‌طور که «ریک رشید» (Rick Rashid)، یکی از رؤسای سابق واحد تحقیقات مایکروسافت چند سال پیش به‌شوخی و جدی گفت، اکنون تعداد بسیار بیشتری از افراد زمان بسیار بیشتری را در جلسات می‌گذرانند. فقط هم جلسات نیستند که وقت ما را به خود اختصاص می‌دهند، همه ما انرژی بسیاری بیشتری را صرف برقراری ارتباط با یکدیگر از روش‌های فراوان می‌کنیم. هر کارمند دفتری به‌طور متوسط روزانه ۱۲۲ ایمیل کاری ارسال و دریافت می‌کند. در سال ۲۰۱۸ مردم دنیا هر روز معادل رقم سرسام‌آور ۲۸۱ میلیارد ایمیل کاری و غیرکاری تولید کردند. اما این ایمیل‌ها فقط بخشی از ارتباطات افراد هستند. افراد در سراسر دنیا روزانه ۱۴۵ میلیارد پیامک و پیام درون‌برنامه‌ای هم می‌فرستند.

از جهت مهمی این ارتباطات روی دیگر سکه هستند. برخی کارها وجود دارند

که هوش مصنوعی احتمالاً به‌خوبی انجام نخواهد داد. بسیاری از این کارها شامل مهارت‌های نرمی مثل همکاری با سایر افراد می‌شود که در همه سازمان‌های بزرگ و کوچک امری زیربنایی خواهند ماند. همان‌طور که ریک می‌گوید، این کارها اغلب نیازمند برگزاری جلسه هستند (جلساتی که بهتر است با برنامه‌ریزی مناسب برگزار شوند). به همین ترتیب بعید است هوش مصنوعی در ایجاد همدلی مورد نیاز در کار پرستاران، مشاوران، معلمان و روان‌درمانگران خیلی توانمند باشد. همه این افراد احتمالاً از هوش مصنوعی در برخی کارها استفاده خواهند کرد، اما بعید به نظر می‌رسد که هوش مصنوعی کاملاً جایگزین کار آنها شود.

هوش مصنوعی هم مانند همه فناوری‌های جدید، فقط شغل‌ها را حذف و عوض نمی‌کند، صنایع و حرفه‌های جدیدی هم به وجود می‌آورد. اما فهمیدن شغل‌های جدیدی که ایجاد می‌کند، بسیار دشوارتر از تحلیل تأثیر بالقوه آن بر نیروی کار امروز است. با این حال همین الان هم شغل‌های جدیدِ دربرگیرنده هوش مصنوعی، در حال ظهور هستند.

در بحث با رهبران سیاسی جهان در مورد هوش مصنوعی، خودمان هم با برخی از این بینش‌ها برخورد کرده‌ایم.

یکی از این فرصت‌ها در بهار ۲۰۱۷ یعنی زمانی فراهم شد که از زیرمجموعه مایکروسافت در بریتانیا بازدید می‌کردم و میزبان بازدید نخست‌وزیر «ترزا می» بودیم. کنار «سیندی رز» (Cindy Rose)، مدیرعامل کسب‌وکارمان در بریتانیا ایستاده بودم که کارآموزی جوان یک هدست هولولنز را روی سر نخست‌وزیر گذاشت. هر دو کمی نفس‌مان را حبس کردیم. وقتی نخست‌وزیر به‌سرعت نمایش واقعیت‌افزوده‌ای را در مورد نحوه استفاده از این دستگاه برای شناسایی عیب در دستگاه‌های پیشرفته تماشا می‌کرد، نفس‌مان را بیرون دادیم (از قرار معلوم کار کردن با هولولنز بسیار آسان‌تر از طراحی استراتژی مذاکره برای برگزیت بود).

بعد از نمایش، نخست‌وزیر می، هدست را از روی سرش برداشت و رو به کارآموز ما کرد تا درباره شغلش از او بپرسد. با افتخار پاسخ داد: «من مشاور تجسم هستم. به مشتریان کمک می‌کنم تجسم کنند که چطور می‌توانند از فناوری‌های جدیدی مثل

واقعیت‌افزوده در شرکت‌شان استفاده کنند.»

نخست‌وزیر تکرار کرد: «مشاور تجسم، چنین شغلی به گوشم نخورده بود.»

شغل‌های جدید زیادی با نام‌های جدیدی وجود خواهند داشت که اکنون برای ما ناشناخته‌اند. دوستان‌مان یا دوستان فرزندان‌مان در میهمانی شغل‌شان را متخصص تشخیص چهره، معمار مبتنی بر واقعیت‌افزوده و تحلیلگر داده‌های اینترنت اشیا توصیف می‌کنند. مانند نسل‌های قبل روزهایی خواهد آمد که احساس می‌کنیم برای درک آنچه افراد توصیف می‌کنند، به فرهنگ واژگان به‌روزشده‌ای نیاز داریم.

در نهایت همه علاقه‌مندند پیش‌بینی دقیقی در مورد این شغل‌های جدید مشاهده کنند، اما متأسفانه آینده مانند گذشته پیچیده و نامنظم است. هیچ غیب‌گویی هم وجود ندارد.

در پاییز ۲۰۱۶ اتفاقی برای ما افتاد که مهر تأییدی بر این نکته بود. به همراه ساتیا با آنگلا مرکل، صدر اعظم آلمان، در دفترش در ساختمان فولاد براق و شیشه‌ای کاخ صدر اعظم در برلین دیدار کردیم. این ساختمان سال ۲۰۰۱ در نزدیکی رایشتاگ، یکی از نمادهای کشور آلمان و ساختمان پارلمان افتتاح شده بود که قدمتش به اواخر قرن نوزدهم برمی‌گشت.

در حالی که پرتره‌ای از «کنراد آدناور»، صدر اعظم معروف آلمان بعد از جنگ جهانی دوم از بالا به ما نگاه می‌کرد، مترجمی در میز جلسه به ما پیوست که به‌سرعت متوجه شدیم حرفه‌ای‌گری دیپلماتیک‌اش کم از تسلط خوبش به آلمانی و انگلیسی ندارد. هرچند مرکل به‌خوبی و بسیار بهتر از چند کلمه آلمانی ما، انگلیسی صحبت می‌کرد، اما بخش‌هایی از گفت‌وگو آن‌قدر فنی بود که حضور مترجم را ضروری می‌کرد. در مقطعی از جلسه ساتیا در مورد هوش مصنوعی و مسیر پیش روی آن و همچنین از توانایی این فناوری در ترجمه زبان‌ها صحبت کرد. وقتی گفت هوش مصنوعی به‌زودی جایگزین مترجمان شفاهی می‌شود، لحظه‌ای مکث کرد، متوجه شد چه حرفی زده و به سمت مترجم نگاه کرد و گفت «متأسفم».

مترجم بی‌درنگ و با آرامش پاسخ داد: «نگران نباشید. ۲۰ سال پیش هم فردی از IBM همین حرف را به من زد و هنوز سر کارم هستم.»

این گفت‌وگو نکته مهمی را نشـان می‌دهـد. پیش‌بینی دقیق شـغل‌هایی که هوش مصنوعی جایگزین‌شان می‌شود، یک مسئله اسـت و پیش‌بینی اینکه جایگزین‌های مبتنی بر کامپیوتر چه زمانی جای انسان را می‌گیرند، مسئله‌ای بسیار متفاوت است. در ۲۵ سال حضور در مایکروسافت، بارها تحت تأثیر توانایی رهبران بخش مهندسی در پیش‌بینی مسیر پیش روی رایانش قرار گرفته‌ام. اما پیش‌بینی‌هایشان از چارچوب زمانی ایـن تغییرات بسـیار متنـوع بوده اسـت. افـراد معمـولاً بیش از حـد خوش‌بین هسـتند و برآوردشـان از زمان وقوع تغییرات بسـیار زودتر از واقعیت است، اما در این زمینه نقل قـول معروفی از بیل گیتس وجـود دارد که می‌گوید: «همیشـه تغییرات دو سال بعد را دست بالا و تغییرات ۱۰ سال بعد را دست‌کم می‌گیریم.»

این پدیده تازگی ندارد. سـروصدا در مورد خودرو اولین‌بار در سـال ۱۸۸۸ به پا شـد؛ سالی که برتا بنز (Bertha Benz)، همسـر کارل بنز، بنیان‌گذار مرسدس بنز، مسافت ۶۰ مایلی تا خانه مادرش را با اختراع همسرش رانندگی کرد تا به مطبوعات نشان دهد خودرو به چه پدیده‌ای تبدیل خواهد شـد، اما وقتی به عکسـی از بـرادوی نیویورک در سال ۱۹۰۵، یعنی ۱۷ سـال بعد نگاه کنید، خیابانی پر از اسـب و تراموا بدون حتی یک خودرو می‌بینید. زمان می‌برد تا فناوری‌های جدید به حدی از پختگی برسند که به‌طور گسـترده مورد پذیرش قـرار بگیرند، اما عکسـی دیگر از همـان تقاطع در ۱۵ سـال بعد یعنی سال ۱۹۲۰ خیابانی پر از خودرو و تراموا را بدون حتی یک اسب نشان می‌دهد.

فناوری‌های جدید به‌ندرت با سرعتی ثابت گسـترش می‌یابند. ابتدا سرعت هیاهو بیشتر از پیشرفت اسـت و توسـعه‌دهندگان فناوری باید مقدار مناسـبی شکیبایی و پشتکار داشته باشـند. بعد فناوری به نقطه‌عطف می‌رسد. در این نقطه اغلب شاهد تلاقی چنـد پیشـرفت متفـاوت و توانایی فردی بـرای تلفیق این پیشـرفت‌ها هسـتیم کـه تجربـه محصـول کلـی را جذاب‌تـر از گذشـته می‌کنـد. موفقیـت اسـتیو جابـز در عرضه آیفون در سـال ۲۰۰۷ به‌خوبی این موضوع را ترسـیم می‌کند. تلفن‌های همراه و دستیارهای دیجیتال شـخصی دسـتی به مدت یک دهه در حال پیشرفت بودند. اما پیشرفت فناوری صفحه نمایش‌های لمسی و طرح جابز برای یکپارچه‌سازی همه‌جانبه با طراحی سـاده و کاربرپسـند بود که به گسترش بسیار سـریع تلفن‌های هوشمند در

سراسر جهان منجر شد.

هوش مصنوعی احتمالاً هم مشابه و هم متفاوت خواهد بود. شواهدی وجود دارد که باور داشته باشیم برای بسیاری از سناریوهای هوش مصنوعی، مثل استفاده از کامپیوتر برای سفارش‌گیری در رستوران‌های ماشینی به نقطه اوج‌گیری رسیده‌ایم. اما به احتمال زیاد در مورد کاربردهای پیچیده‌تری مثل ماشین‌های خودران که در آنها خطا می‌تواند به آسیب یا مرگ منجر شود، زمان بسیار بیشتری نیاز خواهیم داشت. در نتیجه احتمالاً شاهد تحول یکباره تمام اقتصاد یا حتی یک فناوری واحد نخواهیم بود و با موج‌های متوالی در بخش‌های متفاوت مواجه خواهیم شد. شاید این موج‌ها عامل تأثیرگذار اصلی بر فناوری و تغییرات اجتماع در دو یا سه دهه پیش رو باشند.

از این رو فکر کردن به اثر فزاینده این تغییرات بر شغل‌ها و اقتصاد بسیار مهم‌تر می‌شود. نسبت به این آینده باید خوش‌بین باشیم یا بدبین؟ اگر تاریخ در این زمینه چیزی به ما یاد داده باشد که داده، باید همزمان خوش‌بین و بدبین باشیم.

مطالعه موسسه جهانی مک‌کنزی در سال ۲۰۱۷، درباره گذار به خودرو را در نظر بگیرید. طبق برآورد این مطالعه؛ «در فاصله سال‌های ۱۹۱۰ تا ۱۹۵۰ ظهور خودرو ۶٫۹ میلیون شغل خالص در ایالات متحده ایجاد کرد.» این مطالعه نشان می‌دهد گذار اقتصاد از اسب به خودرو در این چهار دهه ۱۰ برابر بیشتر از شغل‌هایی که از بین برد، شغل ایجاد کرد. این شغل‌ها شامل حرفه‌های جدیدی می‌شدند که خودروها را سرویس می‌کردند و از وسایل نقلیه موتوری برای حمل‌ونقل و ارسال کالا استفاده می‌کردند. به نظر می‌رسد این آمار، دلیل قانع‌کننده‌ای برای خوش‌بینی باشد.

اما شاخص متضادی هم وجود دارد. گزارشی در سال ۱۹۳۳ از اداره آمار ایالات متحده که در بحبوحه رکود بزرگ نوشته شده، نشان می‌دهد که گذار از اسب به خودرو «یکی از عوامل اصلی دخیل در وضعیت اقتصادی آن زمان بوده» که تمام کشور را تحت تأثیر قرار داده بود.

چطور می‌توانیم چنین نتیجه‌گیری‌های کاملاً متضادی را توضیح دهیم؟ از جهتی هر دو درست هستند. در بلندمدت نتیجه نهایی رضایت‌بخش است. بعد از ۴۰ سال، اقتصاد با کارآمدی از دوران تحول گذشت و خودرو و همچنین رشد اقتصادی بعد از

جنگ جهانی دوم با قدرت پیش رفتند. اما اقتصاد در دو دهه اول این سیر تحول در شرایط وخیمی قرار داشت.

وقتی در قرن بیست‌ویکم به آن دوران نگاه می‌کنیم، به‌سختی می‌توانیم تصور کنیم گذار از اسب به خودرو تأثیری تا این حد منفی داشته است، اما روایت مهم و پرماجرایی که اداره آمار (نهادی با دیدگاه مبتنی بر داده) به نمایش می‌گذارد، بینش‌هایی را برای عصر ما فراهم می‌کند.

در سال ۱۹۳۳ یک متخصص آمار کشاورزی در این اداره به نام «زلمر پتت» (Zellmer Pettet) مطالعه روی این داده‌ها را شروع کرد. زلمر ابتدا باغداری در جورجیا بود و بعد به‌عنوان مأمور میدانی به اداره آمار پیوست. هرچند در رشته فلسفه مدرک گرفته بود، اما در تلاقی کشاورزی و علمی به استادی رسید که امروزه آن را بیگ‌دیتا می‌خوانیم. ۱۱۵ مقاله نوشت و در جایگاه رئیس آمار کشاورزی بازنشست شد. او از این واقعیت بهره برد که آمارگیرهای ایالات متحده فقط تعداد افراد ساکن در سراسر کشور را نمی‌شمردند؛ بلکه اسب‌ها را هم می‌شمردند.

پتت گزارشی با عنوان «اسب‌های مزرعه» نوشت. هرچند این گزارش پر از ارقام گوناگون است، اما داستان جذابی می‌گوید که برای رکود بزرگ همان کاری را می‌کند که نمایش موزیکال سال ۲۰۰۳ برادوی با عنوان شرور (Wicked) برای فیلم مشهور «جادوگر شهر اوز» محصول ۱۹۳۹ کرد. این گزارش بسیاری از رویدادهایی را توضیح می‌داد که به رکود بزرگ منجر شدند.

داستان با اشاره به اتکای بسیار زیاد اقتصاد آمریکا به اسب‌ها، پیش از ظهور خودرو شروع می‌شود. همان‌طور که تاریخ‌نگاری می‌گوید: «در سال ۱۸۷۰ همه خانواده‌ها در ایالات متحده مستقیم یا غیرمستقیم به اسب وابسته بودند.» در سراسر کشور به ازای هر پنج نفر یک اسب وجود داشت. هر اسب معمولی روزانه ۱۰ برابر هر انسان کالری مصرف می‌کند، بنابراین بسیاری از کشاورزان بیشتر از غذای انسان به کاشت غذای اسب وابسته بودند.

پتت به مطالعه روی حجم زیاد داده‌های اداره آمار پرداخت و اتفاقاتی را مستند کرد که بعد از گسترش موتور درون‌سوز رخ دادند. در فاصله سال‌های ۱۹۲۰ تا ۱۹۳۰

ماشین‌ها، کامیون‌ها و ماشین‌آلات کشاورزی در کنار هم باعث کاهش شدید جمعیت اسب‌های کشور شدند. جمعیت اسب‌ها از ۱۹٫۸ میلیون در سرشماری ۱۹۲۰ به ۱۳٫۵ میلیون در سرشماری ۱۰ سال بعد رسید. تقریباً یک‌سوم جمعیت اسب‌ها کاهش یافته بود؛ بنابراین تقاضا برای مواد غذایی مصرفی آنها یعنی یونجه، جو دوسر و ذرت هم کاهش یافت.

راه‌حل مشهود برای کشاورزان این بود که به کاشت محصولات مصرفی انسان روی بیاورند. دقیقاً همین اتفاق هم افتاد. همان‌طور که پتت گزارش می‌دهد، کشاورزان از ۱۸ میلیون جریب فرنگی که به کاشت مواد غذایی مصرفی اسب اختصاص داشتند، برای تولید پنبه، گندم و تنباکو استفاده کردند. بازار را با این محصولات پر کردند و قیمت‌شان را به‌شدت کاهش دادند. با کاهش قیمت‌ها درآمد کشاورزان هم کاهش یافت. مجموع درآمد کشاورزان از این سه محصول از ۴٫۹ میلیارد دلار در سال ۱۹۱۹ به ۲٫۶ میلیارد دلار در سال ۱۹۲۹ و سپس به ۸۵۷ میلیون دلار در سال ۱۹۳۲ رسید. عوامل دیگری هم در کاهش درآمد مزارع در دهه ۱۹۳۰ دخیل بودند، ولی اثر کاهش جمعیت اسب‌ها غیرمستقیم، اما شدید و بی‌چون‌وچرا بود.

طولی نکشید که خانواده‌های روستایی در پرداخت وام‌های مزارع‌شان دچار مشکل شدند و بانک‌های روستایی نیز شروع به مصادره این مزارع کردند. اما بانک‌ها نمی‌توانستند در مصادره‌ها سرعت لازم را داشته باشند و خیلی زود در بازپرداخت بدهی‌هایشان به بانک‌های بزرگ مراکز مالی کشور دچار مشکل شدند. علاوه بر این همان‌طور که پتت در تحقیقاتش فهمیده بود، در شهرها شغل‌های زیادی به صنایع مبتنی بر کشاورزی مثل بسته‌بندی، تولید و ماشین‌آلات کشاورزی وابسته بودند. این شرایط تمام کشور را درگیر کرد. تا سال ۱۹۳۳ دیگر فقط اسب‌ها شغل‌شان را از دست نداده بودند؛ بلکه تقریباً ۱۳ میلیون نفر یا یک‌چهارم نیروی کار کشور بیکار شده بودند.

وقتی به تأثیر هوش مصنوعی بر شغل‌ها فکر می‌کنیم، چه درس‌هایی از تقریباً یک قرن پیش می‌گیریم؟ باید برای فرازونشیب‌های اجتناب‌ناپذیر آماده باشیم. دلایل زیادی وجود دارند که نشان می‌دهند گذار به عصر هوش مصنوعی تحولی به بزرگی گذار به خودرو خواهد بود. محو شدن اسب‌های کارگر اهمیت آثار اقتصادی

غیرمستقیمی را نشان می‌دهد که پیش‌بینی آنها دشوار است. این گذار هم مانند قرن بیستم گذاری خواهد بود که به نوآوری، نه‌فقط در فناوری؛ بلکه از سوی دولت‌ها و بخش عمومی هم نیاز دارد. دو نوآوری حاصل از رکود بزرگ را در نظر بگیرید؛ سیاست‌های دولتی در پرداخت مبلغی به کشاورزان برای بیش از اندازه تولید نکردن برخی محصولات و بیمه سپرده و رگولیشن‌هایی برای اطمینان یافتن از سلامت بانک‌ها.

هرچند نمی‌توانیم همه حوزه‌هایی را پیش‌بینی کنیم که در آنها به نوآوری‌های عمومی نیاز خواهیم داشت، اما باید فرض کنیم که چنین نیازهایی به وجود می‌آیند. در این بستر شاید بزرگ‌ترین نگرانی ما نه خیلی سریع‌بودن نوآوری فناورانه؛ بلکه خیلی کُند بودن اقدامات دولتی باشد. آیا دولت‌های دموکراتیک می‌توانند در دوران بن‌بست سیاسی و دوقطبی‌سازی کنونی به نیازها و بحران‌های جدید پاسخ بدهند؟ صرف‌نظر از اینکه در کجای طیف سیاسی قرار می‌گیریم، این پرسش یکی از برجسته‌ترین پرسش‌های دوران ماست.

از این داستان می‌توان پیامد مهم دیگری را هم استنباط کرد. این پیامد تأثیر ارزش‌های فرهنگی و انتخاب‌های اجتماعی گسترده‌تر در سیر تکامل فناوری است. امروز از دیدگاه ما جایگزینی اسب با خودرو احتمالاً اجتناب‌ناپذیر به نظر می‌رسد و از دیدگاه بلندمدت حقایق زیادی از این گزاره پشتیبانی می‌کنند. اما همان‌طور که نویسنده‌ای اشاره کرده، بسیاری از تحولات ویژه آنچنان اجتناب‌ناپذیر نبودند. این نویسنده می‌گوید: «جایگزینی قدرت حیوانی به شکل ویژه‌ای انجام شد که نتیجه انتخاب‌های فرهنگی مردم در مورد مصرف انرژی در اواخر قرن نوزدهم و اوایل قرن بیستم بود.» جنبش ترقی‌خواه در ایالات متحده برای بهبود بهره‌وری، بهداشت عمومی و ایمنی در شهرها تلاش می‌کرد و علاوه بر شتاب‌بخشیدن به گسترش خودروهایی که به نظر می‌رسید نماد این منافع هستند، سرعت کنار گذاشتن سفر با اسب را هم افزایش داد که مشکلاتی را در همان سه حوزه ایجاد کرد؛ مشکلاتی که شهرنشینان به‌خوبی آن را درک می‌کردند.

به همین ترتیب اشتباه خواهد بود اگر فرض کنیم روندهای فناوری مثل اتوماسیون

و استفاده از هوش مصنوعی صرفاً از فناوری و اقتصاد تأثیر می‌پذیرند. افراد، شرکت‌ها و حتی کشورها انتخاب‌هایی را بر اساس ارزش‌های فرهنگی، اولویت‌های مصرف‌کننده و رویه‌های سیاسی خودشان انجام می‌دهند. این قوانین و رگولیشن‌ها به احتمال زیاد در نقاط مختلف جهان متفاوت خواهند بود.

آخرین درسی که از این تحول می‌توان گرفت احتمالاً دلگرم‌کننده‌ترین هم هست. همان‌طور که پیش‌بینی تأثیر منفی تغییر فناورانه عمیق غیرممکن است، در مورد نیروهای غیرمستقیمی هم که به ایجاد شغل‌های جدید کمک می‌کنند، غافلگیری‌های مثبت بسیاری وجود خواهد داشت.

آثار مستقیم و غیرمستقیم خودرو را در جایی مثل نیویورک در نظر بگیرید. در سال ۱۹۱۷ یعنی حتی پنج سال پیش از بازنشستگی اسب‌های آتش‌نشان در بروکلین، نیویورک کانون فروش خودروی کشور بود. فروشگاه‌هایی که در برادوی کالسکه و افسار می‌فروختند، جای خود را به فروشگاه‌های عرضه لاستیک و باتری دادند. جایی که زمانی مرکز خریدوفروش اسب در آمریکا بود، به محل برج‌های اداری بلندی تبدیل شد که به بنز، فورد و جنرال‌موتورز تعلق داشتند. تعمیرگاه‌ها، پارکینگ‌ها، پمپ بنزین‌ها و شرکت‌های تاکسیرانی به‌شدت به نیروهای ماهر جدیدی نیاز داشتند تا بتوانند به گرایش روبه‌رشد آمریکایی‌ها به خودرو پاسخ بدهند.

هیچ‌کدام از این آثار مستقیم آنچنان غافلگیرکننده به نظر نمی‌رسند. مسئله عجیب و غافلگیرکننده، حتی با گذشت زمان، ظهور صنایع جدیدی بود که در نگاه اول، پیدایش آنها بسیار بعید به نظر می‌رسید.

یک نمونه خوب در این زمینه، صنعتی بود که خیلی سریع رشد کرد تا اعتباردهی به مصرف‌کننده را ممکن کند. تا سال ۱۹۲۴ درصد خودروهایی که قسطی خریده می‌شدند به ۷۵ درصد رسید. اوراق اقساط خودرو به‌سرعت نیمی از اعتبار اقساط خرد کشور را به خود اختصاص دادند. آن زمان هم مثل حالا خودرو معمولاً بعد از خانه دومین دارایی گران‌بهای هر خانواده‌ای بود. افراد برای خرید خودرو باید پول قرض می‌گرفتند. همان‌طور که تاریخ‌نگاری اقتصادی بیان می‌کند: «اعتبار اقساط و خودرو هر دو علت و معلول موفقیت یکدیگر بودند.»

همه این حرف‌ها به پرسش جالبی منتهی می‌شود. وقتی مردم نیویورک اولین خودرو را در خیابان‌های پایتخت مالی کشور مشاهده کردند، چند درصدشان پیش‌بینی می‌کردند که این اختراع به ایجاد شغل‌های جدیدی در بخش مالی منجر خواهد شد؟ مسیر حرکت از موتور درون‌سوز به وام خرد غیرمستقیم بود و به مرور زمان آشکار شد و تا حد زیادی با اختراع‌ها و فرایندهای کسب‌وکار دیگری در آن زمان مثل خط مونتاژ هنری فورد تقویت شد؛ خط مونتاژی که تولید انبوه و در نتیجه دسترسی ارزان‌تر و گسترده‌تر به خودرو را ممکن کرد.

خودرو جهان تبلیغات را نیز به همین ترتیب متحول کرد. نشان‌ها و تابلوها را حالا مسافرانی می‌دیدند که در خودرویی با سرعت ۳۰ مایل بر ساعت یا بیشتر عبور می‌کردند. در نتیجه «باید بلافاصله دیده و فهمیده می‌شدند؛ وگرنه هیچ فایده‌ای نداشتند.» این شرایط به ساخت لوگوهایی برای شرکت‌ها منجر شد که هر جا قرار می‌گرفتند، بلافاصله شناخته می‌شدند. با این حال گمان نمی‌کنم خریداران اولیه خودرو تصور می‌کردند که در ایجاد شغل‌های جدید در صنعت تبلیغات تأثیرگذار خواهند بود.

چشم‌اندازی به دست می‌آید که همزمان دلگرم‌کننده و هشداردهنده است. فناوری ما را بهره‌ورتر و از انجام کارهای تکراری کسل‌کننده خلاص می‌کند و شرکت‌ها و شغل‌های هیجان‌انگیز جدیدی می‌آفریند که نسل آینده، آن را عادی و پیش‌پاافتاده قلمداد می‌کند. عصری خواهد بود که به افراد ثابت‌قدم (و دارای توانمندی مالی) برای پرورش استعدادهای جدید و پذیرش ریسک‌های ایجاد شرکت‌های جدید پاداش می‌دهد. با این حال بدون شک مانند پیامدهای اقتصادی خودرو و آسیب فرهنگی ناشی از حذف اسب‌های آتش‌نشانان عقب‌نشینی‌هایی را تجربه می‌کنیم و در این فرایند چیزهای مهمی را از دست می‌دهیم. افرادی که می‌خواهند سرعت فناوری را کاهش دهند یا از همه پیامدهای منفی آن اجتناب کنند، احتمالاً سرخورده خواهند شد. اصل کلیدی برقراری تعادل بین فرصت‌ها و چالش‌های جدید در گرو اولویت‌دادن به تطبیق‌پذیری فردی و اجتماعی است.

این مسئله از بسیاری جهات جدید نیست. از آغاز اولین انقلاب صنعتی، افراد

همواره در حال سازگاری با فناوری‌های جدید و آثار آن بر شغل‌ها بوده‌اند. خوب است تأمل کنیم و ببینیم تطبیق‌پذیری در نسل‌های متوالی چه الزاماتی را برای افراد ایجاد کرده است. در حالی که به پیامدهای این مسئله برای محصولات و آینده مایکروسافت فکر می‌کردیم، به این نتیجه رسیدیم که افراد برای رسیدن به موفقیت، همواره باید بر چهار مهارت مسلط می‌بودند. این مهارت‌ها شامل یادگیری موضوعات و رشته‌های جدید، تحلیل و حل مسائل جدید، تبادل ایده‌ها و به اشتراک گذاشتن اطلاعات با دیگران و همکاری مؤثر تیمی می‌شود.

یکی از اهداف‌مان باید این باشد که با بهره‌برداری از هوش مصنوعی و ایجاد فناوری‌های جدید به افراد کمک کنیم در این حوزه‌ها بهتر عمل کنند. اگر بتوانیم به این هدف برسیم، توانمندی فزاینده‌ای را برای مواجهه با موج بعدی تغییر و استفاده از آن برای افراد مهیا می‌کنیم. با چنین چشم‌اندازی نه‌تنها مجالی برای خوش‌بینی وجود دارد؛ بلکه می‌توان تا حدی ایمان داشت که نبوغ انسانی راه‌های جدیدی را برای منفعت‌بردن افراد از فناوری آینده پیدا خواهد کرد.

فصل چهاردهم

ایالات متحده و چین

دنیای فناوری دوقطبی

در شب گرمی در سپتامبر ۲۰۱۵ چهره‌های برجسته‌ای از کسب‌وکار و دولت در ضیافتی مجلل در هتل «وستین سیاتل» دور هم جمع شده بودند. وقتی بساط شام در تالار بزرگ جمع شد، میهمان اصلی با کت‌وشلوار مشکی شیک و کراوات قرمز، پشت تریبون قرار گرفت. سکوت بر جمع ۷۵۰ نفره‌ای که آن شب از سراسر کشور آمده بودند، حاکم شد. در حالی که سخنران از جوانی‌اش حرف می‌زد، تاریخ آمریکا را یادآوری می‌کرد و به فرهنگ عامه غربی ارجاع می‌داد، حاضران مشتاقانه گوش می‌کردند. داستان‌هایی از بزرگ‌شدنش در خانواده‌ای معمولی و از علاقه همیشگی‌اش به آثار ارنست همینگوی، مارک تواین و هنری دیوید ثورو تعریف کرد. به جمعیت گفت که در دوران دانشجویی مقالات فدرالیست (The Federalist Papers) الکساندر همیلتون را می‌خوانده است؛ مجموعه مقالاتی که به لطف نمایش موزیکال موفق همیلتون دوباره مورد توجه قرار گرفته بود. نمایش همیلتون تازه یک ماه پیش در برادوی افتتاح شده بود.

سخنران مقدمه لذت‌بخش خود را با اشاره به هدفش برای فراهم‌کردن زندگی بهتر برای رأی‌دهندگانش تمام کرد. خودش این هدف را «رؤیا» می‌خواند، اما سخنران یک سیاست‌مدار آمریکایی معمولی نبود. اصلاً آمریکایی نبود. او «شی جین‌پینگ»، رئیس‌جمهور چین بود و رؤیایی که به آن اشاره می‌کرد، «رؤیای چینی» بود.

رئیس‌جمهور چین که نزدیک «هنری کیسینجر»، وزیر خارجه سابق و «پنی پریتزکر» (Penny Pritzker)، وزیر بازرگانی وقت ایستاده بود، صحبت‌هایش را با اشاره به مسائل مهمی ادامه داد که در سخنرانی تأثیرگذار او بعد از شام منتظرش بودیم. تعهد به توقف سرقت سایبری چین از شرکت‌های آمریکایی و باز نگه‌داشتن درهای بازار چین از جمله این مسائل مهم بودند.

چند ساعت پیش هواپیمای رئیس‌جمهور «شی» در پایگاه هوایی خصوصی «پین» (Paine) فرود آمده بود. این پایگاه در نزدیکی بزرگ‌ترین کارخانه جهان، یعنی تأسیسات تولید بوئینگ قرار دارد که در ۲۲ مایلی شمال سیاتل در شهر «اورت» (Everett) ایالت واشنگتن واقع شده است. اولین بازدید شی جین‌پینگ از ایالات متحده بعد از رسیدن به جایگاه رهبری پرجمعیت‌ترین کشور و دومین اقتصاد دنیا

بود. توقفش در «دروازه آمریکا به آسیا» اولین توقف در بازدید سریعی از ایالات متحده بود که شامل سفر به نیویورک و واشنگتن دی‌سی هم می‌شد. برنامه‌ریزی این سفر تاریخی از ماه‌ها پیش در دست انجام بود.

روز بعد در کنار سایر مدیران ارشد مایکروسافت، روی فرش قرمزی در داخل ورودی مرکز جلسات توجیهی مدیران ارشد (Executive Briefing Center) مایکروسافت ایستاده و منتظر بودم. کراوات‌هایمان را مرتب کردیم، جایگاه‌مان در صف خوشامدگویی را دوباره بررسی کردیم و از درهای شیشه‌ای به بیرون نگاهی انداختیم، منتظر هیئت نمایندگی ریاست‌جمهوری چین بودیم. همه جزئیات بازدید از مقر مایکروسافت را با دقت به مذاکره گذاشته و طراحی کرده بودیم.

دولت چین در طول دو ماه قبل چهار تیم مقدماتی را برای آماده‌سازی سفر شی جین‌پینگ فرستاده بود. به نظر می‌رسید در هر بازدید تعداد اعضای گروه برنامه‌ریزان چینی نسبت به سفر قبل دوبرابر می‌شود. در جلسه اول شرکت کرده بودم، اما در سه جلسه بعدی حضور نداشتم. یک هفته پیش از بازدید در حالی که جلسه برنامه‌ریزی نهایی تمام شده بود، تصادفاً در حال عبور از راهرو بودم. وقتی ایستادم تا با بازدیدکنندگان دست بدهم، خیلی زود فهمیدم که قرار است با چهل نفر احوال‌پرسی کنم.

هرچند مسئله تدارکات مهم بود، اما در مقایسه با مسائل دیگری که باید به آنها رسیدگی می‌کردیم، جزئی به حساب می‌آمد. همه می‌دانستند که فناوری از بحث‌های اصلی خواهد بود. یکی از مسائل مورد توجه شرکت‌های آمریکایی، از جمله مایکروسافت دسترسی گسترده‌تر به بازار چین بود. در اواخر بهار ۲۰۱۵ به پکن سفر کرده بودیم تا در ملاقات با مسئولان چین استدلال خودمان را برای وضعیتی ارائه بدهیم که معتقد بودیم دسترسی بازتر و منصفانه‌تری خواهد بود که همزمان به نفع تأمین‌کنندگان آمریکایی و مشتریان چینی خواهد بود. آهسته‌آهسته شاهد باز شدن دری به روی‌مان بودیم. بعد از مدت‌ها برای اولین‌بار بارقه امیدی روشن شده بود.

اما تنها یک ماه بعد در اوایل جولای خبری منتشر شد مبنی بر اینکه هکرهای چینی شماره تأمین اجتماعی و سایر اطلاعات شخصی بیش از ۲۱ میلیون آمریکایی را از اداره

مدیریت کارکنان ایالات متحده کپی کرده‌اند. هکرها به پایگاه داده‌ای نفوذ کرده بودند که اطلاعات همه آمریکایی‌های دارای مجوز دسترسی به اطلاعات امنیت ملی در آن ذخیره شده بود. این اتفاق توانمندی‌های چین در سرقت سایبری و نبود وحشتناک تمهیدات امنیتی در اداره مدیریت کارکنان را آشکار کرد.

هفته بعد کاخ سفید گروه کوچکی را دور هم جمع کرد تا در میانه برنامه‌ریزی برای بازدید ماه سپتامبر با مسئولان ارشد دولتی درباره این حادثه گفت‌وگو کنند. مشخص و در عین حال قابل درک بود که چینی‌ها با این هک سایبری روی نقطه حساسی در واشنگتن دست گذاشته‌اند. مسئولان نه‌تنها از سرقت داده‌ها خشمگین بودند؛ بلکه خجالت‌زده بودند که این هک چقدر آسان انجام شده است. این ترکیب از احساسات به‌ندرت به تصمیم‌گیری درست منتهی می‌شود.

تیم کاخ سفید در اقدامی تحسین‌برانگیز تا اواخر آگوست به مذاکره در مورد یک توافق امنیت سایبری جدید بین دو دولت نزدیک می‌شد، اما وضعیت همچنان خطرناک و نامطمئن بود. با پیشرفت فرایند برنامه‌ریزی برای بازدید مشخص شد که منطقی‌تر خواهد بود اگر رئیس‌جمهور شی سفرش را نه از واشنگتن دی‌سی؛ بلکه از جایی دیگر در ایالات متحده شروع کند تا پیش از رفتن به کاخ سفید فرصتی برای ایجاد جوی مثبت فراهم شود. ایالت واشنگتن انتخابی منطقی برای آغاز سفر بود.

۹ سال پیش، رئیس‌جمهور هو جین‌تائو سیاتل را برای شروع اولین سفر رسمی‌اش به ایالات متحده انتخاب کرده بود. بیل و ملیندا گیتس میهمانی شام مفصلی را در منزل‌شان در دریاچه واشنگتن (Lake Washington) برگزار کرده بودند و به نظر می‌رسید هر دو دولت از نتیجه راضی بودند. قبلاً نقش میزبان را ایفا کرده بودیم و پیشنهاد دادیم دوباره نیز همین کار را انجام دهیم و این بار میزبانی شامل بازدیدی از مایکروسافت هم می‌شد. فکر می‌کردیم این بازدید انگیزه‌ای برای پشتیبانی از توافق امنیت سایبری فراهم می‌کند و اگر توافق حاصل نشود، سپری دیپلماتیک ایجاد می‌کند.

آن روز بعدازظهر در انتظار برای رسیدن کاروان بزرگ به مایکروسافت با ترتیبی بسیار منظم ایستاده بودیم. قرار بود ابتدا ساتیا از رئیس‌جمهور استقبال کند و بعد بیل

گیتس و جان تامپسون، رئیس هیئت‌مدیره مایکروسافت به ایشان خوشامد بگویند. بعد رئیس‌جمهور با من و «کی لو» (Qi Lu) ملاقات می‌کرد. کی لو معاون ارشدی است که ریاست کسب‌وکار جست‌وجوی اینترنتی ما را بر عهده دارد و در چین بزرگ شده است. ساتیا با موفقیت رئیس‌جمهور را در بازدید راهنمایی کرد و سخنرانی خوشامدگویی را انجام داد. هری شوم نیز فناوری هولولنز ما را به نمایش گذاشت.

بعد برای مراسمی به اتاق بزرگی وارد شدیم که خبرنگاران آن را «به‌یادماندنی‌ترین لحظه» سفر آمریکا، نه‌فقط در بازدید از مایکروسافت یا سیاتل؛ بلکه در تمام سفر شش‌روزه رئیس‌جمهور شی به نقاط مختلف کشور خواندند. رهبران ۲۸ شرکت فناوری از ایالات متحده و چین برای ثبت عکس یادگاری دور هم جمع شده بودند. در کنار رئیس‌جمهور شی گروهی شامل تیم کوک، جف بزوس، جینی رومتی، مارک زاکربرگ و مدیران عامل تقریباً همه شرکت‌های فناوری برجسته در آمریکا قرار داشتند. عکسی بود که سخنان رئیس‌جمهور شی در مورد امنیت سایبری در میهمانی شام شب گذشته را تقویت می‌کرد؛ عکسی که روی سایر تصاویر این سفر سایه می‌انداخت. فقط یک رئیس‌جمهور دیگر جز رئیس‌جمهور ایالات متحده بود که می‌توانست چنین مخاطبی را دور هم جمع کند. واضح بود که رئیس‌جمهور شی و کشور چین به جایگاهی محوری نه‌فقط در اقتصاد جهانی؛ بلکه در صحنه فناوری جهانی رسیده‌اند.

از برخی زوایا ظهور چین به‌عنوان ابرقدرت فناوری نشان می‌دهد که اکنون در دنیای فناوری بیش از پیش دوقطبی زندگی می‌کنیم. چین و ایالات متحده بزرگ‌ترین مصرف‌کنندگان فناوری اطلاعات و همچنین بزرگ‌ترین تأمین‌کنندگان این فناوری برای سایر نقاط جهان هستند. در بسیاری از روزها هفت مورد از فهرست ۱۰ شرکت ارزشمند بازار سهام شرکت فناوری هستند. پنج مورد از این هفت شرکت آمریکایی و دو شرکت دیگر چینی هستند. یک دهه بعد در ترکیب شرکت‌های صدر این فهرست احتمالاً شرکت‌های چینی بیشتری حضور خواهند داشت.

اما رابطه فناوری ایالات متحده و چین هیچ مشابهی در هیچ جا و در هیچ زمانی ندارد. هرچند جهان در گذشته شاهد رقابت بین‌المللی در فناوری اطلاعات بوده (ایالات متحده و ژاپن در عصر رایانه‌های بزرگ دهه ۱۹۷۰ برای رسیدن به رهبری جهان

رقابت می‌کردند)، اما این بار شرایط متفاوت است. یکی از دلایل تفاوت این است که چین از مقیاسش به نحوی برای کنترل دسترسی به بازارش و منفعت‌رساندن به تأمین‌کنندگان چینی استفاده کرده که هیچ دولت دیگری نمی‌تواند. در نتیجه شرکت‌هایی مثل گوگل و فیس‌بوک که در همه جای دنیا نام‌های آشنایی هستند، در بازار چین تقریباً حضور ندارند.

هرچند شرکت‌های آمریکایی دیگر هم در چین حضور دارند، ولی فقط اپل با آیفون توانسته در این کشور به سطحی از موفقیت برسد که مشابه رهبری‌اش در سایر نقاط دنیاست. اپل توانسته سه‌برابر اینتل، دومین شرکت فناوری آمریکایی، در چین درآمد کسب کند.

در مورد سودآوری، وضعیت برای اپل از این هم بهتر است. سودی که اپل از بازار چین به دست می‌آورد، بیشتر از مجموع بخش فناوری آمریکا در این کشور است. دستاوردی برجسته که در عین حال با توجه به سهم زیاد چین در سودآوری جهانی اپل چالشی برای این شرکت است. همان‌طور که تجربه ما در مایکروسافت در گذر زمان و در سطح جهانی با محصولاتی مثل ویندوز و آفیس نشان می‌دهد، هر وقت بخش زیادی از درآمد یا سودآوری شما به منبعی خاص وابسته می‌شود، در نظر گرفتن تغییرات در آن حوزه دشوار می‌شود. این شرایط همچنین نشان می‌دهد که چرا رهبران اپل سفرهای زیادی به پکن دارند.

مهم‌تر اینکه موفقیت بی‌همتای اپل کمبودهای دیگران را پررنگ‌تر می‌کند. چرا برای شرکت‌های فناوری آمریکایی موفقیت در چین بسیار دشوارتر از سایر نقاط دنیاست؟ این پرسش یکی از پرسش‌های شاخص بخش فناوری در بیش از یک دهه اخیر است و سیاست‌مداران هر دو حزب در واشنگتن دی‌سی بیش از پیش می‌پرسند که با توجه به اینکه موفقیت شرکت‌های فناوری آمریکایی در چین همراه با انتقال بالقوه فناوری است، آیا اساساً می‌خواهند چنین موفقیتی حاصل شود یا خیر.

رابطه ایالات متحده و چین حول محور فناوری به پیچیده‌ترین رابطه در جهان و احتمالاً در تاریخ تبدیل شده است.

با افزایش رقابت، حیاتی است که هر کدام از کشورها دیگری را درک کنند. در موارد

زیادی روابـط بین‌المللی تاریخـی تحت تأثیـر دیدگاه‌هایی از کشـورهای دیگر بوده که بیش از آنکه مبتنی بر درک واقعیت باشند، کاریکاتوری بوده‌اند. چند دلیل وجود دارد که شرکت‌های آمریکایی در چین بیشتر از نقاط دیگر با مشکل روبه‌رو شده‌اند. خوب است که این دلایل را با پیش‌زمینه درست در کنار هم قرار دهیم.

مسـئله‌ای که بیش از پیش روشـن شـده، این اسـت که گاهی اوقات نیازها و علایق مصرف‌کننـدگان چینی در زمینه فنـاوری اطلاعات بـا نیازها و علایـق مصرف‌کنندگان آمریکایی، اروپایی و سـایر نقاط جهان تفاوت دارد. شـرکت‌های فناوری آمریکایی و از جمله مایکروسافت معمولاً محصولاتی را به بازار چین برده‌اند که از ابتدا برای کاربران ایالات متحده طراحی شـده بودند. در مواردی این محصـولات نیازهای کاربران چینی را برطرف کرده و با سلیقه آنها جور بوده؛ سـخت‌افزارهایی مثل آیفون و مایکروسافت سرفیس و نرم‌افزارهای بهره‌وری مثل مایکروسـافت آفیس نمونه‌های خوبی هستند. اما در موارد دیگر کاربران چینی مجذوب رویکردهای کاملاً جدید و متفاوتی شده‌اند.

بیل گیتس بیـش از دو دهه پیش با دوراندیشـی متوجه شـد کـه چین به بـازار بزرگ مشتریان و همچنین کشوری مهم برای استعدادهای حوزه فناوری تبدیل خواهد شد. در نوامبر ۱۹۹۸ واحد «تحقیقات آسیای مایکروسافت» افتتاح شد که اکنون در دو برج در پکن در نزدیکی دو نهاد پژوهشی مهم، دانشگاه چینهوا (Tsinghua) و دانشگاه پکینگ (Peking) قرار دارد. در دو دهه اول پژوهش‌های واحد تحقیقات آسـیای مایکروسـافت علاوه بر بنیان‌های علـوم کامپیوتر بر طیف گسـترده‌ای از حوزه‌ها شـامل زبان طبیعی و رابط‌های کاربری طبیعی، رایانش فشرده داده (dataintensive computing) و فناوری‌های پژوهشی متمرکز بوده اسـت. پژوهشـگران این واحد بیش از ۱۵۰۰ مقاله پژوهشی را در حوزه‌هایی منتشر کرده‌اند که در پیشرفت علوم کامپیوتر در سراسر دنیا سهم داشته‌اند. این واحد نمادی از پایگاه به‌سرعت در حال رشد استعدادهای فناوری چین است.

واحد تحقیقات آسیای مایکروسافت در مواردی از پژوهش‌های بنیادین عبور می‌کند تا محصولات جدیـدی را توسـعه دهـد و آزمایش کند کـه به‌طور ویـژه برای بـازار چین طراحی شـده‌اند. این محصـولات گاهی اوقات بـرای آمریکایی‌ها تعجب‌آور هسـتند. یکی از این محصولات «شـیائوآیس» (XiaoIce) نـام دارد و چت‌بات مبتنی بر هوش

مصنوعی مؤنثی است که به نحوی طراحی شده که با نوجوانان و افراد در اوایل دهه سوم زندگی‌شان گفت‌وگو کند. به نظر می‌رسد این چت‌بات نیازی اجتماعی را در چین برطرف کرده است. کاربران معمولاً هر روز ۱۵ تا ۲۰ دقیقه را به گفت‌وگو با شیائوآیس در مورد روزشان، مشکلات، امیدها و رؤیاهایشان صرف می‌کنند. این محصول شاید نیازی را در جامعه‌ای برطرف می‌کند که کودکان خواهر یا برادر ندارند. این چت‌بات اجتماعی تا جایی رشد کرده که به بیش از ۶۰۰ میلیون کاربر خدمات ارائه می‌کند و قابلیت‌هایش در حال رشد هستند و از جمله شامل اپلیکیشن‌های مبتنی بر هوش مصنوعی برای شعر و ترانه‌سرودن می‌شوند. شیائوآیس به‌نوعی سلبریتی تبدیل شده است. به‌عنوان مجری میهمان اخبار آب‌وهوا حضور یافته و پیوسته برنامه‌های تلویزیونی و رادیویی را اجرا می‌کند.

در بهار ۲۰۱۶ که شیائوآیس را به ایالات متحده آوردیم، سلیقه‌های متفاوت مردم جهان در زمینه فناوری به‌خوبی عیان شد. این چت‌بات را در بازار ایالات متحده با نام «تی» (Tay) عرضه کردیم. این نام جدید تازه شروع مشکلات ما با عرضه شیائوآیس در آمریکا بود.

در مرخصی بودم که با نگاه‌کردن به تلفنم هنگام شام برای خودم دردسر درست کردم. ایمیلی از وکیلی مستقر در بورلی هیلز به دستم رسید که خود را این‌طور معرفی کرده بود: «ما وکیل تیلور سوئیفت هستیم و به نیابت از او این ایمیل را برای شما می‌فرستیم.» همین شروع، آن ایمیل را از بقیه ایمیل‌های صندوق ورودی ایمیلم متمایز می‌کرد. در ادامه نوشته بود: «همان‌طور که حتماً می‌دانید، نام تی تداعی‌کننده موکل ماست.» حقیقتش نمی‌دانستم، اما در هر صورت این ایمیل توجهم را جلب کرد.

این وکیل در ادامه استدلال کرده بود که استفاده از نام تی رابطه اشتباه و گمراه‌کننده‌ای بین این خواننده پرطرفدار و چت‌بات ما ایجاد کرده و این کار قوانین فدرال و ایالتی را نقض می‌کند. وکلای نشان تجاری ما دیدگاه متفاوتی داشتند، اما نمی‌خواستیم به مصاف تیلور سوئیفت برویم یا حتی او را ناراحت کنیم. می‌توانستیم نام‌های بسیار زیاد دیگری را انتخاب کنیم؛ بنابراین به‌سرعت به بحث در مورد پیدا

کردن نامی جایگزین پرداختیم.

اما تقریباً بلافاصله متوجه شدیم که باید نگران مسائل بزرگ‌تری باشیم. تی مانند شیائوآیس می‌توانست بر اساس بازخوردها در گفت‌وگو، تعامل با افراد را آموزش ببیند. گروه کوچکی از افراد در شوخی بچگانه‌ای کمپین مؤثری راه انداخته و با استفاده از توییت‌ها به تی آموزش داده بودند که اظهارات نژادپرستانه‌ای را به زبان بیاورد. در عرض کمی بیشتر از یک روز مجبور شدیم تی را از بازار بیرون بکشیم تا به این مسئله رسیدگی کنیم. این اتفاق به ما درسی در مورد هنجارهای بین‌فرهنگی و همچنین نیاز به اتخاذ تدابیر حفاظتی قدرتمندتر برای هوش مصنوعی داد.

تی فقط یکی از نمونه‌هایی بود که تفاوت سنت‌های فرهنگی آمریکا و چین را نشان می‌داد. دلیل موفق‌نشدن خدمات توسعه‌یافته در ایالات متحده این بود که کاربران چینی محصولات متفاوتی را با رویکردهای متفاوتی ترجیح می‌دهند که برای کشور خودشان توسعه یافته‌اند. موارد بسیار برجسته‌تر از تی، موفقیت خدمات چینی مثل علی‌بابا در برابر آمازون در تجارت الکترونیکی، وی‌چت شرکت تنسنت در برابر خدمات آمریکایی حوزه پیام‌رسانی و بایدو در برابر گوگل در جست‌وجو بوده‌اند. این خدمات در بسیاری از ابعاد مهم و مستند نوآوری‌هایی انجام داده بودند تا به نحوی به سلیقه‌های مردم چین پاسخ بدهند که رقبای آمریکایی‌شان نتوانسته بودند.

این مسئله یکی از ویژگی‌های حوزه فناوری را برجسته می‌کند که در سراسر دنیا به‌ویژه چین مشاهده می‌شود. همه جا آدم‌های باهوش وجود دارند و شرکت‌های چینی نوآوری می‌کنند، سخت تلاش می‌کنند و به واسطه تعهد به نوآوری و وجدان کاری رخنه‌ناپذیری به موفقیت‌های چشم‌گیر دست می‌یابند که از گذشته جزء ارزش‌های طرفداران بازار آزاد از جمله در ایالات متحده بوده است. این ویژگی را نه‌تنها در شرکت‌های چینی سازنده ابزارهای فناوری؛ بلکه در نهادهایی در سراسر جامعه چین می‌بینید که با سرعتی فوق‌العاده در حال پیاده‌سازی پیشرفت‌های مبتنی بر هوش مصنوعی هستند. این رشد سریع در گسترش بازار، سرعت موتورهای پیشران فناوری چین را افزایش می‌دهد. این پدیده‌ها در کنار هم به بخش فناوری چین کمک می‌کنند که برای شرکت‌های فناوری آمریکایی، رقیبی بسیار سرسخت‌تر از هر جای

دیگری در دنیا باشند.

اما سایر عوامل سد راه ما برای موفقیت چالش‌برانگیزترند. اولین عامل موانع دسترسی به بازار چین و موانع فزاینده دسترسی به بازار ایالات متحده است.

چین رهبر جهانی اولیه بی‌چون‌وچرایی در رقابت برای ایجاد موانع دسترسی به بازار فناوری بوده است. مسئله این نیست که سایر کشورها علاقه‌ای به ایجاد این موانع نداشتند. مسئله این است که هزینه مشارکت در سیستم تجارت جهانی به‌ویژه از طریق سازمان تجارت جهانی مانع اجرای این استراتژی می‌شد. ترکیبی از مذاکرات چندجانبه و دوجانبه در کنار تمرکز بی‌وقفه و مصرانه دفتر نماینده تجاری ایالات متحده بازارهای سراسر جهان را در دسترس بخش فناوری آمریکا قرار داد.

فقط چین به واسطه بازار بزرگ و استراتژی قاطع و مشخص خود توانست در برابر این رویکرد مقاومت کند. محصولاتی که آزادانه به هر جای دیگری صادر می‌شدند، برای در دسترس قرار گرفتن در چین باید یک یا چند مجوز دولتی پیچیده دریافت می‌کردند. حتی با وجود مجوز نیز شرکت‌های فناوری آمریکایی اغلب مشاهده می‌کردند که بخش عمومی چین و سایر مشتریان بزرگ تنها زمانی فناوری آنها را می‌خرند و از آن استفاده می‌کنند که در سرمایه‌گذاری مشترک با شریکی چینی ارائه شود.

به نتیجه رساندن سرمایه‌گذاری‌های مشترک در بخش فناوری در بهترین دوره‌ها هم بسیار دشوار است. فناوری اطلاعات به‌سرعت تغییر می‌کند و اغلب با پیچیدگی مهندسی قابل توجهی همراه است. مدل‌های کسب‌وکار نیز اغلب متحول می‌شوند و در مجموع این شرایط تغییر پیوسته بازاریابی، فروش و پشتیبانی را ضروری می‌کند. در صنعتی که اکتساب‌های بزرگ اغلب شکست می‌خورند، سرمایه‌گذاری‌های مشترک به عاقبت بدتری دچار می‌شوند. تازه پیچیدگی کار کردن در کشورها، فرهنگ‌ها و زبان‌های متفاوت را هم باید به همه اینها اضافه کرد.

الزام غیررسمی برای ورود به بازار از طریق سرمایه‌گذاری مشترک، مانند این است که دونده‌ای صحرایی را ملزم به انجام مسابقه با یک کوله‌پشتی پر از وزنه‌های سنگین کنید. به‌ندرت می‌توان در چنین شرایطی موفق شد و وقتی با شرکت‌های

محلی تحسین‌برانگیزی رقابت می‌کنید که با چنین موانعی مواجه نیستند، احتمال موفقیت باز هم کمتر می‌شود. خلاصه اینکه الزام برای ارائه خدمات به چین از طریق سرمایه‌گذاری مشترک، مانع واقعی و معمولاً مؤثری برای دسترسی به بازار خواهد بود.

اما مشکلات فناوری‌محور بین چین و ایالات متحده بسیار فراتر از دسترسی به بازار هستند. با توجه به نقشی که فناوری اطلاعات در ارتباط فراگیر، بیان بدون محدودیت و جنبش‌های اجتماعی ایفا می‌کند، دولت چین از گذشته، استفاده از آن را به نحوی متفاوت با غرب رگوله کرده است. هر شرکت فناوری آمریکایی با ورود به بازار چین ملزم به رعایت مجموعه‌ای سرسام‌آور از رگولیشن‌های همواره در حال تغییر سازمان‌های دولتی بی‌شمار ملی و استانی است. روزهای دشوار زیادی وجود دارند که تعارض آشکار تمرکز چین بر نظم عمومی با تعهد غرب به حقوق بشر، مشکلات پیچیده‌ای را به وجود می‌آورند.

این تفاوت‌ها تا حدودی در تضادهای عمیق‌تری در فلسفه و دیدگاه‌های جهانی ریشه دارند. البته درک همه این مسائل و نسبت و تناسب آنها با یکدیگر مهم است.

همان‌طور که «ریچارد نیزبت» (Richard Nisbett)، استاد دانشگاه میشیگان در سال ۲۰۰۳ در کتاب «جغرافیای تفکر» اشاره می‌کند، این مسائل بازتاب‌دهنده سنت‌های فلسفی متفاوت و عمیقی است که به بیش از دو هزار سال قبل برمی‌گردند. تفکر آمریکایی اغلب تا حدی مبتنی بر فلسفه‌های پرورش‌یافته در یونان باستان است، در حالی که مبنای تفکر چینی آموزه‌های کنفوسیوس و پیروانش است. در طول دو هزار سال این فلسفه‌های متفاوت به رایج‌ترین و تأثیرگذارترین طرز فکرهای جهان تبدیل شده‌اند.

چندین دهه در جلسات گوناگون در سراسر دنیا شرکت کرده‌ام، اما پکن با همه جا فرق می‌کند. در این شهر گاهی اوقات بحث‌های دولتی به‌روشنی به تجربه‌های مربوط به بیش از دو هزار سال قبل یا دقیق‌تر بگویم به ۲۲۱ سال قبل از میلاد عطف می‌شوند، یعنی سالی که سلسله چین این کشور را متحد کرد.

همان‌طور که هنری کیسینجر می‌گوید، چین بقای هزارساله‌اش را مدیون «مجموعه‌ای از ارزش‌های پرورش‌یافته در جامعه و دولتی متشکل از مسئولان

فرهیخته و دانشمند» است. کیسینجر برای تمرکز بر چین احتمالاً بیش از هر مسئول آمریکایی دیگری در قرن گذشته زمان صرف کرده است؛ چنان که می‌گوید ارزش‌هایی که تا امروز همچنان سرلوحه تفکر رسمی در چین هستند، از آموزه‌های کنفوسیوس نشئت می‌گیرند که بیش از دو قرن قبل از ظهور سلسله چین از دنیا رفته‌اند. آموزه‌های او شامل تعهد به فرمانروایی دلسوزانه، سرسپردگی به یادگیری و دنبال‌کردن تناسب و توازن بر اساس منشور سلسله‌مراتبی سلوک اجتماعی می‌شود که وظیفه بنیادین «آگاهی از جایگاه خود» را دربر می‌گیرد.

آن‌طور که نیزبت می‌گوید، فلسفه یونانی که همچنان اساس تفکر سیاسی غرب است، مشابه اصل سرسپردگی به یادگیری کنفوسیوس، به حس کنجکاوی شدید معتقد است، اما در حس عاملیت فردی متفاوتی ریشه دارد؛ حسی که می‌گوید افراد «مسئول زندگی خودشان هستند و آزادند هر طور می‌خواهند زندگی کنند». طبق نظر ارسطو و سقراط تعریف یونانیان باستان از خوشبختی «شامل توانایی استفاده از قدرت‌های خود برای رسیدن به تعالی در زندگی بدون محدودیت می‌شد».

به‌عنوان شرکتی که در ایالات متحده بنیان‌گذاری و مستقر شده است، در ریشه‌های تاریخی‌مان و اهمیت حفاظت از حقوق بشر در سراسر دنیا تردید نداشتیم. یک دهه پیش تصمیم گرفتیم به واسطه ریسک‌های حقوق بشری ایمیل‌های مشتریان عادی را در سرورهای مستقر در چین میزبانی نکنیم. این کار را در حالی انجام دادیم که دولت چین به‌وضوح گفته بود که خدمات‌مان دیگر در دسترس مصرف‌کنندگان این کشور نخواهد بود. همیشه آن تماس‌های آخر شبی را به یاد می‌آورم که به کارمندان حاضر در چین تأکید می‌کردم که بر این نظرمان پافشاری کنند که تقاضاهای چین در مورد خدمت جست‌وجوی ما غیرقانونی است. این طرف خط در آسایش خانه‌ام نشسته بودم، در حالی که می‌دانستم آنها در حالتی ناخوشایند باید پاسخم را به مسئولان محلی انتقال دهند. در این اواخر هم دسترسی به خدمات تشخیص چهره‌مان را با توجه به احتمال استفاده از آن در نظارت الکترونیکی انبوه محدود کردیم.

چنین اتفاقاتی تعهد ما به حقوق بشر را در بوته آزمایش سختی قرار می‌داد. هرچند از مدت‌ها پیش به پشتیبانی از مشتریان‌مان و رشد در چین متعهد بودیم، در عین

حال بـه این جمع‌بنـدی رسـیدیم که اتخـاذ رویکـرد اصولی در برخـورد با این مسـئله ضرورت دارد. همان‌طور که با گذشت زمان روشن‌تر شده، ضروری است فعالیت‌هایمان را بر مبنای رویکردی انجام دهیم که به ارزش‌های بنیادین مثل حقوق جهان‌شمول بشر در برابر رشد درآمد و عملکرد مالی اولویت می‌دهد.

معتقدیـم ایـن تفاوت‌های اساسـی باعث می‌شـود آشـنایی مـردم دو اقتصـاد برتر جهان با سـنت‌های فرهنگی و تاریخی یکدیگر اهمیت بیشتری پیدا کند. اگرچه روی برگرداندن از دیگری برای هر کدام از کشورها آسان است، اما هیچ‌کدام از این تفاوت‌ها را از بین نمی‌برد.

در تابسـتان ۲۰۱۸ فرصت بی‌واسـطه‌ای در چین برای ما فراهم شـد تا بیشـتر با این تفاوت‌ها آشنا شـویم. سـفری یک‌هفته‌ای به آسـیا داشـتیم و قرار بود در یکشنبه‌ای بسـیار سـوزان در مـورد ارتبـاط و تضادهـای مدرن‌تریـن فنـاوری موجود یعنـی هوش مصنوعی و سنت‌های فلسفی و مذهبی پدیدارشده در طول هزاران سال بحث کنیم.

به همراه تیم مایکروسافت روز را با بازدید از معبد «لانگچوان» (Longquan) شروع کردیم که مجموعه‌ای از ساختمان‌های چوبی و سنگی چندطبقه با سقف‌هایی گسترده به سبک معماری بودایی است. این صومعه در منطقه سرسبز کوه «فونیکس» پارکی جنگلی در حومـه غربی پکن یا به قـول محلی‌ها ریه شـهر قرار دارد و در سلسـله لیائو سـاخته شـده اسـت. مکانی آرام در دو سـوی رودخانه‌ای در دامنه کـوه و محل زندگی هزاران جیرجیرک است. با اشتیاق در مسیرهای پرپیچ‌وخم و باغ‌ها قدم زدیم، اما زمانی بسیار مشعوف شدیم که میزبان‌مان پروژه‌های هوش مصنوعی‌اش را به ما نشان داد.

آن‌طور که استاد «زیانزین» (Xianxin) توضیح داد، این صومعه خود را وقف تلفیق آموزه‌ها و سـنت‌های بودایـی با دنیای مـدرن کرده بود. اسـتاد زیانزیـن دانش‌آموخته دانشـگاه فناوری پکن بود. بله، این راهب بودایی مدرک علوم کامپیوتر داشت. هزاران جلد متن بودایی باستان را به ما نشان داد که معبد در حال دیجیتال‌کردن آنها با کمک هوش مصنوعی بـود. اسـتاد در ادامه گفت کـه راهبـان از روش‌های ترجمـه مبتنی بر ماشین استفاده می‌کنند تا کارشـان را به ۱۶ زبان با مردم نقاط دیگر جهان به اشتراک بگذارند. فناوری مدرن به پیشبرد برخی از قدیمی‌ترین آموزه‌های جهان کمک می‌کرد.

بعدازظهر آن روز به مرکز پکن رفتیم تا با پروفسور «هی هوایهانگ» (He Huaihong)، یکی از فیلسوفان و متخصصان اخلاق برجسته این کشور دیدار کنیم. پروفسور هی در دانشگاه پکینگ تدریس می‌کرد و کتابی در مورد تغییر اصول اخلاقی در چین منتشر کرده بود. حتی مطالعه با عجله این کتاب خط بطلانی بر این باور می‌کشید که در چین معاصر گفتمان پرشور و حرارت وجود ندارد.

در مورد مسائل اخلاقی و فلسفی ناشی از هوش مصنوعی و نگاه احتمالاً متفاوت افراد به این مسائل در نقاط مختلف دنیا گفت‌وگو کردیم. وقتی یکی از اولین حرف‌های پروفسور هی به‌نوعی بازگویی برخی از حرف‌های ابتدایی کتاب ۱۵ سال پیش «نیزبت» بود، غافلگیر شدم. پروفسور هی گفت: «در غرب با حرکت روبه‌جلوی فناوری و خوش‌بینی نسبت به بهبود پیوسته، افراد پیشرفت را بیشتر خطی مستقیم می‌بینند.»

همان‌طور که نیزبت اشاره می‌کند، افراد در غرب اغلب بر هدفی خاص متمرکز می‌شوند و معتقدند اگر بتوانید خود را وقف پیشبرد آن کنید، می‌توانید دنیای پیرامون‌تان را تغییر دهید. این تفکر بخشی از روحیه کارآفرینی بود که سیلیکون‌ولی را نه‌فقط به مکانی ویژه؛ بلکه به نگرش محرک نوآوری تبدیل کرد.

پروفسور هی می‌گفت: «در چین ما همه‌چیز را چرخه‌وار می‌بینیم. معتقدیم زندگی مانند برج‌های فلکی یک دایره است و هر چیزی در زمانی در آینده به نقطه اولیه‌اش بازمی‌گردد.» این تفکر باعث می‌شود مردم چین، هم به گذشته و هم به آینده نگاه کنند و به جای قطعه‌ای مجزا، بیشتر بر تصویر کلی تمرکز کنند.

همان‌طور که نیزبت توضیح می‌دهد، وقتی می‌بینیم افراد در دو سوی اقیانوس آرام چه نگاه‌های متفاوتی به تصویری یکسان دارند، گستردگی این اقیانوس بیشتر به چشم می‌آید. تصویری از یک ببر در جنگل را در نظر بگیرید. آمریکایی‌ها احتمالاً بیشتر بر ببر و کارهایی که می‌تواند انجام دهد، تمرکز می‌کنند، اما چینی‌ها احتمالاً بیشتر بر جنگل و نحوه تأثیرگذاری آن بر همه ابعاد زندگی ببر تمرکز می‌کنند. هیچ‌کدام از این رویکردها اشتباه نیستند و می‌توان گفت ترکیبی از هر دو ارزشمندتر خواهد بود، اما تفاوت‌ها انکارناپذیرند.

این سنت‌های متفاوت با طرز تفکر هر کدام از این جوامع در مورد فناوری‌های جدید و رگولیشن آنها همخوانی دارد. آمریکایی‌ها به‌طور غریزی دولت را دور نگه می‌دارند تا فناوری نوپا بتواند به بلوغ برسد، تغییر کند و قدرتمندتر شود. آمریکایی‌ها نسبت به دستاوردهای احتمالی آن خوش‌بین هستند. چینی‌ها خیلی سریع‌تر به محیط رشد آن فناوری توجه می‌کنند و از جمله مجموعه‌ای از رگولیشن‌های دولتی را وضع می‌کنند که بر فعالیت‌های آن فناوری حاکم خواهد بود.

این موضوع دیگری است که به توضیح رابطه پیچیده شرکت‌های فناوری و دولت چین کمک می‌کند. باید بر مانعی بسیار فراتر از مانع زبانی غلبه کنیم. شرکت‌های فناوری با هم و با شورای حقوق بشر جهانی همکاری کرده‌اند تا پیروی از اصول جهانی مربوط به حریم خصوصی و آزادی بیان را ترویج کنند، اما در برخی موارد این اصول با همان حمایت دولت‌های جهان از جمله دولت چین بعد از جنگ جهانی دوم مواجه نمی‌شوند. برخی مواقع بحث‌های پیچیده‌ای وجود دارد که احساس می‌کنید محور اساسی بحث نه رویکردهای سیاسی؛ بلکه جهان‌بینی‌های متفاوت ارسطو و کنفوسیوس است.

انگار پیچیدگی‌های ناشی از این دیدگاه‌های فلسفی متفاوت کافی نبودند که مسائل امنیت سایبری دهه گذشته بر چالش‌ها افزودند. اتفاقاتی مثل هک اداره مدیریت کارکنان و همچنین گزارش‌هایی مبنی بر اینکه هوآوی، تولیدکننده سخت‌افزار چینی روترهایی ساخته که به دولت چین این امکان را می‌دهند که بر ارتباطات کاربران این روترها نظارت کند، با واکنش شدید و البته قابل درک دولت ایالات متحده مواجه شدند. وقتی افشاگری‌های اسنودن شامل تصویری از کارمندی آمریکایی می‌شد که روترهای سیسکو را دست‌کاری می‌کرد تا همین کار را با آنها انجام دهد، دولت چین در همان موقعیت دولت ایالات متحده قرار گرفت. هر دو شرکت از آن زمان تلاش می‌کنند تا اعتبارشان را دوباره در بازار به دست آورند که البته توفیق چندانی نداشته‌اند.

هر دو حزب سیاسی در واشنگتن دی‌سی بیش از پیش به افزایش نفوذ چین با نگرانی نگاه می‌کنند. هرچند رئیس‌جمهور ترامپ به چین فشار آورده که خرید تقریباً همه محصولات آمریکایی را افزایش دهد، اما یک بخش؛ یعنی فناوری اطلاعات برای

پشتیبانی شایسته‌تر بوده است. سیاست‌گذاران آمریکایی با اعتقاد به اینکه این فناوری بیش از پیش در قدرت اقتصادی و نیروی نظامی نقشی اساسی خواهد داشت، نگرانی‌های فزاینده‌ای را درباره انتقال پیوسته فناوری به چین ابراز کرده‌اند.

اگرچه به‌وضوح این نگرانی‌ها مهم و در حال گسترش هستند، ولی به‌کارگیری پاسخ‌های ساده در جواب مسائل پیچیده برای هر دو کشور ریسک‌هایی را به همراه دارد. در هر دو کشور جزئیات مهمی وجود دارد که باید در نظر گرفته شوند؛ نخست اینکه برخی فناوری‌های اطلاعات از دیدگاه امنیت ملی و نظامی حساس هستند، اما بسیاری از فناوری‌های اطلاعات دیگر این‌طور نیستند. ایده مفید بودن برخی فناوری‌ها برای اهداف نظامی و در عین حال صلح‌آمیز به هیچ‌وجه تازه نیست. این محصولات «دارای کاربرد دوگانه» دهه‌هاست در دسترس هستند و نظام کنترل صادرات کاملاً تثبیت‌شده‌ای وجود دارد که بر آنها حاکم است. در هر صورت این ریسک فزاینده وجود دارد که سیاست‌گذاران آمریکایی در بررسی افزایش قدرت پیوسته چین، نتوانند برخی تفاوت‌های حیاتی فناوری اطلاعات و سایر فناوری‌هایی را در نظر بگیرند که برای امنیت ملی مهم هستند.

علاوه بر این اگرچه برخی فناوری‌های اطلاعات محرمانه هستند، اما بسیاری از آنها این‌گونه نیستند. بر خلاف بسیاری از فناوری‌های نظامی، پیشرفت‌های علوم کامپیوتر و داده اغلب در سطح پژوهش‌های بنیادی رخ می‌دهند و ابتدا در قالب مقاله پژوهشی منتشر می‌شوند. یعنی در دسترس همه دنیا قرار دارند. همچنین یکی از ویژگی‌های تقریباً منحصربه‌فرد نرم‌افزارها این است که اغلب شامل کد منبعی می‌شوند که به‌صورت منبع‌باز منتشر می‌شود. یعنی همه در همه‌جا نه‌تنها می‌توانند این کدها را ببینند؛ بلکه می‌توانند در محصولات خودشان هم از آنها استفاده کنند. هرچند نگرانی درباره محافظت از اسرار تجاری مهم است و در برخی حوزه‌های علوم کامپیوتر جایگاه دارند، اما در برخی حوزه‌های نرم‌افزاری اسرار تجاری کاربرد چندانی در عمل ندارند.

همچنین برخی سناریوهای مربوط به فناوری نگرانی‌هایی را نسبت به حقوق بشر ایجاد می‌کنند، در حالی که در سایر سناریوها، چنین نگرانی‌هایی وجود ندارد. خدمات

تشخیص چهره و ذخیره‌سازی داده‌های شهروندان و مصرف‌کنندگان در ابر؛ دو مورد از این سناریوها هستند. از طرف دیگر از دهه ۱۹۸۰ مایکروسافت ورد را توزیع کرده‌ایم تا کاربران بتوانند از این نرم‌افزار استفاده کنند؛ بدون اینکه کسی بفهمد چه می‌نویسند. هرچند نسخه آنلاین ورد اکنون در ابر اجرا می‌شود، ولی افراد می‌توانند انتخاب کنند که می‌خواهند از کدام نسخه و چگونه استفاده کنند. همین نرم‌افزار در موضوع حقوق بشر می‌تواند در سناریوهای متفاوت آثار بسیار متفاوتی از خود بر جای بگذارد.

در نهایت اینکه چین بخشی حیاتی از زنجیره تأمین محصولات فناوری آمریکایی است. معمولاً از این نقش فقط جنبه تولید قطعات سخت‌افزار کامپیوتری شناخته می‌شود، اما چین نقش بسیار گسترده‌تری دارد. تعداد روزافزون مهندسان این کشور با فرایندی جهانی برای تحقیق و توسعه عجین شده است. بیشتر شرکت‌های فناوری پیشرفت‌های پژوهشی حاصل کار مهندسان چینی را با پیشرفت‌های مهندسان آمریکایی، بریتانیایی، هندی و بسیاری از کشورهای دیگر سراسر جهان تلفیق می‌کنند. اگرچه ممکن است سیاست‌گذاران به فکر ایجاد پرده‌ای آهنی در وسط اقیانوس آرام برای جدا کردن توسعه فناوری در این دو قاره باشند، ولی ماهیت جهانی توسعه فناوری اجرای چنین تفکری را دشوار می‌کند. حتی اگر چنین مانعی برداشته شود، باز هم اصلاً مشخص نیست کشوری که از چنین رویکردی پیروی می‌کند، سود خواهد برد یا صرفاً توسعه فناوری را در کشور خودش کُند می‌کند.

در مجموع ایالات متحده و چین در برخورد با تجارت فناوری با معضل روبه‌رشدی مواجه‌اند. سه جنبه بلندمدت وجود دارد که باید در نظر گرفته شود؛ جنبه اول اینکه در حال حاضر بعید است فردی بگوید شرکت‌های فناوری آمریکایی یا چینی دسترسی نامحدودی به بازارهای یکدیگر دارند. اتفاقاً برعکس رهبران فناوری اطلاعات هر کشور در کشور خودشان به‌نوعی مزیت بازی خانگی دست یافته‌اند. در نتیجه شرکت‌های آمریکایی و چینی بیش از پیش در کشور خودشان راحت‌تر موفق می‌شوند و در واقع زمین رقابت‌شان بقیه دنیاست.

از دیدگاه اقتصاد بین‌الملل خوب است به یاد داشته باشیم که این حفاظت از بازارهای خانگی برای شرکت‌های درگیر، نعمتی همراه با نقمت است. حتی در مورد

چین با ۱٫۴ میلیارد نفر جمعیت، باز هم بیش از ۸۰ درصد مصرف‌کنندگان جهان جایی به غیر از این کشور زندگی و کار می‌کنند. تنها راه کسب موفقیت جهانی به‌عنوان رهبر فناوری، جلب احترام جهانی است. وقتی شرکت‌های فناوری آمریکایی و چینی به‌دنبال رشد در اروپا، آمریکای لاتین، سایر نقاط آسیا یا هر جای دیگری در سطح جهان هستند، باید مشتریان خارج از مرزهایشان را جذب کنند. اگر دولت‌های ایالات متحده و چین فناوری‌های بومی کشور دیگر را غیرقابل اعتماد قلمداد کنند، این ریسک وجود خواهد داشت که سایر کشورهای دنیا نتیجه بگیرند که هر دو درست می‌گویند و به منابع دیگری مراجعه کنند.

از طرفی حساسیت‌های روشنی در مورد قطعات شبکه‌ای مثل محصولات شبکه نسل پنجم وجود دارد که هم در دوران صلح و هم در زمان جنگ نقشی اساسی در زیرساخت ملی دارند. با توجه به احتمال و سابقه دست‌کاری و هک توسط نقش‌آفرینان وابسته به حکومت‌ها، تمرکز بر این حوزه قابل درک است. اما حتی در این فضا نیز سیاست‌های ملی باید مبتنی بر واقعیت‌های عینی و تحلیل منطقی باشد. دولت‌ها در بررسی روش‌هایی که با تعقیب کیفری یا سایر راهکارهای قانونی جدی علیه شرکت‌ها یا افراد ویژه، منظور مهمی را به طرف مقابل القا می‌کنند، باید محتاط‌تر و دقیق‌تر باشند.

ورای مسئله نسل پنجم، برداشتن گام‌هایی برای ممنوع‌کردن ورود تعداد زیادی از خدمات فناوری در بسیاری از حوزه‌های دیگر احتمالاً غیرضروری و غیرسازنده خواهد بود. اگر رگولیشن لازم باشد، برای رگوله‌کردن قابل اطمینان و بی‌طرفانه بیشتر خدمات فناوری راه‌های بسیار زیادی وجود دارد. هرچه نباشد در راستای منافع اقتصادی دو رهبر اصلی فناوری جهان است که بیشتر بازارهای فناوری‌شان را برای دیگران باز نگه دارند تا سایر کشورهای دنیا هم با سرمشق قرار دادن آنها همین کار را انجام دهند.

جنبه دوم اینکه تمرکز فزاینده‌ای بر طرف صادرات معادله تجاری (به‌ویژه در واشنگتن دی‌سی) وجود دارد. چنین تفکری این احتمال را افزایش می‌دهد که مسئولان آمریکایی به‌دنبال مسدود کردن صادرات تعداد روزافزونی از محصولات فناوری حیاتی، نه‌فقط به چین؛ بلکه به تعداد بیشتری از کشورها هستند.

این ریسک وجود دارد که مسئولان آمریکایی درک نکنند موفقیت فناوری تقریباً همیشه نیازمند موفقیت در سطح جهانی است. اقتصاد فناوری اطلاعات با توزیع هزینه‌های تحقیق و توسعه و زیرساخت بین بیشترین کاربران ممکن می‌چرخد. این مسئله قیمت‌ها را کاهش می‌دهد و آثار شبکه‌ای مورد نیاز را برای تبدیل‌کردن اپلیکیشن‌های جدید به رهبر بازار ایجاد می‌کند. همان‌طور که «رید هافمن» (Reid Hoffman)، هم‌بنیان‌گذار لینکدین (و عضو هیئت‌مدیره مایکروسافت) نشان داده، توانایی «مقیاس‌پذیری برق‌آسا» (blitzscaling) و رسیدن به رهبری جهانی نقش بنیادینی در موفقیت فناوری دارد. اما اگر محصولات نتوانند ایالات متحده را ترک کنند، رسیدن به رهبری جهانی غیرممکن می‌شود.

این مسائل در مجموع نسل جدید کنترل‌های صادراتی بالقوه ایالات متحده را بیش از گذشته چالش‌برانگیز می‌کنند. در این زمینه باید با در نظر گرفتن رویکردهای صادراتی جدید حرکت کرد. در گذشته مسئولان کنترل صادرات بر اساس فهرست‌های محصولاتی کار می‌کردند که گاهی اوقات صادرات‌شان کاملاً ممنوع شده بود. در مورد بسیاری از فناوری‌های نوظهور مثل هوش مصنوعی و رایانش کوانتومی احتمالاً منطقی‌تر خواهد بود که برخی فناوری‌ها اجازه صادرات داشته باشند، اما محدودیت‌هایی بر آنها اعمال شود تا دسترسی‌شان برای برخی کاربردها و کاربران محدود شود. هرچند این کار مدیریت اجرایی صادرات را برای دولت‌ها و شرکت‌ها پیچیده‌تر می‌کند، اما احتمالاً تنها راهکار حفاظت از امنیت ملی و در عین حال بهبود رشد اقتصادی است.

جنبه آخر اینکه ابعاد گسترده‌تری نه‌فقط در مورد ایالات متحده و چین؛ بلکه برای جهان وجود دارد که باید در نظر گرفته شود. در زمینه استفاده مردم جهان از فناوری، دو کشور بیش از پیش، فضای اینترنت را به دودستگی تقریباً محض می‌کشانند. در سطحی بالاتر از این، بدون برقراری رابطه سالم بین دو کشور، تقریباً غیرممکن است که تصور کنیم دنیا در انتهای این قرن وضعیتی بهتر از آغاز آن داشته باشد. به بیان ساده دنیا، از جمله در مسائل فناوری، نیازمند رابطه‌ای پایدار بین ایالات متحده و چین است.

در این راستا به توسعه پیوسته زیربنای آموزشی و فرهنگی قدرتمندتر برای برقراری ارتباط ایالات متحده و چین نیاز داریم. مسائل فناوری دو کشور نیازمند فهمی مشترک از علم و فناوری و همچنین زبان، علوم اجتماعی و حتی علوم انسانی است. امروزه درک متقابل کشورها از یکدیگر بسیار محدودتر از آن است که باید باشد.

در بیشتر ابعاد، این درک محدود در ایالات متحده شدیدتر است. این واقعیت را در نظر بگیرید که آموزش رئیس‌جمهور شی شامل مطالعه آثار نویسندگانی مثل الکساندر همیلتون و ارنست همینگوی می‌شده است. چند سیاست‌مدار آمریکایی آثار نویسندگان چینی مشابه را مطالعه کرده‌اند؟ با وجود بیش از ۲۵۰۰ سال تاریخ غنی، مسئله نبود منبع نیست، موضوع کمبود علاقه است. تاریخ نشان می‌دهد که اگر ایالات متحده می‌خواهد با موفقیت از چالش‌های جهانی عبور کند، به رهبرانی نیاز دارد که جهان را درک کنند.

دست‌آخر اینکه ایالات متحده و چین به رابطه دوجانبه‌ای نیاز دارند که در راستای منافع هر دو باشد. رهبران هر کشور بحق، با چشمان کاملاً باز و سرسختانه بر منافع خودشان تمرکز خواهند کرد. اما هر وقت دولت‌های دو اقتصاد برتر جهان، دور هم جمع می‌شوند، مسئولیت دارند که نه‌تنها به منافع فردی و جمعی خودشان؛ بلکه به آثار رابطه‌شان بر سایر نقاط جهان نیز فکر کنند. سایر کشورها، با حدود ۸۰ درصد از جمعیت جهان، بیش از پیش به این مسئله وابسته هستند.

۱۵

فصل پانزدهم

دموکراتیک کردن آینده

ضرورت انقلاب داده باز

اینکه داده و هوش مصنوعی چه تأثیری بر توزیع قدرت ژئوپلیتیک و ثروت اقتصادی خواهند داشت، مسئله دیگری است که تا حدی به ایالات متحده و چین وابسته است، اما برای سایر نقاط دنیا پیامدهای گسترده‌تری دارد. این موضوع یکی از مسائل برجسته دوران ماست که در پاییز ۲۰۱۸ چشم‌اندازی بدبینانه نسبت به آن پدیدار شد.

در دیدار با اعضای کنگره در واشنگتن دی‌سی، چند سناتور اشاره کردند که نمونه پیش از چاپ کتاب جدیدی را به نام ابرقدرت‌های هوش مصنوعی (AI Superpowers) خوانده‌اند. نویسنده این کتاب، «کای فو لی» (Kai-Fu Lee) از مدیران ارشد اپل، مایکروسافت و گوگل بوده است. کای فو که در تایوان به دنیا آمده، اکنون سرمایه‌گذار خطرپذیر مطرحی در پکن است. استدلال او هشداردهنده است. ادعا می‌کند که «نظم دنیای هوش مصنوعی، اقتصاد همه چیز مال برنده را با تمرکز بی‌سابقه ثروت در دستان چند شرکت چینی و آمریکایی ترکیب می‌کند». آن‌طور که او می‌گوید «سایر کشورها مجبورند ته‌مانده‌ها را جمع کنند».

مبنای این دیدگاه چیست؟ مبنای آن بیش از همه قدرت داده است. استدلال این است: شرکتی که بیشترین کاربر را به دست آورد، بیشترین داده را به دست می‌آورد و چون داده برای هوش مصنوعی مانند سوخت موشک است، محصول هوش مصنوعی این شرکت قدرتمندتر می‌شود. این شرکت با محصول هوش مصنوعی قدرتمندتر، باز هم کاربران بیشتری و در نتیجه داده بیشتری به دست می‌آورد. این چرخه با افزایش نسبت بازده به مقیاس ادامه می‌یابد تا در نهایت این شرکت همه شرکت‌های دیگر را از بازار خارج می‌کند. به گفته کای فو؛ «هوش مصنوعی در ذات خود به ایجاد انحصار گرایش دارد. وقتی شرکتی از دیگران جلو بیفتد، این نوع چرخه تکرارشونده ادامه‌دار می‌تواند آن فاصله را به مانعی غیرقابل عبور برای ورود دیگر شرکت‌ها به بازار تبدیل کند.»

این انگاره در بازارهای فناوری اطلاعات رایج است و «اثر شبکه‌ای» خوانده می‌شود. برای مثال از دیرباز توسعه اپلیکیشن برای سیستم‌عامل درست بوده است. وقتی سیستم‌عاملی در جایگاه رهبری قرار بگیرد، همه می‌خواهند برای آن اپلیکیشن بسازند و اگر در ادامه سیستم‌عاملی با قابلیت‌های برتر عرضه شود، متقاعد کردن

توسعه‌دهندگان اپلیکیشن به لحاظ کردن آن در برنامه‌هایشان دشوار خواهد بود. در دهه ۱۹۹۰ با ویندوز از این پدیده سود بردیم، اما ۲۰ سال بعد با ویندوز فون در رقابت در برابر آیفون و اندروید در طرف دیگر معادله قرار گرفتیم. اکنون نیز هر پلتفرم رسانه اجتماعی جدیدی که بخواهد با فیس‌بوک رقابت کند، با همین مشکل مواجه می‌شود. یکی از دلایل شکست گوگل‌پلاس همین موضوع بود.

به گفته کای فو؛ هوش مصنوعی از اثر شبکه‌ای مشابه، اما با قدرت بسیار بیشتری بهره می‌برد و به تمرکز بیشتر قدرت در تقریباً همه بخش‌های اقتصاد منجر می‌شود. در هر بخش شرکتی که مؤثرتر از دیگران از هوش مصنوعی استفاده کند، بیشترین داده‌ها را درباره مشتریانش به دست می‌آورد و قدرتمندترین حلقه بازخورد را می‌سازد. در یک حالت نتیجه از این هم بدتر خواهد بود. در این حالت چند شرکت فناوری، داده‌ها را به‌صورت انحصاری در اختیار می‌گیرند و پردازش می‌کنند، در حالی که همه بخش‌های دیگر اقتصاد برای خدمات هوش مصنوعی‌شان به این شرکت‌ها وابسته هستند. با گذشت زمان این وضعیت احتمالاً به انتقال حجم عظیمی از ثروت اقتصادی از سایر بخش‌های صنعتی به این رهبران هوش مصنوعی منجر خواهد شد و اگر آن‌طور که کای فو پیش‌بینی می‌کند، این شرکت‌ها بیشتر در ساحل شرقی چین و ساحل غربی ایالات متحده مستقر باشند، آن‌وقت این دو منطقه به قیمت زیان همه مناطق دیگر سود می‌برند.

در مورد این پیش‌بینی‌ها چه نظری باید داشته باشیم؟ مانند بسیاری از موارد، خالی از واقعیت نیستند، اما ملغمه‌ای از واقعیت و موهومات هستند.

هوش مصنوعی به قدرت رایانش ابری، توسعه الگوریتم‌ها و مقادیر عظیم داده وابسته است. هر سه مؤلفه مهم‌اند، اما مهم‌ترین‌شان داده است؛ داده‌هایی که درباره دنیای فیزیکی، اقتصاد و زندگی روزمره ما هستند. با تکامل سریع یادگیری ماشین در ۱۰ سال اخیر مشخص شده که برای توسعه‌دهندگان هوش مصنوعی چیزی به نام داده بیش از حد معنی ندارد.

پیامدهای داده در جهان داده‌محور بسیار فراتر از اثرگذاری آن بر بخش فناوری است. تصور کنید محصولی مانند خودرویی جدید، در سال ۲۰۳۰ چه شکلی خواهد

بـود. مطالعه تازه‌ای بـرآورد کرده کـه تا آن زمـان نیمـی از هزینه خودرو شـامل قطعات الکترونیکی و رایانش خواهد بود؛ مقداری که در سال ۲۰۰۰ فقط ۲۰ درصد بود. مشـهود اسـت که تا سـال ۲۰۳۰، خودروها برای رانندگی و مسـیریابی خودران یـا نیمه‌خودران و همچنین قابلیت‌هـای ارتباطـات، سـرگرمی، تعمیر و نگهـداری و امنیتی همـواره به اینترنت متصل خواهند بود. همه این موارد احتمالاً شـامل هوش مصنوعی و مقادیر زیادی داده مبتنی بر رایانش ابری خواهند بود.

این سناریو پرسـش مهمی را مطرح می‌کند: کدام صنایع و شـرکت‌ها سود ناشی از کامپیوترهای متحرک مبتنی بر هـوش مصنوعی را از آن خود می‌کنند؟ خودروسـازان متعارف یا شرکت‌های فناوری؟

پاسـخ این پرسـش آثار بسـیار عمیقی به همـراه دارد. اگر ایـن ارزش اقتصـادی نزد خودروسـازان بماند، دلیلی برای خوش‌بینی بیشـتر به آینده بلندمدت‌تر شرکت‌های خودروسـازی مثل جنرال موتور، بی‌ام‌دبلیو، تویوتا و دیگران وجود دارد و البته می‌توان چشم‌انداز روشـن‌تری را برای دسـتمزدها و شـغل‌ها در این شـرکت‌ها و صاحبان این شـغل‌ها متصور بود. در این بسـتر واضح اسـت کـه این مسـئله برای سـهام‌داران این شـرکت‌ها و جوامـع و حتی کشـورهای محـل اسـتقرار این شـرکت‌ها مهم اسـت. اگر بگوییم آینده اقتصاد جاهایی مثل میشیگان، آلمان و ژاپن به این نتیجه وابسته است، بزرگ‌نمایی نکرده‌ایم.

اگر ایـن حـرف باورنکردنی به نظـر می‌رسـد، تأثیر آمـازون بر انتشـار کتـاب و اکنون بسـیاری از بخش‌های خرده‌فروشـی یا تأثیـر گوگل و فیس‌بـوک بر تبلیغـات را در نظر بگیرد. هوش مصنوعی می‌تواند همین تأثیر را بر همه‌چیز؛ از شرکت‌های هواپیمایی تا دارویی و ترابری بگذارد. در عمل این همان آینده‌ای است که کای فو لی ترسیم می‌کند. به همیـن دلیل دسـت‌کم مبنایـی محتمل وجـود کـه نتیجه بگیریـم در آینده شـاهد انتقال فزاینده ثروت به تعداد کمی شـرکت با بیشـترین منابع داده‌ای و مناطق محل استقرارشان خواهیم بود.

با این حال در اغلب موارد هیچ مسـیر واحد و اجتناب‌ناپذیری به سوی آینده وجود ندارد. هرچند ریسک وقوع چنین آینده‌ای وجود دارد، اما مسیر دیگری هم وجود دارد

که می‌توانیم آن را ترسیم و دنبال کنیم. باید افراد را با دسترسی گسترده‌تر به همه ابزارهای مورد نیاز برای بهره‌برداری از داده‌ها توانمند کنیم. همچنین باید رویکردهای اشتراک‌گذاری داده‌ای را توسعه دهیم که برای شرکت‌ها، جوامع و کشورهای بزرگ و کوچک فرصت‌های مؤثری برای کسب مزیت‌های داده فراهم می‌کنند. خلاصه اینکه باید هوش مصنوعی و داده‌هایی را دموکراتیک کنیم که هوش مصنوعی به آنها وابسته است.

حال باید به این پرسش پاسخ داد که چطور می‌توانیم در جهانی که مقادیر زیاد داده اهمیت دارد، فرصت بزرگ‌تری برای نقش‌آفرینان کوچک‌تر ایجاد کنیم؟

یکی از افرادی که احتمالاً پاسخ را می‌داند، «متیو ترونل» است. ترونل مدیر ارشد داده مرکز تحقیقات سرطان «فرد هاچینسون» (Fred Hutchinson) است. این مرکز یکی از مراکز تحقیقات سرطان مطرح در سیاتل است که به‌نام یکی از قهرمانان این شهر نام‌گذاری شده که ۱۰ فصل برای تیم بیس‌بال «دیترویت تایگرز» (Detroit Tigers) بازی کرد و مربی سه تیم بیس‌بال حرفه‌ای بود. فرد هاچینسون در سال ۱۹۶۱ تیم «سینسیناتی ردز» (Cincinnati Reds) را به لیگ جهانی رساند.

متأسفانه دوران حرفه‌ای موفق فرد در بیس‌بال و زندگی‌اش خیلی زود به پایان رسید؛ او در سال ۱۹۶۴ و در ۴۵ سالگی بر اثر سرطان درگذشت. «بیل هاچینسون»، برادرش، جراحی بود که سرطان فرد را درمان کرد. بیل بعد از مرگ برادر کوچک‌ترش مرکز تحقیقات اختصاصی درمان سرطان «فرد هاچ» را بنیان‌گذاری کرد.

ترونل در سال ۲۰۱۶ برای کار در مرکز فرد هاچ به سیاتل آمد. این مؤسسه ۲۷۰۰ کارمند دارد که در ۱۳ ساختمان واقع در ساحل جنوبی دریاچه «یونیون» (Union) کار می‌کنند. از آنجا برج نمادین سوزن فضایی سیاتل در دوردست دیده می‌شود.

این مرکز مأموریت بلندپروازانه‌ای دارد؛ قصد دارد سرطان و مرگ‌های ناشی از آن را به‌عنوان یکی از دلایل رنج انسان محو کند؛ دانشمندانی از جمله سه برنده جایزه نوبل را به همراه پزشکان و دیگر پژوهشگران دور هم جمع کرده تا پیشرفته‌ترین پژوهش‌ها و درمان‌ها را دنبال کنند. همچنین مشارکت نزدیکی با همسایه‌اش، دانشگاه واشنگتن دارد که مراکز علوم پزشکی و کامپیوتر مشهور جهانی دارد. مرکز هاچ دستاوردهای

تحسین‌برانگیزی شامل درمان‌های نوآورانه برای لوسمی و سایر سرطان‌های خون، پیوند مغز استخوان و در حال حاضر درمان‌های جدید در حوزه ایمنی‌درمانی داشته است.

مرکز هاچ تقریباً شبیه همه نهادها و شرکت‌های همه حوزه‌ها شده، یعنی آینده‌اش به داده وابسته است. آن‌طور که «گری گیلیلند» (Gary Gilliland)، رئیس مرکز هاچ می‌گوید، داده «پیشگیری، تشخیص و درمان سرطان را متحول خواهد کرد». او اشاره می‌کند که پژوهشگران در حال تبدیل داده به «میکروسکوپ جدید خارق‌العاده‌ای» هستند که نشان می‌دهد «سیستم ایمنی ما چطور به بیماری‌هایی مثل سرطان واکنش نشان می‌دهد». در نتیجه آینده علوم زیست‌پزشکی دیگر نه‌فقط به زیست‌شناسی؛ بلکه به تلاقی آن با علوم کامپیوتر و داده وابسته است.

هرچند ترونل هرگز با کای فو لی دیداری نداشته، اما این تشخیص او را در مسیری قرار داده که تز این نویسنده را به چالش می‌کشد؛ همان تزی که می‌گوید آینده فقط به آنهایی تعلق دارد که بزرگ‌ترین منابع داده جهان را کنترل می‌کنند. اگر این‌طور بود، حتی برای تیمی متشکل از دانشمندان برتر جهان در شهری با اندازه متوسط در گوشه‌ای دور از آمریکای شمالی، سخت می‌شد که بخواهند در میان اولین افرادی باشند که درمانی برای یکی از چالش‌برانگیزترین بیماری‌های جهان پیدا کنند. دلیل این مسئله روشن است. هرچند مرکز هاچ به مجموعه‌های مهمی از داده‌های پرونده‌های سلامت دسترسی دارد که به آن کمک می‌کنند تا تحقیقات سرطان مبتنی بر هوش مصنوعی را دنبال کند، اما به هیچ‌وجه بزرگ‌ترین مجموعه‌های داده جهان را در اختیار ندارد. مانند بیشتر سازمان‌ها و شرکت‌ها، هاچ هم اگر می‌خواهد در آینده همچنان پیشگام باشد، باید بدون داشتن همه داده‌های مورد نیازش به رقابت ادامه بدهد.

خوشبختانه مسیری روشن به سوی موفقیت وجود دارد و به دو ویژگی داده متکی است که آن را از اغلب منابع مهم دیگر متمایز می‌کنند.

ویژگی اول این است که برخلاف منابع طبیعی متعارف مثل نفت و گاز، داده را خود انسان تولید می‌کند. همان‌طور که ساتیا در یکی از جلسات جمعه تیم مدیریت ارشد گفته بود، داده احتمالاً «تجدیدپذیرترین منبع جهان است». چه منبع ارزشمند

دیگری را ناخواسته به‌کرات تولید می‌کنیم؟ انسان‌ها در حال تولید داده با نرخی روزافزون هستند. بر خلاف منابعی که ذخایرشان تمام‌شدنی یا دچار کمبود است، جهان لبریز از اقیانوسی همواره در حال گسترش از داده است.

منظور این نیست که مقیاس مهم نیست یا نقش‌آفرینان بزرگ‌تر مزیتی ندارند. چین جمعیت بیشتری دارد و در نتیجه بیشتر از هر کشور دیگری برای تولید داده ظرفیت دارد، اما برای مثال بر خلاف خاورمیانه که بیش از نیمی از ذخایر نفت کشف‌شده جهان را دارد، برای هر کشوری دشوار خواهد بود که بازار داده جهان را قبضه کند. افراد همه نقاط دنیا داده تولید می‌کنند و منطقی به نظر می‌رسد که انتظار داشته باشیم کشورها در طول این قرن کم‌وبیش به‌نسبت ترکیب اندازه نسبی جمعیت و فعالیت‌های اقتصادی‌شان داده تولید کنند.

چین و ایالات متحده ممکن است رهبران اول هوش مصنوعی باشند، اما چین هر چقدر هم که بزرگ باشد، جمعیتش فقط معادل ۱۸ درصد جمعیت دنیاست. جمعیت ایالات متحده هم فقط معادل ۴٫۳ درصد جمعیت دنیاست. در زمینه اندازه اقتصاد، ایالات متحده و چین مزیت بیشتری دارند. از کل تولید ناخالص داخلی جهان، ۲۳ درصد به ایالات متحده و ۱۶ درصد به چین تعلق دارد. اما از آنجایی که بسیار بیشتر محتمل است که دو کشور با هم رقابت کنند تا اینکه در کنار هم قرار بگیرند، پرسش اصلی این است که آیا یکی از این کشورها می‌تواند با کمتر از یک‌چهارم منابع جهان بر داده‌های جهان مسلط شود.

هرچند هیچ نتیجه تضمین‌شده واحدی وجود ندارد، بر اساس ویژگی دوم داده که از قرار معلوم مهم‌تر از ویژگی اول است، برای نقش‌آفرینان کوچک‌تر فرصت بیشتری وجود دارد. داده آن‌طور که اقتصاددانان می‌گویند «غیررقابتی» است. وقتی انرژی کارخانه‌ای با بشکه‌ای نفت تأمین می‌شود، آن بشکه در دسترس کارخانه دیگری قرار نمی‌گیرد. اما از داده می‌توان بارها و بارها استفاده کرد و ده‌ها سازمان می‌توانند از داده‌هایی یکسان بینش و درس فرابگیرند؛ بدون آنکه از کاربردپذیری آنها چیزی کم کنند. مسئله کلیدی این است که اطمینان حاصل کنیم مشارکت‌کنندگان گوناگون می‌توانند به داده‌ها دسترسی داشته باشند و از آنها استفاده کنند.

شـاید تعجب‌آور نباشد که جامعه پژوهشـی دانشگاهی در اسـتفاده از داده به این شکل پیشگام بوده است. با توجه به ماهیت و نقش پژوهش دانشگاهی، دانشگاه‌ها ایجاد مخازن داده‌ای را شـروع کرده‌اند که در آنها داده‌ها را می‌توان برای استفاده‌های مختلـف بـه اشـتراک گذاشـت. واحـد تحقیقـات مایکروسـافت نیـز ایـن رویکـرد اشـتراک‌گذاری داده را دنبال می‌کنـد و مجموعـه‌ای از داده‌های رایگان را در دسـترس قرار می‌دهد تا پژوهش را در حوزه‌هایی مثل پردازش زبـان طبیعی و بینایی کامپیوتر و همچنین علوم طبیعی و اجتماعی ارتقا ببخشد.

این توانایی برای اشتراک‌گذاری داده‌ها بود که الهام‌بخش متیو ترونل شد. او دریافت که بهترین راه شتاب‌بخشیدن به تلاش‌ها برای درمان سرطان این است که با روش‌های جدیدی امکان اشتراک‌گذاری داده‌ها بین سازمان‌های پژوهشی مختلف را فراهم کند.

هرچند روی کاغذ ساده به نظر می‌رسـد، اما اجرای آن پیچیده است. به‌عنوان مثال حتی در هر سـازمانی نیز داده‌ها اغلـب در جزیره‌هایی جدا از هم ذخیره می‌شـوند که باید به هم متصل شـوند؛ چالشـی کـه وقتی ایـن جزیره‌هـا در نهادهای متفـاوت قرار دارند، دشـوارتر می‌شـود. ممکن اسـت داده‌هـا در فرمت قابـل خواندن برای ماشـین ذخیره نشده باشند. حتی اگر قابل خواندن باشند، باز هم مجموعه‌های داده متفاوت احتمالاً به شـکل‌های متفاوت فرمت‌بندی، برچسـب‌گذاری و سـاختاربندی شده‌اند که اشـتراک‌گذاری آنها و استفاده مشترک از آنها را دشـوارتر می‌کند. اگر افراد منشاء داده‌ها باشـند، مسـائل قانونی مربـوط به حریم خصوصـی باید حل شـوند. حتی اگر داده‌ها شامل اطلاعات شخصی نباشند، پرسش‌های مهم دیگری مثل فرایند حکمرانی در میان سازمان‌ها و مالکیت داده‌ها همراه با رشد و بهبود آنها باید پاسخ داده شوند.

این چالش‌ها فقط ماهیت فنی ندارند. سـازمانی، حقوقی، اجتماعی و فرهنگی هم هسـتند. همان‌طور کـه ترونل می‌گویـد، ایـن چالش‌ها تا حـدی از این واقعیت ناشـی می‌شوند که اغلب مؤسسات پژوهشی بیشتر پژوهش‌های فناوری را با ابزارهایی انجام داده‌اند که درون مؤسسـه خودشان توسعه داده بودند. چنانچه او می‌گوید: «این رویکرد علاوه بر محصور کـردن داده‌ها در یک سـازمان، اغلب بـه جمع‌آوری تکـراری داده‌ها، گم‌شـدن سـوابق و نتایج بیماران و ناآگاهی از وجود داده‌های تکمیلـی بالقوه در جایی

دیگر منجر می‌شود. این مشکلات در کنار هم مانع اکتشاف می‌شود، سرعت پژوهش در مورد داده‌های سلامت را کاهش می‌دهد و هزینه‌ها را بالا می‌برد.»

ترونل می‌گوید تأثیر جمعی همه این موانع مشارکت سازمان‌های پژوهشی و شرکت‌های فناوری را دشوار می‌کند و در نتیجه مانع جمع‌آوری مجموعه‌های داده‌ای می‌شود که به اندازه کافی برای پشتیبانی از یادگیری ماشین بزرگ هستند. در عمل ناتوانی در غلبه بر این موانع بهترین چشم‌انداز را برای سلطه مبتنی بر هوش مصنوعی شرکت‌ها طبق پیش‌بینی کای فو لی فراهم می‌کند.

ترونل و افراد دیگری در مرکز هاچ مسئله‌ای مربوط به داده را مشاهده کردند که باید حل می‌شد و پا در مسیر حل آن گذاشتند. ساتیا که خودش عضو هیئت‌مدیره مرکز هاچ است، در آگوست ۲۰۱۸ گروهی از کارمندان ارشد مایکروسافت را به میهمانی شامی دعوت کرد تا در مورد تلاش‌های هاچ بشنوند. ترونل از چشم‌اندازش درباره فضاهای داده مشترکی صحبت کرد که به مؤسسات پژوهشی سرطان گوناگون این امکان را می‌دهد که داده‌هایشان را با شیوه‌های جدیدی به اشتراک بگذارند. در چشم‌انداز او چند سازمان کنار هم قرار می‌گرفتند تا داده‌هایشان را در مشارکت با یک شرکت فناوری یکپارچه کنند.

همان‌طور که به ارائه او گوش می‌دادم، اشتیاقم بیشتر می‌شد. این چالش از ابعاد زیادی مانند بسیاری از چالش‌های دیگری بود که در موردشان شنیده یا حتی خودمان تجربه کرده بودیم. توصیف ترونل از برنامه‌هایش مسیر تکامل توسعه نرم‌افزار را به یادم آورد. در روزهای ابتدایی شکل‌گیری مایکروسافت، توسعه‌دهندگان از کد منبع‌شان مثل اسرار تجاری حفاظت می‌کردند و بیشتر شرکت‌های فناوری و سایر سازمان‌ها خودشان کدهایشان را توسعه می‌دادند. اما جنبش منبع‌باز، تولید و استفاده از نرم‌افزار را متحول کرد. توسعه‌دهندگان نرم‌افزار بیش از پیش کدهایشان را بر اساس طیفی از مدل‌های منبع‌باز منتشر می‌کردند. این مدل‌ها به دیگران این امکان را می‌داد که این کدها را تلفیق و از آنها استفاده کنند و آنها را بهبود بخشند. این اتفاق همکاری گسترده میان توسعه‌دهندگان را ممکن ساخت و در نتیجه به افزایش سرعت نوآوری نرم‌افزاری کمک کرد.

وقتی این تحولات شروع شدند، ما در مایکروسافت نه‌تنها در پذیرش آنها کُند عمل کردیم؛ بلکه فعالانه در برابر آنها ایستادیم. از جمله اینکه از پتنت‌هایمان علیه شرکت‌هایی استفاده کردیم که محصولات را با کدهای منبع‌باز عرضه می‌کردند. خودم نیز یکی از مشارکت‌کنندگان اصلی در این زمینه بودم. اما با گذشت زمان، به‌ویژه بعد از مدیرعامل شدن ساتیا در سال ۲۰۱۴، به‌مرور متوجه شدیم که رویکردمان اشتباه بوده است. در سال ۲۰۱۶ «زامارین» (Xamarin)، استارت‌آپ پشتیبان جامعه منبع‌باز را خریدیم. «نت فریدمن» (Nat Friedman)، مدیرعامل این شرکت، به مایکروسافت پیوست و دیدگاه بیرونی مهمی را به مجموعه رهبری شرکت اضافه کرد.

این تحولات به جایی رسید که تا سال ۲۰۱۸ مایکروسافت در محصولاتش از بیش از ۱٫۴ میلیون مؤلفه منبع‌باز استفاده می‌کرد، در بسیاری از این پروژه‌ها و سایر پروژه‌های منبع‌باز مشارکت می‌کرد و حتی بسیاری از فناوری‌های زیربنایی خودش را منبع‌باز کرد. برای آنکه ببینید چقدر متحول شده‌ایم، خوب است اشاره کنم که مایکروسافت به فعال‌ترین مشارکت‌کننده منبع‌باز در گیت‌هاب تبدیل شده است. گیت‌هاب خانه توسعه‌دهندگان نرم‌افزار سراسر دنیا و به‌ویژه جامعه منبع‌باز است. در ماه می تصمیم گرفتیم گیت‌هاب را با مبلغ ۷٫۵ میلیارد دلار خریداری کنیم.

تصمیم گرفتیم «نت» این کسب‌وکار را رهبری کند و هنگام کار روی قرارداد به این نتیجه رسیدیم که باید با گروه‌های کلیدی منبع‌باز متحد شویم و برعکس کار یک دهه پیش‌مان را انجام دهیم. می‌خواستیم از پتنت‌هایمان استفاده کنیم تا از توسعه‌دهندگان منبع‌بازی دفاع کنیم که لینوکس و سایر مؤلفه‌های منبع‌باز کلیدی را ساخته بودند. وقتی با ساتیا، بیل گیتس و بعد سایر اعضای هیئت‌مدیره مایکروسافت در این مورد صحبت می‌کردم، گفتم وقت آن رسیده که تصمیمی دشوار بگیریم. تا آن زمان اشتباه کرده بودیم و همه به این جمع‌بندی رسیده بودیم که وقتش رسیده که مسیرمان را عوض کنیم و کاملاً به رویکرد منبع‌باز متعهد شویم.

وقتی به توصیف ترونل از فضاهای داده مشترک گوش می‌دادم، این درس‌ها را به یاد می‌آوردم. این چالش‌ها پیچیده بودند، ولی مانند بسیاری از چالش‌هایی بودند که جامعه منبع‌باز بر آنها غلبه کرده بود. استفاده بیش از پیش ما از نرم‌افزارهای منبع‌باز

در مایکروسافت باعث شده بود چالش‌های فنی، سازمانی و قانونی دخیل در ایجاد آنها را کاملاً بررسی کنیم. همچنین به‌تازگی یکی از پروژه‌های پیشگام بخش فناوری را برای رسیدگی به چالش‌های حریم خصوصی و قانونی استفاده مشترک از داده‌ها ارائه داده بودیم.

اما مهم‌تر از چالش‌ها، مزایای بالقوه برنامه‌های ترونل بود. چه می‌شود اگر بتوانیم انقلاب داده بازی ایجاد کنیم که همان کاری را برای داده انجام دهد که کدهای منبع‌باز برای نرم‌افزار انجام داده بودند؟ و چه می‌شد اگر این رویکرد می‌توانست عملکردی بهتر از نهادی درون‌نگر داشته باشد که بزرگ‌ترین مجموعه داده انحصاری را دارد؟

این بحث جلسه‌ای را به یادم آورد که چند سال پیش در آن شرکت کرده بودم؛ جلسه‌ای که با غافلگیری به تمرکز بر تأثیر اشتراک‌گذاری داده‌ها بر دنیای واقعی منتهی شده بود.

در اوایل دسامبر ۲۰۱۶، یک ماه بعد از انتخابات ریاست‌جمهوری جلسه‌ای در دفتر واشنگتن دی‌سی مایکروسافت برگزار کردیم تا تأثیر فناوری را بر رقابت‌های ریاست‌جمهوری بررسی کنیم. دو حزب سیاسی و کمپین‌های مختلف از محصولات ما و فناوری شرکت‌های دیگر استفاده کرده بودند. دو گروه دموکرات و جمهوری‌خواه موافقت کرده بودند که جلسات جداگانه‌ای با ما داشته باشند تا در این مورد صحبت کنیم که چطور از فناوری استفاده کرده‌اند و چه درس‌هایی گرفته‌اند.

ابتدا با مشاوران تیم کمپین هیلاری کلینتون دیدار کردیم. در طول دوره کمپین سال ۲۰۱۶ غول داده‌های سیاسی کشور شناخته می‌شدند. واحد آنالیتیکس بزرگی ایجاد کرده بودند که زیربنای کار خود را موفقیت کمیته ملی حزب دموکرات و کمپین موفق باراک اوباما برای انتخاب دوباره در سال ۲۰۱۲ قرار داده بود.

کمپین کلینتون متخصصان فناوری مطرحی را جمع کرده بود که به عبارتی پیشرفته‌ترین راه‌حل‌های فناوری کمپین جهان را برای به‌کارگیری و بهبود مجموعه داده‌ای می‌ساختند که شاید بهترین مجموعه داده سیاسی کشور بود. آن‌طور که مشاوران فناوری و کمپین به ما گفتند، «رابی موک» (Robby Mook)، مدیر باهوش و خوش‌برخورد کمپین کلینتون بینش‌های واحد آنالیتیکس را مبنای اغلب

تصمیم‌گیری‌هایش قرار داده بود. طبق گزارش‌ها هنگام غروب آفتاب روز انتخابات در غرب آمریکا، تمام اعضای کمپین معتقد بودند که در این رقابت پیروز شده‌اند و این پیروزی فرضی را تا حد قابل توجهی مدیون توانمندی‌های آنالیتیکس کمپین می‌دانستند. تقریباً هنگام شام تیم آنالیتیکس از کامپیوترهایشان فاصله گرفتند تا شاهد تشویق ایستاده کارکنان قدردان کمپین باشند.

یک ماه بعد، آن تشویق اولیه جای خود را به سکوت بخش آنالیتیکس کمپین شکست‌خورده کلینتون داد. تیم کمپین به این دلیل هدف انتقادات علنی قرار گرفته بود که در مورد ایالت میشیگان تا یک هفته قبل از انتخابات و در مورد ایالت ویسکانسین تا شب شمارش آرا متوجه تغییر شرایط به نفع نامزد جمهوری‌خواه نشده بود. اما همچنان اطمینان زیادی به توانمندی کمپین در حوزه داده وجود داشت. در اواخر جلسه از تیم دموکرات حاضر سؤالی ساده پرسیدم: «معتقدید به‌دلیل عملکرد بد در حوزه داده یا با وجود عملکرد خوب در این حوزه شکست خوردید؟»

خیلی سریع و با اعتمادبه‌نفس بالا واکنش نشان دادند؛ «بدون تردید عملکردمان در بخش داده بهتر از رقیب بود، اما با وجود این عملکرد برتر شکست خوردیم.»

بعد از خروج تیم دموکرات استراحتی کردیم و بعد تیمی از جمهوری‌خواهان برجسته برای تبادل نظر به ما پیوستند.

آن‌طور که آنها مسیر کمپین را توصیف کردند، اتفاقات غافلگیرکننده‌ای که به نامزدی دونالد ترامپ منجر شده بود، تأثیر تعیین‌کننده‌ای بر استراتژی داده کمپین او گذاشته بود. کمی بعد از انتخاب مجدد باراک اوباما در سال ۲۰۱۲، «راینس پریبس» (Reince Priebus) برای دوره دوم به‌عنوان رئیس کمیته ملی حزب جمهوری‌خواه انتخاب شده بود. بعد از شکست سال ۲۰۱۲، پریبس به همراه «مایک شیلدز» (Mike Shields)، رئیس ستادش، ارزیابی همه‌جانبه‌ای از فعالیت‌های کمیته ملی حزب جمهوری‌خواه و از جمله استراتژی فناوری این کمیته انجام داد. این ارزیابی به اتفاقی منجر شد که در دنیای پرشتاب فناوری زیاد رخ می‌دهد؛ فرصتی برای پیش افتادن سریع از رقیب پدید آمد.

پریبس و شیلدز از مدل‌های داده سه شرکت مشاوره فناوری جمهوری‌خواه استفاده

کردند و آنها را در داخل کمیته ملی حزب جمهوری‌خواه پیاده‌سازی کردند. هرچند دسترسی آسانی به افراد بااستعداد متمایل به حزب دموکرات در سیلیکون‌ولی نداشتند، اما مدیر ارشد فناوری جدیدی را از دانشگاه میشیگان و متخصص فناوری جوانی را از اداره حمل‌ونقل ویرجینیا جذب کردند تا الگوریتم‌های جدیدی را برای دنیای سیاست بنویسند. این دو رهبر کمیته ملی حزب جمهوری‌خواه باور داشتند (و ثابت کردند) که همه‌جا استعدادهای برتر در حوزه علوم داده وجود دارد.

در آن صبح مهم‌ترین نکته برای استراتژیست‌های فناوری جمهوری‌خواه کاری بود که بعد از آن پریبس و تیمش انجام دادند. در ایجاد مدل اشتراک‌گذاری داده‌ای موفق شدند که نه‌تنها نامزدهای جمهوری‌خواه سراسر کشور؛ بلکه طیفی از کمیته‌های اقدام سیاسی و سایر سازمان‌های محافظه‌کار را متقاعد کنند که اطلاعات‌شان را با یک مجموعه داده زیربنایی بزرگ و فدرالی به اشتراک بگذارند. شیلدز معتقد بود باید تا حد ممکن بیشترین داده‌ها را از بیشترین منابع ممکن جمع‌آوری کرد. یکی از دلایلش برای این کار این بود که کمیته ملی حزب جمهوری‌خواه نمی‌دانست نامزد نهایی جمهوری‌خواهان برای ریاست‌جمهوری چه کسی خواهد بود. تا وقتی این نامزد مشخص نشده بود، نمی‌توانستند بدانند آن نامزد چه نوع مسائل یا رأی‌دهندگانی را مهم‌تر می‌داند. بنابراین تیم کمیته ملی حزب جمهوری‌خواه تلاش کرد با بیشترین سازمان‌ها ارتباط برقرار کرده و متنوع‌ترین داده‌های ممکن را جمع‌آوری کند. در نتیجه مجموعه داده کلی این کمیته بسیار غنی‌تر از داده‌های کمیته ملی حزب دموکرات یا کمپین کلینتون بود.

وقتی در بهار ۲۰۱۶ دونالد ترامپ به‌عنوان نامزد جمهوری‌خواهان انتخاب شد، تشکیلات او زیرساخت فناوری عمیقی مانند کمپین کلینتون نداشت. برای جبران این کمبود، «جرد کوشنر»، داماد ترامپ، با «برد پارسکیل» (Brad Parscale)، رئیس بخش دیجیتال کمپین، روی استراتژی دیجیتالی‌ای کار کردند که به جای ایجاد مجموعه داده جدید اختصاصی، با اتکا بر داشته‌های کمیته ملی حزب جمهوری‌خواه تدوین شد. کمیته ملی حزب جمهوری‌خواه، بر اساس داده‌ها، گروهی شامل ۱۴ میلیون جمهوری‌خواه را شناسایی کرده بودند که گفته بودند به دونالد ترامپ علاقه‌ای ندارند.

تیم ترامپ برای تبدیل‌کردن این افراد بدبین به حامی، پروژه «آلامو» (Alamo) را در زادگاه پارسکیل یعنی سن آنتونیو (San Antonio) اجرا کردند تا جمع‌آوری کمک‌های مالی، پیام‌رسانی و هدف‌گیری را به‌ویژه در فیس‌بوک یکپارچه کنند. مدام به این رأی‌دهندگان پیام‌هایی را در مورد مباحثی می‌فرستادند که داده‌ها نشان می‌دادند احتمالاً برای آنها مهم است. از جمله این مباحث می‌توان به شیوع اعتیاد به مواد مخدر و قانون مراقبت مقرون‌به‌صرفه اشاره کرد.

تیم جمهوری‌خواه حاضر در آن جلسه توضیح داد که عملیات داده‌ای آنها در آستانه انتخابات چه موضوعی را آشکار کرد. ۱۰ روز پیش از انتخابات برآورد می‌کردند که در ایالات حساس و کلیدی دو واحد درصد از کلینتون عقب هستند. اما هفت درصد از جمعیت را شناسایی کرده بودند که هنوز در مورد رأی دادن یا ندادن تصمیم نگرفته بودند و کمپین نیز آدرس ایمیل ۷۰۰ هزار نفر از افرادی را داشت که تیم معتقد بود اگر به پای صندوق‌های رأی بروند، احتمالاً به ترامپ رأی خواهند داد. بنابراین تمام انرژی‌شان را صرف متقاعد کردن این گروه به حضور در پای صندوق‌های رأی کردند.

از تیم جمهوری‌خواه پرسیدیم از تجربه‌شان چه درس‌هایی را در زمینه فناوری گرفته‌اند. چند درس را بیان کردند؛ اینکه به اندازه تیم کلینتون در ایجاد تشکیلات داده از صفر عمیق نشوید، در عوض از یکی از پلتفرم‌های فناوری تجاری مهم استفاده کنید و بر بهره‌برداری از آن تمرکز کنید. مانند کمیته حزب جمهوری‌خواه اکوسیستم فدرالی گسترده‌تری ایجاد کنید که بیشترین شرکای ممکن را دور هم جمع می‌کند تا داده‌هایشان را به اشتراک بگذارند. از این رویکرد برای تمرکز منابع بر قابلیت‌های متمایزی مثل قابلیت‌های توسعه‌یافته توسط پارسکیل استفاده کنید که می‌توانند روی پلتفرمی تجاری اجرا شوند. علاوه بر این هیچ‌وقت فرض نکنید الگوریتم‌هایتان آن‌قدر که باور دارید، خوب هستند و پیوسته آنها را آزمایش و اصلاح کنید.

در انتهای جلسه همان پرسشی را پرسیدم که از دموکرات‌ها پرسیده بودم؛ «آیا به این دلیل پیروز شدید که بخش داده شما بهترین عملکرد را داشت یا با وجود اینکه عملکرد بخش داده کمپین کلینتون بهتر بود، برنده شدید؟»

آنها هم به همان سرعت دموکرات‌ها پاسخ دادند؛ «بدون تردید عملکردمان در بخش

داده بهتر بود. پیش از کمپین کلینتون متوجه شدیم که در میشیگان ترامپ در حال جلو افتادن از کلینتون است و مسئله‌ای را فهمیدیم که تیم کلینتون اصلاً متوجه آن نشد. روزهای آخر هفته قبل از انتخابات متوجه شدیم که ترامپ در ویسکانسین جلو افتاده است.»

بعد از خروج هر دو تیم سیاسی از تیم مایکروسافت خواستم با بالا بردن دست‌شان نشان دهند که چه کسانی فکر می‌کنند عملکرد بخش داده تیم کلینتون بهتر بوده و چه کسانی فکر می‌کنند عملکرد بخش داده تیم کمیته ملی حزب جمهوری‌خواه و ترامپ بهتر بوده است. گروه هم‌نظر بودند. همه افراد حاضر به این نتیجه رسیده بودند که رویکرد مورد استفاده راینس پریبس و کمپین ترامپ بهتر بوده است؛ کمپین کلینتون به برتری فنی و پیش‌افتادنش در نظرسنجی‌های اولیه اتکا کرده بود. در مقابل کمپین ترامپ از سر ناچاری بر رویکردی شبیه رویکرد داده مشترک متیو ترونل اتکا کرده بود.

همچنان فضای زیادی برای بحث در مورد عوامل گوناگون تأثیرگذار بر نتیجه رقابت‌های ریاست‌جمهوری سال ۲۰۱۶ به‌ویژه در ایالت‌های حساس و نزدیک مثل میشیگان، ویسکانسین و پنسیلوانیا باقی خواهد ماند، ولی آن روز به این جمع‌بندی رسیدیم که به احتمال زیاد مدل داده راینس پریبس و کمیته ملی حزب جمهوری‌خواه به تغییر مسیر تاریخ آمریکا کمک کرده است.

اگر رویکردی بازتر به داده می‌تواند چنین اتفاقی را رقم بزند، تصور کنید که چه کارهای دیگری را نیز می‌تواند انجام بدهد.

مسئله کلیدی در این نوع همکاری‌های فناوری‌محور نه‌فقط تمرکز بر فناوری؛ بلکه ارزش‌های انسانی و فرایندهاست. سازمان‌ها باید تصمیم بگیرند که آیا می‌خواهند داده‌ها را به اشتراک بگذارند یا خیر و اگر می‌خواهند چطور و بر مبنای چه شرایطی این کار را انجام می‌دهند. چند اصل بسیار مهم خواهند بود.

اصل اول وجود تمهیدات ملموس برای حفاظت از حریم خصوصی است. با توجه به سیر تکامل نگرانی‌ها نسبت به حریم خصوصی، این اصل پیش‌نیازی برای این است که هم سازمان‌ها بتوانند اطلاعات مربوط به افراد را به اشتراک بگذارند و هم افراد

بدون نگرانی داده‌های مربوط به خودشان را به اشتراک بگذارند. یکی از چالش‌های کلیدی، توسعه و انتخاب روش‌هایی برای اشتراک‌گذاری داده‌ها همراه با حفاظت از حریم خصوصی است. در این راستا احتمالاً باید از شیوه‌های جدید به‌اصطلاح «حریم خصوصی تفاضلی» استفاده کرد که با روش‌های جدیدی از حریم خصوصی حفاظت می‌کنند و همچنین دسترسی به داده‌های تجمیعی یا ناشناس‌شده را فراهم می‌کنند یا دسترسی صرفاً پرسمانی را به مجموعه‌های داده امکان‌پذیر می‌کنند. همچنین ممکن است شامل استفاده از سیستم یادگیری ماشینی شود که با داده‌های رمزنگاری‌شده آموزش دیده است. ممکن است شاهد ظهور مدل‌های جدیدی باشیم که به افراد امکان تصمیم‌گیری در مورد به اشتراک گذاشتن داده‌هایشان برای این نوع هدف را می‌دهد.

دومین اصل حیاتی شامل امنیت می‌شود. واضح است که اگر داده‌ها فدرالی شوند و در دسترس بیش از یک سازمان باشند، بُعد جدیدی به چالش‌های امنیت سایبری سال‌های اخیر اضافه خواهد شد. هرچند تداوم پیشرفت‌های امنیتی ضروری است، اما در عین حال به بهبودهایی در امنیت عملیاتی نیاز داریم که به سازمان‌های مختلف امکان مدیریت مشترک امنیت را می‌دهند.

همچنین برای پاسخگویی به پرسش‌های اساسی مربوط به مالکیت داده به تمهیدات عملی نیاز داریم. باید به گروه‌ها این امکان را بدهیم که داده‌ها را بدون از دست دادن مالکیت و کنترل ادامه‌دارشان به اشتراک بگذارند. همان‌طور که زمین‌داران گاهی بر اساس توافق‌نامه‌ها یا تمهیدات دیگری، بدون از دست دادن حقوق مالکیت‌شان به دیگران اجازه می‌دهند وارد ملک‌شان شوند، ما هم باید رویکردهای جدید مشابهی را به مدیریت دسترسی به داده ایجاد کنیم. این رویکردها باید به گروه‌ها این امکان را بدهند که با همکاری شرایط اشتراک‌گذاری داده‌ها، نحوه استفاده از داده‌ها را انتخاب کنند.

جنبش داده باز می‌تواند در پرداختن به این مسائل روندهای منبع‌باز در حوزه نرم‌افزار را سرمشق قرار دهد. در ابتدا مسائلی در مورد حقوق مجوزها سد راه جنبش منبع‌باز شدند، اما با گذشت زمان مجوزهای منبع‌باز استاندارد ظهور کردند. در نتیجه می‌توانیم در مورد داده هم منتظر تلاش‌های مشابهی باشیم.

سیاست‌های دولتی هم می‌توانند به پیشبرد جنبش داده باز کمک کنند. دولت‌ها در شروع می‌توانند داده‌های دولتی بیشتری را برای استفاده عمومی در دسترس قرار دهند و در نتیجه کسری داده سازمان‌های کوچک‌تر را کاهش دهند. یک نمونه خوب در این زمینه تصمیم کنگره ایالات متحده در سال ۲۰۱۴ برای تصویب قانون پاسخگویی و شفافیت دیجیتال (Digital Accountability and Transparency Act) بود که اطلاعات بودجه‌ای بیشتری را به‌صورت استاندارد در دسترس عموم قرار می‌دهد. دولت اوباما در سال ۲۰۱۶ با اتکا بر این قانون، خواستار داده‌های باز برای هوش مصنوعی شد و دولت ترامپ نیز با پیشنهاد استراتژی داده فدرال یکپارچه به‌منظور «استفاده از داده به‌عنوان دارایی استراتژیک» برای سازمان‌های دولتی همین مسیر را در پیش گرفت. بریتانیا و اتحادیه اروپا نیز تلاش‌های مشابهی را دنبال می‌کنند، اما در حال حاضر از هر پنج مجموعه داده فقط یکی باز است. بنابراین کارهای بسیار بیشتری باید انجام شود.

داده باز مسائل مهمی را برای سیر تکامل قوانین حریم خصوصی ایجاد می‌کند. بیشتر قوانین موجود پیش از شتاب‌گرفتن تحولات هوش مصنوعی تدوین شده‌اند و ناسازگاری‌هایی بین قوانین موجود و داده باز وجود دارد که درخور توجه جدی هستند. برای مثال قوانین حریم خصوصی اروپا بر به‌اصطلاح محدودیت‌های هدفی متمرکز هستند که استفاده از اطلاعات را فقط به هدفی محدود می‌کنند که در زمان جمع‌آوری داده‌ها مشخص شده‌اند. اما در موارد زیادی فرصت‌های جدیدی برای به اشتراک گذاشتن داده‌ها ظهور می‌کنند که باعث پیشبرد اهداف اجتماعی مثل درمان سرطان می‌شوند. خوشبختانه این قوانین امکان استفاده از داده‌ها برای اهداف دیگر در شرایط منصفانه و سازگار با هدف اولیه را فراهم می‌کند. حال پرسش‌های مهمی در مورد نحوه تفسیر این شرایط به وجود می‌آید.

همچنین مسائل مهمی حول مالکیت معنوی، به‌ویژه در فضای کپی‌رایت وجود خواهد داشت. از دیرباز پذیرفته شده که همه می‌توانند از آثار تحت کپی‌رایت، برای مثال با مطالعه کتاب، آموزش ببینند. اما اکنون برخی افراد این پرسش را مطرح می‌کنند که آیا این قانون باید شامل یادگیری با ماشین‌ها هم شود یا خیر. اگر می‌خواهیم استفاده گسترده‌تر از داده‌ها را ترویج کنیم، باید ماشین‌ها هم بتوانند از

این توانایی بهره ببرند.

بعد از توسعه تمهیدات عملی برای صاحبان داده‌ها و رسیدگی به سیاست‌های دولتی، به امر دیگری نیاز خواهد بود. این امر توسعه پلتفرم‌ها و ابزارهای فناوری به‌منظور فراهم‌کردن امکان اشتراک‌گذاری آسان‌تر و کم‌هزینه‌تر داده‌هاست.

این مقوله یکی از نیازهای ترونل در هاچ بود. ترونل به تفاوت تلاش‌های جامعه تحقیقات سرطان و شرکت‌های فناوری توجه کرده بود. بخش فناوری در حال توسعه ابزارهای جدید و بسیار پیشرفته برای مدیریت، تلفیق و تحلیل مجموعه‌های داده متنوع است، اما همان‌طور که ترونل تشخیص داده بود؛ «فاصله بین تولیدکنندگان داده و سازندگان ابزارهای بدیع باعث از دست رفتن فرصتی بزرگ برای رسیدن به یافته‌های تأثیرگذار، تحول‌آفرین (و احتمالاً نجات‌بخش زندگی) می‌شود که با استفاده از مقدار عظیم داده‌های علمی، آموزشی و کارآزمایی بالینی تولیدی هر روز به دست می‌آیند.»

اما برای موفقیت در این راه کاربران داده‌ها به پلتفرم فناوری قدرتمند و بهینه‌شده‌ای برای استفاده در مورد داده باز نیاز دارند. در این زمینه شاهد تلاش‌هایی در بازار هستیم. شرکت‌های فناوری گوناگون در بررسی مدل‌های کسب‌وکاری متفاوت، می‌توانند گزینه‌های متنوعی را انتخاب کنند. برخی ممکن است تصمیم بگیرند داده‌ها را جمع‌آوری و در پلتفرم خودشان یکپارچه کنند و دسترسی به بینش‌هایشان را به‌صورت خدمات فناوری یا مشاوره ارائه کنند. این رویکرد تا حد زیادی همان کاری است که IBM در مورد سیستم هوش مصنوعی واتسون (Watson) و فیس‌بوک و گوگل در دنیای تبلیغات آنلاین انجام داده‌اند.

همزمان با آن شب در ماه آگوست که به صحبت‌های متیو ترونل گوش می‌دادم، تیمی از مایکروسافت؛ یعنی سَپ (SAP) و ادوبی در حال کار روی پروژه متفاوت، اما مکملی بودند. این سه شرکت طرح داده باز (Open Data Initiative) را مطرح کردند که یک ماه بعد آغاز شد. این طرح پلتفرم فناوری و ابزارهایی را فراهم می‌کند که به سازمان‌ها امکان فدرالی‌کردن داده‌ها و در عین حال حفظ مالکیت و کنترل داده‌های اشتراک‌گذاری‌شده را می‌دهد. این طرح شامل ابزارهای فناوری‌ای می‌شود که سازمان‌ها

می‌توانند با استفاده از آنها داده‌های مفید متعلق به خودشان را شناسایی و ارزیابی کنند و آنها را به فرمت ساختاریافته، قابل خواندن برای ماشین و مناسب برای اشتراک‌گذاری تبدیل کنند.

شاید انقلاب داده باز برای رسیدن به رویکرد مناسب، به اندازه هر چیز دیگری به آزمایش نیاز داشته باشد. پیش از پایان میهمانی شام کنار ترونل نشستم و پرسیدم چه کارهایی می‌توانیم با هم انجام دهیم. به‌طور ویژه در مورد فرصت پیشبرد فعالیت‌هایی کنجکاو بودم که همان زمان به همراه مؤسسات تحقیقات سرطان دیگری در پیرامون‌مان در آمریکای شمالی انجام می‌دادیم؛ از جمله همکاری‌هایی که با سازمان‌های پیشگامی در شهر ونکوور استان بریتیش کلمبیا داشتیم.

این تلاش‌ها ماه دسامبر به ثمر نشستند و اعلام کردیم مایکروسافت چهار میلیون دلار به پشتیبانی از پروژه هاچ اختصاص می‌دهد. این طرح که به‌صورت رسمی طرح «کاوش داده کاسکادیا» (Cascadia Data Discovery Initiative) خوانده می‌شود، قرار است به شناخت و تسهیل اشتراک‌گذاری داده با روش‌های حفاظت از حریم خصوصی بین مرکز هاچ، دانشگاه واشنگتن و دانشگاه بریتیش کلمبیا و سازمان سرطان بریتیش کلمبیا (BC Cancer Agency)، هر دو مستقر در ونکوور، کمک کند. این طرح یکی از نمونه‌های اولیه روندی در حال گسترش است؛ روندی که از جمله شامل تعاونی داده کالیفرنیا (California Data Collaborative) می‌شود که در آن شهرها، ارائه‌دهندگان خدمات آب‌وفاضلاب و سازمان‌های برنامه‌ریزی زمین داده‌ها را فدرالی می‌کنند تا بتوان با راه‌حل‌های مبتنی بر آنالیتیکس به کم‌آبی‌ها رسیدگی کرد.

این اتفاقات دلیلی برای خوش‌بینی به آینده داده باز فراهم می‌کنند؛ البته اگر فرصت را غنیمت بشماریم. هرچند برخی فناوری‌ها به برخی شرکت‌ها و کشورها منافعی بیشتر از دیگران می‌رسانند، اما همیشه هم این‌گونه نیست. برای مثال هیچ‌وقت رهبری جهانی در زمینه برق وجود نداشته و کشورها مجبور نبودند با مسائل دشوار ناشی از آن دست‌وپنجه نرم کنند. هر کشوری می‌توانست از این اختراع استفاده کند و مسئله این بود که کدام کشورها دوراندیشی لازم برای به‌کارگیری آن به گسترده‌ترین شکل ممکن را داشتند.

هدف ما به‌عنوان جامعه باید این باشد که استفاده مؤثر از داده را به اندازه برق در دسترس قرار دهیم. البته کار آسانی نیست، اما با رویکرد درست به‌اشتراک‌گذاری داده و پشتیبانی مناسب دولت‌ها، جهان کاملاً قادر خواهد بود مدلی ایجاد کند که اطمینان حاصل می‌کند داده به قلمرو چند شرکت و کشور بزرگ تبدیل نمی‌شود؛ بلکه می‌تواند به چیزی تبدیل شود که جهان به آن نیاز دارد؛ موتور پیشران مهمی که محرک دور جدیدی از رشد اقتصادی در تمام جهان می‌شود.

فصل شانزدهم

جمع‌بندی

مدیریت فناوری بزرگ‌تر از خودمان

وقتی «آنه تیلـور» (Anne Taylor) نوجوان بود و در مدرسـه نابینایان کنتاکی تحصیل می‌کرد، ایده‌ای را دنبال کرد که بعداً به شـکوفایی رسـید و به کارش تبدیل شد. آنه کمک می‌کند محصولات‌مان بیشتر در دسـترس افراد کم‌توان قرار بگیرد. اما وقتی در این مورد حرف می‌زند که در زمان فراغتش چه کار می‌کند، شور و اشتیاق بیشتری در چهره‌اش نمایان می‌شود. می‌گوید: «من هکر هستم.»

در سـال ۲۰۱۶ آنه دومین هکری بود که برای پروژه توسـعه اپلیکیشـنی جذب شد که از هوش مصنوعی، بینایی کامپیوتر و دوربین تلفن هوشمند استفاده می‌کند. یکی از کارهایش این بود که به همراه تلفنی که به پیشانی‌اش بسته شده بود، در محوطه ساختمان مرکزی مایکروسافت قدم بزند تا این اپلیکیشن را آزمایش کند. زندگی مخترعان گاهی اوقات به درد افراد حساس به پوشش و مد نمی‌خورد، اما در مایکروسافت تقریباً هر نوع پوشش و مدی را مشاهده می‌کنید.

کار این تیم به پیشـرفتی شگرف منجر شـد؛ اپلیکیشـنی متکی به هوش مصنوعی که به افراد نابینا کمک می‌کند دنیا را طبق توصیف تلفن هوشمندشان ببینند. اکنون آنه که خودش نابیناست، می‌تواند با هوش مصنوعی بینا (Seeing AI) نوشته‌ای دست‌نویس از خانواده‌اش را بدون کمک دیگران بخواند. می‌گوید: «این توانایی احتمالاً برای شـما ساده به نظر می‌رسد؛ زیرا خیلی وقت اسـت که می‌توانید این کار را انجام دهید، اما وقتی فردی چیزی برایم می‌نویسد که ماهیت شخصی یا خصوصی دارد، همیشه مجبورم از فرد دیگری بخواهم آن را برایم بخواند. حالا دیگر مجبور نیستم. این اتفاق خیلی مهم است.»

تشـخیص متن فقط در خوانـدن نامه‌های امـروزی اهمیت ندارد. در نیوجرسـی هوش مصنوعی، پژوهش «مارینا راسـتو» (Marina Rustow)، اسـتاد مطالعـات خاور نزدیک در آزمایشـگاه «گنیزا»ی دانشـگاه پرینسـتون را دگرگـون کرده اسـت. این پژوهشـگر در این آزمایشگاه گنجینه عظیمی شامل ۴۰۰ هزار سـند از معبد بن عزرای مصر را تفسیر و رمزگشایی می‌کند. این گنجینه بزرگ‌ترین منبع ثبت‌شده متون یهودی است.

مطالعه این اسناد چالشـی وحشـت‌آفرین است. بسـیاری از آنها چندتکه شـده و در کتابخانه‌هـا و موزه‌هـای سراسـر جهان پخـش شـده‌اند. حجم عظیـم و مکان ایـن متون، یکپارچه‌کردن آنها را تقریباً غیرممکن می‌کند. تیم راستو با هوش مصنوعی توانسته است

با جست‌وجو در نسخه‌های دیجیتال و پیدا کردن تکه‌های گمشده نگهداری شده در هزاران مایل آن طرف‌تر تصویر ناقص قبلی در مورد نحوه هم‌زیستی یهودیان و مسلمانان در قرون وسطی را کامل کند.

وقتی یک الگوریتم هوش مصنوعی می‌تواند به راستو کمک کند گذشته دور را حفظ کند، برای حفاظت از تاریخ زنده جهان چه کاری می‌تواند انجام دهد؟

در آفریقا شکار غیرقانونی مسئله‌ای همیشگی است که گونه‌های در خطر انقراض، از جمله برخی از شاخص‌ترین و شناخته‌شده‌ترین حیوانات را در معرض تهدید نابودی قرار می‌دهد. تیم هوش مصنوعی برای زمین (AI for Earth) مایکروسافت با پژوهشگران دانشگاه کارنگی ملون همکاری می‌کند تا به محیط‌بانان اداره حیات‌وحش اوگاندا کمک کند که همیشه یک گام از شکارچیان جلوتر باشند. اپلیکیشن دستیار حفاظت برای امنیت حیات‌وحش (Protection Assistant for Wildlife Security) با استفاده از الگوریتمی، داده‌های ۱۴ سال از گشت‌زنی پارک‌های ملی را بررسی می‌کند و از نظریه الگوریتمی بازی‌ها استفاده می‌کند تا رفتار شکارچیان غیرقانونی را یاد بگیرد و پیش‌بینی کند و از این طریق به مسئولان این توانایی را بدهد که گشت‌هایشان را بر اساس شناسایی قبلی کانون‌های شکار غیرقانونی تنظیم کنند.

همان‌طور که این نمونه‌ها به ما نشان می‌دهند، قدرت فناوری می‌تواند به نابینایان در دیدن دنیا با روش‌های جدید، به تاریخ‌نگاران در کاوش گذشته و به دانشمندان در دنبال‌کردن استراتژی‌های جدید برای این سیاره بیمار کمک کند. دامنه فرصت‌های بالقوه فناوری تقریباً نامحدود است.

هوش مصنوعی شبیه اختراعات منحصربه‌فرد گذشته مثل خودرو، تلفن یا حتی کامپیوتر شخصی نیست. بیشتر شبیه برق رفتار می‌کند؛ یعنی به ابزارها و دستگاه‌هایی قدرت می‌دهد که تقریباً در همه ابعاد جامعه و زندگی ما حضور فعال دارند. هوش مصنوعی مانند برق در پشت صحنه حضور دارد و در بسیاری موارد اصلاً فراموش می‌شود تا اینکه روزی قطع شود.

ساتیا برای این واقعیت جدید عنوان «تشدید فناوری» را انتخاب کرده؛ عبارتی که

آکندگی فناوری در دنیای پیرامون ما را توصیف می‌کند. این عصر جدید فرصتی برای شرکت‌ها، سازمان‌ها و حتی کشورهاست تا نه‌تنها با به‌کارگیری فناوری؛ بلکه با ساخت فناوری خودشان به رشدشان شتاب ببخشند. در نتیجه برای سازمان‌ها ضروری است که کارمندان‌شان را با مهارت‌ها و توانمندی‌های جدیدی تجهیز کنند که برای بهره‌برداری از این فناوری مورد نیاز است.

این دوران فرصت‌های بسیار بزرگ و در عین حال چالش‌های جدیدی به همراه دارد. فناوری‌های دیجیتال همزمان به ابزار و سلاح تبدیل شده‌اند؛ پدیده‌ای که سخنان آلبرت اینشتین در سال ۱۹۳۲ را به یادمان می‌آورد؛ اینکه مزیت‌های عصر ماشین را به افراد یادآوری می‌کرد، اما در عین حال از انسان‌ها می‌خواست اطمینان حاصل کنند که توسعه سازمان‌دهی قدرت، همگام با پیشرفت‌های فنی این عصر پیش می‌رود. در عین حال که تلاش می‌کنیم فناوری بیشتری را به دنیای انسان‌ها اضافه کنیم، باید تلاش کنیم انسانیت بیشتری را هم به فناوری اضافه کنیم.

همان‌طور که در این فصل‌ها توضیح دادیم، امروزه فناوری اثرگذاری اقتصادی بسیار نابرابری دارد، برای برخی پیشرفت و ثروت بسیار زیادی ایجاد می‌کند، اما با از بین بردن شغل‌ها و ناکامی در ورود به جوامعی که به اینترنت پرسرعت دسترسی ندارند، دیگران را به حال خودشان رها می‌کند. فناوری در حال تغییر چهره جنگ و صلح و ایجاد میدان نبرد جدید در فضای سایبری و تهدیدات تازه برای دموکراسی از طریق حمله و دروغ‌پراکنی تحت حمایت دولت‌هاست. همچنین در حال افزایش دوقطبی‌سازی جوامع داخلی، از بین بردن حریم خصوصی و ارائه توانایی نوظهوری به رژیم‌های استبدادی برای اعمال نظارت بی‌سابقه بر شهروندان‌شان است. با استمرار پیشرفت هوش مصنوعی همه این تحولات با سرعت بیشتری به پیش می‌روند.

شاهد تأثیرگذاری این شرایط در مسائل سیاسی این دوران هستیم. افراد درباره مهاجرت، تجارت و نرخ‌های مالیات برای افراد و شرکت‌های ثروتمند بحث می‌کنند، اما به‌ندرت می‌بینیم که سیاست‌مداران نقش فناوری در ایجاد این چالش‌ها را در نظر بگیرند یا بخش فناوری به این نقش اذعان کند. انگار آن‌قدر در نشانه‌های بیماری غرق شده‌ایم که زمان و انرژی لازم برای تمرکز روی دلایل ریشه‌ای مهم را نداریم. به‌ویژه با استمرار افزایش

تأثیرگذاری فناوری با ریسک گسترش درکی کوته‌بینانه مواجهیم.

اینکه انتظار داشته باشیم سرعت تغییرات مبتنی بر فناوری کاهش یابد، واقع‌بینانه نیست، اما انتظار نابجایی نیست که بخواهیم برای مدیریت این تغییرات تلاش بیشتری انجام شود. فناوری دیجیتال بر خلاف عصرهای فناوری و ابداعات قبلی مثل راه‌آهن، تلفن، خودرو و تلویزیون، چند دهه با مقدار بسیار کمی رگولیشن یا حتی رگولیشن خود پیشرفت کرده است. وقت آن رسیده که بپذیریم این نگرش عدم مداخله باید جای خود را به رویکرد فعالانه‌تری بدهد که قاطعانه‌تر به چالش‌های در حال تکامل می‌پردازد.

منظور از رویکرد فعالانه‌تر این نیست که همه مسائل به دولت‌ها و رگولیشن واگذار شود. چنین رویکردی همان‌قدر کوته‌بینانه و ناموفق خواهد بود که از دولت‌ها بخواهیم هیچ کاری نکنند. برعکس تلاش در این زمینه باید با شرکت‌ها و تشریک مساعی بیشتر در بخش فناوری آغاز شود.

وقتی دو دهه پیش مایکروسافت تحت فشار بود، متوجه شدیم که باید تغییر کنیم. از نبردهایمان در آن سال‌ها سه درس گرفتم که همچنان از آنها یاد می‌گیریم و آنها را به کار می‌بندیم. با نگاه به نقش کنونی فناوری در جهان، به نظر می‌رسد امروز این درس‌ها همان‌قدر برای بخش فناوری مناسب هستند که در گذشته برای شرکت ما مناسب بودند.

درس اول این بود که باید انتظارات بیشتر دولت، صنعت، مشتریان و به‌طور کلی جامعه از خودمان را می‌پذیرفتیم. فرقی نمی‌کرد در قانون آمده بود یا خیر، در هر صورت باید مسئولیت بیشتری می‌پذیرفتیم. دیگر شرکتی کوچک نبودیم. باید تلاش می‌کردیم الگو باشیم، نه اینکه استدلال کنیم می‌توانیم هر کاری بخواهیم انجام دهیم.

دوم اینکه باید بیشتر به حرف‌های افراد گوش می‌دادیم و برای کمک به حل مشکلات فناوری‌محوری که باید حل می‌شدند، بیشتر تلاش می‌کردیم. این اقدام با برقراری روابط کاری سازنده‌تر با افراد بیشتر شروع شد، اما این فقط شروع کار بود. باید نگاه افراد دیگر به ما و نگرانی‌هایشان نسبت به خودمان را بهتر درک می‌کردیم. باید در حل مسائل کوچک عملکرد بهتری می‌داشتیم تا اجازه ندهیم از کنترل خارج شوند. در این راستا باید بیشتر با دولت‌ها و رقبایمان جلسه برگزار می‌کردیم تا به تفاهم برسیم. می‌دانستیم که بدون شک با پرسش‌های دشواری مواجه می‌شویم و باید شهامت لازم برای مصالحه و سازش

را داشته باشیم.

در مواردی برخی مهندسان استدلال می‌کردند که نباید سازش کنیم و باید به مبارزه ادامه بدهیم. گاهی اوقات فکر می‌کردم شهامت من را زیر سؤال می‌برند. هرچند مواردی بودند که باید بر موضع‌مان می‌ایستادیم، موارد زیاد دیگری هم بودند که استدلال می‌کردم سازش بیشتر از تداوم مبارزه، به شجاعت نیاز دارد. به ثبات قدم هم نیاز داشتیم. تلاش برای رسیدن به تفاهم اغلب به مذاکراتی منجر می‌شد که با بن‌بست و شکست تمام می‌شدند، اما مجدداً دور هم جمع می‌شدیم و به توافق می‌رسیدیم. باید توانایی حفظ وقار و متانت در زمان شکست را در خود پرورش می‌دادیم و حتی وقتی به نتیجه‌ای نمی‌رسیدیم، طرف دیگر را تحسین می‌کردیم تا وقتی فرصت مناسب از راه می‌رسید، توانایی حل مشکلات سخت را حفظ کرده باشیم. این فرصت‌های مناسب تقریباً همیشه پیش می‌آمدند.

درس آخر اینکه باید رویکرد اصولی‌تری را تدوین می‌کردیم. باید فرهنگ کارآفرینی را حفظ می‌کردیم و در عین حال آن را با اصولی تلفیق می‌کردیم که می‌توانستیم در داخل و خارج از شرکت در موردشان حرف بزنیم. ابتدا در مورد مسائل ضدانحصار و بعد در مورد مسائل قابلیت تعامل و حقوق بشر، پرورش توانایی تدوین چنین اصولی را شروع کردیم. همان‌طور که ساتیا در سال ۲۰۱۵ در مورد مسائل نظارت الکترونیکی پیشنهاد داده بود که در فصل دوم به آن پرداختیم، برای هدایت تصمیم‌گیری‌هایمان در این مورد نیز اصولی را تدوین کردیم. تعهدات ابری حاصل، همچنان الگوی ما در سایر بخش‌ها هستند. این رویکرد علاوه بر مزایای فراوان دیگر به ما کمک کرده و وادارمان می‌کند که به مسئولیت‌هایمان و بهترین راه برای عمل کردن به آنها فکر کنیم.

این رویکردها نشان‌دهنده نیاز به تغییر فرهنگی در بخش فناوری هستند. شرکت‌های فناوری از گذشته به دلایل درست فراوان ابتدا بر توسعه محصول یا خدمتی هیجان‌انگیز و بعد بر جذب بیشترین کاربر ممکن با بیشترین سرعت ممکن تمرکز کرده‌اند. همان‌طور که رید هافمن با عبارت مقیاس‌پذیری برق‌آسا به‌درستی ترسیم می‌کند، «مسیر پرشتابی» که سرعت را به بهره‌وری ترجیح می‌دهد، بهترین رویکرد برای توسعه فناوری رهبر بازار در سطح جهانی است. حتی وقتی شرکت‌ها به این نوع جایگاه رهبری می‌رسند، نیاز به حرکت سریع همچنان باقی می‌ماند. می‌توان به‌راحتی تصور کرد که وقتی الزامات پردردسر باعث

می‌شوند نوآوری با تهدید کاهش سرعت روبه‌رو شود، چه نگرانی‌هایی در سیلیکون‌ولی به وجود می‌آید.

این نگرانی‌ها مهم‌اند، اما با توجه به نقشی که اکنون فناوری در جهان ایفا می‌کند، اینکه یک شرکت فناوری سریع‌تر از تفکر پیش برود یا اینکه اصلاً به پیامدهای گسترده‌تر خدمات یا محصولاتش فکر نکند، بسیار خطرناک است. یکی از تزهای این کتاب این است که شرکت‌ها هم می‌توانند موفق شوند؛ البته در صورتی که برای عمل به مسئولیت‌های اجتماعی‌شان بیشتر تلاش کنند. همان‌طور که ساتیا هنگام طرح چنین مسائلی به سرعت اشاره می‌کند، باید سریع اما همراه با در نظر گرفتن «گاردریل‌هایی» برای فناوری‌مان پیش برویم. توانایی پیش‌بینی مسائل و تعریف رویکرد اصولی برای برطرف‌کردن آنها تا حد زیادی اجازه نمی‌دهد با افزایش سرعت از مسیر درست خارج شویم. این توانایی کمک می‌کند دست‌کم از برخی جنجال‌های عمومی و آسیب‌های بالقوه آنها به شهرت و اعتبار شرکت جلوگیری کنیم؛ آسیب‌هایی که می‌توانند مدیران ارشد را مجبور کنند وقت بیشتری را برای مسائلی به‌جز توسعه محصول و رشد کاربر صرف کنند.

اما حتی با وجود بهترین نیت‌ها نیز این نوع تلاش‌ها به‌راحتی پذیرفته نمی‌شوند. طبیعی‌ترین مسیر این است که محصول را تا سرحد ممکن گسترش دهیم و به هر کسی که می‌خرد، بفروشیم. ایجاد محدودیت برای خود، همیشه مخالفانی در داخل شرکت دارد (طبق تجربه این حرف را می‌زنم). در نتیجه تعهد یک شرکت به کنترل رفتار خود نیازمند رهبری در سطح بالاست. رهبران ارشد باید با نگاه فراگیرتری بیندیشند و افرادشان را تشویق کنند که فقط به‌دنبال پیدا کردن مسئله برای هر راه‌حل بالقوه نباشند؛ بلکه به پیدا کردن راه‌حل برای هر مسئله بالقوه کمک کنند.

برای رسیدن به بخشی از راه‌حل شرکت‌های فناوری باید توانمندی‌های بیشتری را در بخش‌هایی به‌جز بخش‌های متعارف توسعه، بازاریابی و فروش محصول پرورش دهند. در تلاقی فناوری با مسائل جهان واقعی، هیچ جایگزینی برای رهبران قدرتمند در بخش‌های فایننس، حقوقی و منابع انسانی وجود ندارد. در گذشته بخش فناوری این نقش‌ها را بیشتر برای جذب سرمایه، فروش شرکت یا عرضه اولیه سهام مهم می‌دانست، اما مسائل و نیازهای امروز بسیار گسترده‌ترند.

یکی از دلایل اهمیت این بخش‌ها این است که تعریف اصول اساسی حاکم بر مسیر یک محصول آسان نیست؛ بلکه نیازمند تفکر حساب‌شده و درک غنی از انتظارات مردم، سناریوهای واقعی و نیازهای توسعه عملی است که همه به تعامل نزدیک با تیم‌های مهندسی و فروش بستگی دارند. در طول هفته‌ای عادی در مایکروسافت گاهی می‌بینیم که «دو اشتالکاف»، رئیس اداره حقوقی شرکت، بخشی از وقتش را با افراد برای کار روی پروژه‌هایی صرف می‌کند که می‌خواهند اتفاقات بعدی را پیش‌بینی کنند تا از مشکلات و جنجال‌های آتی جلو باشند.

چالش دیگر این است که با پذیرش اصول جدید کار تمام نمی‌شود. همان‌طور که تیم ارزیابی داخلی خودمان به ایمی هود و من توصیه کرد، حیاتی بود که شناسایی مسائل اخلاقی هوش مصنوعی (بحث فصل یازدهم) را با تعریف اصول جدید و همچنین تعیین سیاست‌های ملموس، ساختار حکمرانی، چارچوب پاسخگویی و آموزش کارمندان ادامه دهیم تا این تعهد اخلاقی را کارا و مؤثر کنیم. این موضوع توجه ما را به یکی از بزرگ‌ترین آزمایش‌های پیش روی شرکت‌های فناوری بزرگ و ریشه‌داری جلب می‌کند که به صدها میلیون مشتری در سراسر جهان خدمات ارائه می‌دهند. همان‌طور که تلاش تیم‌های مهندسی ما برای پیاده‌سازی مقررات عمومی حفاظت از داده اروپا در فصل هشتم نشان داد، اصول باید در مقیاس جهانی عملیاتی و پیاده‌سازی شود. این نوع تلاش‌ها نیازمند پشتیبانی گسترده همه بخش‌های گوناگونی است که در اداره یک شرکت جهانی امروزی مشارکت دارند.

در نهایت رهبری آگاهانه و با نگاه فراگیر باید به گام‌های کنشگرایانه‌تر در شرکت‌های فناوری و همچنین تشریک مساعی بیشتر در کلیت بخش فناوری تبدیل شود. در زمینه روابط تجاری و تلاش‌های داوطلبانه، بخش فناوری اغلب پراکنده‌تر و حتی متفرق‌تر از بسیاری از صنایع دیگر عمل می‌کند. با توجه به ماهیت متنوع فناوری و مدل‌های کسب‌وکاری رقیب، در مجموع این مسئله خیلی غافلگیرکننده نیست، اما با وجود تفاوت‌های همیشگی، باز هم امکان همکاری بیشتر در بخش فناوری وجود دارد.

این نیاز به‌ویژه زمانی برجسته‌تر می‌شود که با اولویت‌هایی مثل تقویت امنیت سایبری و مقابله با دروغ‌پراکنی سروکار داریم. در سال‌های اخیر طرح‌های مهمی وجود داشته‌اند،

برای مثال واکنش به باج‌افزار واناکرای که در فصل چهارم تشریح شد و منشور اعتماد زیمنس و پیمان امنیت سایبری شرکت‌های فناوری که در فصل هفتم تشریح شدند، اما این طرح‌ها در مقایسه با آنچه ممکن است و آنچه مردم و دولت‌ها بیش از پیش انتظار دارند، کار چندانی انجام نداده‌اند.

در این زمینه هم به تغییر فرهنگی نیاز داریم. امروزه زیاد اتفاق می‌افتد که حتی شرکت‌های فناوری پیشگام نیز به مسئله‌ای مثل امنیت سایبری نگاه کنند و نتیجه بگیرند که نیازی نیست در این مورد همکاری نزدیکی با بقیه صنعت داشته باشند یا تصمیم بگیرند به جریانی نپیوندند؛ مگر اینکه خودشان رهبری آن را بر عهده داشته باشند یا تصمیم بگیرند بخشی از جریانی نخواهند بود که شامل شرکت فناوری دیگری است که در آن زمان آماج انتقادات سیاسی است؛ زیرا می‌ترسند با قرار گرفتن در کنار شرکتی که با انتقاد عمومی مواجه شده، «آلوده» شوند. هرچند این نگرانی‌ها تا حدودی قابل درک هستند، اما رهبران فناوری باید در برابر آنها مقاومت کنند. این دیدگاه‌ها در مجموع عمل به مسئولیت‌های مورد انتظار جهان از بخش فناوری را دشوارتر می‌کنند.

هرچند فرصت بسیار زیادی برای شرکت‌ها و بخش فناوری وجود دارد که در کنار هم کار بیشتری انجام دهند، اما این شرایط دولت‌ها را از مسئولیت‌شان برای تلاش بیشتر در این زمینه مبرا می‌کند. بخش فناوری مملو از افراد خوب و متفکر است، ولی در سه قرنی که از آغاز انقلاب صنعتی گذشته، هرگز مشاهده نشده صنعتی بزرگ بتواند با موفقیت همه مسائل مربوط به خودش را به‌تنهایی رگوله کند. ساده‌انگارانه خواهد بود اگر فکر کنیم اکنون شاهد اولین مورد موفق خواهیم بود.

حتی اگر ممکن باشد، باز هم باید بپرسیم آیا بهترین مسیر پیش رو همین است. مسائل گسترده مربوط به فناوری تقریباً روی همه جنبه‌های اقتصادها، جامعه‌ها و زندگی شخصی ما تأثیر می‌گذارند. یکی از گرانمایه‌ترین ارزش‌ها در حکومت‌های دموکراسی جهان این است که مردم مسیر جامعه را با انتخاب افرادی تعیین می‌کنند که قوانین حاکم بر ما را وضع می‌کنند. ممکن است رهبران فناوری را هیئت‌مدیره‌هایی انتخاب کرده باشند که از سوی سهام‌داران انتخاب شده‌اند، اما مردم آنها را انتخاب نکرده‌اند. کشورهای دموکراتیک نباید آینده را به رهبرانی واگذار کنند که مردم انتخاب نکرده‌اند.

در نتیجه دولت‌ها باید رویکرد فعالانه‌تر و قاطعانه‌تری را به رگوله‌کردن فناوری دیجیتال برگزینند. این مورد نیز مانند همه بحث‌های مطرح‌شده در این کتاب، در حرف آسان‌تر از عمل است. اما درس‌های مهمی وجود دارند که به‌کارگیری آنها ارزشمند خواهد بود؛ یکی اینکه توجیه مستدلی وجود دارد که دولت‌ها باید درست به سبک نوآوری‌های بخش فناوری دست به نوآوری در حوزه رگولاتوری بزنند. دولت‌ها می‌توانند به جای انتظار و انفعال تا به تکامل رسیدن هر مسئله‌ای، سریع‌تر و تدریجی‌تر و با گام‌های رگولاتوری اولیه محدودتر، دست به کار شوند و بعد تجربه حاصله را بررسی کنند و یاد بگیرند. به عبارت دیگر مفهوم «کمینه محصول پذیرفتنی» را در نظر بگیرید و به نوع رویکردی فکر کنید که در مورد هوش مصنوعی و تشخیص چهره از آن پشتیبانی کردیم و در فصل دوازدهم تشریح شد. بی‌درنگ متوجه شدیم که اولین گام رگولاتوری، درست مانند اولین گام در توسعه هر محصول تجاری یا نرم‌افزاری جدیدی، آخرین گام نیست، اما باور داشتیم هوشمندانه‌تر است اگر دولت‌ها مجموعه‌ای از گام‌های محدودتر را با سرعت بیشتری بردارند.

آیا این رویکرد می‌تواند برای رگولیشن فناوری در برخی حوزه‌ها نتیجه‌بخش باشد؟ اگر این‌طور باشد، می‌تواند به ابزار رگولاتوری جدیدی برای عصر حاضر تبدیل شود. اگر دولت‌ها بتوانند قوانین محدود وضع کنند، از تجربه‌شان یاد بگیرند و بعد به همان شکلی که شرکت‌ها قابلیت‌های جدید را به محصولات اضافه می‌کنند، از این یادگیری برای اضافه‌کردن شرایط رگولاتوری جدید استفاده کنند، قوانین در مسیر پرشتاب‌تری قرار می‌گیرند. البته مسئولان همچنان باید از نظرها و پیشنهادهای فراگیر استفاده کنند، باملاحظه باقی بمانند و مطمئن باشند که دست‌کم برای مجموعه محدودی از مسائل پاسخ درست را دارند. اما دولت‌ها می‌توانند با اضافه‌کردن برخی هنجارهای فرهنگی پرورش‌یافته در بخش فناوری با رگولیشن فناوری آسان‌تر، آن هم با سرعت تغییر فناوری همگام شوند.

دولت‌ها همچنین می‌توانند تأثیر مثبت‌تر و عملی‌تری داشته باشند؛ به شرط اینکه روندهای در حال تغییر فناوری را بررسی کنند و به‌دنبال فرصت‌هایی برای ترویج راه‌حل‌های بازار گسترده‌تر باشند. مبنای رویکرد ما به اینترنت پرسرعت، همان‌طور که در فصل نهم تشریح شد، همین نگاه است. منطقی‌تر است که منابع دولتی به جای آنکه صرف سرمایه‌گذاری‌های عمومی گران در کابل‌های فیبر نوری پرهزینه‌ای شود که دهه‌ها

طول می‌کشد تا به خانه‌های روستایی برسند، صرف تقویت فناوری‌های بی‌سیم جدید از روش‌هایی شود که به نیروهای بازار شتاب می‌بخشند تا بتوانند به نقطه آمادگی برای اجرا برسند و بعد روی پای خودشان مسیر را ادامه دهند.

دولت‌ها بیش از همیشه برای تقویت نیروهای بازار فناوری از طریق اقدامات‌شان فرصت دارند. معمولاً در میان بزرگ‌ترین خریداران فناوری قرار دارند و تصمیمات‌شان در مورد خرید و تدارکات، می‌تواند تأثیر زیادی بر روندهای کلی بازار داشته باشد. از این مهم‌تر دولت‌ها منابع داده بزرگ و ارزشمندی دارند و می‌توانند با در دسترس قرار دادن این داده‌ها با روش‌های مناسب و تعریف‌شده، تأثیری تعیین‌کننده بر بازارهای فناوری‌ای داشته باشند که از این داده‌ها استفاده می‌کنند. برای مثال می‌توانند به تقویت تلاش‌های آگاهانه‌تر بخش عمومی و شهری کمک کنند که برای مهارت‌های مورد نیاز در شغل‌های جدید افرادی را پیدا می‌کنند که جویای این شغل‌ها هستند (در فصل دهم به این موضوع پرداختیم). به‌علاوه این داده‌ها ابزار قدرتمندی فراهم می‌کنند که دولت‌ها می‌توانند با استفاده از آنها به افزایش سرعت پذیرش مدل‌های داده باز کمک کنند (در فصل پانزدهم به این موضوع پرداختیم).

مسئولان دولتی برای اتخاذ رویکرد فعالانه‌تر به رگولاتوری باید درک بیشتری از روندهای فناوری به دست آورند. برای رسیدن به این هدف باید گفت‌وگوی بیشتری بین سازندگان فناوری و رگولاتورهای آن شکل بگیرد. در این زمینه هم چالش‌های زیادی وجود دارد. در گذشته هرگز کسب‌وکاری ملی یا مرکز فناوری وجود نداشته که به اندازه سیلیکون‌ولی از واشنگتن فاصله داشته باشد. البته فاصله واقعی پایتخت‌های سیاسی و فناوری آمریکا از این فاصله ظاهری هم بیشتر است. همان‌طور که «مارگارت اُمارا» (Margaret O'Mara)، تاریخ‌نگاری در دانشگاه واشنگتن می‌گوید: «بخش فناوری با فعالیت در فاصله‌ای زیاد از قدرت سیاسی و مالی، در گوشه‌ای دلپذیر و آرام از شمال کالیفرنیا جزیره‌ای کارآفرینی ایجاد کرده که خانه گونه جدیدی از شرکت‌ها، انواع متمایزی از فرهنگ شرکتی و پذیرش مقداری خلق‌وخوی عجیب شده است.»

فاصله فیزیکی تقریباً ۲۵۰۰ مایلی واشنگتن دی‌سی و سیلیکون‌ولی وجه مشترک این دو مکان را پنهان می‌کند. با سفر به هر کدام از این نقاط از محلی مثل سیاتل (که آن هم

به‌خوبی پذیرای عجیب‌وغریب بودن است)، می‌توانید با توجه به شور و هیجان و فعالیت هر کدام از این مناطق درک کنید چرا وقتی در این مکان‌ها هستید، به‌راحتی احساس می‌کنید که در مرکز جهان قرار دارید. اما اکنون بیش از هر زمانی به ایجاد پلی مستحکم‌تر در فاصله این دو مکان نیاز داریم.

یکی از چالش‌ها این است که بسیاری از افراد از دیرباز در محافل فناوری ادعا کرده‌اند که در دولت، افراد فناوری را به اندازه کافی نمی‌فهمند تا رگولیشن مناسبی بر آن وضع کنند. این سخنان در شرایطی است که شرکت‌های فناوری از همه انواع تأمین مالی و پشتیبانی دولتی بهره برده‌اند. در این میان رسانه‌ها کمک فراوانی به تقویت این دیدگاه می‌کنند. وقتی قانون‌گذاری پرسش اشتباهی را از مدیر ارشدی در حوزه فناوری می‌پرسد، یا حتی پرسش درستی را به‌صورت اشتباه می‌پرسد، رسانه‌ها به‌سرعت این اشتباه را بزرگ می‌کنند. اما با توجه به تجربیاتم می‌توانم بگویم از آن صبح ۱۵ سال پیش که در مورد تبلیغات دیجیتال با یکی از سناتورهای آمریکایی صحبت می‌کردم و او نمی‌دانست می‌تواند واشنگتن‌پست را آنلاین بخواند، مسئولان دولتی پیشرفت زیادی کرده‌اند.

با سابقه کار بیش از یک‌چهارم قرن در بخش فناوری، می‌فهمم که محصولات این بخش پیچیده‌اند، اما هواپیماهای تجاری، خودروها، آسمان‌خراش‌ها، داروها و حتی محصولات غذایی هم پیچیده‌اند. هیچ‌کس با جدیت پیشنهاد نمی‌دهد که اداره هوانوردی فدرال نباید هواپیماها را رگوله کند؛ زیرا پیچیده‌تر از میزان درک افراد حاضر در دولت هستند. افرادی که از هواپیما استفاده می‌کنند، چنین پیشنهادی را نمی‌پذیرد. چرا فناوری اطلاعات باید اساساً متفاوت باشد، به‌ویژه با توجه به اینکه اکنون بسیاری از قطعات هواپیما به این فناوری وابسته‌اند؟

واقعیت این است که سازمان‌های دولتی از گذشته ثابت کرده‌اند که در پرورش توانایی واقعی برای درک محصولاتی که رگوله می‌کنند، مهارت دارند. منظور این نیست که این فرایند عاری از ناکامی است یا همه عملکرد خوب یکسانی دارند. منظور این هم نیست که همه رویکردهای رگولاتوری با منطق یا حتی عقل سلیم سازگارند، اما بخش فناوری باید این توهم را کنار بگذارد که فقط خودش می‌تواند فناوری اطلاعات و ریزه‌کاری‌هایش را درک کند و در عوض در به اشتراک گذاشتن اطلاعات مربوط به این ریزه‌کاری‌ها بیشتر تلاش کند تا

مردم و دولت‌ها، آنها را بهتر درک کنند.

چالش دوم برای دولت‌ها از بسیاری جهات خیلی برجسته‌تر است. فناوری اطلاعات و شرکت‌های سازنده آن جهانی شده‌اند. اینترنت از ابتدا برای تبدیل‌شدن به شبکه‌ای جهانی طراحی شد و بسیاری از مزیت‌هایش از ماهیت مرتبط آن ناشی می‌شود. شاید تأثیرگذاری و نفوذ جغرافیایی آن بیشتر از هر فناوری دیگری در تاریخ، ورای هر دولت واحدی باشد. این وضعیت، اینترنت را از اختراعات گذشته مثل تلفن، تلویزیون و برق متمایز می‌کند. این اختراعات مبتنی بر شبکه‌هایی هستند که معمولاً درون مرزهای ملی یا ایالتی قرار می‌گیرند.

یکی از راه‌ها برای درک این چالش در نظر گرفتن فناوری‌ای است که شاید از لحاظ اثرگذاری رگولاتوری بیشترین شباهت را به فناوری دیجیتال داشت. هرچه بیشتر از قرن نوزدهم گذشت، نقش راه‌آهن در بازتعریف ایالات متحده از هر اختراع دیگری بیشتر شد. وقتی راه‌آهن از مرزهای ایالتی عبور کرد، دولت‌های ایالتی بیشترین قدرت را در رگوله‌کردن اقتصاد بر عهده داشتند. در دهه‌های بعد از جنگ داخلی آمریکا، شرکت‌های راه‌آهن کشور از بسیاری جنبه‌ها بزرگ‌تر و قدرتمندتر از بسیاری از دولت‌های ایالتی شدند.

در دهه ۱۸۸۰ اوضاع بحرانی شد. به‌جز دوران جنگ هیچ سابقه دیگری از رگوله‌کردن اقتصاد در سطح فدرال وجود نداشت و در واشنگتن دی‌سی پیشنهادها برای رگوله‌کردن راه‌آهن مدام شکست می‌خوردند. دولت‌های ایالتی با تصویب قوانینی برای رگوله‌کردن نرخ‌های راه‌آهن واکنش نشان دادند که روی سفرها، فراتر از مرزهای این ایالت‌ها تأثیر می‌گذاشتند. دیوان عالی در سال ۱۸۸۶ این قوانین را لغو کرد و حکم داد که این قدرت فقط در اختیار دولت فدرال است. ناگهان مردم با واقعیتی ناخوشایند مواجه شدند؛ «ایالت‌ها نمی‌توانستند و دولت فدرال نمی‌خواست راه‌آهن را رگوله کند». این شرایط سیاسی جدید بن‌بست را شکست و سال بعد کنگره کمیسیون تجارت میان‌ایالتی (Interstate Commerce Commission) را ایجاد کرد تا راه‌آهن را رگوله کند. این‌گونه بود که دولت فدرال مدرن متولد شد.

نفوذ جهانی فناوری اطلاعات معاصر مشابه راه‌آهن در دهه ۱۸۸۰ است که مدام ورای مرزهای حوزه‌های استحفاظی پیشرفت می‌کرد. اما امروزه نظیری جهانی برای کمیسیون

تجارت میان‌ایالتی وجود ندارد. در عین حال قابل درک است که هیچ تمایلی هم برای ایجاد آن وجود نداشته باشد.

دولت‌ها چطور می‌توانند فناوری‌ای را رگوله کنند که از خودشان بزرگ‌تر است؟ شاید این مسئله بزرگ‌ترین معمای پیش روی آینده رگولاتوری فناوری باشد. اما همین که سؤال را می‌پرسید، بخشی از پاسخ خودنمایی می‌کند؛ دولت‌ها باید با یکدیگر همکاری کنند.

در این زمینه موانع زیادی وجود دارد که باید بر آنها غلبه کنیم. در دورانی زندگی می‌کنیم که بادهای پرتلاطم مخالف ژئوپلیتیک باعث شده بسیاری از دولت‌ها ملی‌گراتر شوند. وقتی تیترهای خبری پربازدید روز به خارج‌شدن کشورها از توافقات همکاری تجاری یا پیمان‌های پرسابقه مربوط می‌شوند، خیلی نمی‌توان انتظار داشت که در همکاری کشورها شاهد پیشرفت شگرفی باشیم. علاوه بر این در دورانی قرار داریم که بسیاری از دولت‌ها حتی در تصمیم‌گیری در مورد مسائلی که فقط برای خودشان مهم است نیز با مشکل مواجه‌اند.

اما در بحبوحه این فشارها حرکت بی‌وقفه فناوری، همکاری بین‌المللی بیشتر را اجتناب‌ناپذیر می‌کند. همان‌طور که این کتاب نشان می‌دهد، مسائلی مثل اصلاحات در نظارت الکترونیکی، حفظ حریم خصوصی و تمهیدات حفاظت از امنیت سایبری، دولت‌ها را وادار کرده که با روش‌های جدیدی با یکدیگر تعامل کنند. یکی از دلایلی که بسیاری از طرح‌های ما در مایکروسافت بر پشتیبانی از عناصر مورد نیاز برای پیشرفت بین‌المللی متمرکز بوده، همین موضوع است. از ابتدای سال ۲۰۱۶ این طرح‌ها شامل واکنش هماهنگ به واناکرای، پیمان امنیت سایبری شرکت‌های فناوری، فراخوان‌های چندذی‌نفعی پاریس و کرایست‌چرچ، سپر حریم خصوصی ایالات متحده و اتحادیه اروپا، مجوز قانون کلاود برای توافق‌نامه‌های بین‌المللی و چشم‌اندازی بلندمدت برای کنوانسیون دیجیتال ژنو بوده‌اند. در همین سال‌ها شاهد افزایش حفاظت از حریم خصوصی در ایالات متحده و اروپا و ظهور بحث جهانی جدیدی در مورد هوش مصنوعی و اخلاقیات بوده‌ایم. وقتی در دوران افزایش ملی‌گرایی این نوع پیشرفت‌ها امکان‌پذیر است، می‌توان امیدوار بود که با بازگشت میانه‌روی به صحنه بین‌الملل، شاهد پیشرفت‌های بیشتری باشیم.

همچنان باید تشکیل ائتلاف‌های طرفین علاقه‌مند را ادامه دهیم. شش دولت و دو شرکت در کنار هم قرار گرفتند تا به مسئله واناکرای واکنش نشان بدهند. در ابتدای کار،

گروهی متشکل از ۳۴ شرکت، پیمان شرکت‌های فناوری را امضا کردند و گروه اولیه‌ای متشکل از ۵۱ دولت بخشی از پشتیبانی چندذی‌نفعی از فراخوان پاریس بودند. در همه این موارد طرفینی که مهم و حتی حیاتی بودند، مشارکت نداشتند. اما پیشرفت نه با متمرکز شدن بر طرفین غایب؛ بلکه با توجه به متقاعد کردن دیگران به حضور حاصل شد. این رویکرد نیز به حرکت ادامه‌دار و گسترش بیشتر در ادامه منجر شد.

همچنین باید بپذیریم که برخی مسائل به اجماع جهانی منجر می‌شوند و برخی دیگر نمی‌شوند. بسیاری از مسائل کنونی فناوری شامل بحث‌های مربوط به حریم خصوصی، آزادی بیان و حقوق بشر می‌شوند که از پشتیبانی جهانی برخوردار نیستند. ائتلاف طرفین علاقه‌مند، به احتمال زیاد مستلزم کنار هم قرار گرفتن کشورهای دموکراتیک جهان است که گروه کوچکی نیستند. در حال حاضر تقریباً ۷۵ کشور دموکراتیک با جمعیتی در حدود چهار میلیارد نفر وجود دارد. یعنی اکنون افراد بیشتری از هر زمانی در تاریخ، در جوامع دموکراتیک زندگی می‌کنند. اما در سال‌های اخیر سلامت حکومت‌های دموکراسی جهان افت کرده است. شاید سلامت بلندمدت این جوامع، بیشتر از هر نوع جامعه دیگری به همکاری‌های جدید برای مدیریت فناوری و آثارش وابسته باشد.

در نتیجه بسیار مهم است که این حرکت‌ها حتماً تا روزی ادامه داشته باشند که دولت ایالات متحده با پشتیبانی از این نوع طرح‌های چندجانبه و پذیرش رهبری آنها دوباره نقش دیپلماتیک دیرینش را بر عهده بگیرد. تردیدی نیست که وقتی ایالات متحده در کنار سایر حکومت‌هایی که دموکراسی در آنها برقرار است قرار نمی‌گیرد، آنها ضعیف‌ترند.

علاوه بر این برای استمرار پیشرفت، دولت‌ها باید بپذیرند که علاوه بر فناوری، خودشان را نیز باید رگوله کنند. مسائلی مثل امنیت سایبری و دروغ‌پراکنی به جنگ‌های آینده و حفاظت از فرایندهای دموکراتیک ما شکل خواهند داد. همان‌طور که هیچ صنعتی در تاریخ به‌تنهایی موفق به رگولیشن خود نشده، هیچ موردی هم وجود ندارد که کشوری صرفاً با اتکا به بخش خصوصی یا حتی با رگوله‌کردن آن از خودش محافظت کرده باشد. دولت‌ها باید همراه با هم اقدام کنند. یکی از کارهایی که در این راستا باید انجام شود، ایجاد هنجارها و قوانین بین‌المللی جدیدی است که رفتار ملی را محدود و کشورها را در برابر نقض این قوانین پاسخگو می‌کنند.

این کار در نهایت به شـکل‌گیری بحث‌های جدیدی در مورد مزایـای قوانین بین‌المللی منجر خواهد شد. از همین حالا می‌توان حدس زد که افرادی ابراز نگرانی می‌کنند که برخی کشورها از این قوانین پیروی خواهند کرد، اما سایر کشورها پیروی نمی‌کنند. جهان اولین ممنوعیت‌ها و محدودیت‌ها برای کنترل تسلیحات را از نیمه دوم قرن نوزدهم وضع کرد، اما تا بیش از یک قرن بعد مشاجرات همواره حول همین نگرانی‌ها می‌چرخید. حقیقت تلخ این است که بعضی کشورها این توافقات را نقض می‌کنند، اما وقتی هنجار یا قانونی بین‌المللی وجود دارد، سایر کشورها راحت‌تر می‌توانند واکنش مؤثری نشان دهند.

مواجهه با چالش‌هـای جدید فناوری‌های دیجیتال، مسـتلزم همـکاری فعالانه‌تر ورای مرزهای نهادی مرسـوم اسـت. برای مثال این نوع همـکاری را در پروژه‌های موفق مدیریت آثار اجتماعی گسـترده فناوری می‌بینیم که دولت‌ها، گروه‌های غیرانتفاعی و شرکت‌ها را دور هم جمع می‌کند تا به مسئله شـغل و نیاز افراد به پرورش مهارت‌های جدید بپردازند (در فصل‌های دهم و سیزدهم به چنین نمونه‌هایی پرداختیم). این نوع ائتلاف‌ها همچنین می‌توانند در رسـیدگی به چالش‌های دیگر جامعه مثل مسکن ارزان‌قیمت مفید باشند. نمونه‌ای از این ائتلاف‌ها را در طرح‌های اخیر منطقه سیاتل دیدیم.

اما فرصت شـکل‌گیری انواع جدیـدی از ایـن همکاری‌ها و نیـاز به آنها، به این مسـائل اجتماعی محدود نمی‌شود. حفاظت از حقوق بنیادین بشر بیش از همیشه به گام‌هایی وابسته اسـت که دولت‌ها، سـازمان‌های غیردولتی و شـرکت‌ها باید با هم بردارند. هرچه داده بیشـتری به ابر منتقل شـود و دولت‌های بیشـتری خواسـتار ایجاد مراکز داده درون مرزهایشـان شـوند، این مسـئله مهم‌تر می‌شـود. پرداختن به مسـائل قرن بیست‌ویکم نیازمند طرح‌های چندجانبه و چندذی‌نفعی است.

یکی از نکات کلیدی در همکاری چندذی‌نفعی پذیرش نقش‌هایی است که هر گروه باید ایفا کند. مسئولان دولتی به‌عنوان افراد انتخاب‌شده از سوی مردم برای اتخاذ تصمیمات اجتماعی، نقش رهبری منحصربه‌فردی را، به‌ویژه در جوامع دموکراتیک ایفا می‌کنند. البته آنها فقط قدرت و مسئولیت ترسیم مسیر آموزش عمومی و تصویب و اعمال قوانین حاکم بر ما را دارند. شرکت‌ها و گروه‌های غیرانتفاعی می‌توانند روحیه شهروندی را با خود به همراه بیاورند و دولت‌ها را تکمیل و با آنها مشارکت کنند تا منابع، تخصص یا داده‌های بیشتری

را تأمین کنند که بخش عمومی اغلب به آن نیاز دارد. شرکت‌ها و سازمان‌های غیردولتی نیز می‌توانند ایده‌های جدید را آزمایش کنند و به‌ویژه در خارج از مرزها با سرعت بیشتری پیش بروند. همه باید نقش‌های یکدیگر را درک کنیم و به این نقش‌ها احترام بگذاریم.

علاوه بر این در مورد بسیاری از مسائل باید سازش و مصالحه کنیم. برای رهبران کسب‌وکاری که در ساختن برخی از ارزشمندترین شرکت‌های جهان نقش داشته‌اند، پذیرش این مسئله همیشه آسان نیست. این افراد معمولاً بر خلاف پیش‌بینی‌ها و با در پیش گرفتن روش خودشان، موفق شده‌اند. رگولیشن آزادی آنها را در آینده محدود می‌کند.

شاید به همین دلیل است که برخی رهبران فناوری در محافل عمومی استدلال می‌کنند و در محافل خصوصی با قاطعیت می‌گویند که بزرگ‌ترین ریسک نوآوری این است که دولت‌ها زیاده‌روی کنند و فناوری را بیش از حد رگوله کنند. این ریسک به‌وضوح وجود دارد، اما در حال حاضر با گرفتار شدن در این ورطه فاصله زیادی داریم. سیاست‌مداران و مسئولان خواستار رگولیشن شده‌اند، اما تاکنون بیش از آنکه عمل ببینیم، حرف شنیده‌ایم. برای بخش فناوری بهتر است که به جای دلواپسی افراطی در مورد خطرات رگولیشنِ بیش از حد، به این فکر کند که رگولیشن هوشمند چه ساختاری باید داشته باشد.

آخرین و مهم‌ترین مطلب این است که این مسائل بزرگ‌تر از هر فرد، شرکت، صنعت یا حتی خود فناوری هستند و شامل دو ارزش بنیادین آزادی‌های دموکراتیک و حقوق بشر می‌شوند. بخش فناوری با بهره‌برداری از این آزادی‌ها متولد شد و رشد کرد. به آیندگان مدیونیم که کمک کنیم این ارزش‌ها حتی مدت‌ها بعد از خروج ما و محصولات‌مان از صفحه روزگار همچنان حفظ شوند و شکوفا بمانند.

یک موضوع روشن است؛ بزرگ‌ترین ریسک این نیست که جهان برای حل این مسائل خیلی زیاد تلاش کند؛ بلکه این است که خیلی کم تلاش کند و بزرگ‌ترین ریسک این نیست که دولت‌ها خیلی سریع اقدام کنند؛ بلکه این است که خیلی کُند اقدام کنند.

سرعت نوآوری فناورانه کم نخواهد شد؛ بلکه سرعت تلاش‌ها برای مدیریت آن باید زیاد شود.

انتشارات
راه پرداخت

[دربارهٔ انتشارات راه پرداخت]

ما از دل فناوری آمده‌ایم.
از جهانی که هر روز دگرگون می‌شود.
می‌خواهیم این دگرگونی‌ها را بفهمیم و روایت کنیم.
راه پرداخت از دل راه‌کار زاده شد؛
از دل رسانه‌ای که سال‌ها روایت‌گر نوآوری و اقتصاد دیجیتال ایران بوده است.
در راه پرداخت، کتاب فقط یک محصول نیست.
رسانه‌ای است برای اندیشیدن، برای گفت‌وگو، برای ماندن.
ما بهترین کتاب‌های جهان در حوزه‌های فناوری، مالی، نوآوری و کسب‌وکار را جست‌وجو می‌کنیم.
می‌خوانیم، می‌سنجیم، برمی‌گردانیم به زبان فارسی؛
تا روایت جهانی دانش در زبان ما ادامه پیدا کند.
برای ما ترجمه یعنی گفت‌وگو؛
میان فرهنگ‌ها، میان نسل‌ها.
واژه‌ها را با وسواس می‌چینیم،
جمله‌ها را به‌دقت می‌تراشیم.
تا امروز بیش از صد کتاب منتشر کرده‌ایم.
اما هنوز آغاز راهیم.
به هزار کتاب فکر می‌کنیم.
به هزار پنجره که به روی آینده باز می‌شود.
ما با حمایت بخش خصوصی پیش می‌رویم؛
با کسانی که باور دارند نشر دانش، سرمایه‌ای ماندگار است.
راه پرداخت جایی است برای خواندن،
برای فهمیدن،
برای ساختن آینده.

ابزارها و سلاح‌ها

کتاب «ابزارها و سلاح‌ها» اثر «برد اسمیت»، مدیر ارشد شرکت مایکروسافت است که روایتی جذاب از کابین خلبان یکی از بزرگ‌ترین شرکت‌های فناوری حال حاضر دنیا؛ یعنی مایکروسافت ارائه می‌کند. اسمیت در این کتاب توضیح می‌دهد که چگونه فناوری، هم به ما قدرت می‌دهد و هم ما را تهدید می‌کند. او همچنین نقش و قدرت داده‌ها در جهان کنونی را به تصویر می‌کشد و گزارشی دقیق و هیجان‌انگیز از جنجال‌هایی ارائه می‌کند که دنیای فناوری در یک دهه گذشته با آن مواجه بوده است.

هیچ‌کس هیچ‌چیز مدنظر نیست

برای سفارش اینترنتی این کتاب به وبسایت
فروشگاه انتشارات راه پرداخت مراجعه کنید
way2pay.shop

انتشارات راه پرداخت

کتاب «ابزارها و سلاح‌ها» اثر «برد اسمیت»، مدیر ارشد شرکت مایکروسافت است که روایتی جذاب از کابین خلبان یکی از بزرگ‌ترین شرکت‌های فناوری حال حاضر دنیا؛ یعنی مایکروسافت ارائه می‌کند. اسمیت در این کتاب توضیح می‌دهد که چگونه فناوری، هم به ما قدرت می‌دهد و هم ما را تهدید می‌کند. او همچنین نقش و قدرت داده‌ها در جهان کنونی را به تصویر می‌کشد و گزارشی دقیق و هیجان‌انگیز از جنجال‌هایی ارائه می‌کند که دنیای فناوری در یک دهه گذشته با آن مواجه بوده است.

ISBN 978-622-97829-0-3

۸۴۵ هزار تومان

انتشارات راه پرداخت

ناشر فناوری و نوآوری

way2pay.press