شناسهٔ دیجیتال (DOI): 10.22106/JLJ.2020.115984.2978

مقالهٔ پژوهشی، سال ۸۴، شمارهٔ ۱۱۱، پاییز ۱۳۹۹، صفحات ۱۴۷ الی ۱۷۲
تاریخ دریافت: ۱۳۹۸/۰۷/۲۷ - تاریخ پذیرش: ۱۳۹۹/۰۲/۱۳

قانون کِلود: از کارکرد تا دستاوردها و نقایص آن در تحقیقات کیفری فراسرزمینی در حامل دیتای کاربران شرکت‌های فناوری

جواد صالحی*

چکیده

دولت ایالات متحده به‌زعم خویش با تصویب و اجرای قانون کِلود، بعد از شکست در پروندهٔ مایکروسافت پیش‌روی محاکم کیفری داخلی، درصدد عبور از این محدودیت‌ها بر اساس قانون داخلی است. این وضعیت تجربه‌ای است که دستاوردهای آن پیش‌روی سایر کشورها قرار گرفته است تا از ابعاد منفی آن احتراز شود. لذا بررسی ابعاد حقوقی قانون کِلود، از کارکرد تا دستاوردها و نقایص آن در تحقیقات کیفری فراسرزمینی در اَبررایانش شرکت‌های فناوری، موضوع و از اهداف این نوشتار است که با رویکرد توصیفی‌تحلیلی و انتقادی مدنظر قرار گرفته است. سؤال اصلی پژوهش این است که کارکرد و دستاوردهای قانون کِلود در نظام عدالت کیفری ایالات متحده و سایر دولت‌ها برای پیشبرد تحقیقات کیفری فراسرزمینی در اَبررایانش و نقایص آن چیست. یافته‌های پژوهش نشان می‌دهد که قانون کِلود به هرحال دولت ایالات متحده را به هدف اصلی وی برای دسترسی به دیتای ذخیره‌شدهٔ کاربر اَبررایانش در حامل دیتای فراسرزمینی می‌رساند. اما دسترسی به دیتای کاربر اَبررایانش در این شرایط هم متأثر از نادیده‌گرفتن محدودیت‌های ناشی از اصل حاکمیت درون‌سرزمینی و اصل ممنوعیت مداخله در امور دولت خارجی است که این بار در هیئت قانون داخلی ایالات متحده توجیه شده است، ولی به‌دلیل نقض محدودیت‌های حریم خصوصی کاربرانِ اَبررایانش مجاز و مقبول نشده است.

واژگان کلیدی: قانون کِلود ایالات متحده، دیتای کاربر اَبررایانش، تحقیقات کیفری فراسرزمینی، محدودیت اصل حاکمیت درون‌سرزمینی، اصل ممنوعیت مداخله در امور دولت خارجی

* دانشیار گروه حقوق، دانشگاه پیام نور تهران، تهران، ایران Javadsalehi@pnu.ac.ir

مقدمه

اطلاعات یا دیتا در جوامع مدرن یکی از کالاهای باارزش در مالکیت یا تصرف انسان است. ولی دولت‌ها در راستای اعمال حاکمیت درون‌سرزمینی تمایل دارند که حفاظت و مدیریت دیتای اتباع در اینترنت را در اختیار داشته باشند. لیکن این خواستهٔ دولت‌ها با سازوکار اَبرایانش[1] مسلوب است. ابرایانش یکی از حوزه‌های در حال‌توسعهٔ فناوری اطلاعات در فضای مجازی است. ساختار ابرایانش به‌نحوی است که شرکت‌های فناوری می‌توانند دیتای کاربران خود را با بهره‌گیری از آن در دیتاسنتر[2] (حامل یا حامل دیتا) مستقر در محلی دور از محل اقامت کاربران یا دور از محل استقرار مرکز اصلی فعالیت شرکت ذخیره کنند. از این حیث، دیتا در این شرایط در ابرایانش از دستگاه رایانه یا گوشی همراه کاربر به سرورهای[3] قابل‌کنترل برای شرکت فناوری از راه دور منتقل می‌شود (Schwartz, 2018: 1682) و بدین‌طریق از دسترس دولت متبوع کاربر خارج است. این وضعیت به یک اعتبار ضامن رعایت الزامات حریم خصوصی کاربر است، در جایی‌که شائبهٔ نقض مقررات از سوی دولت سرزمینی محل استقرار مرکز اصلی فعالیت شرکت فناوری یا دولت متبوع کاربر وجود دارد. فعالیت پلیس زیرنظر دولت ایالات متحده نمونه‌ای از این شرایط است. پلیس ایالات متحده اغلب خواهان آن است تا بدون رعایت سازوکار قضایی و اخذ مجوز خاص قضایی به دیتای کاربر در ابرایانش دسترسی یابد، در جایی که تحقیقات اولیهٔ کیفری وی ایجاب می‌کند. اما قانون هم پلیس ایالات متحده را محدود می‌کند و هم تحقیقات کیفری فراسرزمینی را از منظر وی مختل می‌کند. اما ایراد از قانون نیست؛ ایراد از ماهیت دیتا و ذخیرهٔ آن در حامل فراسرزمینی است که از حاکمیت قانون و دسترس پلیس در انجام تحقیقات کیفری خارج شده است. عبور از این وضعیت همکاری فراقانونی شرکت فناوری با پلیس را می‌طلبد که بنا به معذوریت حمایت از حریم خصوصی کاربر ابرایانش مفقود است.

ذخیرهٔ دیتا در حامل فراسرزمینی[4] به باور برخی ناشی از جهانی‌شدن دیتاست که بر روند تحقیقات کیفری تأثیر منفی گذاشته است (Swire, Hemmings and Vergnolle, 2016: 327). این وضعیت با جهانی‌شدن جرایم و نقض فاحش امنیت ملی و بین‌المللی و ضرورت تنظیم سیاست جنایی جهانی برای تضمین امنیت حداکثری نیز در ارتباط است (نک: قناد و اکبری، ۱۳۹۶: ۳۹)، چراکه استفاده از ابرایانش یکی از امکانات پیش‌روی بزهکاران است تا آن‌ها نیز مستندات

1. Cloud Computing.
2. Data Centers.
3. Companies' Servers.
4. Data Centers Overseas.

فعالیت‌های مجرمانه خویش را از طریق ارتباطات الکترونیک در حامل فراسرزمینی دیتا ذخیره و نگهداری کنند (Mulligan, 2018: 1). وقوع جرم در قلمرو سرزمینی متفاوت از قلمرو سرزمینی محل استقرار حامل دیتا نتیجه‌ای است که دلایل مجرمانهٔ ثبت‌شده در حامل دیتا را از دسترس مقامات قضایی یا پلیسی خارج می‌سازد. حامل دیتا یا محل استقرار آن در سرتاسر دنیا در مالکیت یا اجارهٔ شرکت‌های فناوری است. استفاده از حامل یا محل استقرار آن تابع قرارداد تنظیمی با دولت مالک حامل یا دولت سرزمینی محل استقرار آن است. این وضعیت هیچ ارتباطی به الزام یا عدم الزام شرکت فناوری در افشاء یا عدم افشای دیتای ذخیره‌شده در حامل از قلمرو سرزمینی محل استقرار مرکز اصلی فعالیت شرکت ندارد. تلاش مقامات قضایی دولت سرزمینیِ محل وقوع جرم در این شرایط برای دسترسی به محتوای ارتباطات الکترونیک افراد در قالب ایمیل یا پست‌های آن‌ها در شبکه‌های اجتماعی بخشی از فرایند تحقیقات کیفری فراسرزمینی است که معمولاً به حامل فراسرزمینی دیتا منتهی می‌شود که از اِعمال حاکمیت درون‌سرزمینی وی خارج است. مقامات پلیسی و قضایی در این شرایط با محدودیت صلاحیت کیفری سرزمینی و ممنوعیت تحقیقات کیفری در قلمرو فراسرزمینی و دسترسی به دیتای ذخیره‌شده در حامل فراسرزمینی از قلمرو سرزمینی متبوع مواجه هستند.

تکنولوژی ابررایانش باعث شده است که نحوهٔ ذخیرهٔ دیتا با شکسته‌شدن مرزها و توسعهٔ اِعمال صلاحیت دولت‌ها برای دسترسی به آن تغییر کند (Schultheis, 2015: 661). نظام عدالت کیفری ایالات متحده با تصویب و اتکای به قانونِ تبیین استفادهٔ قانون از داده‌های فراسرزمینی[1] (قانون کِلود) برای دسترسی به دیتای ذخیره‌شدهٔ فراسرزمینی و الزام شرکت فناوری دارای مرکز اصلی فعالیت در قلمرو سرزمینی متبوع به‌تبعیت از وی درصدد القای این مفهوم است. ایالات متحده با تصویب قانون کِلود درصدد تسهیل دسترسی به دلایل ذخیره‌شده در حامل‌های فراسرزمینی از طریق شرکت فناوری تحت حاکمیت و فائق‌آمدن بر موانع سرزمینی حاکم بر تحقیقات کیفری فراسرزمینی بدون نیاز به موافقت‌نامهٔ همکاری قضایی است. این در حالی است که تصویب قانون داخلی نافی ضرورت انعقاد موافقت‌نامهٔ همکاری بین‌المللی قضایی نیست، هرچند که به اتکای قانون داخلی برخی از همکاری‌ها صورت گیرد (شریعت‌باقری، ۱۳۹۳: ۶۱). اما ایالات متحده با تصویب قانون کِلود درصدد است تا به دو خواستهٔ مرتبط با یکدیگر برای دسترسی به دیتای ذخیره‌شده فراسرزمینی نائل شود که بررسی ابعاد حقوقی آن، موضوع و از اهداف این نوشتار است. سؤال اصلی پژوهش این است که کارکرد و دستاوردهای قانون کِلود در نظام عدالت کیفری ایالات متحده و سایر دولت‌ها برای پیشبرد

1. Clarifying Lawful Overseas Use of Data (CLOUD Act).

تحقیقات کیفری فراسرزمینی در اَبررایانش و نقایص آن چیست. فرض بر این است که قانون کِلود واجد دو وضعیت است که اجرای هر دو بُعد آن با نقایصی مواجه است که دستاوردهای آن را ناچیز جلوه می‌دهد. لذا در این نوشتار ابتدا به تحقیقات کیفری و ضرورت دسترسی دولت‌ها به دیتای کاربران اَبررایانش پرداخته و در ادامه به رویکرد شرکت‌های فناوری در افشای دیتای کاربر اَبررایانش در حامل فراسرزمینی و سپس به الزامات ناشی از قانون ارتباطات ذخیره‌شده و ضرورت تغییر آن در قانون کِلود می‌پردازیم تا نتایج تطبیقی حاصل از این مطالعه به علاقه‌مندان حوزهٔ فناوری اطلاعات و رعایت اصول حاکم بر آن و حریم خصوصی کاربر اَبررایانش در قلمرو تحقیقات کیفری فراسرزمینی ارائه شود.

۱. تحقیقات کیفری و ضرورت دسترسی دولت‌ها به دیتای کاربران ابررایانش

اَبررایانش یکی از حوزه‌های در حال‌توسعه تکنولوژی اطلاعات است. دیتای کاربر در ابررایانش از گوشی تلفن‌همراه یا لپ‌تاپ به سرورهای قابل‌کنترل از راه دور برای شرکت فناوری با تنظیمات مختلف منتقل و ذخیره می‌شود. سرورهایی که دیتای کاربر را پشتیبانی می‌کنند از سوی شرکت فناوری در سرتاسر دنیا شبکه می‌شوند. هریک از سرورها بخشی از ابررایانش جهانی هستند و محتوای ذخیره‌شده در آن‌ها از تمام دنیا در دسترس کاربر ابررایانش است که از طریق نام کاربری و رمز عبور میسر است. از این‌رو، دیتای کاربر ابررایانش شرکت‌های اپل، گوگل یا مایکروسافت از دسترسی و کنترل دولت‌ها خارج است. این وضعیت موجد چالش‌های متعددی برای مقامات قانونی در دسترسی به اطلاعات ذخیره‌شده در حامل فراسرزمینی دیتا شده است. مقامات قانونی حسب قوانین داخلی امکان دسترسی به اطلاعات ذخیره‌شدهٔ کاربران فضای مجازی در حامل‌های فراسرزمینی دیتا را ندارند. این شرایط موجب نگرانی مقامات قانونی در تأمین امنیت ملی و تعقیب جرایم و دسترسی به دلایل مجرمانه آن در حامل فراسرزمینی دیتاست که جلوه‌ای از پیوند عدالت کیفری و امنیت ملی است. مسئلهٔ اصلی در این شرایط عدم دسترسی به حامل فراسرزمینی دیتا و انتقال اطلاعات آن برای تکمیل تحقیقات کیفری در قلمرو سرزمینی است. این وضعیت بر امنیت ملی تأثیرگذار است. به‌عنوان نمونه، جرم جاسوسی رایانه‌ای یکی از جرایم مرتبط با فضای مجازی و امنیت ملی است که با همین شرایط مواجه است (نک: محمدنسل، ۱۳۹۵: ۴۰).

ابررایانش تحت مدیریت شرکت‌های دارای تابعیت ایالات متحده و مشمول صلاحیت قضایی مرتبط است. اگرچه شرکت‌های ارائه‌کنندهٔ ابررایانش تابع اصل صلاحیت سرزمینی و قوانین دولت محل استقرار مرکز اصلی فعالیت خویش هستند، لیکن مشتریان آن‌ها فقط محدود به اتباع ایالات متحده نیستند و سرتاسر دنیا را پوشش می‌دهند. بنابراین عدم امکان دسترسی سایر دولت‌ها به دیتای اتباع خویش که از مشتریان این شرکت‌ها هستند و جواز دسترسی مطلق دولت ایالات متحده به

صرف تابعیت شرکت ارائه‌کنندهٔ ابررایانش یا سرزمینی‌بودن محل فعالیت آن‌ها مطلوب سایر دولت‌ها در سرتاسر دنیا نیست. دولت‌ها مدعی هستند که ذخیرهٔ دیتای اتباع آن‌ها در حامل‌های شرکت‌های متبوع ایالات متحده موجب نگرانی نقض حریم خصوصی شهروندی، نظارت خارجی و ممنوعیت دولت متبوع کاربر به دیتای تبعهٔ خویش شده است. کما اینکه به اعتقاد برخی نظارت بر عملکرد کاربران اینترنتی بدون اطلاع آن‌ها در ایالات متحده مسبوق به سابقه است (فتحی و شاهمرادی، ۱۳۹۶: ۲۳۹). البته وضعیت به این بدی هم نیست، چراکه شرکت‌های فناوری متبوع ایالات متحده تابع سیاست‌های حرفه‌ای و قراردادهای استفاده از حامل دیتا در سرتاسر دنیا از یک‌طرف و تابع شرایط توافق‌شده با کاربر در زمان ثبت‌نام و استفاده از ابررایانش از طرف دیگر هستند. پروندهٔ مایکروسافت در دیوان‌عالی و قطعیت شکست دولت ایالات متحده در دسترسی به دیتای کاربر نمونه‌ای از شرایط است. بر این اساس دولت ایالات متحده در دسترسی به دیتای کاربران این شرکت‌ها با محدودیت مواجه است، به‌نحوی که در برخی موارد حتی توسل به محاکم کیفری و قرار الزام شرکت فناوری به همکاری و افشای دیتای کاربر به پلیس یا دولت ایالات متحده نیز با بن‌بست مواجه شده است.

۱-۱. گزینه‌های پیش‌روی دولت‌ها برای دسترسی به دیتای کاربران ابررایانش

دولت‌ها درصدد بومی‌سازی و تصویب قوانین داخلی در ارتباط با دیتای اتباع برای رفع نگرانی‌های امنیت بین‌المللی هستند. این رویکرد مشترک دولت‌ها حاکی از تنظیم سیاست جنایی برای پاسخ به پدیدهٔ مجرمانه در ابررایانش است. دو تئوری برای رفع این نگرانی دولت‌ها وجود دارد: اول اینکه حامل فراسرزمینی دیتا به قلمرو سرزمینی کاربران آن منتقل شود. بر این اساس، دیتای کاربران ابررایانش از هر کشور به حامل دیتای همان کشور منتقل و ذخیره می‌شود. اما مخالفت با بالکانیزه‌شدن[1] شبکهٔ اینترنت جهانی از موانع اصلی این تئوری است (Swire and Kennedy-Mayo, 2017: 662). دوم اینکه الزام شرکت‌های فناوری بر اساس قوانین داخلی کشوری میسر باشد که مرکز فعالیت آن‌ها در قلمرو سرزمینی وی مستقر شده است (Schwartz and Peifer, 2017: 118). بر این اساس شرکت فناوری تابع مقررات دولت محل استقرار مرکز اصلی فعالیت است، هرچند که دیتای کاربران خویش را در حامل فراسرزمینی ذخیره و مدیریت کرده باشد. اما این رویکرد با منافع شرکت‌های فناوری در تضاد است که دارای کاربرانی از سرتاسر دنیا هستند و تاب پذیرش قوانین سرزمینی محل استقرار مرکز فعالیت شرکت فناوری را ندارند، صرف‌نظر از اینکه اکثر شرکت‌های فناوری در قلمرو سرزمینی ایالات متحده مستقر بوده و بر اساس تئوری دوم تابع مقررات

۱. تقسیم و تجزیهٔ نواحی به قطعات کوچک‌تر را گویند.

وی هستند. اکثر شرکت‌های فناوری از جمله گوگل و مایکروسافت دارای تابعیت و مرکز اصلی فعالیت در قلمرو سرزمینی ایالات متحده هستند، در حالی که کاربران آن‌ها از سرتاسر دنیا هستند. لذا اجرایی‌شدن گزینهٔ دوم باعث می‌شود تا شرکت‌های فناوری بخش زیادی از مشتریان خود را از سرتاسر دنیا از دست بدهند.

دسترسی مقامات قانونی ایالات متحده به دیتای ذخیره‌شدهٔ کاربران دارای ملیت‌های متفاوت این شرکت‌ها حسب الزام ناشی از گزینهٔ دوم فراهم است، در حالی که دسترسی مقامات قانونی دولت‌های متبوع کاربران این شرکت‌ها حسب گزینهٔ اول همچنان به دو دلیل میسر نیست: اول اینکه شرکت‌های فناوری متبوع ایالات متحده در استقرار حامل دیتا تابع سیاست‌های متفاوت دولت‌ها در سرتاسر دنیا نیستند تا حسب تقاضای آن‌ها دیتای اتباع آن‌ها را به حامل مستقر در قلمرو سرزمینی آن‌ها ارسال و ذخیره کنند؛ دوم اینکه سایر کشورها، بر فرض دراختیارگرفتن حامل دیتای کاربران ملی این شرکت‌ها در قلمرو سرزمینی، حق دسترسی به دیتای ذخیره‌شده بدون همکاری و مجوزهای قانونی از شرکت‌های فناوری حسب قوانین داخلی ایالات متحده را ندارند. درواقع در این شرایط استقرار حامل‌های دیتای کاربران ملی در قلمرو سرزمینی دولت متبوع آن‌ها امتیازی تلقی نمی‌شود، در حالی که شرکت فناوری آن دارای تابعیت و مرکز اصلی فعالیت در قلمرو سرزمینی ایالات متحده است. این وضعیت باعث می‌شود تا دولت متقاضی دیتای کاربر ملی از شرکت فناوری با وجود دراختیارداشتن حامل دیتا در قلمرو سرزمینی از مقررات ایالات متحده تبعیت کند که در اکثر موارد با ممنوعیت دسترسی مواجه است.

تبعیت دولت سرزمینی محل استقرار حامل دیتا از مقررات ایالات متحده با اصل حاکمیت درون‌سرزمینی وی و تبعیت از قوانین خارجی راجع به مسائل داخلی منافات دارد. دولت ایالات متحده در این ارتباط نیز در وضعیت مشابه قرار دارد، با این تفاوت که شرکت‌های فناوری در قلمرو سرزمینی وی دارای مرکز اصلی فعالیت هستند، ولی حامل‌های ذخیره‌کنندهٔ دیتای کاربران خویش را در سرتاسر دنیا مستقر کرده‌اند. الزام شرکت‌های فناوری از سوی محاکم ایالات متحده به افشای محتوای ارتباطات الکترونیک کاربران از یک‌طرف با تعهدات آن‌ها در قبال کاربران و لزوم رعایت حریم خصوصی آن‌ها و از طرف‌دیگر با تعهدات آن‌ها در قبال دولت خارجی محل استقرار حامل دیتا بر لزوم کسب مجوز برای تبادل دیتای سرزمینی آن‌ها تداخل پیدا کرده است. این وضعیت ناشی از فراملی‌بودن جرایم فضای مجازی است (نک: دلخون‌اصل، گلدوزیان و کلانتری، ۱۳۹۸: ۱۳۶) که باعث شده است تا مقامات پلیسی و قضایی برای دسترسی به دیتای ذخیره‌شدهٔ کاربران این شرکت‌ها نیز با مشکلات مشابه سایر دولت‌ها مواجه باشند، هرچند که شرکت‌های فناوری در قلمرو

سرزمینی آن‌ها مستقر هستند و از این حیث نسبت به سایر دولت‌ها دارای امتیازند. اما این امتیاز با حربهٔ اصل سرزمینی‌بودن قوانین کیفری برای آن‌ها کارآمد نیست. شرکت‌های فناوری معتقدند که مقامات قانونی و به طریق اولی محاکم کیفری نمی‌توانند آن‌ها را به استناد قوانین کیفری داخلی ملزم به افشای دیتای کاربران ابررایانش نمایند، در حالی که دیتا در حامل‌های فراسرزمینی ذخیره شده‌اند.

اصل سرزمینی‌بودن قوانین و مکانیزم‌های دسترسی به دیتای ذخیره‌شده در حامل‌های فراسرزمینی مسئله‌ای است که باید برای آن چاره‌اندیشی شود. گزینه‌های متعددی در اعمال صلاحیت سرزمینی وجود دارد که شامل محل استقرار دیتا، محل اقامت کاربر، محل استقرار مرکز اصلی فعالیت شرکت میزبان دیتا می‌باشند. گزینهٔ جایگزین برای پوشش‌دادن اِعمال صلاحیت سرزمینی و دسترسی به دیتای ذخیره‌شده در حامل‌های فراسرزمینی شامل الزام شرکت‌های متبوع ایالات متحده در زمان طراحی شبکه به‌نحوی است که آن‌ها از قلمرو سرزمینی و بدون کسب مجوز از دولت سرزمینی حامل به دیتای ذخیره‌شده دسترسی و حق برداشت و افشاء به مقامات سرزمینی محل استقرار مرکز اصلی فعالیت یعنی ایالات متحده را داشته باشند، منوط به اینکه دولت سرزمینی محل استقرار حامل دارای چنین امتیازی نباشد، چراکه دیتا متعلق به کاربران شرکت متبوع ایالات متحده است که از مرکز اصلی پردازش و مدیریت شده و برای ذخیره به حامل فراسرزمینی هدایت می‌شود. اجارهٔ حامل‌های فراسرزمینی موجد حقی برای دولت مؤجر به‌منظور دسترسی به دیتای ذخیره‌شده در حامل سرزمینی خویش نیست. در عین‌حال این وضعیت منصرف از حق دسترسی دولت‌های خارجی به دیتای کاربران شرکت‌های متبوع ایالات متحده است. هریک از دولت‌های خارجی حسب صلاحیتی که نسبت به دیتای کاربران شرکت‌های فناوری متبوع ایالات متحده پیدا می‌کنند حق دارند دسترسی به دیتای ذخیره‌شدهٔ شرکت‌های فناوری متبوع ایالات متحده را تقاضا کنند، ولو اینکه دیتا در قلمرو سرزمینی دیگری ذخیره شده باشد. این وضعیت با عدم حق دسترسی دولت سرزمینی محل استقرار حامل نیز تشدید و توجیه می‌شود. دولت محل استقرار حامل نه‌تنها حق دسترسی به دیتای ذخیره‌شده در حامل تحت حاکمیت سرزمینی ندارد، بلکه حق افشای آن را بدون کسب مجوز از شرکت فناوری یا مجوزهای لازم از محاکم دولت متبوع مرکز اصلی فعالیت شرکت فناوری ایالات متحده به طریق اولی ندارد. لذا باید سازوکاری برای الزام شرکت‌های متبوع ایالات متحده بر افشای دیتا بر اساس قرار محاکم دولت‌های خارجی یا بر اساس معاهدات همکاری حقوقی دوجانبه نیز وجود داشته باشد.

اما این شرایط میان دولت ایالات متحده و هریک از دولت‌های عضو اتحادیهٔ اروپا سالب به انتفاء موضوع است. مقررات عمومی اتحادیهٔ اروپا راجع به حفاظت از داده[1] نمونه‌ای از این وضعیت است. اتحادیهٔ اروپا مُصر به لزوم تبعیت شرکت‌های فناوری در حفاظت از دیتای کاربران تبعهٔ اتحادیهٔ اروپا در مقابل دولت‌های غیراروپایی از جمله ایالات متحده است. تصویب قانون کلود ناخواسته این نگرانی را برطرف کرده است، چراکه شرکت‌های فناوری به‌موجب آن حق دارند که با استناد به قوانین دولت محل استقرار مرکز اصلی فعالیت و با ادعای نقض احتمالی حریم‌خصوصی کاربران از دسترسی دولت ایالات متحده به دیتای ذخیره‌شدهٔ فراسرزمینی کاربران خویش جلوگیری کنند. این وضعیت منجر به لزوم توسل ایالات متحده به سازوکار معاهدهٔ همکاری حقوق دوجانبه می‌شود که سابق بر این نیز امکان آن وجود داشت، لیکن ایالات متحده به استفاده از آن به دلیل محدودیت‌های آن تمایلی نداشت، چراکه تجربهٔ همکاری ایالات متحده و اتحادیهٔ اروپا از این طریق برای دسترسی به دیتای ذخیره‌شدهٔ کاربران فضای مجازی با بن‌بست مواجه شده بود؛ زمانی که ایالات متحده با ادعای حمایت از تبعهٔ ایالات متحده و اتحادیهٔ اروپا نیز با ادعای حمایت از تبعهٔ اتحادیهٔ اروپا از افشای دیتای ذخیره‌شدهٔ کاربران متبوع خودداری می‌کردند.

۲-۱. لزوم همکاری دولت‌ها برای دسترسی به دیتای کاربر ابررایانش

حریم خصوصی کاربر ابررایانش موضوع مقررات اصلاحیهٔ چهارم قانون اساسی ایالات متحده است. الزامات ناشی از اصلاحیهٔ چهارم قانون اساسی نسبت به اتباع ایالات متحده در قلمرو فراسرزمینی با توجه به بایسته‌های صلاحیت و قوانین سرزمینی محل تحقیقات کیفری و بازرسی لازم‌الاجراء است، لیکن رعایت این الزامات در ارتباط با تحقیقات کیفری فراسرزمینی همیشه صادق نیست. رعایت این الزام در تحقیقات کیفری فراسرزمینی و دسترسی به متعلقات واجد حریم خصوصی متهم از این طریق فقط مربوط به زمانی است که ارتباط اختیاری وی، شمول یا تبعیت وی از قوانین ایالات متحده برقرار باشد. بدین‌معنا که متهم تابعیت ایالات متحده را داشته باشد و تحت شمول یا تبعیت از قوانین کیفری ایالات متحده قرار گرفته باشد تا الزامات ناشی از مقررات اصلاحیهٔ چهارم قانون اساسی نسبت به وی مجری باشد. در شرایطی که متهم تابعیت ایالات متحده را نداشته باشد، برای انجام تحقیقات کیفری و بازرسی‌های لازم از وی در قلمرو فراسرزمینی به قرار یا حکم محاکم کیفری ایالات متحده نیازی نیست.

1. EU General Data Protection Regulation.

دولت ایالات متحده برای انجام تحقیقات کیفری نسبت به غیراتباع در قلمرو فراسرزمینی مشمول محدودیت‌های قانونی نیست. بر این اساس تحقیقات کیفری از اشخاص دارای تابعیت یا اموال متعلق به ایالات متحده یا بازرسی آن‌ها در قلمرو فراسرزمینی نیازمند مجوزهای قانونی از محاکم کیفری ایالات متحده است (United States v. Verdugo-Urquidez, 1990: 259). تحقق این وضعیت نه‌تنها باعث دسترسی ایالات متحده به حامل‌های فراسرزمینی، بلکه باعث دسترسی سایر دولت‌ها به حامل‌های مستقر در ایالات متحده هم می‌شود. این رویکرد با شعار مبارزه و پیشگیری از جرایم تروریستی برای تمام دولت‌ها توجیه‌پذیر است، چراکه دولت‌ها هریک بر اساس قوانین داخلی از یک‌طرف قائل به الزام شرکت‌های فناوری در همکاری با آن‌ها به افشای دیتای کاربران خویش هستند، وقتی که آن کاربر از اتباع دولت متقاضی هست. ولی از طرف دیگر خواهان عدم افشای دیتای کاربران به سایر دولت‌ها هستند، زمانی‌که آن کاربر از اتباع دولت متقاضی نیست. این سیاست یک بام و دو هواست. بر این اساس دولت‌ها از شرکت‌های فناوری می‌خواهند که دیتای کاربران خویش را از دسترسی سایر دولت‌ها محفوظ نگه دارند، وقتی که آن کاربر از اتباع دولت متقاضی نیست. در حالی که مبنای دسترسی دولت متبوع به دیتای کاربر شرکت فناوری شعار مبارزه و پیشگیری از جرایم تروریستی است که وقوع آن در هر نقطه از دنیا و از سوی هر تبعه‌ای محتمل است. در این شرایط فرقی میان تبعهٔ داخلی و تبعهٔ خارجی نیست.

بر این اساس تبعیت شرکت‌های فناوری از دستورات و دسترسی مقامات دولت ایالات متحده به دیتای ذخیره‌شده فراسرزمینی کاربران خویش منوط به سازوکارهای بین‌المللی یکسان برای تمام دولت‌هاست (نک: جلالی و توسلی اردکانی، ۱۳۹۸: ۱۳۵۱). حق دسترسی دولت ایالات متحده به دیتای کاربران با هر توجیه در جایی پذیرفتنی است که سایر دولت‌ها هم با توجیه مشابه از چنین حقی برخوردار باشند. این در حالی است که هیچ موافقت‌نامهٔ الزام‌آوری بر لزوم رعایت یا نادیده‌گرفتن بایسته‌های حریم خصوصی کاربران فضای مجازی در عرصهٔ بین‌المللی وجود ندارد، ولو اینکه منافع امنیت ملی دولت‌ها موضوعیت داشته باشد. بنابراین اعمال صلاحیت مأموران قانونی یک دولت در قلمرو سرزمینی دولت دیگر منوط به رضایت و انجام آن اقدامات توسط مأموران دولت اخیر (دولت سرزمینی) است. ورود و اقدامات عملیاتی مأموران دولت متقاضی در قلمرو سرزمینی دولت دیگر با ممنوعیت ناشی از اصل حاکمیت و اِعمال مقتضیات آن توسط عوامل دولت سرزمینی است. اگر دولت متقاضی بتواند مقامات رسمی دولت سرزمینی را مجاب کند که به دیتای ذخیره‌شده در حامل سرزمینی وی برای شروع یا تکمیل تحقیقات کیفری در یک پروندهٔ داخلی دسترسی داشته

باشد، بر این اساس استخراج، توقیف یا ارائهٔ دیتا حسب صلاحدید از سوی مقامات رسمی دولت سرزمینی صورت می‌گیرد و نتایج آن به مقامات قانونی دولت متقاضی اعلام می‌شود.

مقامات ذی‌صلاح سرزمینی چه‌بسا به این نتیجه برسند که امکان افشای دیتا به مقامات رسمی دولت متقاضی نیست. در هر شرایط مقامات پلیسی دولتِ متقاضی حق ندارند که رأساً وارد قلمرو سرزمینی دولت دیگر شوند و اقدامات لازم را نسبت به حامل مستقر در این سرزمین انجام دهند. ورود مقامات رسمی دولت مقاضی اعم از ورود فیزیکی یا مجازی است. ورود از طریق اینترنت به‌نحو غیرمجاز یا هک‌کردن صفحات مجازی نیز مشمول این ممنوعیت است. این وضعیت راجع به شرایطی است که دولت متقاضی توانسته باشد رضایت دولت سرزمینی را برای دسترسی به دیتای ذخیره‌شده در حامل مستقر در قلمرو سرزمینی وی جلب کند. مقامات قانونی دولت متقاضی بدون کسب رضایت دولت سرزمینی محل استقرار حامل دیتا حق ورود ندارند، ولو اینکه ورود از نوع مجازی و از طریق اینترنت باشد. بدین‌معنا که مقامات دولت متقاضی بتوانند از قلمرو سرزمینی خویش به حامل دیتای دولت دیگر نفوذ کنند و مأموریت خویش را در کشف، استخراج و تصاحب دیتا انجام دهند. وضعیت اخیر نه‌تنها نقض حریم خصوصی کاربر شرکت فناوری است، بلکه مداخله در امور داخلی کشور دیگر است که در حقوق بین‌الملل نه‌تنها با ممنوعیت، بلکه با مسئولیت بین‌المللی دولت خاطی توأم است.

۲. رویکرد شرکت‌های فناوری در افشای دیتای کاربر ابررایانش در حامل فراسرزمینی

ارتباط‌دادن میان دستگاه‌های رایانه از طریق اینترنت برای نمایش دیتای ذخیره‌شده در حامل‌های فراسرزمینی به‌جای ذخیره در دستگاه‌های رایانه از قابلیت‌های اصلی ابررایانش است. این تکنولوژی با ذخیرهٔ ارتباطات الکترونیک کاربر در سرورهای سرویس‌دهنده و اجازه به گیرندهٔ مدنظر کاربر برای دسترسی به محتوای آن کار می‌کند. کاربر شرکت گوگل یا شرکت مایکروسافت از دستگاه رایانهٔ متصل به اینترنت به برقراری ارتباط الکترونیک می‌پردازد (Schwartz, 2013: 1633)، در حالی که پیام الکترونیک از رایانهٔ وی با مشخصات گیرندهٔ مدنظر به حامل فراسرزمینی سرویس‌دهندهٔ ایمیل منتقل و ذخیره می‌شود تا اینکه محتوی پیام در اولین فرصت در اختیار گیرندهٔ آن قرار گیرد. طراحی شبکه به ارادهٔ سرویس‌دهنده است که مکان و نحوهٔ ذخیرهٔ حجم گستردهٔ مبادلات الکترونیک کاربران را بر اساس اهداف و سیاست‌های سازمانی تعیین می‌کند (Schwartz, 2018: 1686). دیتا در ابررایانش با دو مدل شامل بومی‌سازی[1] و تقسیم‌سازی[2] ذخیره می‌شود. دیتای کاربر در الگوی

1. Data Localization.
2. Data Shard.

بومی‌سازی در سرورهای مستقر در قلمرو سرزمینی یک کشور ذخیره می‌شود که ممکن است با قلمرو سرزمینی محل استقرار مرکز اصلی فعالیت شرکت یکسان نباشد. شرکت مایکروسافت از این الگو تبعیت می‌کند. دیتای کاربر در الگوی تقسیم‌سازی به چند بخش تقسیم می‌شود و هر بخش دیتا در سرور جداگانه‌ای ذخیره می‌شود (Chander and Le, 2015: 719). تقسیم داده از این طریق و ذخیرهٔ آن در سرورهای متفاوت دارای مزایای امنیتی است.

دولت ایالات متحده برای دسترسی به دیتای ذخیره‌شده در حامل فراسرزمینی با مقاومت شرکت‌های فناوری مواجه است. شرکت‌های فناوری مخالف دسترسی مقامات دولتی هستند. آن‌ها مدعی هستند که دسترسی مقامات دولت ایالات متحده به دیتای کاربران آن‌ها ناقض الزامات حریم خصوصی کاربران و تعهدات شرکت در این رابطه است. هرچند که این شرکت‌ها دارای تابعیت و مستقر در خاک سرزمینی ایالات متحده هستند و از قوانین آن باید تبعیت کنند. با وجود این، دولت ایالات متحده برای نیل به این خواسته به محاکم کیفری متوسل می‌شود و برای الزام شرکت‌های فناوری قرار کیفری صادر می‌شود. لیکن قرار الزام شرکت‌های فناوری به افشای دیتای کاربر ابررایانش با بن‌بست مواجه می‌شود. از منظر دولت ایالات متحده این اِشکال ناشی از آن است که دیتای کاربران فضای مجازی در حامل‌های ایالات متحده ذخیره نمی‌شوند، بلکه در حامل‌های فراسرزمینی ذخیره می‌شوند که به‌جز از طریق همکاری شرکت‌های فناوری دسترسی به آن‌ها به‌دلیل فراسرزمینی‌بودن غیرممکن است. دسترسی به دیتای فراسرزمینی فقط برای شرکت فناوری طرف قرارداد حامل‌های دیگر کشورها میسر است.

شرکت‌های فناوری مانع اصلی دسترسی مقامات ایالات متحده به دیتای ذخیره‌شدهٔ کاربران در حامل‌های فراسرزمینی بدون طی‌کردن تشریفات همکاری دو یا چندجانبهٔ قضایی هستند. این در حالی است که شرکت‌های فناوری مانند مایکروسافت، گوگل و اپل از اتباع ایالات متحده و در قلمرو سرزمینی وی دارای مرکز اصلی فعالیت هستند. این شرکت‌ها از یک‌طرف تابع مقررات سرزمینی ایالات متحده قرار می‌گیرند، اما از طرف‌دیگر به‌لحاظ ممنوعیت‌های ناشی از قراردادهای شرکت با کاربران و دولت دارندهٔ حامل از افشای دیتای ذخیره‌شده به مقامات دولت محل استقرار مرکز اصلی فعالیت ممنوع هستند. افشای دیتای کاربران به مقامات دولت ایالات متحده برخلاف تعهدات شرکت فناوری بر رعایت الزامات حریم‌خصوصی کاربران از سرتاسر دنیا و عدم افشای آن به ثالث حتی با صدور حکم قضایی است. لذا تحقق این وضعیت در پروندهٔ مایکروسافت و صدور حکم به نفع این شرکت در محاکم کیفری تجدیدنظر و دیوان‌عالی ایالات متحده به مذاق مقامات پلیسی دولت ایالات متحده سازگار نیامده است. در حالی که ایالات متحده در پروندهٔ گوگل با شرایط مشابه

به‌خواستهٔ خود بر دسترسی به دیتای کاربران ابررایانش رسیده بود، هرچند که موفقیت وی ناشی از سیاست‌های حرفه‌ای شرکت گوگل در ذخیرهٔ دیتای کاربران ابررایانش بوده است.

۱-۲. شرکت مایکروسافت و الزام وی به افشای دیتای کاربران ابررایانش

شرکت مایکروسافت در مقابل قرار الزام دادگاه کیفری ایالات متحده بر افشای اطلاعات کاربری و محتوی ارتباطات الکترونیکِ احد از کاربران ابررایانش استدلال کرد که اطلاعات کاربر در سرورهای شرکت مایکروسافت در قلمرو سرزمینی ایالات متحده ذخیره شده است، لیکن محتوی ایمیل کاربر در حامل داپلین ایرلند ذخیره شده است که در اختیار شرکت مایکروسافت و دولت ایرلند است. شرکت مایکروسافت اگرچه توانایی دسترسی به دیتای ذخیره‌شده در حامل فراسرزمینی و ارائهٔ آن‌ها را به پلیس ایالات متحده داشت، لیکن با استدلال اینکه قرار دادگاه کیفری کارکرد فراسرزمینی ندارد، از همکاری با پلیس ایالات متحده امتناع کرد (صالحی، ۱۳۹۸: ۱۹۵). همین استدلال شرکت مایکروسافت در مقام اعتراض به رأی بدوی در مرحلهٔ تجدیدنظر مقبولیت یافت و مدنظر قضات دادگاه تجدیدنظر در عدم امکان الزام شرکت مایکروسافت در افشای دیتای کاربر ابررایانش قرار گرفت. مایکروسافت معتقد بود که الزام وی از سوی دادگاه کیفری به افشای دیتایی است که در حامل فراسرزمینی ذخیره شده است. این در حالی است که دسترسی به دیتای ذخیره‌شده در حامل فراسرزمینی مستلزم همکاری دولت ایرلند با دولت ایالات متحده است. عملکرد دولت ایالات متحده در دسترسی به دیتای حامل فراسرزمینی به اعتقاد برخی بدون جلب تمایل و همکاری دولت سرزمینی محل استقرار حامل دیتا با اصل حاکمیت سرزمینی و اصل ممنوعیت مداخله در امور سایر کشورها منطبق نیست (Brenner, 2010: 136).

القاء استدلال شرکت مایکروسافت در عدم همکاری با مقامات قانونی به‌معنای شکست پلیس دولت ایالات متحده در دسترسی به دیتای کاربر این شرکت بود. این رویکرد به‌معنای تضعیف توانایی مقامات قانونی و قضایی در کشف و تعقیب جرایم است (نک: طهماسبی و شاهمرادی، ۱۳۹۷: ۱۰۶-۱۰۵). اما دادگاه تجدیدنظر ایالات متحده در تأیید نظریهٔ شرکت مایکروسافت استدلال کرد که دولت بر اساس قانون ارتباطات ذخیره‌شده نمی‌تواند دسترسی به دیتای ذخیره‌شده در سرورهای خارجی را حتی از شرکت‌های فناوری دارای مرکز اصلی فعالیت در قلمرو سرزمینی ایالات متحده تقاضا کند (United States v. Microsoft Corp., 2017: 356)، چراکه دیتا در حامل فراسرزمینی ذخیره‌شده است و قانون داخلی ایالات متحده نسبت به آن کارایی ندارد. لذا الزام شرکت فناوری به افشای دیتای ذخیره‌شدهٔ فراسرزمینی، ولو اینکه از مرکز اصلی فعالیت در قلمرو سرزمینی ایالات متحده صورت گیرد، به‌معنای اعتبار بین‌المللی قائل‌شدن برای قوانین داخلی ایالات

متحده است که در مانحن‌فیه میسر نیست. قانون ارتباطات ذخیره‌شدهٔ ایالات متحده دارای کارکرد فراسرزمینی نیست تا محاکم داخلی بر اساس آن قراری را صادر کنند تا شرکت مایکروسافت بتواند در امور دولت خارجی دخل‌وتصرف کند. افشای دیتای ذخیره‌شده در حامل مستقر در قلمرو فراسرزمینی از امور مرتبط با دولت سرزمینی آن است و نسبت به شرکت مایکروسافت و دولت ایالات متحده عامل خارجی است.

دیتای ذخیره‌شده در حامل مستقر در قلمرو سرزمینی دولت ایراند از امور داخلی و تابع ارادهٔ وی است. بنابراین دولت ایالات متحده و محاکم کیفری آن بر اساس این قانون می‌توانند نسبت به امور داخلی و در قلمرو سرزمینی دخل‌وتصرف کند، در جایی که حامل دیتای شرکت مایکروسافت در قلمرو سرزمینی ایالات متحده مستقر باشد. این وضعیت با محدودیت اصل حاکمیت درون‌سرزمینی قوانین کیفری نیز منطبق است. اما دسترسی به دیتای ذخیره‌شدهٔ فراسرزمینی بر اساس این قانون، هرچند که از سوی شرکت مایکروسافت و در قلمرو سرزمینی ایالات متحده صورت گیرد، مداخله در امور و متعلقات دولت ایرلند بوده و با ممنوعیت ناشی از اصل ممنوعیت در امور داخلی دولت خارجی مواجه است. شرکت مایکروسافت به صرف تبعیت از قوانین و قرارهای محاکم کیفری ایالات متحده نمی‌تواند در امور داخلی دولت خارجی مداخله کند و ارادهٔ حاکم وی را نادیده بگیرد. بر این اساس دیوان‌عالی ایالات متحده در پروندهٔ مایکروسافت به لزوم اصلاح قانون ارتباطات ذخیره‌شده اذعان کرد تا بر اساس اصلاحات جدید بتوان شرکت مایکروسافت را به افشای دیتای ذخیره‌شده در حامل فراسرزمینی ملزم کرد که از محل استقرار مرکز اصلی فعالیت شرکت در قلمرو سرزمینی ایالات متحده نسبت به آن‌ها مالکیت، دسترسی یا کنترل دارد.

۲-۲. شرکت گوگل و الزام وی به افشای دیتای کاربران ابررایانش

تقاضای دولت ایالات متحده بر افشای دیتای کاربر ابررایانش شرکت گوگل پیش‌روی دیوان‌عالی ایالات متحده نیز مسبوق به سابقه است، با این تفاوت که رویهٔ قضایی محاکم ایالات متحده در این پرونده متفاوت از پروندهٔ مایکروسافت است. الزام شرکت گوگل به افشای دیتای کاربر خویش در این پرونده به معنای کارکرد فراسرزمینی قانون ارتباطات ذخیره‌شده تلقی نشده است (United States v. Google, 2017: 725). در این پرونده مسئلهٔ مکان دسترسی شرکت گوگل به دیتای ذخیره‌شده و ارزیابی پلیس ایالات متحده از این دیتا برای تکمیل تحقیقات کیفری موضوعیت دارد که از محل مرکز اصلی فعالیت شرکت گوگل و از حامل دیتای مستقر در قلمرو سرزمینی ایالات متحده صورت می‌گیرد. این سوءبرداشت ناشی از ذخیرهٔ توأمان اطلاعات کاربر به‌نحو داخلی و بین‌المللی است. سیاست حرفه‌ای شرکت گوگل در نحوهٔ ذخیرهٔ اطلاعات و دیتای کاربران ابررایانش

از سیاست حرفه‌ای شرکت مایکروسافت متفاوت است. شرکت گوگل، برخلاف شرکت مایکروسافت، اطلاعات و دیتای کاربران را به‌صورت هم‌زمان در دو حامل سرزمینی و فراسرزمینی ذخیره می‌کند. از این منظر اِعمال صلاحیت کیفری سرزمینی و اتکا به قانون داخلی در پروندهٔ گوگل باعث دسترسی به دیتا و ارزیابی آن در قلمرو سرزمینی ایالات متحده شده است. این رویکرد حاکی از اِعمال صلاحیت کیفری بر اساس محل دسترسی به دیتا است، ولو اینکه نسخهٔ دیگری از این دیتا به‌نحو فیزیکی در حامل فراسرزمینی هم ذخیره شده باشد. امکان دسترسی شرکت گوگل از هر موقعیت جغرافیایی به دیتای کاربران خویش ناشی از الگوی مورد استفادهٔ مدنظر وی برای ذخیرهٔ دیتای کاربران است. لیکن شرکت مایکروسافت در ذخیرهٔ دیتای کاربران خویش از الگوی مشابه استفاده نمی‌کند. ذخیرهٔ دیتا از سوی شرکت مایکروسافت به‌نحوی است که دسترسی بدان فقط در قلمرو سرزمینی محل استقرار حامل امکان‌پذیر است، چراکه نسخهٔ دیگری از دیتا در حامل سرزمینی مفقود است. این وضعیت برعکس ذخیره و امکان دسترسی به دیتای کاربران ابرایانش شرکت گوگل است.

از منظر شرکت گوگل امکان دسترسی به دیتا از قلمرو سرزمینی موجد صلاحیت کیفری محاکم ایالات متحده نیست، چراکه که دیتا در حامل فراسرزمینی ذخیره شده است. بر اساس محل استقرار حامل، صلاحیت کیفری مقام قضایی صادره‌کنندهٔ قرار الزام به افشای دیتای کاربر و قانون مورد استناد وی فراسرزمینی است (United States v. Google, 2017: 710). اگر صلاحیت کیفری و قانون مورد استناد قاضی ایالات متحده محدود به قلمرو سرزمینی ایالات متحده باشد و او بخواهد از این طریق نسبت به مسائل فراسرزمینی اعمال صلاحیت کیفری کند، این رویکرد به معنای فراسرزمینی تلقی‌کردن صلاحیت کیفری قاضی و قانون ارتباطات ذخیره‌شدهٔ ایالات متحده است. در حالی که قوانین داخلی ایالات متحده در خارج از قلمرو سرزمینی ایالات متحده کاربرد ندارند، مگر اینکه کارکرد فراسرزمینی در همان قانون تصریح شده باشد. اما موضع‌گیری شرکت گوگل در محاکم کیفری ایالات متحده مقبولیت پیدا نکرد. امکان دسترسی شرکت گوگل به دیتا از قلمرو سرزمینی ایالات متحده از حیث فنی تأیید شده بود. ذخیرهٔ دیتا از سوی شرکت گوگل به‌نحوی بوده است که دسترسی بدان از هر موقعیت جغرافیایی برای اپراتور امکان‌پذیر است، وقتی که یک نسخه از دیتا در حامل مستقر در قلمرو سرزمینی است.

۳. الزامات ناشی از قانون ارتباطات ذخیره‌شده و ضرورت تغییر آن در قانون کِلود

محتویات ایمیل کاربر در اَبرایانش جلوه‌ای از حریم خصوصی وی است که برای بازرسی آن به حکم قضایی نیاز است (United States v. Warshak, 2010: 274). بر این اساس کپی محتوی ایمیل ناقض حریم خصوصی کاربر آن و مصداق بازرسی غیرقانونی است (Kerr, 2010: 703). لذا

دسترسی مقامات قضایی و پلیسی به ایمیل یا ارتباطات الکترونیک مجرمانه پس از طی تشریفات قانونی میسر است. اما گاهی اوقات قوانین مانع از به‌نتیجه‌رسیدن از طی تشریفات لازم می‌شوند، در جایی‌که الزامات حریم خصوصی موضوعیت دارند. الزامات حریم خصوصی کاربر باعث می‌شود تا پلیس در موارد حدس و گمان نتواند دادگاه را برای صدور مجوز دسترسی به دادهٔ کاربر در ابررایانش اقناع کند. منصرف از اینکه پس از صدور قرار دادگاه بر الزام شرکت فناوری راجع به افشای دیتای کاربر در ابررایانش هنوز پلیس اطمینان زیادی حسب رویهٔ محاکم کیفری ایالات متحده در پروندهٔ مایکروسافت برای دسترسی به محتویات مدنظر ندارد. اگرچه در حالت اول یعنی اقناع دادگاه برای صدور قرار الزام شرکت فناوری گریزی نیست، اما در حالت دوم برای ملزم‌کردن شرکت فناوری راهکار تصویب قانون جدید محتمل است. بر این اساس، تسهیل فرایند دسترسی دولت ایالات متحده به دیتای ذخیره‌شدهٔ فراسرزمینی مرتبط با منافع امنیت ملی وی موضوع قانون کِلود قرار گرفته است، با این تفاوت که الزامات حریم خصوصی کاربر آن و تعهدات شرکت فناوری بر لزوم رعایت حریم خصوصی کاربر ابررایانش مانع از دسترسی دولت به دیتای ذخیره‌شده در حامل دیتای مستقر در قلمرو فراسرزمینی نیست. این وضعیت از نوآوری‌های قانون کلود بر قانون ارتباطات ذخیره‌شده[1] است که پلیس ایالات متحده در پروندهٔ مایکروسافت به استناد آن با شکست مواجه شد.

قانون کِلود مسبوق به قانون ارتباطات ذخیره‌شده و برای رفع کاستی‌های آن در ارتباط با حامل دیتای مستقر در قلمرو فراسرزمینی است. قانون ارتباطات ذخیره‌شده بخشی از قانون حریم خصوصی ارتباطات الکترونیک[2] است که در رویهٔ قضایی ایالات متحده برای دسترسی به دیتای کاربران در فضای مجازی شناسایی شده است. قانون ارتباطات ذخیره‌شده واجد کارکرد سرزمینی است، در حالی که دیتای کاربران فضای مجازی ماهیت فراسرزمینی دارد. تشریفات مقرر در قانون ارتباطات ذخیره‌شده مربوط به سرورها و حامل‌های ذخیره‌کنندهٔ دیتای کاربران شرکت فناوری است که در قلمرو سرزمینی ایالات متحده مستقر هستند. در این قانون به الزام شرکت فناوری بر ارائهٔ محتوی ارتباطات الکترونیک کاربر و اطلاعات ذخیره‌شدهٔ وی در حامل‌های فراسرزمینی اشاره‌ای نشده است. اتکا به این قانون برای دسترسی به دیتای ذخیره‌شدهٔ کاربر ابررایانش شرکت فناوری متبوع یا دارای مرکز اصلی فعالیت در ایالات متحده در حامل‌های فراسرزمینی کارآمد نیست، چراکه این قانون واجد اعتبار سرزمینی است و به موضوعات فراسرزمینی سرایت ندارد. اما قانون ارتباطات ذخیره‌شده ایالات متحده

1. Stored Communications Act, 1986.
2. Electronic Communications Privacy Act, 1986.

با اصلاحات قانون کلود زین‌پس نسبت به دیتای ذخیره‌شدهٔ فراسرزمینی قابل‌اعمال و تأثیر است. با تصویب قانون کلود، گسترهٔ اجرایی قانون ارتباطات ذخیره‌شده واجد اعتبار بین‌المللی شده است.

قانون کلود در الزام شرکت‌های فناوری به افشای دیتای کاربران خویش، صرف‌نظر از محل استقرار حامل دیتا در قلمرو سرزمینی یا فراسرزمینی، واجد اصلاح قانون ارتباطات ذخیره‌شده است که سابق بر این چنین تصریحی نداشت. از یک طرف، قلمرو اجرایی قانون ارتباطات ذخیره‌شدهٔ ایالات متحده تا پیش از تصویب قانون کلود سرزمینی و نسبت به دیتای ذخیره‌شده در حامل مستقر در قلمرو سرزمینی کاربرد داشت. از طرف‌دیگر، سایر دولت‌ها بر اساس قانون ارتباطات ذخیره‌شده از مکاتبهٔ مستقیم با شرکت‌های فناوری برای دریافت دیتای کاربران آن‌ها راجع به محتوای ارتباطات الکترونیک منع شده بودند[1]، ولو اینکه کاربران مدنظر از اتباع داخلی آن‌ها بودند. رویکرد سابق قانون ارتباطات ذخیره‌شده به معنای الزام دولت‌ها به توسل از طریق معاهدهٔ همکاری حقوقی دوجانبه و تقاضای مساعدت از دولت ایالات متحده برای کسب مجوز افشای محتوی ارتباطات الکترونیک بود. این در حالی است که بر اساس قانون کلود این محدودیت برداشته شده است. دولت‌ها با امضای موافقت‌نامهٔ اجرایی با ایالات متحده مجاز به برقراری ارتباط مستقیم با شرکت‌های فناوری برای دریافت دیتای کاربران این شرکت‌ها هستند، مشروط به اینکه اولاً افشای دیتا به دولت متقاضی در تعارض با قوانین داخلی وی نباشد[2] و ثانیاً کاربر مدنظر از اتباع داخلی دولت متقاضی باشد. بر این اساس، افشای دیتای تبعه یا مقیم ایالات متحده به سایر دولت‌ها یا افشای دیتای کاربر متبوع دولت متقاضی برخلاف الزامات ناشی از قوانین داخلی وی راجع به حریم خصوصی شهروندان با ممنوعیت مواجه است.

۱-۳. قانون ارتباطات ذخیره‌شده و خلأءهای اجرایی آن

بر اساس قانون ارتباطات ذخیره‌شده، شرکت‌های فناوری به‌جز در موارد استثنایی به تشخیص خود از افشای محتوی ارتباطات الکترونیک (متن ایمیل) به هر شخص یا نهادی منع شده‌اند، مگر اینکه برخی از الزامات فنی ضرورت آن را توجیه کند.[3] علاوه بر این، شرکت فناوری از افشای سوابق یا مشخصات کاربر منع شده است.[4] اما این ممنوعیت شامل افشای اطلاعات غیرمحتوایی نیست.[5] بر اساس قانون ارتباطات ذخیره‌شده، الزامات حریم خصوصی کاربر و لزوم رعایت آن از سوی شرکت فناوری مزید بر علت شده است تا شرکت‌های فناوری حتی‌الامکان از افشای دیتا به مقامات

1. Stored Communications Act, 1986, 2702(a)(3)
2. CLOUD Act, 2018, 103(b).
3. Stored Communications Act, 1986, 2702(a)(1).
4. Stored Communications Act, 1986, 2702(a)(3).
5. Stored Communications Act, 1986, 2702(c)(6).

پلیسی و قضایی به بهانهٔ ذخیرهٔ دیتا در حامل‌های فراسرزمینی امتناع کنند. ازاین‌رو، مقامات پلیسی، که در ایالات متحده زیرنظر دولت و بخشی از آن می‌باشد، برای الزام شرکت‌های فناوری ناگزیر از مراجعه به دادگاه و دریافت قرار الزام شرکت فناوری بر اساس قوانین فدرال آیین دادرسی کیفری هستند، منوط به اینکه محتوی ارتباطات حاکی از وقوع جرم و دلایل مؤید آن باشد و از زمان ذخیرهٔ آن بیش از ۱۸۰ روز سپری نشده باشد.[1] اگر از زمان ذخیرهٔ اطلاعات بیش از ۱۸۰ روز گذشته باشد، پلیس با طی تشریفات دیگری که منجر به اطلاع و اعتراض صاحب اطلاعات در دادگاه می‌شود مجاز به تقاضای رسیدگی و صدور قرار الزام شرکت فناوری به افشای اطلاعات ذخیره‌شده است[2]، منصرف از اینکه پلیس در چنین شرایطی باید اثبات کند که محتوی مورد درخواست وی با تحقیقات کیفریِ در جریان مرتبط است.[3]

برای رفع این نقیصه، لایحهٔ اصلاح قانون ارتباطات ذخیره‌شده به تصویب رسید[4] تا به‌موجب آن شرکت فناوری ملزم به افشای دیتای در مالکیت، دسترسی و کنترل به پلیس باشد، صرف‌نظر از اینکه این دیتا را در کجا ذخیره کرده باشد، چراکه دولت ایالات متحده خواهان حفظ تبعیت شرکت‌های فناوری از دستورات دادگاه بر اساس قانون ارتباطات ذخیره‌شده نسبت به دیتای ذخیره‌شدهٔ فراسرزمینی است. این وضعیت با تجربهٔ شکست دولت ایالات متحده در پروندهٔ مایکروسافت توأم شده بود. دیوان‌عالی ایالات متحده در پروندهٔ مایکروسافت اذعان کرد بر اساس قرار صادره از سوی دادگاه کیفری بر اساس قانون ارتباطات الکترونیک که در سرتاسر قلمرو سرزمینی ایالات متحده کاربرد دارد، نمی‌توان شرکت مایکروسافت را ملزم به افشای دیتایی کرد که در حامل دولت ثالث ذخیره شده است (United States v. Microsoft Corp., 2018: 548)، لیکن گزینهٔ دیگری برای آن وجود دارد. تصویب قانون جدید و تقاضای مجدد دولت از شرکت مایکروسافت بر لزوم افشای دیتای کاربر وی چاره‌ساز است.

دولت بر اساس قانون کلود پس از این مرحله بود که تقاضای جدیدی را برای دراختیارگرفتن دیتای کاربر شرکت مایکروسافت در دادگاه مطرح کرد. دادگاه کیفری قرار جدیدی را بر اساس قانون کلود به‌منظور الزام شرکت مایکروسافت صادر کرد (United States v. Microsoft Corp., 2018: 548). دولت در نهایت از این طریق به دیتای ذخیره‌شدهٔ فراسرزمینی دست یافت، چراکه شرکت

1. Stored Communications Act, 1986, 2703(a).
2. Stored Communications Act, 1986, 2703(d).
3. Stored Communications Act, 1986, 2703(b)(1)(b).
4. Consolidated Appropriations Act, 2018.

مایکروسافت بر اساس قانون جدید ملزم بود به‌موجب قرار دادگاه ایالات متحده دیتای در مالکیت، دسترسی یا کنترل را صرف‌نظر از محل ذخیرهٔ دیتا اعم از قلمرو سرزمینی ایالات متحده یا دولت ثالث افشا کند.[1] دیوان‌عالی ایالات متحده نیز، با توجه به موافقت دولت و شرکت مایکروسافت بر جایگزینی قرار جدید با قرار سابق دادگاه و تبعیت از آن، احکام دادگاه بدوی و تجدیدنظر در پروندهٔ مایکروسافت را نقض کرد (United States v. Microsoft Corp., 2018: 548). دیوان عالی ایالات متحده در این پرونده استدلال کرد که با توجه به تصویب قانون کلود این پرونده و احکام صادره در آن از درجهٔ اعتبار ساقط است (United States v. Microsoft Corp., 2018: 1186)، چراکه قانون کلود در قلمرو فراسرزمینی قابل‌اجراست و بر این اساس شرکت مایکروسافت مکلف به ارائهٔ دیتای ذخیره‌شدهٔ کاربر در حامل‌های فراسرزمینی به پلیس ایالات متحده است.

۲-۳. قانون کلود: از مزایا و امتیازات تا نقیصه‌های آن

ایالات متحده به دیتای کاربران شرکت‌های فناوری دارای تابعیت وی یا مستقر در خاک سرزمینی خویش نیاز دارد. لیکن این دیتا حسب سیاست‌های حرفه‌ای شرکت‌های فناوری در حامل فراسرزمینی ذخیره می‌شوند. دولت ایالات متحده برای دسترسی به دیتای ذخیره‌شده در حامل فراسرزمینی به استناد قانون ارتباطات ذخیره‌شده با بن‌بست مواجه بود. پلیس ایالات متحده بر اساس قانون کلود از این مانع عبور کرده است، هرچند که قانون کلود در مرحلهٔ اجرا هنوز با ایراداتی مواجه است. پیش از این، سایر دولت‌ها برای دسترسی به دیتای ذخیره‌شده در حامل‌های ایالات متحده مجبور به طی تشریفات معاهدات همکاری حقوق دوجانبه[2] یا دیگر سازوکارهای قضایی بودند. ایالات متحده نیز تابع همین شرایط بود. این در حالی بود که شرکت‌های فناوری متبوع یا دارای مرکز فعالیت در قلمرو سرزمینی ایالات متحده از مذاکره و ارسال مستقیم دیتا به سایر دولت‌ها ممنوع بودند.[3] این محدودیت تاحدودی برای دولت ایالات متحده نیز وجود داشت، چراکه شرکت‌های فناوری در صورتی مجاز به ارائهٔ دیتا به دولت ایالات متحده بودند که دولت با ارائهٔ مستنداتی به دادگاه ثابت می‌کرد که در مبادلات الکترونیکِ کاربر شرکت احتمال وجود دلائل مجرمانه وجود دارد. اگر دادگاه متقاعد می‌شد و قرار الزام شرکت به افشای دیتای کاربر را صادر می‌کرد، آن زمان شرکت مجاز به ارائهٔ دیتا به دولت بود.[4] این تقاضاها سابق بر این به محاکم دولت مورد تقاضا ارجاع

1. CLOUD Act, 2018, 103.
2. Mutual Legal Assistance Treaties.
3. Stored Communications Act, 1986, 2702(a).
4. Stored Communications Act, 1986, 2703(a).

می‌شد. انطباق خواستهٔ دولت متقاضی از دولت سرزمینی حامل دیتا با قوانین، تابع تشریفاتی بود که باید در محاکم کیفری طی می‌شد تا مجوز افشای دیتای کاربر صادر شود.

این فرایند زمان‌بر بود و اغلب با شکست در حصول نتیجهٔ مدنظر دولت متقاضی توأم بود؛ کما اینکه این فرمول در پروندهٔ مایکروسافت نیز موفقیت‌آمیز نبود. این وضعیت به‌دلیل ناکارآمدی در مبارزهٔ همه‌جانبه و عکس‌العمل سریع در مقابله با جرایم روزافزون سایبری با انتقاداتی مواجه شد (White House, 2013: 227). توسل به قانون کلود به‌جای توسل به معاهدهٔ همکاری حقوقی دوجانبه برای تحقق چنین خواسته‌ای از پیشنهادات وزارت دادگستری ایالات متحده است. قانون کلود مشکلات ایالات متحده را مرتفع می‌کند، لیکن مشکلاتی برای تمام دولت‌ها ایجاد می‌کند. توسل به قانون کلود، اگر مداخله در امور داخلی سایر کشورها بر اساس قوانین ایالات متحده تلقی نشود، حداقل به‌معنای غلبهٔ ارادهٔ مقنن ایالات متحده بر ارادهٔ تمام دولت‌ها در سرتاسر دنیا در مسئلهٔ همکاری یا عدم همکاری با ایالات متحده در افشای دیتای ذخیره‌شده در حامل‌های مستقر در خاک سرزمینی است. اتباع سایر دولت‌ها که دیتای آن‌ها نزد شرکت‌های متبوع ایالات متحده پردازش و مدیریت شده و در حامل‌های فراسرزمینی ذخیره می‌شد، پیش از این، مشمول مقررات سرزمینی ایالات متحده نبودند. این یکی از نقاط ضعف قانون کلود به‌صورت بالقوه برای تمام دولت‌ها و اتباع آن‌هاست که از ابررایانش شرکت‌های فناوری گوگل، مایکروسافت و اپل استفاده می‌کنند، چراکه این اراده نباید از سوی یک دولت برای سایر دولت‌ها محقق شود، بلکه این سازوکاری است که باید در موافقت‌نامه‌های بین‌المللی و حسب ارادهٔ جمعی دولت‌های عضو آن محقق شود تا مثمرثمر باشد. اما ایالات متحده با وضع و تصویب قانون کلود اتفاقاً درصدد برآمده است تا بر اشکالات و وابستگی به معاهدهٔ همکاری حقوقی دوجانبه با سایر دولت‌ها در شرایط لزوم دسترسی به دیتای ذخیره‌شده در حامل‌های فراسرزمینی فائق آید.

این رویکرد به معنای حاکمیت ارادهٔ ایالات متحده بر ارادهٔ تمام دولت‌ها و یکجانبه‌گرایی وی است. وضع و تصویب قانون کلود از مظاهر اعمال حاکمیت و تحقق ارادهٔ ایالات متحده است، بدون اینکه برای اجرای آن نیازی به کسب رضایت سایر دولت‌ها باشد. بر اساس قانون کِلود به رئیس‌جمهور ایالات متحده اجازه داده شده است تا به تنظیم قراردادهای انحصاری با دولت‌های خارجی برای دسترسی مستقیم به دیتای کاربران از طریق شرکت‌های فناوری بپردازد. این وضعیت بدین معناست که دولت ایالات متحده بدون درنظرگرفتن محل استقرار حامل ذخیره‌کنندهٔ دیتای کاربران فضای مجازی و الزامات حریم خصوصی می‌تواند به دیتای مورد نظر دست یابد. اما این رویهٔ ایالات متحده موجب نگرانی رفتار مشابه سایر دولت‌ها با دیتای ذخیره‌شده در حامل‌های مستقر

در ایالات متحده است، منصرف از اینکه در هر دو حالت اصل سرزمینی‌بودن اعمال حاکمیت و صلاحیت کیفری به‌عنوان جزء لاینفک حقوق بین‌الملل کیفری نیز تحت‌الشعاع است. این در حالی است که باید مبنایی برای این رفتار وجود داشته باشد. این مبنا از دو حال خارج نیست. در این شرایط، محل فعالیت شرکت فناوری و محل استقرار حاملْ تعیین‌کننده است. شرکت مایکروسافت در پروندهٔ ایالات متحده علیه مایکروسافت معتقد بود که دولت بر مبنای محل استقرار شرکت مایکروسافت و صلاحیت خود برای تقاضای دسترسی به دیتای کاربران استناد می‌کند، در حالی که حامل دیتا از قلمرو سرزمینی وی خارج است. این وضعیت دربرگیرندهٔ دو مبنا به‌صورت توأمان است. مبنا بر این اساس، محل فعالیت شرکت فناوری است که دولت محل استقرار آن مجاز به دریافت دیتای کاربر است، ولو اینکه دیتا در حامل فراسرزمینی ذخیره شده باشد. مفهوم مخالف این فرمول آن است که دولت محل استقرار حامل که به ذخیرهٔ دیتای کاربران شرکت فناوری می‌پردازد و نسبت به آن صلاحیت سرزمینی دارد نیز مجاز به دسترسی به دیتای کاربران شرکت فناوری فراسرزمینی می‌باشد که محل فعالیت آن در قلمرو سرزمینی دولت ثالث است. این نتیجه‌گیری به معنای جواز مداخله در امور داخلی و اتباع سایر کشورهاست که در حقوق بین‌الملل با ممنوعیت مواجه است.

تقاضای دولت سرزمینی محل فعالیت شرکت فناوری برای دسترسی به دیتای ذخیرشدهٔ کاربران وی به‌معنای نادیده‌گرفتن تعهدات شرکت فناوری در قبال کاربران ابررایانش و در قبال دولت محل استقرار حامل است که برای استفادهٔ وی از حامل‌های فراسرزمینی مشخص شده‌اند. دسترسی دولت محل استقرار حامل به دیتای ذخیره‌شدهٔ کاربران فراسرزمینی نیز به معنای زیرپاگذاشتن تعهدات شرکت فناوری در قبال کاربران و در قبال دولت محل فعالیت شرکت فناوری است که بر اساس آن اجازهٔ فعالیت به شرکت فناوری داده شده است. پافشاری هریک از دو دولت محل استقرار مرکز اصلی فعالیت شرکت فناوری یا دولت محل استقرار حامل دیتا به معنای ناگزیربودن شرکت فناوری به نادیده‌گرفتن و نقض قوانینِ دیگر دولت به‌بهای رعایت قوانین دولت متقاضی است. وجه اشتراک هر دو نادیده‌گرفتن تعهدات شرکت در قبال کاربران است که چه‌بسا از اتباع هیچ‌یک از دو دولت نباشند. چارهٔ خروج از این وضعیت الزام شرکت فناوری از قوانین کیفری محل فعالیت است، هرچند که دیتای کاربران وی در حامل فراسرزمینی ذخیره شود، در عین حال که دولت محل استقرار حامل نیز برای دسترسی به دیتای ذخیره‌شده در قلمرو سرزمینی مجاز به تقاضا و کسب موافقت دولت سرزمینی محل فعالیت شرکت فناوری باشد. این وضعیت بدین‌معناست که شرکت فناوری حسب قراردادهای استفاده از حامل فراسرزمینی مکلف به‌تبعیت از قوانین کیفری دولت محل استقرار حامل نباشد و دولت محل استقرار حامل نیز به‌واسطهٔ دراختیارداشتن حامل دارای حق اولویت به دیتای

ذخیره‌شده در حامل سرزمینی و الزام شرکت فناوری به‌تبعیت از قوانین وی برای عدم افشای دیتای ذخیره‌شده در حامل سرزمینی وی نباشد.

نتیجه

دولت‌ها درصدد هستند تا با ذخیرهٔ دیتای اتباع به‌عنوان بخشی از سرمایه‌های ملی در حامل مستقر در قلمرو سرزمینی شرایط دسترسی و مدیریت دیتای کاربران ابررایانش تحت حاکمیت قوانین داخلی متجلی شود. اما شرکت‌های فناوری برای فعالیت ناگزیر از پذیرش و اولویت به قوانین سرزمینی محل استقرار مرکز اصلی فعالیت شرکت هستند. استفادهٔ شرکت فناوری از امکانات دیگر دولت‌ها و حامل‌های مستقر در قلمرو سرزمینی آن‌ها حسب قرارداد اجاره نیز به نادیده‌گرفتن قوانین کیفری محل فعالیت و استقرار مرکز اصلی شرکت منتهی نمی‌شود. هرچند که دولت محل استقرار مرکز اصلی شرکت فناوری ممکن است دارای حامل دیتا باشد، لیکن شرکت فناوری به هر دلیل فنی تمایل به استفاده از حامل فراسرزمینی دارد. از یک‌طرف، استفاده از حامل‌های فراسرزمینی مجوز عدول شرکت فناوری در تبعیت از قوانین سرزمینی محل استقرار مرکز اصلی فعالیت نیست. از طرف‌دیگر، استفاده از حامل‌های فراسرزمینی برای دولت صاحب‌سرزمین موجد حق تحمیل قوانین کیفری نسبت به شرکت فناوری و نوع فعالیت‌های وی در سرزمین ثالث (دولت محل استقرار مرکز اصلی شرکت) نیست. لذا دولت سرزمینی محل استقرار حامل دیتا نمی‌تواند شرکت فناوری را که در قلمرو سرزمینی دولت ثالث فعالیت می‌کند، ملزم به تبعیت از قوانین داخلی در فعالیت‌های فراسرزمینی وی کند، به این استناد که از حامل مستقر در قلمرو سرزمینی وی استفاده می‌کند. البته این به معنای نادیده‌گرفتن اِعمال حاکمیت دولت محل استقرار حامل نسبت به استفادهٔ شرکت فناوری از امکانات سرزمینی وی نیست. ایجاد محدودیت برای شرکت فناوری از سوی دولت محل استقرار حامل دیتا در زمان لزوم افشای دیتا به سایر دولت‌ها نمونه‌ای از این وضعیت است، هرچند که منجر به آزادی عمل دولت سرزمینی محل استقرار حامل دیتا هم نمی‌شود.

اِعمال حاکمیت دولت محل استقرار حامل دیتا مجوز سرپیچی شرکت فناوری از قوانین محل استقرار مرکز اصلی فعالیت وی نیست. کما اینکه اگر حامل در قلمرو سرزمینی دولت محل استقرار مرکز اصلی فعالیت مستقر باشد، شرکت فناوری امکان دسترسی آزادانه به آن و نادیده‌گرفتن مقررات دولت سرزمینی در این ارتباط را ندارد. این وضعیت حاکی از گِره‌خوردن فعالیت‌های اقتصادی شرکت‌های فناوری با ملاحظات اعمال حاکمیت دولت سرزمینی محل استقرار مرکز فعالیت یا محل استقرار حامل دیتاست. اما این وضعیت برای دولت ایالات متحده و پلیس وی مطلوب و قابل‌قبول نیست. الزام شرکت فناوری مستقر در قلمرو سرزمینی ایالات متحده به نادیده‌گرفتن مقررات دولت

سرزمینی محل استقرار حامل دیتا و افشای دیتای کاربران از محل مرکز اصلی فعالیت شرکت مورد تقاضاست. اما شرکت فناوری این فرایند را نیازمند مجوزهای قضایی می‌داند. پلیس و دولت ایالات متحده هم ابایی ندارد تا از سازوکارهای قضایی برای تحقق این خواسته استفاده کند، اما رویهٔ قضایی محاکم کیفری ایالات متحده در این ارتباط متکی به قوانین داخلی است که با بن‌بست روبه‌رو هستند. به بیان دیگر، قوانین داخلی و قلمرو اجرایی آن‌ها تا سرحد مرزهای سرزمینی و تحت حاکمیت ایالات متحده است و فراتر از آن کاربرد ندارد. در این شرایط، صدور قرار الزام شرکت فناوری به افشای دیتای کاربر از سوی محاکم کیفری ایالات متحده ناکارآمد است، وقتی که قرار است دیتا از حامل دیتای مستقر در قلمرو فراسرزمینی بازخوانده شود. بازخوانی دیتا از حامل مستقر فراسرزمینی جلوه‌ای از مداخله در امور دولت خارجی است که با قوانین داخلی نمی‌توان آن را توجیه کرد، وقتی که قانون به قلمرو فراسرزمینی و کارکرد خود در آن اشاره نکرده است. دولت ایالات متحده برای عبور از این محدودیت‌ها به تصویب قانون کلود پرداخته است.

قانون کِلود دارای دو جزء اصلی است. جزء اول آن واجد الزام شرکت‌های فناوری به افشای محتوی ارتباطات الکترونیک ذخیره‌شده در سرورهای شرکت و حامل‌های فراسرزمینی است. جزء دوم آن مجوز طرح و بررسی تقاضای سایر دولت‌ها از ایالات متحده برای دسترسی به دیتای ذخیره‌شده در حامل‌های مستقر در ایالات متحده است، مشروط به اینکه این تقاضا برای تکمیل تحقیقات کیفری یا تعقیب جرایم ضرورت داشته باشد. سابق بر این، راجع به جزء اول قانون کِلود شرکت‌های فناوری در ایالات متحده به‌موجب قانون ارتباطات ذخیره‌شده و قرار صادره از محاکم ایالات متحده با ظن به وجود دلیل جرم ملزم به افشای محتوی ارتباطات الکترونیک کاربران بودند. اما زمانی که حامل ذخیره‌کنندهٔ مبادلات الکترونیک کاربران شرکت‌های فناوری در قلمرو سرزمینی ایالات متحده مستقر نبودند، این رویه با بن‌بست مواجه می‌شد. این اشکالْ قرار صادره از محاکم ایالات متحده را با مانع صلاحیت کیفری سرزمینی مواجه می‌کرد. بر این اساس، تصویب قانون کلود مجوز صدور و اجرای قرار محاکم ایالات متحده برای دسترسی به دیتای ذخیره‌شده در حامل فراسرزمینی از قلمرو سرزمینی ایالات متحده است. بر این اساس، استقرار حامل دیتا در قلمرو فراسرزمینی مانع از دسترسی مقامات قانونی یا پلیس ایالات متحده نیست، با این مزیت که ایالات متحده برای تحقق آن نیازی به توسل به سازوکار معاهدهٔ همکاری حقوقی دوجانبه هم ندارد.

ازاین‌رو، قانون کِلود واجد دو وضعیت است که اجرای هر دو بُعد آن با مضراتی مواجه است که منافع آن را ناچیز جلوه می‌دهد. از یک‌طرف به قرارهای صادره از محاکم کیفری ایالات متحده بر لزوم افشای دیتای ذخیره‌شده در حامل‌های فراسرزمینی اعتبار فراسرزمینی داده شده است، بدون

اینکه ارادهٔ قضایی سایر دولت‌ها در آن لحاظ شود. بر این اساس، دسترسی دولت ایالات متحده به حامل‌های مستقر در قلمرو سرزمینی دولت‌های ثالث تسهیل شده است که می‌تواند شرکت‌های فناوری درون‌سرزمینی را بر اساس قانون داخلی ملزم به افشای دیتای کاربر در حامل مستقر در قلمرو فراسرزمینی کند. حامل دیتا عامل ارتباط دولت محل استقرار آن با شرکت فناوری است. بر این اساس، لزوم اعمال حاکمیت قضایی وی بر امور شرکت فناوری بدیهی است. اما ایالات متحده به صرف استقرار مرکز اصلی فعالیت شرکت فناوری نمی‌تواند اراده و حاکمیت قضایی دولت محل استقرار حامل دیتا را نادیده بگیرد، چراکه رویکرد ایالات متحده به معنای وضع و تصویب قوانین دارای اعتبار فراسرزمینی و افزایش صلاحیت کیفری سرزمینی به سرتاسر دنیاست که با اصل ممنوعیت مداخله در امور داخلی سایر کشورها در تعارض است. اما وضعیت اول که مجوز دسترسی ایالات متحده به دیتای ذخیره‌شده در حامل‌های فراسرزمینی است، امتیازی است که دولت ایالات متحده از طریق قانون داخلی و به نیابت از تمام دولت‌ها در سرتاسر دنیا به خود داده است که جلوه‌ای از نقض اصل ممنوعیت مداخله در امور داخلی سایر کشورهاست. دادن امتیاز به تمام دولت‌ها تحت ارادهٔ دولت معطی است، لیکن گرفتن امتیاز از تمام دولت‌ها نیازمند ارادهٔ جمعی و موافقت سایر دولت‌هاست که معمولاً در قالب موافقت‌نامه‌های بین‌المللی متبلور می‌شود. از طرف‌دیگر، زمینهٔ دسترسی دولت‌های ثالث به حامل‌های مستقر در قلمرو سرزمینی ایالات متحده در قانون کلود بدون مداخله و مجوز محاکم کیفری یکدیگر تسهیل شده است. این رویکرد بدین معناست که دولت‌های ثالث بدون نیاز به موافقت‌نامهٔ همکاری قضایی و سیر مراحل قضایی در محاکم دولت ایالات متحده می‌توانند دیتای لازم را با مکاتبه با شرکت فناوری ارائه‌کنندهٔ خدمات کلود به کاربر فضای مجازی دریافت کنند، به صرف اینکه دولت ایالات متحده آن‌ها را تأیید کرده باشد.

وضعیت دوم، امتیاز ایالات متحده به تمام دولت‌ها در سرتاسر دنیاست که نسبت به شرکت‌های فناوری مستقر در قلمرو سرزمینی اعطاء می‌کند که تحقق آن جلوه‌ای از اعمال حاکمیت درون‌سرزمینی و دارای مقبولیت است. اما تأیید سایر دولت‌ها از سوی دولت ایالات متحده برای دسترسی به دیتای کاربر متبوع خویش از طریق شرکت فناوری مستقر در قلمرو سرزمینی ایالات متحده متکی به رعایت الزامات حقوق بشری و سازوکارهای محافظت و مراقبت از دیتای کاربر و عدم سوءاستفاده از آن است. این در حالی است که وضع قانون داخلی با کارکرد فراسرزمینی برای دسترسی به دیتای کاربران فضای مجازی زمینه‌ساز نقض الزامات حقوق بشری کاربران است، منصرف از اینکه واگذاری صلاحدید به دولت ایالات متحده و حذف فرایند قضایی در بررسی تقاضای سایر دولت‌ها برای دسترسی به دیتای کاربر فضای مجازی ناقض حریم خصوصی کاربر

است. بر این اساس، ایالات متحده در هر دو وضعیت ناشی از اجرای قانون کِلود الزامات حریم خصوصی و تعهدات متقابل شرکت‌های فناوری به کاربران و برعکس آن را نادیده گرفته است و زیر پا گذاشته است. یکی از نتایج قانون کلود در تعیین سازوکارهای لازم برای سایر دولت‌ها در دسترسی به دیتای کاربران متبوع از طریق شرکت‌های فناوری متبوع ایالات متحده تشدید بالکانیزه‌شدن اینترنت و تشویق اتباع سایر دولت‌ها به استفاده از اَبررایانش‌هایی است که شرکت ارائه‌کنندهٔ آن در قلمرو سرزمینی دولت متبوع آن‌ها مستقر و تابع مقررات قانون کِلود ایالات متحده نباشند.

منابع

فارسی

- دلخون‌اصل، رامین؛ ایرج گلدوزیان و کیومرث کلانتری (۱۳۹۸)، «نقش پلیس در جمع‌آوری ادله الکترونیکی در فضای مجازی در نظام حقوقی ایران، فرانسه و کنوانسیون جرایم سایبری»، **فصلنامه پژوهش‌های اطلاعاتی و جنایی**، دوره ۱۴، شماره ۵۴.
- جلالی، محمود و سعیده توسلی اردکانی (۱۳۹۸)، «ضرورت ایجاد نظام هماهنگ حقوقی بین‌المللی در مقابله با جرایم در فضای مجازی»، **فصلنامه مطالعات حقوق عمومی**، دوره ۴۹، شماره ۴.
- شریعت‌باقری، محمدجواد (۱۳۹۳)، «تصویب موافقت‌نامه‌های همکاری‌های قضایی بین‌المللی؛ مشکلات و راه‌حل‌ها»، دوره ۱۹، شماره ۶۶.
- صالحی، جواد (۱۳۹۸)، «دسترسی به اطلاعات دیتاسنتر دولت خارجی در تقابل با اصول صلاحیت کیفری سرزمینی و اعمال حاکمیت در حقوق بین‌الملل»، **مجله حقوقی بین‌المللی**، دوره ۳۶، شماره ۶۰.
- طهماسبی، جواد و خیراله شاهمرادی (۱۳۹۷)، «چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری»، **مجله حقوقی دادگستری**، سال ۸۲، شماره ۱۰۴.
- فتحی، یونس و خیراله شاهمرادی (۱۳۹۶)، «گستره و قلمرو حریم خصوصی در فضای مجازی»، **مجله حقوقی دادگستری**، سال ۸۱، شماره ۹۹.
- قناد، فاطمه و مسعود اکبری (۱۳۹۶)، «امنیت‌گرایی سیاست جنایی»، **فصلنامه پژوهش حقوق کیفری**، دوره ۵، شماره ۱۸.
- محمدنسل، غلامرضا (۱۳۹۵)، **حقوق جزای اختصاصی؛ جرایم رایانه‌ای در ایران**، چاپ دوم، تهران: نشر میزان.

انگلیسی

- Brenner, W. Susan (2010), **Cybercrime: Criminal Threats from Cyberspace**, Praeger Publishing.
- Chander, Anupam and Uyen P. Le (2015), "Data Nationalism", **Emory Law Journal**, Vol. 64(3).
- Kerr, S. Orin (2010), "Fourth Amendment Seizures of Computer Data", **Yale Law Journal**, Vol. 119.
- Mulligan, P. Stephen (2018), **Cross-Border Data Sharing Under the CLOUD Act**, Congressional Research Service, No. 7-5700.
- S. 2383, 115th Cong. (2018).
- Schwartz, M. Paul (2013), "Information Privacy in the Cloud", **University of Pennsylvania Law Review**, Vol. 161.
- Schwartz, M. Paul (2018), "Legal Access to the Global Cloud", **Columbia Law Review**, Vol. 118.
- Schwartz, M. Paul and Karl-Nikolaus Peifer (2017), "Transatlantic Data Privacy Law", **Georgetown Law Journal**, Vol. 106.
- Schultheis, Ned (2015), "Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States

Cloud Storage Industry", **Brooklyn Journal of Corporate, Financial & Commercial Law**, Vol. 9.

- Swire, Peter and DeBrae Kennedy-Mayo (2017), "How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information", **Emory Law Journal**, Vol. 66.
- Swire, Peter; Justin Hemmings and Suzanne Vergnolle (2016), "A Mutual Legal Assistance Case Study: The United States and France", **Wisconsin International Law Journal**, Vol. 34.
- United States (2017), Proposed Legislation to Permit Secure and Privacy-Protected Access to Cross-border Electronic Data for Law Enforcement to Combat Serious Crime and Terrorism.
- United States (1986), Stored Communications Act.
- United States (2018), Clarifying Lawful Overseas Use of Data (CLOUD Act).
- United States (2018), Consolidated Appropriations Act.
- United States (2018), Electronic Communications Privacy Act.
- United States v. Google (2017), 232 F. Supp. 3d.
- United States v. Microsoft Corp. (2017), 138 S. Ct.
- United States v. Microsoft Corp. (2018), 138 S. Ct.
- United States v. Microsoft Corp. (2018), No. 17-2.
- United States v. Verdugo-Urquidez (1990), 494 U.S.
- United States v. Warshak (2010), 631 F.3d.
- White House (2013), Liberty and Security in a Changing World the President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, Available at:
  https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (last visited on 5/5/2020).