Public Law Studies Quarterly, Vol. 51, No 3, Autumn 2021
DOI: 10.22059/jplsq.2019.272648.1893

Necessity of Cross-border Stored Data's Disclosure and Regime of Bilateral Legal Cooperation Treaties in Criminal Investigations

(Type of Paper: Research Article)

Javad Salehi*

Abstract
Microsoft Corporation has access to the emails of its users and their contents from the United States territory. However, this information is stored and held in a cross-border data center that is considered to be alien to the Microsoft Corporation and the territory where the center of its activity is located. Access of the United States is interference in internal affairs of the Irish government, which is location of the Microsoft data center. But location of the Microsoft and its ability to access it from the territory of the United States to the information stored by its users, even in cross-border is important and obtaining criminal jurisdiction for United States Courts. Whereas United States criminal law is effective and enforceable on the territory. Accordingly, the approach of the United States courts is not justifiable on the basis of territorial rules for access to cross-border stored data. The research question is, what is the mechanism of cybercriminal investigation in the cross-border data center and its challenges? Findings of the research show that approve of a treaty about legal cooperation in criminal investigations and adherence to its provisions are the only mechanism for access to the cross-border data center, whose implementation is facing serious challenges.

Keywords
Cross-border Criminal Investigation, Data Center, Microsoft Corporation, Territorial Criminal Jurisdiction, Bilateral Legal Cooperation Treaties.

* Associate Prof., University of Payame Noor, Tehran, Iran. Email: Javadsalehi@pnu.ac.ir
Received: April 7, 2019 - Accepted: June 24, 2019

فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۵۱، شمارهٔ ۳، پاییز ۱۴۰۰: ۱۱۸۳-۱۲۰۱
DOI: 10.22059/jplsq.2019.272648.1893

لزوم افشای دیتای ذخیره‌شدهٔ فراسرزمینی و رژیم معاهدات همکاری حقوقی دوجانبه در تحقیقات کیفری

(نوع مقاله: علمی _ پژوهشی)

جواد صالحی*

چکیده

شرکت مایکروسافت بر ایمیل کاربران خویش و محتویات آنها از سرزمین ایالات متحده دسترسی دارد. لیکن این اطلاعات در دیتاسنتر فراسرزمینی ذخیره و نگهداری می‌شوند که نسبت به شرکت مایکروسافت و سرزمین محل استقرار مرکز فعالیت آن عامل بیگانه تلقی می‌شوند. دسترسی ایالات متحده، مداخله در امور داخلی دولت ایرلند است که محل استقرار دیتاسنتر شرکت مایکروسافت است. لیکن محل فعالیت شرکت مایکروسافت و امکان دسترسی آن از قلمرو سرزمینی ایالات متحده به اطلاعات ذخیره‌شدهٔ کاربران خود، ولو در قلمرو فراسرزمینی برای محاکم ایالات متحده واجد اهمیت و موجد صلاحیت کیفری است. این در حالی است که قوانین کیفری ایالات متحده در قلمرو سرزمینی کارامد و قابل اجراست. بر این اساس رویکرد محاکم قضایی ایالات متحده به استناد قوانین سرزمینی برای دسترسی به دیتای ذخیره‌شدهٔ فراسرزمینی توجیه ندارد. پرسش پژوهش این است که سازوکار تحقیقات کیفری سایبری در دیتاسنتر فراسرزمینی و چالش‌های آن چیست؟ یافته‌های پژوهش نشان می‌دهد که انعقاد معاهدهٔ همکاری حقوقی در تحقیقات کیفری و پایبندی به مفاد آن، تنها سازوکار دسترسی به دیتاسنتر فراسرزمینی است که البته اجرای آن نیز با چالش‌هایی جدی مواجه است.

کلیدواژگان

تحقیقات کیفری فراسرزمینی، دیتاسنتر، شرکت مایکروسافت، صلاحیت کیفری سرزمینی، معاهدات همکاری حقوقی دوجانبه.

---

* دانشیار گروه حقوق دانشگاه پیام‌نور، تهران، ایران. Email: Javadsalehi@pnu.ac.ir

تاریخ دریافت: ۱۳۹۷/۱۰/۰۹ - تاریخ پذیرش: ۱۳۹۸/۰۴/۰۳

مقدمه

سایبر یا جامعهٔ اطلاعاتی، ابزاری در خدمت آزادی اطلاعات است تا اینکه مردم به‌واسطهٔ آن از حقوق و تکالیف متقابل آگاه شوند. فضای سایبر، مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و ابزارهای مخابراتی است. سایبر، شامل شبکه‌هایی است که از طریق اینترنت به‌هم وصل‌اند. تمام اطلاعات در خصوص روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها در این فضا به شکل دیجیتال در دسترسِ کاربران و قابل استفاده برای آنهاست (وطنی و اسدی، ۱۳۹۵: ۱۰۲). مبادلات دیجیتال، مجموعه‌ای از صفر و یک هستند که داده‌های الکترونیکی را تشکیل می‌دهند و تمامی مفاهیم را به شکل الکترونیک منعکس می‌کنند، بدون اینکه اثری از آن در تجهیزات الکترونیکی باقی بماند. اطلاعات دیجیتال، بخشی از واقعیت ناگزیر زندگی اجتماعی‌اند. لیکن تقابل آزادی اطلاعات و الزامات حریم خصوصی در سایبر موجب نگرانی است. از یک طرف، مطالبهٔ جامعهٔ آزاد برای دسترسی به تمام اطلاعات و از طرف دیگر، حق افراد به داشتن حریم خصوصی اطلاعاتی در فضای امن و به دور از مداخلهٔ دیگران وجود دارد. با وجود این توقف شتاب سریع تحولات فضای سایبر و اطلاعات دیجیتال متصور نیست، ولو اینکه بهای آن نقض الزامات حریم خصوصی باشد.

بهره‌گیری از فضای سایبر در تسریع گردش اطلاعات و بهبود روابط اجتماعی مؤثر است، لیکن به همین میزان در متحول شدن وقوع جرائم و نحوهٔ مبارزه با آن دارای کارکرد اساسی است. این وضعیت سبب دشواری‌هایی در کشف جرم و تحقیقات کیفری پلیس می‌شود. توانایی مجرمان برای فعالیت در فضای سایبر و دسترسی به اهداف بالقوه و بهره‌برداری از قربانیان احتمالی به مدد ارتباطات اینترنتی پرسرعت افزایش یافته است (Finklea, 2013: 5). جرائم با گمنامی مرتکب آن در محیط سایبر با قوت بیشتری به‌جای محیط حقیقی در حال وقوع هستند (بهره‌مند، ۱۳۹۶: ۵۶). استفاده از تلفن هوشمند و رایانه سبب شده است تا پلیس به‌جای بازرسی متعلقات فیزیکی، بیشتر متکی به بازرسی تجهیزات الکترونیکی تحت کنترل مظنون باشد. تفتیش و توقیف داده یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرف قانونی یا متصدیان سامانه‌ها در مادهٔ ۶۷۲ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، نمونه‌ای عینی از این نحوهٔ تحقیقات کیفری است. اما ظهور سرویس ابررایانش[1] این شیوه از کشف جرم و تعقیب آن را نیز ناکارامد کرده است. در چنین شرایطی بازرسی دستگاه رایانه یا گوشی تلفن همراه با هدف جمع‌آوری دلایل مجرمانه دیگر مؤثر نیست. ولو اینکه مسیر فعالیت کاربر در فضای مجازی از طریق شناسه و گذرواژه‌های به‌جامانده در حافظهٔ کوتاه‌مدت رایانه یا گوشی تلفن همراه همچنان برای مقام تحقیق قابل ردیابی باشد. پلیس می‌تواند در زمان انتقال

1. Cloud-Computing

اطلاعات از حافظهٔ رایانه یا گوشی تلفن همراه به فضای ابررایانش بدون مداخلهٔ فیزیکی در رایانه یا گوشی تلفن همراه مظنون به تحقیقات کیفری بپردازد، لیکن تحقیقات پلیس در صورتی کارامد است که برای دورهٔ زمانی طولانی صورت گیرد. بر این اساس بزهکار سایبری با بهره‌مندی پلیس از آموزه‌های جرم‌شناسی سایبری شناسایی می‌شود. لیکن کشف جرم و دامنهٔ تحقیقات کیفری پلیس در دسترسی به دیتای ذخیره‌شدهٔ کاربر در دیتاسنترهای فراسرزمینی با بن‌بست مواجه می‌شود، وقتی‌که شرکت ارائه‌کنندهٔ خدمات ابررایانش با آن همکاری نمی‌کند.

ابررایانش، جلوه‌ای جدید از فضای سایبر است. سرویس ابررایانش به کاربر این امکان را می‌دهد که از سرویس ایمیل و سایت‌های شبکه‌های اجتماعی بهره گیرد. کاربر می‌تواند تصاویر و فایل‌های خود را به‌جای ذخیره در رایانه شخصی به‌صورت آنلاین در فضای ابر[1] ذخیره کند (Vincent & Hart, 2011: 50). ابررایانش، مجموعه‌ای از منابع و سرویس‌هایی شامل شبکه‌ها، سرورها، فضای ذخیره‌سازی و برنامه‌های کاربردی است که در ابر سرویس‌دهی می‌شوند. اطلاعات به‌جای حافظهٔ رایانه در ابر ذخیره می‌شوند، با این مزیت که حتی دیگران نیز می‌توانند به درخواست کاربر به آنها دسترسی داشته باشند و از مطالب آن استفاده کنند. درحالی‌که این فرایند مستلزم پیچیدگی‌های فنی و تخصصی است، لیکن کاربر با استفاده از اپلیکیشن‌های مبتنی بر شبکه به منابع گسترده‌ای از سرورهای اینترنتی دسترسی پیدا می‌کند، بدون اینکه از مرورگر شبکه برای محاسبات ابری خود استفاده کند. این وضعیت منصرف از مزایای آن سبب شده است تا فناوری اطلاعات به‌شدت آسیب‌پذیر و به تهدیدی علیه جامعهٔ اطلاعاتی تبدیل شود، چراکه ابررایانش برای مجرمان نیز ابزار جدیدی است تا در محیط آن به اعمال مجرمانهٔ خویش بپردازند یا به داده‌های دیگران دسترسی غیرمجاز پیدا کنند. ابررایانش با حفظ گمنامی کاربر موجبات دسترسی به محتویات الکترونیک دیگر کاربران را با ورود به حساب کاربری ایمیل آنها در فضای ابر یا سرقت گذرواژهٔ آنها فراهم کرده است.

دولت‌ها در راستای اعمال حاکمیت درون‌سرزمینی انتظار دارند شرکت‌های ارائه‌کنندهٔ خدمات سایبری حسب قوانین سرزمینی محل ارائهٔ خدمات یا اقامت کاربران متبوع ملزم به همکاری کامل با آنها در افشای دیتای الکترونیک باشند، وقتی‌که پروسهٔ کشف جرم و تعقیب مرتکب احتمالی آن به فضای ابررایانش می‌رسد، صرف‌نظر از اینکه محاکم قضایی آنها برای اثبات جرم تا چه میزان به دیتای الکترونیک اعتبار قائل شوند. لیکن شرکت‌های ارائه‌کنندهٔ خدمات سایبری در فرایند تحقیقات کیفری پلیس تابع محدودیت‌های درون‌سازمانی خویش با دولت‌های محل استقرار دیتاسنتر و کاربران الکترونیک از سرتاسر دنیا هستند. افزایش تعهدات بر افشای دیتای ذخیره‌شدهٔ کاربران در دیتاسنترهای فراسرزمینی در قوانین داخلی یک کشور

1. Cloud

الزاماً مورد پذیرش دیگر کشورها نیست. چه‌بسا قوانین سایر کشورها در این زمینه با ممنوعیت یا رعایت تشریفات قانونی برای افشای دیتای ذخیره‌شده توأم باشد. بر این اساس تعهدات و ممنوعیت‌های متفاوت براساس قوانین سرزمینی در زمینهٔ افشای دیتای کاربران سبب عدم افشای دیتای ذخیره‌شده می‌شود که خوشایند برخی دولت‌ها نیست. هماهنگ‌سازی قوانین کشورها در این حوزه یکی از سازوکارهای عبور از این وضعیت است[۱] لیکن به دلایل خاص این امر محقق نیست. در این شرایط نگرانی کشف جرم و تعقیب مرتکب آن همچنان قابل درک و در راستای اعمال حاکمیت دولت‌ها امری بدیهی است. ازاین‌رو باید سازوکاری برای تحقیقات کیفری سایبری دولت‌ها در دیتاسنترهای شرکت‌های ارائه‌کنندهٔ سرویس ابرایانش منصرف از محل استقرار دیتاسنتر متصور باشد. بر این اساس سؤال پژوهش این است که سازوکار تحقیقات کیفری سایبری در دیتاسنتر فراسرزمینی و چالش‌های آن چیست؟ رویکرد قضایی محاکم ایالات متحده در پروندهٔ شرکت مایکروسافت نمونه‌ای تجربه‌شده از این ابهام است. رویکرد قضایی محاکم ایالات متحده برای تحقیقات کیفری سایبری در دیتاسنترهای سرزمینی دولت ثالث موضوع این نوشتار است. بر این اساس ابتدا فضای سایبر و انتقال و ذخیرهٔ اطلاعات کاربران اینترنت در رویهٔ قضایی و سپس بایسته‌های رژیم معاهدات همکاری حقوقی آن در تحقیقات کیفری واجد اهمیت است.

فضای سایبر و انتقال و ذخیرهٔ اطلاعات کاربران اینترنت در رویه قضایی

در خصوص فضای سایبر تحت عنوان فضای فاقد حاکمیت یا فضای تحت حکومت قواعد صلاحیت فضای فیزیکی اختلاف‌نظرهایی وجود دارد. بر این اساس صلاحیت سرزمینی به‌عنوان مهم‌ترین اصل صلاحیتی حقوق کیفری بین‌المللی در فضای سایبر به چالش کشیده شده است. اعمال صلاحیت سرزمینی مستلزم ترسیم قلمرو حاکمیتی کشور و تبیین محل وقوع جرم است. قلمرو حاکمیتی کشورها در فضای واقعی شامل قلمرو زمینی، دریایی و هوایی است. لیکن ترسیم این قلمرو در فضای سایبر دشوار است. اینترنت بر قواعد صلاحیت درون‌سرزمینی دولت‌ها تأثیرات چشمگیری گذاشته است، چراکه وقوع جرم در فضای سایبری از قاعدهٔ «مکان جرم» در فضای فیزیکی تبعیت نمی‌کند تا اینکه قائل بر وقوع جرم در یک مکان و عدم وقوع آن در سایر مکان‌ها باشیم؛ اگرچه نحوهٔ برخورد دولت‌ها در اعمال صلاحیت بر فضای مجازی تحت شبکه باز هم در قالب همان فرمول «مکان» اعم از مکان فیزیکی دسترسی مجرم به فضای اینترنت یا مکان سرور ذخیره‌کنندهٔ اطلاعات قرار می‌گیرد. بر این

۱. برای مطالعهٔ بیشتر در این زمینه ر.ک: جلالی و توسلی اردکانی، ۱۳۹۸: ۱۳۵۱.

اساس اگر ملاک سرزمین محل دسترسی مجرم به فضای اینترنت باشد، دولت سرزمینی اعم از متبوع یا غیرمتبوع مجرم دارای صلاحیت است، مشروط به آنکه نیازی به اطلاعات ذخیره‌شده در سرور مستقر در سرزمین دیگر نداشته باشد. اما اگر ملاک سرزمین محل سرور ذخیره‌کنندهٔ اطلاعات باشد، دولت سرزمینی سرور اطلاعات صلاحیت دارد.

نفوذ برای دستیابی غیرمجاز به اطلاعات ذخیره‌شدهٔ سرورهای دولت خارجی، مداخله در امور حاکمیتی آن است، ولو اینکه از طریق فضای مجازی تحت شبکه انجام گیرد. اعمال حاکمیت برابر دولت‌ها ریشه در آموزه‌های حقوق بین‌الملل عرفی دارد. صلاحیت کیفری دولت‌ها در کشف و تعقیب جرائم براساس تعریف مرزهای سرزمینی با اعمال حاکمیت در عرصهٔ داخلی گِره می‌خورد. استقرار درون‌سرزمینی دیتاسنترهای ذخیره‌کنندهٔ اطلاعات الکترونیک کاربران فضای مجازی جلوه‌ای از اعمال حاکمیت درون‌سرزمینی است، لیکن تحقق آن با موانع جدی مواجه است (Selby, 2017: 215). بر این اساس دسترسی به سرورهای الکترونیک حاوی دلایل مجرمانه به‌دلیل استقرار در خارج از قلمرو سرزمین متأثر از وقوع جرم، از چالش‌های دولت‌ها در تعقیب جرائم است. این وضعیت برای اولین بار در سیستم قضایی ایالات متحده تجربه و خلأهای قانونی اعمال صلاحیت سرزمینی در جرائم سایبری نمایان شده است. شرکت مایکروسافت با در اختیار داشتن دیتاسنترهای مختلف در سرتاسر دنیا اقدام به ذخیرهٔ ایمیل‌های کاربران خویش کرده است. دادستان در تحقیقات کیفری ایالات متحده متوجه برخی از ارتباطات مظنون به قاچاق مواد مخدر از طریق ایمیل با همدستان وی شد، ازاین‌رو درصدد کسب اطلاعات حساب کاربری و محتویات ایمیل مدنظر برآمد. دادستان از دادگاه بخش نیویورک تقاضا کرد تا مجوزی برای دسترسی به این اطلاعات از طریق شرکت مایکروسافت صادر شود (United States v. Microsoft Corp, 2014: 1).

بر این اساس دادگاه بخش با پذیرش تقاضای دادستان بر ضرورت تکمیل تحقیقات کیفری سایبری، شرکت مایکروسافت را ملزم می‌کند که اطلاعات یکی از کاربران خود را افشا کند که در دیتاسنتر ایرلند ثبت و ذخیره شده است. دادگاه بخش قرار الزام مایکروسافت به افشای حساب و محتویات ایمیل کاربر را با استناد به قانون ارتباطات ذخیره‌شده[1] صادر می‌کند، با این باور که محدودیت‌های صلاحیت سرزمینی نباید مانع تحقیقات کیفری سایبری شود (Narayanan, 2012: 472). شرکت مایکروسافت ملزم به افشای حساب کاربری و محتویات ایمیل تبعهٔ خارجی ذخیره‌شده در دیتاسنتر مایکروسافت، ولو مستقر در صندوق امانات بانک کشور خارجی است، به صرف اینکه مرکز فعالیت مایکروسافت در ایالات متحده است. شرکت‌های عامل خدمات الکترونیک در مادهٔ ۴۱ قانون آیین دادرسی کیفری ایالات متحده

1. Stored Communication Act, 1986

مخاطب روند تحقیقات کیفری دادستان قرار گرفته‌اند تا از طریق آنها ثبت و جمع‌آوری اطلاعات الکترونیک کاربران صرف‌نظر از محل استقرار دیتاسنتر میسر شود. اما رویکرد دادگاه بخش برخلاف قوانین کشور محل استقرار دیتاسنتر است که بنابر اصل حاکمیت درون‌سرزمینی لازم‌الرعایه است، ولو اینکه قوانین ایالات متحده برخلاف آن باشد.

تعارض میان قوانین بر جواز یا ممنوعیت افشای اطلاعات کاربران موجب شده است که شرکت‌های ارائه‌کنندهٔ خدمات الکترونیک بااحتیاط برخورد کنند، در جایی که حسب دستور مقامات قضایی ملزم به افشای اطلاعات می‌شوند. با وجود این رویهٔ دادگاه بخش حاکی از اعمال صلاحیت سرزمینی و عدم نیاز به قاعدهٔ همکاری بین‌المللی با دولت ایرلند در این زمینه است. با این استدلال قرار الزام همکاری شرکت مایکروسافت با دادستان برای افشای اطلاعات حساب کاربری و محتویات ایمیل مظنون به قاچاق مواد مخدر صادر می‌شود. براساس استدلال دادگاه بخش نیازی نیست نمایندهٔ دولت وارد قلمرو دولت خارجی برای دستیابی به دیتای ذخیره‌شده در دیتاسنترهای ایرلند شود، بلکه تنها کافی است که مایکروسافت عامل درون‌سرزمینی با دسترسی به سِرورهای خود این اطلاعات را استخراج کند و در اختیار ایالات متحده قرار دهد. ازاین‌رو دادگاه از صلاحیت درون‌سرزمینی خود استفاده کرده است. دادگاه با محل ذخیرهٔ برون‌سرزمینی دیتا سروکار ندارد. دیتا در کنترل عامل درون‌سرزمینی است. برای الزام عامل درون‌سرزمینی نیازی به اعمال صلاحیت فراسرزمینی ایالات متحده نیست (United States v. Microsoft Corp., 2014: 472). ازاین‌رو نیازی نیست شرکت مایکروسافت به دیتاسنتر ایرلند دسترسی فیزیکی داشته باشد، بلکه دسترسی آن به اطلاعات ذخیره‌شده از طریق سیستم رایانه‌ای متصل به اینترنت با گذرواژه‌های در اختیار کفایت می‌کند. لیکن شرکت مایکروسافت معتقد است که کاربر برای ایمیل خویش نام کاربری و گذرواژه درنظر گرفته است که این حاکی از تلقی حریم خصوصی بودن آن است. محتویات ایمیل مانند تراکنش حساب‌های بانکی نیست که دادگاه از بانک الزام افشای پرینت تراکنش‌های حساب‌های بانکی فردی را درخواست کند و بانک عامل با رعایت استثنای اصل رازداری بانکی این اطلاعات را در اختیار دادگاه کیفری قرار دهد. کاربر در ایمیل با دیگران ارتباط برقرار می‌کند. او با تلقی حریم خصوصی از آن به تبادل افکار، اطلاعات و اسنادی می‌پردازد که حاضر به تبادل آن با همگان نیست. تبادل اطلاعات از طریق ایمیل متفاوت از تبادل اطلاعات یا اظهارنظر در فضای عمومی مجازی یا شبکه‌های اجتماعی قابل دسترسی برای تمامی اعضای آن است. با وجود این دادگاه بخش معتقد است که صِرف کنترل مایکروسافت بر حساب کاربری و محتویات ایمیل برای ملزم کردن آن به همکاری با دولت ایالات متحده کفایت می‌کند. حال آنکه الزام مایکروسافت به افشای اطلاعات خصوصی مجوزی برای بازرسی و توقیف فراسرزمینی اطلاعات بدون جلب رضایت دولت ایرلند است که فراتر از صلاحیت سرزمینی ایالات متحده است. عملکرد دادگاه بخش ناقض اصل صلاحیت کیفری سرزمینی و مداخله در امور دولت

خارجی است. دولت نیز همسو با دادگاه بخش معتقد است که به‌دلیل دسترسی مایکروسافت به اطلاعات مذکور از مرکز فعالیت آن در سرزمین ایالات متحده اعمال صلاحیت فراسرزمینی یا نقض آن رخ نداده است. لیکن این استدلال‌ها مقبولیت ندارند.

شرکت مایکروسافت در خصوص مسائل اداری تابع قوانین محل استقرار مرکز فعالیت خویش است، لیکن در زمینهٔ موضوعات فنی و تخصصی تابع قراردادهایی است که با دیگر سازمان‌ها یا کشورها تنظیم کرده است. سازمان‌ها و کشورهای طرف قرارداد آن ملزم به تبعیت از مقررات محل استقرار مرکز فعالیت شرکت مایکروسافت نیستند، ولو اینکه برای شرکت مایکروسافت اقتضائات یا مصالح دیگری وجود داشته باشد. با وجود این برخی معتقدند که حمایت از حریم خصوصی افراد در فضای مجازی تحت شبکه مشمول قوانین کیفری هستند (Green, 2015: 193). بر این اساس دیتاسنتر ذخیره‌کنندهٔ اطلاعات کاربران مایکروسافت و محدودیت‌های حاکم بر آن مشمول قوانین کیفری نیستند. از این منظر مجوز دسترسی ایالات متحده به اطلاعات کاربران شرکت سرویس‌دهندهٔ مایکروسافت در چارچوب صلاحیت سرزمینی تعریف می‌شود، حتی زمانی‌که اطلاعات کاربران در فضای مجازی تحت وب از قلمرو سرزمینی ایالات متحده ثبت می‌شوند. پذیرش این استدلال به معنای ایجاد رویه‌ای برای دولت ایالات متحده به‌منظور دسترسی به اطلاعات ذخیره‌شده، ولو در هر نقطه از دنیا به صرف محل استقرار و فعالیت درون‌سرزمینی شرکت سرویس‌دهندهٔ مایکروسافت در قلمرو ایالات متحده یا تابعیت کاربر الکترونیک یا بزه‌دیدهٔ جرم سایبری از این طریق است. این وضعیت به معنای دسترسی به اطلاعات تمامی کاربران شرکت مایکروسافت از سرتاسر دنیاست، ولو اینکه هیچ ارتباطی از حیث تابعیت یا اقامت در قلمرو سرزمینی ایالات متحده وجود نداشته باشد، چراکه مرکز فعالیت شرکت سرویس‌دهندهٔ مایکروسافت کفایت می‌کند که در خاک ایالات متحده است. کاربران شرکت‌های فعال در قلمرو سرزمینی ایالات متحده محدود به اتباع داخلی نیستند. این شرکت‌ها از سرتاسر جهان کاربرانی دارند، درحالی‌که هریک از کاربران حسب قوانین دولت متبوع خویش موضوع الزامات و محدودیت‌های متفاوتی‌اند. ازاین‌رو حمایت از حریم خصوصی تمام کاربران صرف‌نظر از ملیت آنها از اولویت‌های اصلی شرکت سرویس‌دهندهٔ مایکروسافت است. نادیده گرفتن این الزامات سبب می‌شود تا مردم از خدمات الکترونیکی شرکت‌هایی استفاده کنند که به آنها اعتماد دارند. رویکرد محاکم قضایی ایالات متحده در الزام مایکروسافت به افشای کاربران به نادیده گرفتن تعهدات مایکروسافت نسبت به کاربران خویش در حفظ امنیت اطلاعات آنها منجر می‌شود (Heuvel & Cohen, 2014). الزامات حریم خصوصی ارتباطات الکترونیک کاربران نقض می‌شود، اگر دسترسی دولت به اطلاعات ذخیره‌شده در دیتاسنترهای برون‌سرزمینی شایع شود، منصرف از اینکه کاربران از ملیت‌های مختلف اعتماد خود را به استفاده از خدمات شرکت‌های فعال در حوزهٔ الکترونیک مستقر در قلمرو سرزمینی ایالات متحده از دست می‌دهند.

صلاحیت سرزمینی براساس محل ذخیرهٔ اطلاعات در دیتاسنتر ایرلند اولویت دارد تا صلاحیت ایالات متحده بدان فراسرزمینی و غیرقابل دسترس تلقی شود (Hsiao, 2015: 234). بر این اساس ایالات متحده باید مخاطب معاهدات همکاری حقوقی متقابل در زمینهٔ جرائم سایبری باشد، به‌جای اینکه به گسترش صلاحیت خود فراتر از مرزهای داخلی و دخالت در اعمال حاکمیت در امور داخلی سایر کشورها بپردازد. اعمال صلاحیت درون‌سرزمینی در قلمرو خارجی جز در پرتو قواعد ناشی از عرف یا معاهدات بین‌المللی میسر نیست. رویهٔ دیوان بین‌المللی دادگستری در قضیهٔ لوتوس موضوع دعوای فرانسه علیه ترکیه نیز نشان می‌دهد که یک کشور در هیچ شرایطی مجاز به اعمال قدرت در قلمرو کشور دیگر نیست.[1] با این وصف رأی دادگاه بخش ایالات متحده متوجه دیتاسنتر مستقر در خاک ایرلند است. درحالی‌که قضات ایالات متحده در صدور آرای کیفری صلاحیت فراسرزمینی ندارند. صلاحیت آنها تنها محدود به قلمرو جغرافیایی مدنظر در تقسیمات ایالات متحده است. دستورهای قضات بر بازرسی و توقیف اشیا در خارج از قلمرو قضایی محل مأموریت آنها کارامد نیست. رویهٔ دیوان عالی ایالات متحده نیز مؤید این برداشت است مبنی بر اینکه «قلمرو حکومت قوانین ایالات متحده درون‌سرزمینی است و کل دنیا را در برنمی‌گیرد» (Microsoft Corp. v. AT&T Corp., 2007: 437). بر این اساس رأی دادگاه بخش نمی‌تواند مجوزی برای دسترسی مقامات دولت ایالات متحده به اطلاعات ذخیره‌شده در دیتاسنتر خارج از کشور باشد، ولو اینکه مایکروسافت از مرکز فعالیت خود بدان دسترسی و با این اطلاعات سروکار داشته باشد. بی‌تردید رویکرد دادگاه بخش برخلاف بایسته‌های معاهدات همکاری حقوقی متقابل در عرصهٔ بین‌المللی است (Swire and Hemmings, 2017: 687). رویهٔ قضایی ایالات متحده در چنین شرایطی بدعتی فاقد مبنا و در نهایت ناقض حریم خصوصی کاربران الکترونیک است (Daskal, 2016: 474). عمده شرکت‌های فعال در زمینهٔ ارتباطات و فناوری تبعه و مستقر در قلمرو سرزمینی ایالات متحده و اتحادیهٔ اروپا هستند. الزام این شرکت‌ها از سوی دولت‌هایی که نمایندگی آنها را پذیرفته‌اند، بنا به اصل سرزمینی بودن محل فعالیت شعب در نهایت به نادیده گرفتن الزامات حریم خصوصی کاربران آنها منجر می‌شود که از اتباع سایر دولت‌ها هستند. کاربران هریک حسب قوانین دولت متبوع خویش تابع الزامات و امتیازاتی هستند که در قوانین سایر کشورها مقبولیت ندارند. پیچیدن نسخهٔ واحد برای تمام کاربران شرکت مایکروسافت به‌واسطهٔ مرکز فعالیت شرکت مایکروسافت براساس قوانین کیفری ایالات متحده مقبولیت ندارد. کاربران مایکروسافت از سرتاسر دنیا مشمول قوانین ایالات متحده یا اتحادیهٔ اروپا نیستند تا از این طریق امنیت حریم خصوصی دیتای آنها به خطر بیفتد.

تقاضای همکاری از دولت محل استقرار دیتاسنتر مطابق مقررات معاهدات بین‌المللی

---

۱. برای مطالعهٔ بیشتر در این زمینه ر.ک: حبیبی و شاملو، ۱۳۹۲: ۸۱.

فی‌مابین، تنها طریق مجاز برای دسترسی به اطلاعات الکترونیک در فضای سایبر است. عدم صلاحیت دادگاه بخش در صدور مجوز دسترسی مقامات ایالات متحده به اطلاعات ذخیره‌شدهٔ کاربران در دیتاسنتر مستقر در خارج از قلمرو سرزمینی ایالات متحده نیز به معنای لزوم همکاری و تبعیت ایالات متحده از مقررات سرزمین محل استقرار دیتاسنتر از طریق مجاری قانونی آن یعنی موافقت‌نامه‌های همکاری قضایی فی‌مابین است. دولت ایرلند در راستای اعمال حاکمیت درون‌سرزمینی با عملکرد دادگاه بخش بر صدور مجوز بازرسی اطلاعات ذخیره‌شده در دیتاسنتر ایرلند مخالفت کرده است. البته دولت ایرلند حسب معاهدات بین‌المللی فی‌مابین با ایالات متحده مکلف به رسیدگی به تقاضای ایالات متحده در چارچوب مصالح ملی و مقررات سرزمینی خویش است. لیکن این همکاری در تحقیقات کیفری سایبری به‌دلیل عضویت ایرلند در اتحادیهٔ اروپا با الزاماتی مواجه است که حتی تقویت همکاری کیفری بین‌المللی فی‌مابین ایرلند و ایالات متحده راهگشا نیست. رأی دادگاه بخش مورد اعتراض شرکت مایکروسافت قرار می‌گیرد (Microsoft Corp. v. United States, 2016: 197). قضات شعبهٔ تجدیدنظر قائل به عدم صلاحیت ایالات متحده در دسترسی به اطلاعات ذخیره‌شده در دیتاسنتر فراسرزمینی‌اند. ثبت و افشای اطلاعات ذخیره‌شده در دیتاسنتر مستقر در خاک ایرلند تابع قوانین ایرلند است. محل استقرار و فعالیت شرکت سرویس‌دهندهٔ مایکروسافت در سرزمین ایالات متحده تأثیری در نادیده گرفتن مقررات دولت ایرلند ندارد. شرکت مایکروسافت برای استفاده از دیتاسنتر مستقر در ایرلند تابع مقررات ایرلند است. شرکت مایکروسافت در زمینهٔ فعالیت‌های خویش در سرزمین ایالات متحده به‌صورت توأمان مشمول قوانین ایالات متحده است، لیکن این به معنای چشم‌پوشی از تعهدات شرکت مایکروسافت در بهره‌برداری از امکانات دولت ایرلند نیست. بر این اساس قرار دادگاه بخش در اعتراض مایکروسافت نقض می‌شود. رویکرد قضات شعبهٔ تجدیدنظر حاکی از ممنوعیت پلیس ایالات متحده در دسترسی به اطلاعات ذخیره‌شده در دیتاسنترهای فراسرزمینی بدون رعایت سازوکارهای بین‌المللی است. رژیم معاهدات همکاری حقوقی در تحقیقات کیفری حسب ارادهٔ دو یا چند طرف قراردادهای بین‌المللی تنظیم و با رعایت اصل حاکمیت درون‌سرزمینی آنها به‌کار گرفته می‌شود. ارادهٔ یک طرف بدون رعایت سازوکارهای مقدماتی آن یا توسل به سیستم قضایی داخلی برای امور فراسرزمینی ثمربخش نیست.

بایسته‌های رژیم معاهدات همکاری حقوقی در تحقیقات کیفری

توسعهٔ فناوری و رویکرد جهانی به ذخیرهٔ دیتا در ابرایانش به اختلاف‌نظرهایی در قلمرو تحقیقات کیفری منجر شده است. فناوری ابرایانش سبب شده است تا نحوهٔ ذخیرهٔ اطلاعات با شکسته شدن مرزهای جغرافیایی و توسعهٔ صلاحیت‌های قضایی دگرگون شود. قانونگذاری

داخلی کشورها نتوانسته است پا به پای تغییرات سریع و ماهیت فراسرزمینی صنعت فناوری ابررایانش قدم بردارد. دعوای ایالات متحده علیه مایکروسافت اختلاف در سه حوزه شامل جهانی شدن ذخیرهٔ دیتا، حریم خصوصی بین‌المللی و قانونگذاری در سطح ملی را نمایان کرده است (United States v. Microsoft Corp., 2014: 466). دولت‌ها در پرتو معاهدات همکاری حقوقی متقابل به‌نحو سنتی ملزم به اعمال اشکال مختلف صلاحیت در انجام تحقیقات کیفری سایبری در قلمرو خویش به درخواست هریک از اعضا شده‌اند، اعم از اینکه تحقیقات در راستای تعقیب و محاکمهٔ مجرم سایبری یا حمایت از بزه‌دیدهٔ آن باشد.[1] دولت‌های عضو این معاهدات مکلف به همکاری متقابل با یکدیگر و پذیرش نتایج عملیات دولت مجری تحقیقات براساس قوانین متبوع هستند. دولت مورد تقاضا در قلمرو سرزمینی خویش براساس قوانین داخلی به اعمال حاکمیت خود به تقاضای طرف دیگر می‌پردازد و نتایج تحقیقات را به مقامات قضایی آن تحمیل می‌کند (Currie & Rikhof, 2013: 22). دولت تقاضاکنندهٔ تحقیقات کیفری براساس معاهدهٔ فی‌مابین به تحقیقات سایبری فراسرزمینی اعتبار قائل می‌شود و در عرصهٔ داخلی آن را ملاک عمل قرار می‌دهد. نتیجهٔ اعتبارسنجی به تحقیقات کیفری انجام‌گرفته براساس قوانین خارجی، تحمیل مجازات به اتباع داخلی است. نقض احتمالی حقوق شهروندی در حین تحقیقات کیفری دولت خارجی نیز مزید بر علت است. اگرچه تحقیقات فراقانونی با ضمانت اجراهای کیفری و سلب اعتبار مواجه است، معلوم نیست این برخورد براساس کدام‌یک از قوانین کیفری دولت تقاضاکننده یا تقاضاشوندهٔ تحقیقات کیفری صورت می‌گیرد. پرواضح است که در این شرایط مبانی جمع‌آوری دلایل کیفری براساس بایسته‌های قانونی کشور تقاضاشونده و محکومیت براساس ممنوعیت‌های قانونی کشور تقاضاکننده است. این رویکرد متفاوت از انتظارات اتباع داخلی از قوانین کیفری متبوع است. در عین حال که این نحوه از تحقیقات کیفری و روند دادرسی براساس آنها با اصول سنتی اعمال صلاحیت کیفری واقعی، جهانی و سرزمینی وجه اشتراک ندارد. از یک طرف، این وضعیت چیزی غیر از اعمال صلاحیت واقعی است. اصل صلاحیت واقعی به معنای توسعهٔ صلاحیت تقنینی و قضایی یک کشور نسبت به جرائمی است که خارج از قلمرو حاکمیت آن کشور واقع می‌شود و به منافع اساسی و حیاتی آن صدمه می‌زند. منافع مدنظر دولت‌ها برای ایجاد صلاحیت واقعی دادگاه‌های داخلی جلوه‌ای از این صلاحیت است. برای نمونه این منافع در بند «ج» مادهٔ ۲۸ قانون جرائم رایانه‌ای ایران متوجه «... سامانه‌های رایانه‌ای و مخابراتی و تارنماهای وب‌سایت‌های مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای وب‌سایت‌های دارای دامنهٔ مرتبه بالای کد

۱. برای مطالعهٔ بیشتر در این زمینه ر.ک: پورقهرمانی، ۱۳۹۶: ۲۵.

کشوری ایران در سطح گسترده ...» است. سایر موارد از این مقررات خارج است. اعمال صلاحیت جهانی در بند «د» مادهٔ ۲۲ کنوانسیون جرائم سایبری[1] جلوهٔ دیگری از این وضعیت است. بر این اساس کشورها باید به وضع مقررات برای اعمال صلاحیت نسبت به جرائمی بپردازند که خارج از قلمرو سرزمینی آنها ارتکاب می‌یابند. لیکن کشورهای عضو در صورتی باید نسبت به جرم ارتکابی اتباع خویش اعمال صلاحیت کنند که عمل ارتکابی از منظر قانون محل وقوع نیز جرم باشد یا خارج از قلمرو سرزمینی تمام کشورها ارتکاب یافته باشد. لیکن پروندهٔ ایالات متحده علیه مایکروسافت در خصوص جرم یکی از اتباع خارجی در قلمرو داخلی ایالات متحده است که مشمول اصل صلاحیت سرزمینی قرار می‌گیرد، درحالی‌که جمع‌آوری اطلاعات کاربری و محتویات ایمیل مظنون به‌دلیل محل استقرار دیتاسنتر و برخورد با منافع کشور ثالث در ادارهٔ امور داخلی خویش از این قاعده هم مستثناست.

از طرف دیگر، تقاضای پلیس برای جمع‌آوری دلایل الکترونیک در جرائم سایبری از چالش‌های پیش‌روی دولت‌هاست تا براساس الگوی سنتی همکاری‌های متقابل بین‌المللی به جمع‌آوری و ارائهٔ اطلاعات به دولت متقاضی منجر شود. اینترپل، به‌عنوان شبکهٔ دائم تبادل اطلاعات میان نیروهای پلیس ملی کشورها زمینهٔ دستگیری و بازداشت افراد را خارج از قلمرو سرزمینی دولت متقاضی فراهم می‌کند. افزون‌بر این در سال‌های اخیر همکاری مستقیم نیروی پلیس دو یا چند دولت در تشکیل تیم‌های تحقیقات مشترک و اعزام نیروی پلیس به کشور طرف قرارداد همکاری دو یا چندجانبه رو به افزایش است (Hufnagel & McCartney, 2015: 109). اما این نحوهٔ همکاری‌ها هم با محدودیت‌هایی همراه است. اعمال حاکمیت درون‌سرزمینی دولت میزبان در مدیریت تحقیقات نیروهای پلیس خارجی براساس قوانین داخلی از جملهٔ این محدودیت‌هاست. تحقیقات مدنظر دولت خارجی اعم از اینکه توسط نیروهای پلیس اعزامی آن یا نیروی پلیس کشور میزبان انجام گیرد، الزاماً مطابق مقررات دولت میزبان صورت می‌گیرد. این وضعیت به اقتضای اعمال حاکمیت دولت میزبان در قلمرو سرزمینی خویش است. این مسئله در مورد دلایل الکترونیک مجرمانه در فضای سایبر و ابررایانش تا حدودی متفاوت و ظاهراً سهل‌تر است. تکنولوژی موجد ارتباطات الکترونیک از راه دور زمینه را برای جمع‌آوری این دلایل بدون اعزام نیرو به کشور طرف مقابل فراهم کرده است. لیکن چالش اصلی در این زمینه نحوهٔ برخورد کشورها با اینترنت و ارتباطات مجازی بین‌المللی با محدودیت‌های درون‌سرزمینی در اعمال صلاحیت سرزمینی و اعمال حاکمیت خویش در

---

۱. کنوانسیون جرائم سایبری معروف به «کنوانسیون جرایم سایبری بوداپست» نخستین معاهدهٔ بین‌المللی از سوی شورای اروپا در سال ۲۰۰۱ در خصوص جرائم رایانه‌ای است. در این کنوانسیون تلاش شده است تا سازگاری قوانین ملی، ارتقای روش‌های تحقیقات کیفری و همکاری بین کشورها بهبود یابد.

پرتو صلاحیت واقعی است (Scassa & Currie, 2011: 1017). بر این اساس پلیس قضایی در قلمرو سرزمینی تحت حاکمیت دولت متبوع به رایان] مجرم دسترسی فیزیکی پیدا می‌کند. لیکن سِرور اطلاعات ذخیره‌شده از طریق فضای مجازی تحت وب در سرزمین دولت خارجی مستقر است. اگر پلیس بخواهد از سرزمین دولت متبوع و فضای ابر به اطلاعات دسترسی و آنها را از سِرور برون‌سرزمینی استخراج کند، این دسترسی با درنظر گرفتن فرمول سنتی حاکم بر دلایل فیزیکی از نوع غیرقانونی و مداخله در امور حاکمیتی دولت خارجی است؛ مگر اینکه حسب مورد اطلاعات ذخیره‌شده در سِرور به‌صورت آزاد در فضای مجازی برای همگان و آزادانه قابل دسترسی باشد، یا اینکه مشمول حمایت‌های قانونی و در شرایط خاص برای کاربران قابل دسترسی باشد. ازاین‌رو دولت‌ها تمایل دارند برای دسترسی به اطلاعات ذخیره‌شده در سرورهای فراسرزمینی از طریق مقامات رسمی و احترام به حاکمیت دولت متبوع اقدام شود. لیکن دولت‌های سرزمینی سرورهای ذخیره‌کنندهٔ اطلاعات در حد انتظار عمل نمی‌کنند. آخرین گزارش سازمان ملل متحد در این زمینه نشان می‌دهد که دوسوم کشورهای محل استقرار سرورهای ذخیره‌کنندهٔ اطلاعات تمایلی به همکاری با سایر دولت‌ها در افشای اطلاعات ذخیره‌شده در دیتاسنترهای خویش ندارند و تنها در موارد خاص چنین تقاضاهایی را از مجاری رسمی قضایی بررسی می‌کنند (United Nations Office on Drugs and Crime, 2013: 220)؛ درحالی‌که دولت‌ها برای انجام تحقیقات کیفری ناگزیر از مساعدت‌های حقوقی و قضایی متقابل‌اند. قاعدهٔ اصلی در تحقیقات کیفری این است که هرگونه عملیات اجرایی فراتر از مرزهای سرزمینی مستلزم کسب رضایت دولت متأثر از این عملیات تحقیقاتی در امور کیفری باشد. اعمال صلاحیت سرزمینی از سوی دولت غیرسرزمینی و از خارج از مرزهای کشور با اتکای به قوانین داخلی یا قوانین منبعث از عرف یا کنوانسیون‌های بین‌المللی ممکن نیست (رضوی‌فرد و موسوی، ۱۳۹۶: ۸۴). دولت‌ها در صورتی مجاز به انجام تحقیقات کیفری در خارج از مرزهای خود هستند که برای آن مبنایی در معاهده یا عرف بین‌المللی یا مجوز دولت مربوط داشته باشند. اگرچه به‌طور معمول دولت‌ها اشکال مختلف همکاری دوجانبه در تحقیقات فرامرزی را با ابزارها و رویه‌های حقوقی و قضایی می‌پذیرند، این مسئله ناشی از طبیعت یا خصوصیت فرامرزی یا جهانی فعالیت مجرمانه نیست، بلکه ناشی از اولویت دولت‌ها در مبارزه با جرائم بین‌المللی یا موجد صلاحیت جهانی است. تحقیقات فرامرزی در قالب همکاری قضایی دوجانبه، تبادل دوجانبهٔ اطلاعات یا ایجاد دیتابیس‌های مشترک، انجام تحقیقات کیفری در سرزمین دیگر و تشکیل تیم‌های تحقیقات مشترک در همکاری حقوقی دوجانبه که به‌طور معمول انجام تحقیقات کیفری مورد درخواست دولت خارجی در قلمرو سرزمینی توسط عوامل داخلی انجام می‌گیرند (Koops & Goodwin, 2014: 24)، تحت تأثیر قوانین و مقررات و رویهٔ داخلی‌اند. ازاین‌رو تقاضای اعمال حاکمیت داخلی از سوی دولت خارجی منوط به رعایت

مقررات داخلی دولت دارندهٔ حق حاکمیت است.

این وضعیت در مورد دولت‌های عضو اتحادیهٔ اروپا به‌مراتب سخت‌تر است. هریک از دولت‌های عضو اتحادیهٔ اروپا مکلف به همکاری با دیگر دولت‌های عضو اتحادیه در امور کیفری و تبعیت از قرار جلب، دستگیری، بازداشت و جمع‌آوری دلایل و دیگر دستورهای قضایی بدون رعایت کامل قوانین داخلی خویش هستند. در خصوص نوع جرائم نیز دولت‌های عضو اتحادیهٔ اروپا براساس فهرست مقرر جرائم خاص برای دولت‌های عضو مکلف به همکاری هستند، صرف‌نظر از اینکه این جرائم در قوانین داخلی آنها جرم‌انگاری شده باشند. در عین حال که بسیاری از دولت‌های عضو اتحادیهٔ اروپا از همکاری‌های دوجانبه در زمینهٔ جرائم خارج از فهرست مقرر سرباز می‌زنند، لیکن برخی دیگر از کشورهای عضو اتحادیهٔ اروپا در خصوص سایر جرائم غیرمشابه در قوانین داخلی حداکثر همکاری را در تبعیت از قوانین دولت متقاضی انجام تحقیقات توسط تیم‌های مشترک تحقیقاتی قوی و قابل اعتماد به‌عمل می‌آورند (Fijnaut, 2012: 10). کشورهای عضو اتحادیهٔ اروپا حتی در برخی موارد با داشتن منافع مشترک در تعقیب جرم یا بسته به نوع جرم با صرف‌نظر کردن از اعمال حق حاکمیت خویش اجازهٔ محاکمهٔ مجرم در سرزمین خارجی را نیز صادر می‌کنند. لیکن این نحوه از همکاری‌های قضایی فرامرزی دولت‌های اروپایی با ایالات متحده بنا به دلایل مختلف وجود ندارد. موفقیت در همکاری در سطح ملی منوط به توانایی و امکانات در اختیار دستگاه قضایی و نیروهای پلیس است. مشابهت داشتن جرم تحت تعقیب دولت متقاضی با فهرست جرم‌انگاری‌های دولت سرزمینی در بیشتر موارد مدنظر است. برخی جرائم به‌عنوان جرائم مشترک مدنظر دولت‌ها در همکاری‌های قضایی مصرح در معاهدات بین‌المللی قرار می‌گیرند تا دولت‌های امضاکنندهٔ معاهدات مکلف به قانونگذاری داخلی باشند، لیکن تفاوت در میزان و مبنای مجازات از چالش‌های اصلی میان دولت‌های امضاکننده است که حتی در شرایط تنظیم معاهدهٔ همکاری فی‌مابین همچنان لاینحل باقی می‌ماند. در چنین شرایطی اجماع نظر میان دو دولت متقاضی و سرزمینی در زمینهٔ جرم تحت تعقیب برای ایجاد حس مشترک ضرورت بر تعقیب و مجازات عامل آن فراهم نمی‌شود.

این وضعیت مطلوب شرکت‌های فعال در زمینهٔ ارتباطات الکترونیک نیست، چراکه به اعتقاد آنها تبعیت از این الزامات در هر صورت به از بین رفتن شبکهٔ جهانی ارتباطات الکترونیک منجر می‌شود (Chertoff, 2017: 1). صرف‌نظر از اینکه هیچ تضمینی وجود ندارد که اتباع داخلی از خدمات الکترونیک آنها استفاده کنند، درحالی‌که برای آنها جایگزین مشابه فراسرزمینی وجود دارد که الزامات حریم خصوصی آنها را به‌مراتب بیشتر رعایت می‌کنند. عدم تمایل اتباع داخلی یک کشور به شبکه‌های اجتماعی یا تارنماهای خاص با منشأ سرزمینی، نمونه‌ای از این وضعیت است، چراکه فضای سایبر زمینه‌ای را برای کاربران الکترونیک فراهم

کرده است که آنها بدون تبعیت از محدودیت‌های سرزمینی از خدمات ارتباطاتی شرکت‌هایی استفاده کنند که کمترین ریسک افشای دیتای آنها را دربرداشته باشد. سرزمینی کردن دیتاسنترهای این شرکت‌ها و الزام آنها به تبعیت از قوانین ملی، از راهکارهای فراهم کردن زمینهٔ همکاری است. لیکن این وضعیت هم به از بین رفتن فضای باز اینترنت و تحمیل هزینه‌ها و موانعی برای کاربران در دسترسی آزادانه به اطلاعات منجر می‌شود که مطلوب کاربران آنها از عضویت در این سایت‌ها نیست (Chander & Le, 2015: 679). با وجود این برخی کشورها حسب مقررات داخلی شرکت‌های ارائه‌کنندهٔ خدمات ارتباطات الکترونیک را ملزم به استقرار دیتاسنترهای ذخیره‌کنندهٔ دیتای اتباع داخلی در قلمرو درون‌سرزمینی کرده‌اند. شرکت اپل به‌عنوان اولین شرکت، تبعیت خود از قوانین داخلی محل فعالیت شعبهٔ نمایندگی را برای استقرار دیتاسنتر ذخیره‌کنندهٔ دیتای اتباع داخلی در قلمرو سرزمینی چین اعلام کرده است (Mozur, Wakabayashi & Wingfield, 2017: 1). این نمونه حاکی از تمایل شدید کشورها به اعمال حاکمیت درون‌سرزمینی و کنترل اینترنت با توسل به اقدامات یکجانبه و سرزمینی کردن دیتاسنترهاست (Daskal, 2017: 45). ازاین‌رو زمینهٔ اجرای قوانین بین‌المللی و همکاری جامعهٔ اطلاعاتی در حوزهٔ دیتای کاربران شبکهٔ مجازی به نفع اعمال حاکمیت درون‌سرزمینی رو به زوال است. بر این اساس توسعهٔ همکاری‌های حقوقی متقابل در زمینهٔ مبارزه با جرائم سایبری با مانع مواجه است. اما دستیابی غیرمجاز با توسل به نرم‌افزارهای شنود سایت‌های اطلاعاتی فرامرزی از گزینه‌های جایگزین است[1] وقتی الزام شرکت‌های ارائه‌کنندهٔ خدمات الکترونیک به استقرار درون‌سرزمینی دیتاسنترها یا توسل به دیتای کاربران از طریق همکاری‌های بین‌المللی فراهم نباشد.

نتیجه‌گیری

ابررایانش، فناوری اطلاعات در فضای سایبر است. تحقیقات جنایی در سایبر به‌منظور دسترسی به حساب کاربری یا محتویات ایمیل و اسناد ذخیره‌شده در ابر است. دسترسی و جمع‌آوری دلایل الکترونیک از فضای مجازی تحت شبکه در قلمرو سرزمینی هر کشوری از مزیت‌های پیش‌روی دولت‌ها در کشف، تعقیب و مجازات جرائم فرامرزی سایبری است، لیکن با عدم تمایل دولت دارندهٔ دیتاسنتر به مداخله و نفوذ سایر دولت‌ها به مرزهای الکترونیک آن مواجه است. دولت‌های محل استقرار دیتاسنتر در اعمال حاکمیت درون‌سرزمینی با هیچ کشوری شریک نمی‌شوند. این دولت‌ها هم اطلاعات اتباع داخلی را به دولت‌های ثالث نمی‌دهند و هم از شرکت‌های متبوع تقاضا نمی‌کنند تا با دولت‌های ثالث در این زمینه همکاری کنند. صرف‌نظر

۱. برای مطالعهٔ بیشتر در این زمینه ر.ک: شهبازی و آقاجانی رونقی، ۱۳۹۹: ۱۴۸۷.

از اینکه الزام شرکت‌های فعال در زمینهٔ الکترونیک با دولت مرکزی نیز با محدودیت‌هایی مواجه است. اگر دولت ایالات متحده براساس قوانین داخلی مجاز به الزام مایکروسافت به افشای اطلاعات ذخیره‌شده در دیتاسنتر فراسرزمینی شود، به همین نحو سایر کشورها نیز با اتکا به قوانین داخلی تقاضای افشای اطلاعات ذخیره‌شده در دیتاسنترهای ایالات متحده را خواهند داشت. صرف‌نظر از اینکه شرکت سرویس‌دهندهٔ مایکروسافت در قلمرو سرزمینی ایالات متحده مستقر و مشغول به فعالیت است، لیکن نوع خدمات و کاربران آن در سرتاسر دنیا پراکنده‌اند. ایجاد حق برای دولت ایالات متحده بر دسترسی به حساب و اطلاعات کاربری شرکت مایکروسافت مستوجب نگرانی نقض حریم خصوصی آنها و سلب صلاحیت از شرکت مایکروسافت است. شرکت مایکروسافت بنا به الزامات ناشی از قراردادهای خود با دولت‌های محل استقرار دیتاسنتر و قراردادهای ارائهٔ خدمات به کاربران الکترونیک تابع محدودیت‌هایی است که حتی الزام دادگاه‌های کیفری ایالات متحده سبب خنثی شدن آنها نمی‌شود.

از یک طرف، شرکت‌های سرویس‌دهندهٔ اینترنت با محدودیت حفظ حریم خصوصی کاربران خود مواجه‌اند. بی‌توجهی آنها به استانداردهای ارائهٔ خدمات الکترونیک به کاربران و لو رفتن دیتای آنها سبب خدشه به منافع اقتصادی و اعتبار جهانی آنها می‌شود. با وجود این ذخیره شدن دیتای کاربران شرکت مایکروسافت در دیتاسنتر ایرلند مانع از دسترسی و کنترل مایکروسافت در قلمرو سرزمینی ایالات متحده بر اطلاعات کاربری و محتویات آنها نیست. لیکن عملکرد دادگاه بخش ایالات متحده در الزام مایکروسافت به افشای اطلاعات الکترونیک احد از کاربران مجازی خود زمینه‌ساز مداخله در امور حاکمیتی دولت ایرلند است که دیتاسنتر ذخیره‌کنندهٔ اطلاعات و محتویات مبادلات الکترونیک کاربران شرکت مایکروسافت را در اختیار دارد. صرف‌نظر از اینکه ایجاد رویهٔ قضایی بر تجویز دسترسی ایالات متحده به اطلاعات ذخیره‌شده در دیتاسنترهای فراسرزمینی به صدور احکام مشابه از سوی دادگاه‌های داخلی سایر کشورها بر افشای اطلاعات ذخیره‌شده در دیتاسنترهای مستقر در قلمرو سرزمینی ایالات متحده منجر خواهد شد. بی‌تردید رویکرد دادگاه بخش ایالات متحده برخلاف رویکرد شعبهٔ تجدیدنظر سبب از بین رفتن همکاری‌های بین‌المللی در زمینهٔ تحقیقات کیفری می‌شود. حال آنکه ابزار معاهدات همکاری حقوقی متقابل برای جلوگیری از مداخله در امور داخلی کشورها پیش‌بینی شده است تا با رعایت الزامات قانونی طرفین هم هدف دسترسی به اطلاعات فرامرزی محقق شود و هم مداخله در امور داخلی سایر کشورها صورت نگیرد. البته مسیر همکاری‌های بین‌المللی در امور کیفری نیز با چالش‌هایی مواجه است. لیکن این چالش‌ها به‌مراتب از آرای کیفری مشکوک به مداخله در امور حاکمیتی سایر دولت‌ها با هزینهٔ کمتری در عرصهٔ بین‌الملل مواجه است. از طرف دیگر، درصورتی‌که قوانین داخلی دولت تقاضاشونده بر ممنوعیت افشا و انتقال دیتا به سرزمین دولت تقاضاکنندهٔ اطلاعات الکترونیک باشد، باز هم زمینهٔ همکاری

حقوقی متقابل در امور کیفری با بن‌بست مواجه می‌شود. لیکن راهکار مقابله با آن توسل به قوانین داخلی بر دسترسی به دیتای ذخیره‌شده در قلمرو فراسرزمینی نیست، بلکه راهکار آن ذخیرهٔ اطلاعات اتباع داخلی در دیتاسنترهای درون‌سرزمینی است. اعمال حاکمیت درون‌سرزمینی جوازی بر الزام شرکت‌های فعال در زمینهٔ ارتباطات الکترونیک بر استقرار دیتاسنترهای ذخیره‌کنندهٔ دیتای کاربران متبوع دولت سرزمینی است. دولت میزبان شعبهٔ نمایندگی شرکت‌های فراملی می‌تواند حضور و فعالیت نمایندگی را مشروط به استقرار دیتاسنترهای ذخیره‌کنندهٔ دیتای اتباع داخلی در قلمرو سرزمینی متبوع کند تا در صورت لزوم دسترسی آن به دیتای ذخیره‌شدهٔ درون‌سرزمینی حسب بایسته‌های اعمال حاکمیت داخلی میسر باشد. با وجود این بر سر راه تحقیقات کیفری سایبری در فضای ابر موانعی وجود دارد. اطلاعات الکترونیک در فضای ابررایانش با ابزارهای امنیتی و گذرواژه از دسترس عموم خارج شده‌اند و فقط برای کاربر یا شرکت پشتیبانی‌کنندهٔ سرور آن قابل دسترسی‌اند. در این حالت دسترسی به اطلاعات برای پلیس غیرممکن است، مگر اینکه بدان نفوذ غیرمجاز شود. سازوکار همکاری‌های پلیسی در این حوزه نیز مسدود است، چراکه پلیس دولت خارجی دارندهٔ دیتاسنتر اگر بخواهد اطلاعات الکترونیک را از طریق فضای مجازی تحت وب به خارج از مرزهای سرزمینی دولت متبوع ارسال کند، ممکن است مرتکب جرم جاسوسی یا اقدام علیه مصالح دولت متبوع شده باشد. اعم از اینکه پلیس خارجی این اطلاعات را به سرزمینی بفرستد که از آنجا یا توسط تبعهٔ آن به سرور ارسال و ذخیره شده است یا اینکه آنها را به سرزمین دولت ثالث بفرستد. زمانی‌که اجماع عمومی دولت‌ها در عرصهٔ بین‌الملل در قالب معاهدات بین‌المللی در نحوهٔ برخورد با اطلاعات ذخیره‌شده در فضای ابر حاصل شود، این اشکال مرتفع می‌شود، در غیر این صورت یکجانبه‌گرایی دولت‌ها اگرچه می‌تواند در الزام شرکت‌های الکترونیک مستقر در قلمرو سرزمینی یا دیتاسنترهای سرزمینی کارساز باشد، لیکن این رویکرد در خصوص شرکت‌های چندملیتی یا فراسرزمینی یا ذخیره‌کنندهٔ اطلاعات کاربران در دیتاسنترهای مستقر در کشورهای متفاوت با بن‌بست مواجه است، وقتی‌که الزام شرکت‌های درون‌سرزمینی برای افشای دیتای ذخیره‌شده در دیتاسنتر فراسرزمینی با ممنوعیت دولت سرزمینی محل استقرار دیتاسنتر روبه‌روست.

منابع

۱. فارسی

الف) مقالات

۱. بهره‌مند، حمید (۱۳۹۶)، «چالش‌های مقررات تعدد جرم در جرائم سایبری»، *مجلهٔ حقوقی*

دادگستری، ش ۱۰۰، صص ۵۳-۶۶.
۲. پورقهرمانی، بابک (۱۳۹۶)، «مطالعهٔ تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرائم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست»، *پژوهشنامهٔ حقوق کیفری*، ش ۱۵، صص ۱-۳۶.
۳. حبیبی، همایون؛ شاملو، سوده (۱۳۹۲)، «نقش دیوان بین‌المللی دادگستری در توسعهٔ حقوق بین‌الملل»، *فصلنامهٔ پژوهش حقوق عمومی*، ش ۴۱، صص ۷۱-۱۱۴.
۴. جلالی، محمود؛ توسلی اردکانی، سعیده (۱۳۹۸)، «ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرائم در فضای مجازی»، *مطالعات حقوق عمومی*، ش ۴، صص ۱۳۵۱-۱۳۷۲.
۵. رضوی‌فرد، بهزاد؛ موسوی، نعمت‌اله (۱۳۹۶)، «محدودیت‌ها و راهبردهای صلاحیت در جرائم سایبری»، *مجلهٔ حقوقی دادگستری*، ش ۹۸، صص ۸۳-۱۰۲.
۶. شهبازی، آرامش؛ آقاجانی رونقی، آیدا (۱۳۹۹)، «جاسوسی سایبری در حقوق بین‌الملل: مسئلهٔ انتساب مسئولیت بین‌المللی به دولت در هاله‌ای از ابهام»، *مطالعات حقوق عمومی*، ش ۴، صص ۱۴۸۷-۱۵۰۳.
۷. وطنی، امیر؛ اسدی، حمید (۱۳۹۵)، «سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم»، *پژوهشنامهٔ حقوق اسلامی*، ش ۴۴، صص ۹۹-۱۲۶.

۲. انگلیسی

A) Books

1. Currie, J. Robert & Rikhof, Joseph (2013), *International and Transnational Criminal Law*, 2nd ed., Irwin Law.
2. Koops, B. Jaap & Goodwin, Morag (2014), 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation the Limits and Possibilities of International Law', Tilburg Law School Legal Studies Research Paper, Tilburg University.

B) Articles

3. Bahremand, Hamid (2018), "Challenges of Concurrence of Crimes Regulations in Cybercrime", *The Legal Journal of Justice*, Vol. 81, No. 100, pp. 53-66 (in Persian).
4. Chander, Anupam & Uyen P. Le (2015), "Data Nationalism", *Emory Law Journal*, Vol. 64(3).
5. Chertoff, Michael (2017), "Opinion: Data Localization is Misguided", *The Chertoff Group*. Available at ;https://www.chertoffgroup.com/blog/opinion-data-localization-is-misguided.

6. Daskal, Jennifer (2016), "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues", *The Journal of the ACS Issue Briefs*, Vol. 11, pp. 45-57.
7. Daskal, Jennifer (2017), "Access to Data Across Borders: The Critical Role for Congress to Play Now", *American Constitution Society for Law and Policy*.
8. Fijnaut, Cyrille (2012), "The Globalisation of Police and Judicial Cooperation: Drivers, Substance and Organisational Arrangements, Political Complications", in Saskia Hufnagel, Clive Harfield, and Simon Bronitt (eds.), *Cross-border Law Enforcement: Regional Law Enforcement Cooperation European, Australian and Asia Pacific Perspectives*, Routledge.
9. Finklea, M. Kristin (2013), "The Interplay of Borders, Turf, Cyberspace and Jurisdiction; Issues Confronting Us Law Enforcement", *Congressional Research Service Report for Congress'*, No. 7-5700, , Available at: https://fas.org/sgp/crs/misc/R41927.pdf.
10. Green, Y. Jason (2015), "Railing Against Cyber Imperialism: Discussing the Issues Surrounding the Pending Appeal of United States V. Microsoft Corp.", *North Carolina Journal of Law & Technology*, Vol. 16.
11. Habibi, Homayoon & Shamloo, Soodeh (2014), "The Role of the ICJ in the Development of International Law", *Journal of Public Law*, Vol. 14, No.41, pp. 71-114 (in Persian).
12. Heuvel, V. Katrina and Stephen F. Cohen (2014), *Edward Snowden: A 'Nation' Interview*.
13. Hsiao, Russell (2015), "Implications for the Future of Global Data Security and Privacy: the Territorial Application of the Stored Communications Act and the Microsoft Case", *Catholic University Journal of Law & Technology*, Vol. 24, No.1.
14. Hufnagel, Saskia and Carole McCartney (2015), "Police Cooperation Against Transnational Criminals"; in Neil Boister and Robert J. Currie, *Handbook of Transnational Criminal Law*, Routledge.
15. Jalali, Mahmoud & Tavassoli Ardakani, Saeede (2020), "Necessity of Establishment of an International Harmonized Legal System against Crimes in Cyberspace", *Public Law Studies Quarterly*, Vol. 49, No.4, pp. 1351-1372 (in Persian).
16. Mozur, Paul; Daisuke Wakabayashi and Nick Wingfield (2017), *Apple Opening Data Center in China to Comply with Cybersecurity Law*, New York Times.
17. Narayanan, Vineeth (2012), "Harnessing the Cloud: International Law Implications of Cloud-Computing", *Chicago Journal of International Law*, Vol. 12, No.2.
18. Pourghahramani, Babak (2017), "Comparative Study of Strategies to Protect Victims of Computer Crimes in the Criminal Law of Iran and International Documents with Emphasis on the Budapest Convention", *Journal of Criminal Law Research*, Vol. 8, No.1, pp. 1-36 (in Persian).
19. Razavifard, Behzad & Mousavi, Neamat Allah (2017), "Limitations and Strategies of Jurisdiction in Cybercrimes", *The Legal Journal of Justice*, Vol. 81, No. 98, pp. 83-102 (in Persian).
20. Scassa, Teresa & Robert J. Currie (2011), "New First Principles? Assessing the

Internet's Challenges to Jurisdiction", *Georgetown Journal of International Law*, Vol. 42.
21. Selby, John (2017), "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?", *International Journal of Law and Information Technology*, Vol. 25(3), Vol. 25, No. 3, pp. 213-232.
22. Shahbazi, Aramesh & Ronaghi, Aida Aghajani (2021), "Cyber Espionage in International Law: Attribution of International Responsibility to States in a State of Uncertainty", *Public Law Studies Quarterly*, Vol. 50, No.4, pp. 1487-1503 (in Persian).
23. Swire, Peter & Justin D. Hemmings (2017), "Mutual Legal Assistance in an Area of Globalized Commc'ns: The Analogy to the Visa Waiver Program", *N.Y.U. Annual Survey American Law*, Vol. 71.
24. Vatani, Amir & Asadi, Hamid (2016), "Criminal Policy of the Islamic Republic of Iran in Dealing with Cyber Crimes", *Islamic Law Research Journal*, Vol. 17, No.44, pp. 99-126 (in Persian).
25. Vincent, Mark & Nick Hart (2011), "Law in the Cloud: Legal Issues Relating to the Location of Data, Security and Reliability", *Law Society Journal: Official Journal of the Law Society of New South Wales*, Vol. 49, No.5, pp .50-55.

C) Cases and Documents

26. Microsoft Corp. v. United States (2016), In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained, No. 829 F.3d.
27. Microsoft Corp. v. AT&T Corp. (2007), No. 550 U.S.
28. United States v. Microsoft Corp. (2014), In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, No. 2014 WL 1661004.