دسترسی به داده‌های رایانه‌ای فرامرزی در تحقیقات کیفری

توقان نظامی نرج‌آباد*
لیلا رئیسی دزکی**

تاریخ دریافت: ۹۸/۰۳/۱۲ تاریخ پذیرش: ۹۸/۱۰/۱۲

چکیده

داده‌های رایانه‌ای فارغ از مرزهای ملی در فضای سایبری سیال‌اند و در بسیاری از موارد، داده‌های مربوط به جرم که در واقع ادلهٔ الکترونیکی جرم‌اند، در قلمروی سرزمینی دولت تعقیب‌کنندهٔ جرم قابل دسترسی نیستند. موفقیت در تعقیب بسیاری از جرایم سایبری مستلزم دسترسی آنان به داده‌های فرامرزی است. این دسترسی به‌طور سنتی از طریق معاضدات قضایی و بر مبنای موافقت دولتی که از صلاحیت دسترسی به داده‌های مورد نظر برخوردار است، صورت می‌گیرد. چنین رویکردی در مطابقت با اصل حاکمیت قرار دارد، اما تأمین‌کنندهٔ سرعت عملی که لازمهٔ جمع‌آوری ادلهٔ الکترونیکی است، نمی‌باشد. امروزه بسیاری از دولت‌ها به صورت مستقیم و بدون جلب موافقت دولت ذی‌صلاح به داده‌ها دسترسی می‌یابند. ناکارآمدی روش‌های سنتی همکاری همراه با اهمیت یافتن نقش شرکت‌های خدمات اینترنتی در کنترل داده‌های فرامرزی موجب شده تا معاضدت قضایی در زمینهٔ دسترسی به این داده‌ها رفته‌رفته جای خود را به دسترسی از طریق شرکت‌های مزبور بدهد. برخی از چارچوب‌های بین‌المللی نیز دسترسی فرامرزی مستقیم به داده‌ها را تحت شرایطی پذیرفته‌اند. اما با این‌حال، هیچ رویکرد بین‌المللی واحدی در خصوص دسترسی به داده‌های فرامرزی وجود ندارد. هر یک از روش‌های دسترسی به داده‌های فرامرزی دارای مزایا و معایبی هستند که باید در ایجاد چارچوب‌های بین‌المللی جدید مورد توجه قرار گیرند.

کلیدواژگان:

ادلهٔ الکترونیکی، داده‌های رایانه‌ای، دسترسی فرامرزی، کنوانسیون بوداپست، معاضدت قضایی.

* دانشجوی دکتری حقوق بین‌الملل، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان) (نویسنده مسئول)
Toghan_nezami@yahoo.com

** دانشیار، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)
aisi.leila@gmail.com

مقدمه

امروزه گسترش شبکهٔ اینترنت منشأ فرصت‌ها و امکانات بیشماری در زمینه‌های مختلف است. ارتکاب جرم یکی از این زمینه‌هاست. در فضای سایبری فواصل مکانی مانعی برای ارتکاب جرم محسوب نمی‌شوند و مرتکبین نیازی به حضور در محل قربانی ندارند. از طرفی با انتقال داده‌های رایانه‌ای از طریق اینترنت، نظارت‌های مرزی معمول، کارایی خود را از دست داده‌اند. داده‌های رایانه‌ای در فضای سایبری سیال‌اند و می‌توانند فارغ از مرزهای ملی در سِرور یا رایانه‌ای در سوی دیگر جهان ذخیره شوند. به‌طور مثال، بسیاری از شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی داده‌های کاربران خود را در کشور مقر خود ذخیره می‌نمایند. در نتیجه، در بسیاری از موارد داده‌های مربوط به یک جرم در خارج از قلمروی دولت تعقیب‌کنندهٔ جرم قابل دسترسی‌اند. از طرفی، دسترسی مأموران به داده‌های ذخیره‌شده در قلمروی یک دولت خارجی موجب نقض حاکمیت آن دولت خواهد شد. مطابق اصل سرزمینی بودن صلاحیت، جلب موافقت دولت ذی‌صلاح با دسترسی مقامات خارجی به داده‌ها ضروری است. در این‌گونه موارد، معاضدت قضایی سازکاری است که به‌طور سنتی مورد استفاده قرار می‌گیرد. با این‌حال، روش‌های سنتی جمع‌آوری ادلهٔ فرامرزی بسیار کُندند؛ چرا که تکمیل روندهای قانونی و فرایندهای دیپلماتیک معمول بسیار زمان‌بر است. به علاوه ممکن است مأمورین بلافاصله پس از ارتکاب یک جرم سایبری منشأ آن را شناسایی نمایند، اما قادر به جمع‌آوری و ارائهٔ فوری اطلاعاتی که دولت‌های خارجی برای پذیرش درخواست معاضدت به آنها نیاز دارند، نباشند. هر چه زمان بیشتری برای ارائهٔ این اطلاعات مورد نیاز باشد، احتمال از بین رفتن یا دستکاری داده‌ها بیشتر خواهد بود. اصولاً یکی از ویژگی‌های ادلهٔ الکترونیکی قابلیت دستکاری، انتقال و حذف فوری و آسان آنها از راه دور است. ممکن است این تغییرات در نتیجهٔ اقدامات مرتکبین برای از بین بردن ادله یا در اثر اقدامات معمول شرکت‌های خدمات اینترنتی از جمله حذف داده‌های ترافیکی به وجود آیند. از این‌رو ممکن است ادلهٔ الکترونیکی حتی پیش از ارسال درخواست معاضدت از بین بروند. در اینجا این پرسش مطرح می‌شود که آیا مأموران می‌توانند مستقیماً و بدون اطلاع و توافق دولت ذی‌صلاح به داده‌ها دسترسی یابند. شرایط اضطراری ممکن است مستلزم دسترسی فوری به

داده‌ها یا حداقل حفظ ارزش استنادی داده‌ها از طریق توقیف آنها باشد؛ چرا که مرتکبین می‌توانند با استفاده از سرعت و مهارت کافی، داده‌ها را مختل، حذف یا منتقل نمایند.

تعقیب جرایم فرامرزی مستلزم استفادهٔ مأمورین تحقیق از روش‌های مؤثر جمع‌آوری ادلهٔ فرامرزی است. این روش‌ها باید قانونی باشند تا ادلهٔ جمع‌آوری‌شده در دادگاه قابلیت استناد داشته باشند. از طرفی تشخیص مرزهای ملی در فضای سایبری به آسانی میسر نیست و مأموران نمی‌توانند محل ذخیرهٔ داده‌هایی را که از طریق اینترنت به آنها دسترسی می‌یابند، به راحتی تعیین نمایند. گسترش فعالیت‌های ارائه‌دهندگان خدمات اینترنتی خارجی و ابرهای رایانه‌ای[۱] بر پیچیدگی این امر افزوده است. دسترسی مستقیم به داده‌های فرامرزی ابزاری است که امروزه دولت‌ها برای جمع‌آوری ادلهٔ الکترونیکی فرامرزی از آن استفاده می‌نمایند. البته دسترسی فرامرزی مستقیم به داده‌های تحت حاکمیت دول خارجی در تضاد با اصول پذیرفته‌شدهٔ حقوق بین‌الملل، به ویژه اصل حاکمیت سرزمینی و همچنین در تضاد با تضمینات حقوق شکلی برای حفظ حقوق کاربران قرار دارد. با این‌حال، بسیاری از دولت‌ها به منظور جمع‌آوری ادلهٔ الکترونیکی به تفتیش مستقیم داده‌های فرامرزی می‌پردازند، گرچه رویه‌های متفاوتی را در این زمینه دنبال می‌کنند. مطابق کنوانسیون بوداپست نیز دولت‌های عضو در شرایطی می‌توانند مستقیماً به داده‌های فرامرزی دسترسی یابند. در کنوانسیون اتحادیهٔ عرب در زمینهٔ مبارزه با جرایم فناوری اطلاعات نیز مقررات مشابهی وجود دارد.

در این مقاله، سازکارهای دسترسی به داده‌های فرامرزی، مشکلات و ضعف‌هایشان مورد بررسی قرار خواهد گرفت. ارزیابی سازکارهای موجود، از جمله معاضدت قضایی با توجه به افزایش نیاز به دسترسی مستقیم به داده‌های فرامرزی برای تعقیب جرایم، نشان‌دهندهٔ ناکارآمدی‌های روش‌های سنتی همکاری است. دولت‌ها نیازمند روش‌های کارآمدتری برای همکاری در این زمینه‌اند تا سرعت عمل لازم برای جمع‌آوری ادلهٔ الکترونیکی تأمین گردد. البته این روش‌ها باید در مطابقت با چارچوب‌های حقوقی داخلی و بین‌المللی باشند. تا زمانی‌که

۱. ابر رایانه‌ای (Computer Cloud) به سیستمی رایانه‌ای اطلاق می‌شود که کاربران مختلف از سراسر جهان می‌توانند داده‌های خود را به وسیلهٔ شبکهٔ اینترنت بر روی آن ذخیره نمایند و آنان را قادر می‌سازد تا بدون نیاز به ذخیره‌سازی داده‌ها در رایانه‌های شخصی یا سازمانی، در هر زمان و مکان از طریق اینترنت به داده‌های مزبور دسترسی یابند.

ناکارآمدی‌های روش‌های سنتی همکاری بین‌المللی مورد توجه قرار نگیرد، رویکرد سرزمینی دولت‌ها و مفروض پنداشتن لزوم همکاری با دولت ذی‌صلاح برای دسترسی به داده‌ها مانع از جایگزینی روش‌های سنتی همکاری با شیوه‌های مؤثرتری خواهد بود.

روش‌های سنتی دسترسی فرامرزی به داده‌ها با چالش‌هایی جدی، از جمله طولانی بودن فرایند اجرای درخواست‌های همکاری و عدم هماهنگی اختیارات شکلی جمع‌آوری ادلهٔ الکترونیکی همراه‌اند. شناسایی حوزهٔ صلاحیت قضایی مربوطه برای ارائهٔ درخواست همکاری، چالش دیگری است که در این خصوص وجود دارد. با توجه به گسترهٔ پراکندگی جغرافیایی سِرورها و مراکز داده و استفادهٔ روزافزون از رایانش ابری این چالش، در حال تبدیل شدن به یک بحران است. از طرفی دسترسی مستقیم به داده‌های فرامرزی با خطر نقض حاکمیت ملی دولت‌ها از طریق اِعمال فراسرزمینی قوانین داخلی، عدم شفافیت دولت‌ها در انجام تحقیقات کیفری فراسرزمینی و نقض حقوق فردی کاربران همراه است.

۱. مفهوم دادهٔ فرامرزی

داده‌های فرامرزی داده‌هایی هستند که از طریق شبکه‌های ارتباط دیجیتالی بین‌المللی از کشوری به کشور دیگر منتقل می‌شوند. این داده‌ها در بستر اینترنت جهانی سیال‌اند و مأموران تحقیق داخلی، صرف نظر از محل ذخیرهٔ آنها، قادر به دسترسی به آنها نیستند. به‌طور مثال داده‌هایی که تراکنش‌های مالی را در مقیاس بین‌المللی ممکن می‌سازند و داده‌های ترافیکی در مواردی که ارتباطات اینترنتی مظنونین از طریق شرکت‌های خارجی ارائه‌دهندهٔ خدمات اینترنتی برقرار می‌شود، داده‌های فرامرزی هستند.[۱]

اغلب داده‌های فرامرزی، از جمله نامه‌های الکترونیکی، ارتباطات صوتی اینترنتی، فرسته‌های شبکه‌های اجتماعی، تراکنش‌های مالی بین‌المللی، پیشینه‌های جستجوی اینترنتی، داده‌های هوانوردی، مسیرهای پرواز و ... توسط شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی نظیر گوگل، یاهو،

۱. خدمات بزرگ‌ترین شبکه‌های اجتماعی در بسیاری از کشورها از جمله کشورهای بزرگ توسط شرکت‌های آمریکایی ارائه می‌شود. همچنین بزرگ‌ترین فروشگاه‌های آنلاین بین‌المللی اغلب متعلق به شرکت‌های آمریکایی است. نک:

https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/; https://www.bloggersideas.com/top-10-online-shopping-sites-in-world-best-shopping-sites-in-world/

مایکروسافت، اپل و آمازون منتقل می‌شوند و در کنترل آنها قرار دارند. معمولاً تارنماها یا نرم‌افزارهای مورد استفاده برای تبادل داده‌ها تنها نقطهٔ شروع برای انجام تحقیقات کیفری هستند. مأموران از این طریق می‌توانند شرکتی را که احتمالاً داده‌ها را در اختیار دارد، شناسایی نمایند.

به طور کلی می‌توان گفت داده‌های فرامرزی داده‌هایی هستند که صرف‌نظر از محل ذخیره‌شان، تحت حاکمیت دولت‌های خارجی قرار دارند و قوانین دولت‌های خارجی بر آنها اعمال می‌شود. حاکمیت بر داده‌ها بیش از هر چیز در اختیار قانونی تفتیش و توقیف آنها متجلی است. در جهان تبادل داده‌های سیال، موقعیت مکانی داده‌ها به عنوان معیار صلاحیت و انتخاب قانون حاکم به طور فزاینده‌ای اهمیت خود را از دست می‌دهد و دولت‌ها نمی‌توانند به آسانی احکام و تصمیمات خود را در خصوص داده‌های فرامرزی اجرا نمایند، مگر با همکاری بازیگرانی در دیگر کشورها. همه‌گیری تبادل داده‌ها در سطح جهانی و وابستگی فزایندهٔ جوامع به آن، سبب شکل‌گیری مفهوم جدیدی از حاکمیت می شود که دیگر محدود به مرزهای جغرافیایی نیست، بلکه مجموعه‌ای از وابستگی‌هاست که می‌تواند ورای مرزهای ملی باشد.[1]

۲. صلاحیت در دسترسی به داده‌های فرامرزی

اولین گام در دسترسی به داده‌های فرامرزی، تعیین دولت ذی‌صلاح برای تفتیش و توقیف داده‌هاست. صلاحیت در جمع‌آوری ادلهٔ جرم، از جمله داده‌های رایانه‌ای، نمودی از صلاحیت اجرایی دولت‌هاست. برخلاف صلاحیت‌های تجویزی و قضایی، صلاحیت اجرایی دولت‌ها محدود به قلمروی سرزمینی آنهاست؛ مطابق حقوق بین الملل، دولت‌ها از صلاحیت اجرای قوانین داخلی خود در قلمروی یکدیگر برخوردار نیستند؛ مگر در شرایط خاص یا موافقت صریح دولت طرف مقابل.[2] بنابراین انجام اقدامات قهری برای اجرای قوانین یا احکام قضایی جلوه و نمود حاکمیت دولت‌هاست و هیچ دولتی به مقامات خارجی اجازه نمی‌دهد تا از اختیارات تعقیبی خود در قلمروی حاکمیتی او استفاده نمایند. دسترسی بدون رضایت ممکن است مداخله در امور داخلی دیگر دولت‌ها و نقض حاکمیت آنان تلقی گردد.[3]

1. .Daskal, J., "Borders and Bits," *Vanderbilt Law Review 71*. 2018,pp 232-235.
2. Cassese, A. *International Law*. First Ed. Oxford: Oxford University Press. 2001,p 53.
3. Trudel, P. 1998, "Jurisdiction over the Internet: A Canadian Perspective," *The International Lawyer* 32, 1998, p 1047.

تعارض صلاحیت در زمینهٔ دسترسی به داده‌های فرامرزی، در صورتی ایجاد می‌شود که مأمورین تحقیق دولت تعقیب‌کنندهٔ جرم درصدد برآیند تا داده‌های فرامرزی مورد نظرشان را جمع‌آوری کنند و در عین حال، دولت متبوع یا مقر شرکت یا شخصی که داده‌ها را در اختیار دارد و یا دولت محل استقرار سِرور ذخیره‌کنندهٔ داده‌ها قوانین متفاوتی را در زمینهٔ شرایط و نحوهٔ دسترسی مأمورین به داده‌های کاربران اِعمال نمایند. موضوع زمانی پیچیده‌تر می‌شود که داده‌ها متعلق به کاربری خارجی باشند یا همان‌طور که در رایانش ابری متداول است، نسخه‌های متعددی از داده‌های مورد نظر در سِرورهای متعدد در نقاط مختلف جهان ذخیره شده باشند. ممکن است یک تارنما از قسمت‌های مختلفی ساخته شده باشد که در سرورهای مختلفی در نقاط مختف جهان ذخیره شده‌اند.[۱] انجام اقدامات قهرآمیز برای دسترسی دولت تعقیب‌کنندهٔ جرم به داده‌ها اغلب مستلزم استفاده از حکم یا مجوز تفتیش است. این در حالی است که حکم صادرشده از سوی دادگاه دولت تعقیب‌کنندهٔ جرم تنها در حوزهٔ صلاحیتی همان دادگاه قابل اجراست. هنوز راه‌حل قانونی تثبیت‌شده‌ای برای حل این تعارض وجود ندارد، اما با افزایش شمار دعاوی در زمینهٔ دسترسی فرامرزی، رویهٔ دولت‌ها در این زمینه در حال تکوین است.[۲]

شاید تصور شود حاکمیت دولت بر داده‌ها همچون حاکمیت آن بر فضاهای جغرافیایی است؛ زیرا داده‌ها به ابزارهای فیزیکی وابسته‌اند و این ابزارها در حاکمیت دولت‌های محل استقرارشان قرار دارند. اما در واقع این ابزارها در بسیاری از موارد موضوعیت خود را از دست داده‌اند و آنچه در این فضا دارای محوریت است، «اطلاعات» می‌باشد که به دشواری می‌توان محل دقیق ایجاد و ذخیرهٔ آن را تعیین نمود.[۳] با غیرسرزمینی شدن حاکمیت بر فضای مجازی، تعیین قواعدی مطلق در زمینهٔ صلاحیت بر داده‌ها ممکن نیست، بلکه باید در هر مورد بسته به شرایط و با استفاده از معیارهای راهنما به دنبال پاسخ بود.

موقعیت سرزمینی داده‌ها یا سِرور ذخیره‌کننده به‌طور کلی نمی‌تواند به عنوان معیاری برای تعیین دولت ذی‌صالح در دسترسی به داده‌ها به کار رود. در فضای مجازی مرز وجود ندارد تا به

۱. سیفی، سیدجمال و نگار عقیقی، **اصول حاکم بر اعمال صلاحیت تجویزی در فضای مجازی**، ویژه‌نامهٔ مجلهٔ حقیقات حقوقی، ۱۳۸۹، شمارهٔ ۲، ص۳۳۵.

2. Daskal, J., "Borders and Bits," *Vanderbilt Law Review 71*. 2018, pp 186-209.

۳. خانعلی پور، سکینه، ***بازاندیشی معیارهای صلاحیت کیفری سایبری***، مجموعه مقالات همایش جنبه‌های حقوقی فناوری اطلاعات ایران، تهران: دانشگاه علم و فرهنگ. ۱۳۹۷، ص۱۵۱.

روشنی بتوان به قاعدهٔ صلاحیت سرزمینی استناد کرد.[۱] داده‌های ابرهای رایانه‌ای به طور خودکار در مراکز دادهٔ متعدد در کشورهای مختلف ذخیره می‌شوند[۲] و ممکن است شرکت‌های ارائه‌دهندهٔ خدمات ابررایانه‌ای به دلیل پیچیدگی‌های ذخیره‌سازی داده‌ها قادر به تعیین محل داده‌ها نباشند.[۳] قراردادهای میان شرکت‌های خدمات ابررایانه‌ای و کاربران نیز همیشه موقعیت مراکز داده‌ای را که اطلاعات در آنها ذخیره می‌شوند، آشکار نمی‌سازند.[۴] چنانچه محل ذخیره‌سازی داده‌ها به عنوان معیار صلاحیت بر دسترسی پذیرفته شود، در صورت مشخص نبودن محل مزبور، معلوم نیست قوانین کدام دولت بر دسترسی به داده‌ها و حفاظت از حریم شخصی کاربران حاکم خواهد بود. دعوای شرکت مایکروسافت در برابر ایالات متحده[۵] نشان داد که حتی داده‌های یک نامهٔ الکترونیکی ممکن است در موقعیتی کاملاً بی‌ارتباط با محل فرستنده و گیرنده و حتی محل شرکت ارائه‌کنندهٔ خدمات اینترنتی ذخیره شوند. به علاوه، حتی ممکن است داده‌ها در چندین موقعیت ذخیره شوند تا سریع‌تر بازیابی گردند. همچنین ممکن است داده‌ها بدون دخالت انسانی و بر اساس الگوریتم‌های تبادل داده‌ها، از موقعیتی به موقعیتی دیگر منتقل شوند. موقعیت تصادفی و غیرقابل پیش‌بینی داده‌ها صلاحیت مبتنی بر سرزمین را با چالش روبرو ساخته، سبب شده برخی از دولت‌ها به وضع قوانینی برای داخلی‌سازی داده‌ها[۶] روی آورند. البته به نظر

۱. فروغی، فضل‌الله و امیر البوعلی، **صلاحیت کیفری مراجع قضایی در فضای سایبری**، ویژه‌نامهٔ مجلهٔ تحقیقات حقوقی، ۱۳۸۹، ص۳۴۹.

2. Peterson, Z.N.J., and M. Gondree, and R. Beverly, **A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud**, Usenix (June 2011), 3, available at:
https://www.usenix.org/legacy/events/hotcloud11/tech/final_files/Peterson.pdf (last visited on 11/10/2018).

3. Schwerha, J. J., **Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from Cloud Computing Providers**, Council of Europe Project on Cybercrime Discussion (January 2010), available at:
https://rm.coe.int/16802fa3dc (last visited on 11/10/2018).

4. Benson, K., and R. Dowsley, and H. Shacham, **Do you know where your cloud files are?**, Proceedings of the 3rd ACM Workshop on Cloud Computing Security (October 2010), available at:
http://iks.ira.uka.de/fileadmin/User/Dowsley/pdf/BenDowSha11.pdf (last visited on 11/10/2018).

5. Microsoft Corp. V. United States (2017).

۶. داخلی‌سازی داده‌ها (Data localization) عبارت است از ذخیره‌سازی داده‌های رایانه‌ای کاربران داخلی پیش از آنکه از طریق شبکهٔ اینترنت به خارج از مرزهای ملی منتقل و در سرورهای خارجی ذخیره گردند. داخلی‌سازی داده‌ها بر مفهوم حاکمیت بر داده‌های داخلی مبتنی است.

نمی‌رسد داخلی‌سازی داده‌ها راه حل مناسبی باشد؛ زیرا چنانچه اصول صلاحیتی به خوبی با واقعیات فعالیت‌های بشری منطبق نباشند، نشانگر ضرورت تغییر اصول مزبور است، نه نیاز به تغییر و محدودسازی فعالیت‌ها.[1]

مقر شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی نیز می‌تواند به عنوان معیاری کمکی برای تعیین صلاحیت به کار رود، نه معیاری مطلق. مقر شرکت در بسیاری از موارد، نشانگر وجود پیوندهای قوی میان شرکت و حاکمیت دولت مقر است و تمایل شرکت به متابعت از قانون آن دولت را نشان می‌دهد، اما گاهی غیرواقعی و صوری است. ممکن است شرکت‌ها به منظور دور زدن قوانین مالیاتی کشور محل فعالیت خود در کشوری خارجی به ثبت برسند. بنابراین، تعیین صلاحیت صرفاً بر اساس مقر شرکت و بدون توجه به واقعیت‌های اقتصادی و اجتماعی می‌تواند گمراه‌کننده باشد. پیوستگی اجتماعی–اقتصادی با جامعه در مقایسه با ارتباطات اختیاری، تحریف‌شده و غیراساسی با حاکمیت سرزمینی معیار مقبول‌تری برای تعیین صلاحیت است. پرسش اصلی این است که طرفین به چه میزانی در پیوند با یک جامعه قرار دارند و اختلاف آنها تا چه حد با منافع آن جامعه در ارتباط است. دعوای مایکروسافت و ایالات متحده نشان داد که معیار مناسب برای تعیین دولت صالح، نه محل ذخیره‌سازی داده‌ها که موقعیت و تابعیت کاربر یا شرکتی است که دولت، خواستار دسترسی به داده‌های متعلق به او یا تحت کنترل اوست؛ چرا که دسترسی به داده‌های کاربر و نقض حریم خصوصی او بیشترین ارتباط را با جامعهٔ کاربر داراست. به علاوه یکی از مهم‌ترین پیوندها با یک کشور، ارائهٔ خدمات در آن کشور است که می‌تواند به عنوان معیاری برای سنجش پیوستگی شرکت‌های خدمات اینترنتی با کشورها به کار رود. تلاش مستمر یک شرکت برای دسترسی به بازار خدمات اینترنتی یک کشور به عنوان یک راهبرد تجاری، آن شرکت را در پیوند با منافع کشور مزبور قرار می دهد. استفاده از این معیار در مقایسه با معیار موقعیت شرکت امکان کمتری را برای فرار از صلاحیت به وجود می‌آورد.[2]

آثار و نتایج ایجاد شده به وسیلهٔ داده‌ها یا فعالیت‌های مرتبط با آنها نیز ممکن است مبنایی برای صلاحیت دسترسی به داده‌ها تلقی شود. اِعمال صلاحیت فراسرزمینی در بسیاری از موارد بر اساس تأثیر فعل یا موضوع قابل توجیه است. با وجود این، و با توجه به گستردگی جهانی

1. Chander A. and Lê U.," Data Nationalism," *Emory Law Journal* 64, 2015.
2. Daskal, J., "Borders and Bits," *Vanderbilt Law Review 71*. 2018: 195.

اینترنت، محتوای تارنماهای اینترنتی در هر نقطه‌ای از جهان قابل دسترسی هستند و به طور بالقوه می‌توانند بر قلمروی هر دولتی تأثیر بگذارند. در نتیجه، صلاحیت بر اساس آثار و نتایج می‌تواند منجر به پذیرش صلاحیت جهانی شود. از این‌رو این معیار باید با در نظر گرفتن دیگر معیارها و بر اساس تفسیری مضیق به کار گرفته شود.[۱]

شروط قراردادی، یکی دیگر از معیارهای تعیین صلاحیت برای دسترسی است. بیشتر روابط میان کاربران و شرکت‌های خدمات اینترنتی دست‌کم در ظاهر بر این شروط مبتنی‌اند. ممکن است این شروط شامل پذیرش صلاحیت یک حوزهٔ صلاحیتی و همچنین پذیرش قانون آن حوزه به عنوان قانون حاکم بر قرارداد باشد. البته ممکن است این شروط به دلایل مختلف اجرا نشوند. ارزیابی اولیهٔ اعتبار قرارداد بر اساس قانون داخلی صورت می‌گیرد نه قانون انتخابی، و در صورت عدم اعتبار قرارداد نزد دادگاه، شروط آن نیز بی‌اعتبار خواهند بود. قراردادهای ارائهٔ خدمات، مورد مذاکرهٔ طرفین قرار نمی‌گیرند و قراردادهایی الحاقی هستند. در نتیجه، ممکن است شروط ناعادلانه لازم‌الاجرا تلقی نشوند. به علاوه، برخی از دادگاه‌ها به طرفین اجازه نمی‌دهند تا قانون داخلی را با انتخاب قانون خارجی دور بزنند. همچنین دادگاه می‌تواند ارزیابی خود از اختلاف را تغییر دهد و موضوع اختلاف را یک شبه‌جرم یا یک موضوع دیگر مربوط به حقوق جزا یا یک رژیم غیرقراردادی دیگر قلمداد نماید.[۲] در نتیجه شروط قراردادی همیشه نمی‌توانند تعیین‌کنندهٔ دولت ذی‌صلاح در دسترسی به داده‌ها باشند. شورای اروپا نیز موافقت کلی کاربران با شروط قراردادی را رضایت صریح آنان نسبت به دسترسی دولتی به داده‌هایشان قلمداد نمی‌نماید، حتی اگر در این شروط امکان دسترسی به داده‌ها در صورت سوءاستفاده از آنها پیش‌بینی شده باشد.[۳]

۳. دسترسی به داده‌های فرامرزی از طریق معاضدت قضایی

معاضدت قضایی روشی برای همکاری بین‌المللی در امور کیفری است که از دههٔ ۷۰ میلادی

1. Kuner. C.. "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)," *International Journal of Law and Information Technology* 18. 2010,p 197.
2. Schiff Berman, P., "Legal Jurisdiction and the Deterritorialization of Data," *Vanderbilt Law Review 71*. 2018: 30.
3. Council of Europe Cybercrime Convention Committee (T-CY), Transborder Access to (Data Article 32), Council of Europe (December 2014), available at: https://rm.coe.int/16802e726a (last visited on 11/10/2018).

و به دلیل نیاز فزاینده به همکاری در زمینهٔ مبارزه با جرایم فراملی و از طریق انعقاد معاهدات دو یا چندجانبه، جایگزین فرایند زمان‌بر و پرهزینهٔ تبادل‌نامه‌های نیابت قضایی شده است.[1] در معاضدت قضایی دولت‌ها بنا به درخواست دولت تعقیب‌کنندهٔ جرم و به منظور انجام تحقیقات کیفری از اختیارات شکلی خود نظیر تفتیش و توقیف ادله، اخذ شهادت، بازداشت متهمین، ضبط عایدات جرم و کنترل ارتباطات راه دور استفاده می‌کنند. چنانچه دولت‌ها در فرایند تعقیب جرم نیازمند دسترسی به ادله‌ای باشند که تحت حاکمیت دولت دیگری قرار دارد، معاضدت قضایی راه‌حل معمول برای اجتناب از نقض حاکمیت آن دولت است. ممکن است درخواست معاضدت قضایی به دولتی غیر از دولت محل ذخیرهٔ داده‌ها ارائه شود. برای مثال، با اینکه شرکت فیس‌بوک[2] داده‌های بسیاری از کاربرانش را در اروپا ذخیره می‌نماید، اما مطابق مقررات داخلی خود فقط زمانی داده‌ها را در دسترس دولت‌های خارجی قرار می‌دهد که درخواست معاضدت قضایی به دولت ایالات متحده ارائه و با آن موافقت شود.[3] در نتیجه، گاهی عملاً منافع دولت محل کنترل داده‌ها بر منافع دولت محل ذخیره‌سازی آنها اولویت دارد.

امروزه دولت‌ها برای دسترسی به داده‌های تحت حاکمیت یکدیگر، عمدتاً بر مبنای معاهدات دو یا چندجانبهٔ معاضدت قضایی یا بر اساس عمل متقابل همکاری می‌نمایند.[4] فرایندهای معاضدت قضایی بسته به چارچوب‌های بین‌المللی و قوانین داخلی متفاوت است. به طور مثال، ممکن است درخواست‌ها فقط توسط مقام مرکزی معینی دریافت گردند یا استفاده از مجاری ارتباطی نظیر اینترپل مجاز باشد.[5] همچنین مقاماتی که اجازهٔ دسترسی مأموران خارجی به داده‌ها را صادر می‌کنند، در کشورهای مختلف و بسته به نوع داده‌ها متفاوت‌اند. به طور مثال، ممکن

1. Davis, D. J. Criminal Law and the Internet: The Investigator's Perspective, in: *Crime, Criminal Justice and the Internet*, edited by Clive walker. 1th Ed. London: Sweet & Maxwell, 1998, p 51.
2. Facebook.
3. Facebook Company, **Information for Law Enforcement Authorities**, Facebook Website, available at: http://www.facebook.com/safety/groups/law/guidelines/(last visited on 11/10/2018).
4. Council of Europe Cybercrime Convention Committee (T-CY), **T-CY Assessment report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime**, Council of Europe (December 2014), 31, available at: https://rm.coe.int/16802e726c (last visited on 11/9/2018).
5. Ibid, 38.

است صدور اجازهٔ دسترسی فرامرزی به داده‌های ترافیکی[۱] در یک کشور در صلاحیت پلیس باشد و در کشور دیگری در صلاحیت دادگاه. برخی از دولت‌ها رویه‌هایی را برای اجرای سریع درخواست‌های همکاری اتخاذ نموده‌اند؛ به عنوان مثال، مقامات ذی‌صلاح برخی دولت‌ها در موارد اضطراری می‌توانند درخواست‌هایی را که از طریق اینترپل ارائه شده است، پیش از آنکه توسط مقامات مرکزی دریافت شوند، اجرا نمایند.[۲]

در حدود ۷۰ درصد همکاری‌ها از طریق بین‌المللی برای تعقیب جرایم سایبری با استفاده از معاضدت قضایی صورت می‌گیرد که اغلب در زمینهٔ دسترسی به داده‌های فرامرزی هستند.[۳] با این‌حال، در زمینهٔ روش‌ها و مقتضیات معاضدت قضایی رویکرد واحدی میان دولت‌ها وجود ندارد. در برخی از کشورها، داده‌های به دست‌آمده از طریق معاضدت قضای در مقایسه با داده‌هایی که از طریق سایر روش‌های همکاری- نظیر همکاری پلیسی- به دست آمده‌اند، از ارزش استنادی کمتری برخوردارند. قوانین برخی دیگر از دولت‌ها از انعطاف‌پذیری بیشتری برخوردارند و برخی از انواع داده‌های به دست‌آمده از طریق معاضدت قضایی (نظیر داده‌های محتوایی) را ادله‌ای قابل استناد می‌دانند؛ در حالی‌که برخی از دادگاه‌ها تمامی داده‌های به دست‌آمده از طریق معاضدت قضایی را استنادپذیر تلقی می‌کنند و فقط کافی است داده‌ها مطابق قانون دولت ذی‌صلاح و بدون نقض رویه‌های شکلی داخلی به دست آمده باشند.[۴]

در بیشتر موارد گزارش‌شده، معاضدت قضایی نیاز به سرعت عمل در تعقیب جرایم سایبری را برآورده نساخته است.[۵] بر اساس مطالعهٔ کمیتهٔ شورای اروپا، معاضدت قضایی روشی پیچیده، زمان‌بر و پرهزینه است[۶] و دسترسی به داده‌ها از این طریق ممکن است ماه‌ها یا حتی سال‌ها به

۱. داده‌های ترافیکی (Traffic data) داده‌هایی هستند که شبکهٔ اینترنت از آنها برای تعیین موقعیت مبدأ و مقصد یک ارتباط استفاده می‌کنند و برقراری ارتباط و انتقال داده‌های محتوایی را در مسیر ارتباط میسر می‌سازند.

2. Ibid, 152.

3. United Nation Office of Drugs and Crime. *Comprehensive Study on Cybercrime.* First Ed. Vienna: UNODC Publications, 2012: 201.

4. Council of Europe Cybercrime Convention Committee (T-CY), **T-CY Assessment report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime**, Council of Europe (December 2014), 31, available at: https://rm.coe.int/16802e726c (last visited on 11/9/2018).

5. Ibid, 38-9.

6. Ibid, 123.

طول بینجامد.[۱] این در حالی است که با توجه بـه ناپایـداری ادلـهٔ الکترونیکـی، انجـام تحقیقـات کیفری در محیط سایبری مستلزم سرعت عملی بالاست. در واقع سـازکارهای کنـونی معاضـدت قضایی پیش از پیدایش اینترنت شکل گرفتـه‌انـد و تناسـبی بـا واقعیـات جهـان امـروز ندارنـد. بروکراسی، کمبود منابع مالی و انسانی، ناآگاهی از ضوابط و معیارهای قانونی دولت طرف مقابـل، عدم شفافیت در بررسی و اجرای درخواست‌ها، عدم کفایت ادله برای اثبات ضرورت دسترسی بـه داده‌ها و فقدان یک چارچوب استاندارد برای تنظیم درخواسـت‌هـای معاضـدت از جملـه عوامـل کندی فرایندهای معاضدتی هستند. علاوه بر این، در بسیاری از موارد دولت‌هـا بـه دلیـل فقـدان چارچوب‌های معاهداتی نمی‌توانند از سازکار معاضدت قضایی استفاده نمایند؛ هنوز میان برخـی از دولت‌ها هیچ توافقی در زمینهٔ معاضدت قضایی وجود ندارد و یا در صورت وجـود، در مـورد ادلـهٔ الکترونیکی فاقد کارایی هستند. به عبارتی، رژیم‌های معاهداتی معاضـدت قضـایی هنـوز فراگیـر نیستند. البته ممکن است دولت‌ها درخواست‌های معاضدت را فقط بـر اسـاس اصـل همکـاری و برای رعایت نزاکت بین‌المللی اجرا نمایند. با این‌حال، همکاری بین‌المللی در امور کیفـری بـدون وجود یک چارچوب حقوقی از پیش تعیین شده و الزام‌آور، کُند و پرهزینه است و به دلیـل فقـدان تعهدات قانونی، تضمینی بـرای موفقیـت‌آمیـز بـودن آن وجـود نـدارد.[۲] حتـی در صـورت وجـود چارچوب‌های معاهداتی، ممکن است دولت‌ها قادر یا مایل به همکاری نباشـند یـا اساسـاً تعیـین دولت ذی‌صلاح – به طور مثال به دلیل ویژگی‌های ابرهای رایانه‌ای ممکن نباشد.[۳] با وجود این، معاضدت قضایی تضمین‌کنندهٔ احترام به حاکمیت دولت‌هاسـت؛ چـرا کـه شـفافیت در دسترسـی دیگر دولت‌ها به داده‌های تحت حاکمیتشان را در حد مطلـوبی تـأمین مـی‌نمایـد. بـا ایـن‌حـال، دولت‌ها برای استفادهٔ کارآمد از این سازکار بایـد ابتکـار بیشـتری بـرای اصـلاح و بـه‌روزرسـانی معاهدات معاضدت قضایی به عمل آورند.

1. Ibid, 39.
2. Andrew K. Woods**, Data Beyond Borders: Mutual Legal Assistance in the Internet Era**, 2015, p 3, available at: https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub (last visited on 10/10/2018).
3. New Zealand Law Commission, **Search and Surveillance Powers**, lawcom.govt.nz (June 2007), available at: http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf (last visited on 11/9/2018).

٤. دسترسی مستقیم به داده‌های فرامرزی

دسترسی مستقیم به داده‌های فرامرزی عبارت است از دسترسی به داده‌های تحت حاکمیت دیگر دولت‌ها بدون کسب مستقیم مجوز از آنها.[1] بسیاری از دولت‌ها از طریق شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی و دیگر دست‌اندرکاران بخش خصوصی به داده‌های فرامرزی دسترسی پیدا می‌کنند، بی‌آنکه موافقت دولت ذی‌صلاح را جلب نمایند.[2] پیشرفت فناوری، گسترش تهدیدات سایبری و ضرورت مقابلهٔ سریع با فعالیت‌های مجرمانهٔ فرامرزی سبب شده تا دسترسی مستقیم به داده‌های فرامرزی اهمیت فزاینده‌ای یابد، هر چندکه به صورت رسمی مورد پذیرش و حمایت اکثریت دولت‌ها قرار نگرفته است.[3]

درخواست مستقیم مأموران تحقیق از شرکت‌های خارجی ارائه‌دهندهٔ خدمات اینترنتی برای افشای داده‌ها امر غیرمعمولی نیست[4] و به ویژه در مواردی صورت می‌گیرد که مظنون و قربانی از اتباع دولت درخواست‌کننده باشد و جرم نیز در قلمروی همان دولت ارتکاب یافته و حقوق هیچ یک از اتباع دولت متبوع شرکت تحت تأثیر قرار نگرفته باشد.[5] همکاری شرکت‌های مزبور با مقامات خارجی می‌تواند بر مبنای قانون دولت متبوعشان یا قراردادشان با کاربران صورت گیرد. به موجب این قراردادها، شرکت‌ها می‌توانند داده‌های کاربران را در شرایط خاصی در اختیار مقامات تعقیب جرم قرار دهند.[6] البته رویهٔ دولت‌ها در این زمینه متفاوت است. در برخی کشورها

1. European Committee of Crime Problem, **Explanatory Report to the Convention on Cybercrime**, Council of Europe (November 2001), available at: https://rm.coe.int/16800ce5b (last visited on 11/9/2018).
2. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December 2012), available at: https://rm.coe.int/16802e79e8 (last visited on 11/10/2018).
3. Goldsmith J, L. "The Internet and the Legitimacy of Remote Cross-Border Searches," *The University of Chicago Legal Forum* 103, 2001,p 7.
4. Walden, I. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, in: *Privacy and Security for Cloud Computing*, Edited by Pearson, S. First Ed. New York: Springer, 2011, p 55.
5. Swire, p. & Hemmings, J. D., "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," *New York Annual Survey of American Law 71*. 2015, p 720.
6. Bradshaw, S., C. Millard and I. Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services," *International Journal of Law and Information Technology* 19, 2011,p 199.

شرکت‌ها تنها می‌توانند داده‌های ترافیکی و داده‌های مربوط به اشتراک اینترنتی[۱] کاربران را در اختیار دولت‌های خارجی قرار دهند. در برخی دیگر از کشورها تنها داده‌های مربوط به اشترک اینترنتی بر اساس عمل متقابل به اشتراک گذارده می‌شوند و در شماری از کشورها نیز فقط داده‌هایی افشا می‌شوند که توسط پلیس و از طریق اقدامات غیرقهری و بدون حکم دادگاه به دست آمده باشند. با اینکه دسترسی مستقیم به داده‌های فرامرزی در رویهٔ دولت‌ها در حال افزایش است و سازمان‌های بین‌المللی به طور فزاینده‌ای از آن حمایت می‌کنند. در خصوص قاعده‌مندسازی آن رویکرد واحدی وجود ندارد و در قوانین داخلی چندان به آن پرداخته نشده است.[۲] اگرچه به تدریج شرکت های غیرآمریکایی بیشتری به ارائهٔ خدمات اینترنتی در سطح جهانی می‌پردازند، با این‌حال، امروزه شرکت‌های آمریکایی بخش عمدهٔ بازار جهانی خدمات اینترنتی را در اختیار دارند و از این‌رو قوانین و رویهٔ دولت ایالات متحده بیش از قانون هر کشور دیگری بر دسترسی به داده‌های کاربران اِعمال می‌شود.[۳]

علاوه بر دسترسی از طریق شرکت‌های خدمات اینترنتی، دولت‌ها با استفاده از ابزارهای فنی جدید می‌توانند تحقیقات خود را از راه دور انجام دهند و به جمع‌آوری داده‌ها از قلمروی حاکمیتی دیگر دولت‌ها بپردازند. به عنوان مثال، اف‌بی‌آی با استفاده از یک برنامهٔ ردیابی به نام «فانوس جادویی» مرتکبین جرایم سایبری را ردیابی می‌کند. این برنامه با نصب یک ویروس بر روی رایانهٔ مظنونان، کل داده‌های آنها را ضبط و منتقل می‌نماید.[۴] این بدان معناست که اف‌بی‌آی نیازی به دسترسی مستقیم به رایانهٔ مظنونان در هر کجای دنیا که باشد، ندارد و این امر می‌تواند منجر به نقض حاکمیت دولت محل استقرار سیستم‌های هدف گردد. به‌علاوه شماری از دولت‌ها

۱. داده‌های مربوط به اشتراک اینترنتی (Subscriber data) داده‌هایی هستند که نشانی‌های اینترنتی را به اشخاصی که از آنها استفاده می‌کنند، مربوط می‌سازند و به وسیلهٔ آنها می‌توان به هویت کاربران خدمات اینترنتی، موقعیت جغرافیایی یا آدرس پستی آنان، نوع خدمات و امکانات فنی مورد استفاده و مدت زمان آن پی برد.

2. O'Floinn, M., "It Wasn't All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe," *Computer Law & Security Review* 29, 2013, p 611.

3. Westmoreland, K. and Kent, G., "Foreign Law Enforcement Access to User Data: A Survival Guide and Call for Action," *Canadian Journal of Law and Technology 13*, 2015,p 227.

۴. عقیقی، نگار، ***صلاحیت در فضای مجازی از منظر حقوق بین‌الملل***، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش، ۱۳۹۶، ص ۱۶۷.

استفادهٔ مأموران تحقیق از نرم‌افزارهای جاسوسی نظیر کِیلاگرز[1] و اسنیفرز[2] را برای دسترسیِ از راه دور به داده‌های فرامرزی قانونی می‌دانند.[3]

گروه هشت کشور صنعتی، هم‌زمان با مذاکرات تدوین کنوانسیون بوداپست، دسترسی مستقیم به داده‌های فرامرزی را مورد بحث قرار داد و در سال ۱۹۹۹ «اصول دسترسی فرامرزی به داده‌های رایانه‌ای ذخیره‌شده»[4] را تصویب نمود. مطابق اصل ششم، دسترسی به داده‌های فرامرزی که در دسترس عموم قرار دارند (داده‌های با منبع باز) و نیز دسترسی با جلب رضایت قانونی اشخاصی که از اختیار افشای داده‌ها برخوردارند، مستلزم معاضدت قضایی نمی‌باشد. البته چنانچه داده‌های مورد نظر، نقض قوانین کیفری را آشکار نماید یا به نحو دیگری به منافع دولت محل ذخیرهٔ داده‌ها مربوط باشد، دولت تفتیش‌کننده باید آن دولت را مطلع نماید. به نظر می‌رسد مادهٔ ۳۲ کنوانسیون بوداپست از این اصل الگوبرداری شده است.[5] این ماده نیز دسترسی فرامرزی مستقیم به داده‌های عمومی و دسترسی مستقیم با رضایت را پیش‌بینی نموده است، هرچند اطلاع‌رسانی به دولت محل ذخیرهٔ داده‌ها را ضروری نمی‌داند. در واقع می‌توان این ماده را استثنایی بر اصل حاکمیت سرزمینی دانست.

کنوانسیون بوداپست پیش از فراگیر شدن رایانش ابری و سیطرهٔ شرکت‌های خدمات اینترنتی بر ارتباطات جهانی تدوین شده است و از این‌رو با واقعیات امروز چندان هم‌خوانی ندارد. در نتیجه، تمرکز اصلی آن بر صلاحیت دولت محل ذخیرهٔ داده‌ها قرار دارد، درحالی‌که امروزه این معیار کمتر مورد توجه است. علاوه بر این، تدوین‌کنندگان کنوانسیون بوداپست از تبیین جزئیات

1. Key Loggers.

2. Sniffers.

3. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December 2012).

4. G8 Principles on Trans-Border Access to Stored Computer Data.

۵. مطابق مادهٔ ۳۲ کنوانسیون بوداپست «هریک از دولت‌های عضو می‌توانند بدون کسب مجوز از دولت طرف مقابل:

الف) به داده‌های عمومی بدون توجه به موقعیت جغرافیایی آنها، دسترسی یابند؛ یا

ب) از طریق یک سیستم رایانه‌ای مستقر در قلمروی خود به داده‌های ذخیره‌شده در قلمروی دولت عضو دیگر دسترسی یابند مشروط بر اینکه رضایت قانونی و داوطلبانهٔ شخصی را که از اختیار قانونی افشاء داده‌ها از طریق آن سیستم رایانه‌ای برخوردار است جلب نمایند».

بیشتر در مورد دسترسی فرامرزی به داده‌ها اجتناب نموده، پس از مذاکرات بسیار از ایجاد یک نظام جامع و الزام‌آور در زمینهٔ دسترسی فرامرزی به داده‌ها خودداری کردند. دلیل این تصمیم، از یک طرف فقدان تجربیات عینی و از طرف دیگر این واقعیت بود که راه‌حل مناسب در هر مورد ممکن است، بسته به شرایط خاص متفاوت باشد. مادهٔ ۳۲ الزامی برای طرفین ایجاد نمی‌کند و تنها به تبیین شرایطی می‌پردازد که دسترسی مستقیم به داده‌های فرامرزی بنا به توافق تمامی طرفین مجاز است. البته، برخی بر این باورند که دسترسی مستقیم به داده‌هایی که در دسترس عموم قرار دارند، چنانچه با هدف اجرای عدالت کیفری صورت گیرد یک رویهٔ پذیرفته‌شدهٔ بین‌المللی است و در نتیجه جزئی از حقوق بین‌الملل عرفی می‌باشد.[۱]

بند «ب» مادهٔ ۳۲ ممکن است به عنوان مجوز تفتیش و توقیف از راه دورِ داده‌ها تفسیر گردد.[۲] این بند استثنایی بر اصل حاکمیت سرزمینی است که دسترسی یک جانبه به داده‌های فرامرزی بدون نیاز به معاضدت قضایی را تحت شرایطی مجاز می‌داند؛[۳] هرچند شرایط دقیق چنین اقدامی را مشخص نمی‌نماید. این بند ناظر به شرایطی است که داده‌ها در قلمروی کشور دیگری ذخیره‌شده و همچنین نسبت به این موضوع علم وجود دارد. در نتیجه، این ماده در شرایطی که محل ذخیرهٔ داده‌ها معلوم نباشد- نظیر رایانش ابری- کاربرد ندارد. در نتیجه، رضایت در شرایطی که محل ذخیرهٔ داده‌ها معلوم نیست، نمی‌تواند مجوز دسترسی تلقی گردد. برخی مفسران مقررات این بند را مغایر با اصول حقوق بین‌الملل می‌دانند؛ چراکه مطابق اصل حاکمیت، تعقیب جرم در قلمروی دولت‌های خارجی بدون توافق مجاز نمی‌باشد[۴] و تصمیم‌گیری در مورد دسترسی دولت‌های خارجی نباید در اختیار شخص دارندهٔ داده‌ها باشد؛ زیرا این امر علاوه بر نقض حاکمیت دولت‌ها، موجب عدم شفافیت خواهد شد. این مقررات سبب ایجاد اختلاف

1. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December 2012).
2. Walden, I. *Computer Crimes and Digital Investigations*. Second Ed. Oxford: Oxford University Press, 2007, p 319.
3. Cybercrime Convention Committee (T-CY), 2013, **Transborder Access to Data (Article 32)**, Council of Europe (December 2014), available at: https://rm.coe.int/16802e726a (last visited on 11/9/2018).
4. Gercke, M. *Understanding Cybercrime: Phenomena, Challenge and Legal Response.* First Ed. Vienna: International Telecommunication Union, 2012, p 227.

نظرهای بسیاری میان اعضا شده، به‌طوری‌که دولت روسیه آن را دلیلی برای عدم پذیرش کنوانسیون دانسته است.[1]

مادهٔ ۳۲ در مورد اینکه رضایت شخص ذی‌صلاح تابع قانون کدام کشور است و صلاحیت وی برای افشای داده‌ها بر اساس قانون کدام کشور ارزیابی می‌شود، ساکت است. در دیدگاهی عمل‌گرایانه، رضایت شخص نسبت به دسترسی مستقیم به داده‌ها و صلاحیت او برای افشای داده‌ها، باید بر اساس قانون دولت درخواست‌کننده ارزیابی شود؛ زیرا مأموران تحقیق در شرایط اضطراری قادر به بازشناسی و رعایت مقررات دولت ذی‌صلاح نیستند و عموماً بر اساس قانون دولت خود عمل می‌کنند. با این‌حال، چنانچه دسترسی مستقیم به داده‌ها موجب نقض قوانین دولت محل ذخیرهٔ آنها گردد، نباید مجاز تلقی گردد؛ حتی ممکن است قوانین دولت درخواست‌کنندهٔ ارائهٔ اطلاعات به مقامات خارجی را به طور کلی ممنوع نموده باشند.[2]

اینکه چه کسی از اختیار قانونی افشای داده‌ها برخوردار است، بسته به شرایط و قانون حاکم متفاوت خواهد بود. این شخص ممکن است شخصی حقیقی باشد که دسترسی به اطلاعات پست الکترونیکی خود را میسر می‌سازد یا ممکن است یک شرکت ارائه‌دهندهٔ خدمات اینترنتی یا خدمات ابر رایانه‌ای باشد که از اختیار افشای داده‌های کاربران برخوردار است و یا مالکیت داده‌ها را در اختیار دارد. مطابق بند «ب»، شرکت‌های خدمات اینترنتی باید از اختیار قانونی افشای داده‌ها برخوردار باشند. افشای داده‌ها نباید منجر به نقض حریم خصوصی و دیگر حقوق فردی کاربران شود. بنابراین شرکت‌های خدمات اینترنتی فقط می‌توانند به افشای داده‌هایی بپردازند که مالکیت آنها را در اختیار دارند و داده‌های ترافیکی و داده‌های مربوط به اشتراک اینترنتی از آن جمله‌اند.[3]

1. Giles, K., **Russia's Public Stance on Cyberspace Issues**, 4th International Conference on Cyber Conflict (January 2012), available at: https://www.researchgate.net/publication/261044707_Russia's_public_stance_on_cyberspace_issues (last visited on 11/9/2018).
2. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December 2012), available at: https://rm.coe.int/16802e79e8 (last visited on 11/10/2018).
3. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December 2012), available at: https://rm.coe.int/16802e79e8 (last visited on 11/10/2018).

جمع‌آوری فرامرزی داده‌ها باید مطابق قانون دولت ذی‌صلاح انجام پذیرد. مأموران تحقیق خارجی باید در تحقیقات فرامرزی خود، حقوقی را که دولت حاکم بر داده‌ها برای کاربران به رسمیت شناخته است، حفظ کنند و شروط آن دولت برای دسترسی را رعایت نمایند. البته رویکرد دولت‌ها در زمینهٔ شروط و تضمینات قانونی تعقیب جرم متفاوت است. تفاوت دیدگاه دولت‌ها در خصوص آزادی بیان یا محدودیت‌های تحقیقات قضایی بهترین مثال‌ها در این زمینه شمرده می‌شوند.[۱]

گسترش استفاده از دسترسی مستقیم به داده‌های فرامرزی ممکن است منجر به سوءاستفادهٔ دولت‌هایی شود که پایبندی چندانی به حاکمیت قانون ندارند. برای مثال، دسترسی فرامرزی می‌تواند در ظاهری قانونی، به عنوان ابزاری برای تعقیب مخالفان سیاسی و سرکوب فعالیت‌های سیاسی قانونی به کار رود. دسترسی مستقیم، همچنین امکان دسترسی غیرموجه و نامتناسب به داده‌ها را افزایش می‌دهد. ممکن است دولت‌ها علاوه بر داده‌های مورد نیاز، به جمع‌آوری داده‌هایی بپردازند که برای مقاصد مشروع کیفری نیازی به آنها ندارند. به طور مثال، ممکن است دولت‌ها در مواردی که دسترسی به داده‌های ترافیکی برای ردیابی یک ارتباط کافی می‌باشد، داده‌های محتوایی آن ارتباط را نیز جمع‌آوری کنند. دولت‌ها با در نظر گرفتن منافع قانونی اشخاص ثالث، شرایط و تضمیناتی را در خصوص تفتیش سیستم‌ها و شبکه‌های رایانه‌ای پیش‌بینی می‌نمایند.[۲] با این‌حال، دسترسی مستقیم می‌تواند فعالیت‌های اشخاص ثالث، به خصوص شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی را تحت تأثیر قرار دهد و موجب شود تا این شرکت‌ها مجبور به متابعت از قوانین متفاوت و گاه متعارض دولت‌های ذی‌ربط شوند.[۳]

---

۱. در زمینهٔ تفاوت دیدگاه دولت‌ها در زمینهٔ آزادی بیان، نک:
UN General Assembly, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. A/67/357, 7 September 2012, available at:
https://documents-dds-..

و در زمینهٔ محدودیت‌های تحقیقات قضایی، برای مثال نک:
UN Office of Drug and Crime, The use of the Internet for Terrorist Purposes, 2012, paras 35, 106, 110.

2. European Committee of Crime Problem, **Explanatory Report to the Convention on Cybercrime**, Council of Europe (November 2001), 24, available at: https://rm.coe.int/16800ce5b (last visited on 11/9/2018).

3. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December→

با این همه، دسترسی فرامرزی مستقیم در شرایط خاصی نظیر وجود خطر قریب‌الوقوع، احتمال فرار مظنونین یا احتمال از بین رفتن ادلهٔ جرم باید مجاز باشد. البته در این صورت پیش‌بینی ضوابطی نظیر لزوم اطلاع‌رسانی به دولت صالح ضروری خواهد بود. موافقت دولت‌ها با دسترسی مستقیم به داده‌های فرامرزی مستلزم آن است که این نوع دسترسی با تضمینات شکلی کافی برای حفظ حقوق افراد و اشخاص و منافع قانونی دولت‌ها همراه باشد تا امکان سوءاستفاده از آن محدود گردد. ملاحظات مربوط به حقوق متهمین، حریم خصواصی اشخاص و حفاظت از داده‌های شخصی مسائلی هستند که باید در دسترسی مستقیم به داده‌های فرامرزی مورد توجه دولت‌ها قرار گیرند.

←2012), pp 13-14, available at: https://rm.coe.int/16802e79e8 (last visited on 11/10/2018).

نتیجه‌گیری

روش‌های دسترسی فرامرزی به داده‌ها به دو دسته قابل تقسیم‌اند: نخست معاضدت قضایی است که عموماً بر موافقت دولت ذی‌صلاح مبتنی است و دیگری روش‌های جایگزینی نظیر دسترسی مستقیم و مشروط به داده‌های فرامرزی را شامل می‌شود که دولت حاکم بر داده‌ها نقش مستقیمی در آنها بر عهده ندارد و دسترسی سریع به داده‌ها اولویت اصلی در این روش‌هاست. هر دو دسته دارای مزایا و معایبی هستند.

دسترسی به داده‌ها از طریق معاضدت قضایی بر جلب موافقت دولت ذی‌صلاح متمرکز است و در نتیجه کنترل دولت‌ها بر دسترسی فرامرزی به داده‌های تحت حاکمیتشان را حفظ می‌کند. این روش علی‌رغم استفادهٔ گسترده دولت‌ها، بنا به دلایلی که ذکر شد، بسیار ناکارآمد است و با ماهیت ناپایدار ادلهٔ الکترونیکی سازگار نمی‌باشد. با اینکه معاضدت قضایی برای دسترسی داده‌ها سال‌ها مورد انتقاد قرار گرفته، اما تلاش چندانی برای کارآمدسازی آن صورت نپذیرفته است. چنانچه ضعف‌های این سازکار برطرف نگردد، تمرکز سنتی بر صلاحیت سرزمینی و بدیهی انگاشتن نقش اصلی دولت ذی‌صلاح در انجام تحقیقات فرامرزی به‌تدریج جای خود را به سازکارهای کارآمدتری خواهند داد که لزوماً مستلزم موافقت موردی دولت ذی‌صلاح نیستند. تحولات فناورانهٔ جهان امروز در حال تغییر مفهوم حامیت و به تبع آن دامنهٔ صلاحیت اجرایی است. البته رویگردانی از معاضدت قضایی چالش‌هایی را در زمینهٔ شفافیت تحقیقات کیفری به وجود می‌آورد و کنترل دولت ذی‌صلاح بر تحقیقات کیفری را کاهش می‌دهد.

دسترسی مستقیم به داده‌های فرامرزی، جمع‌آوری سریع ادلهٔ فراسرزمینی را میسر می‌سازد. روشن است که استفاده از چنین روش‌هایی کنترل دولت‌ها بر اقدامات مقامات خارجی برای دسترسی به داده‌های تحت حکمیتشان را دشوار می‌سازد و شفافیت تحقیقات کیفری را کاهش می‌دهد. در این روش‌ها به جای تمرکز بر سرزمینی بودن تحقیقات کیفری، دسترسی سریع به ادله در اولویت قرار دارد. دسترسی به داده‌های فرامرزی از طریق همکاری رسمی دولت‌ها به سرعت در حال جایگزینی با دسترسی مستقیم از طریق همکاری با شرکت‌های خدمات اینترنتی است. این نوع دسترسی باید از طریق وضع قوانین در سطح داخلی چارچوب‌مند شود. قانون‌گذاران می‌توانند به شرکت‌های داخلی اجازه دهند تا در صورت درخواست دولت‌های خارجی، داده‌هایی را که در مالکیت یا کنترل خود دارند، با رعایت شروطی در اختیار آنان قرار

دهند. وضع چنین قوانینی مستلزم وجود اعتماد متقابل دولت‌ها بـه حاکمیـت قـانون در قلمـروی یکدیگر است و ممکن است در چارچوب قانون‌گـذاری متقابـل صـورت گیـرد. البتـه، دسترسـی مستقیم علاوه بر اینکه احتمال نقض حاکمیت دولت‌ها را به دنبال دارد، سبب ایجاد نگرانی‌هـایی پیرامون نقض حریم خصوصی افراد نیز می‌شود. بنابراین، از آنجا که نیـاز شـدیدی بـه ابزارهـای کارآمد برای مبارزه با جرایم سایبری وجود دارد، دولت‌ها باید فعالانه به دنبال راه‌حلی برای غلبـه بر این مشکلات باشند. به طور کلی دولت‌ها در این زمینه دو راه‌حـل پـیش رو دارنـد کـه لزومـاً مغایرتی با یکدیگر ندارند: حرکت به سوی دستیابی به اجماع در خصـوص اسـتفاده از روش‌هـای جایگزین برای دسترسی به داده‌های فرامرزی، نظیر آنچه در کنوانسیون بوداپست پیش‌بینی شده، نخستین راه‌حل است. چنین راه‌حلی مستلزم دستیبابی به مبانی مشترکی دربارهٔ معیـار صـلاحیت اجرایی بر داده‌هاست. این موضوع به خصوص در مواردی که تعیین موقعیت داده‌ها ممکن نباشد، حائز اهمیت است. دولت‌ها برای دستیابی به چنین مبانی مشترکی باید محدودیت‌هـای ناشـی از حاکمیت سرزمینی را به گونه‌ای تفسیر نمایند که دسترسی مستقیم به داده‌های فرامـرزی بـدون موافقت موردی دولت دارای حاکمیت ممکن گردد. به علاوه، دامنهٔ اِعمـال فراسـرزمینی قـوانین ملی نیز باید تعیین گردد. این امر بـه‌خصـوص دربـارهٔ جمـع‌آوری آنلایـن داده‌هـای فرامـرزی و تحقیقات از راه دور اهمیت دارد. دولت‌ها باید به صورت دوجانبه و همچنین از طریق سازمان‌های بین‌المللی در راستای تدوین ضوابط کلی تحقیقات از راه دور تلاش نمایند و بـا تعیـین شـروطی نظیر اطلاع‌رسانی فوری به دولت ذی‌صلاح و عدم دسترسی به داده‌های محرمانـهٔ دولتـی، آن را به رسمیت بشناسند تا امکان ضابطه‌مند شدن این تحقیقات فراهم آید. توافـق دولـت‌هـا دربـارهٔ دسترسی مستقیم، همچنین مسـتلزم وجـود تضـمینات شـکلی بـرای حمایـت از حقـوق افـراد و طرف‌های ثالث و حفظ منافع قانونی دولت‌هاست تا از سوءاستفاده از این نوع دسترسی جلوگیری به عمل آید. دسترسی مستقیم به داده‌های فرامرزی بر دو فرض اساسـی مبتنـی اسـت: نخسـت اعتماد دولت‌ها به یکدیگر و دوم احترام دولت‌ها به حاکمیت قانون و حقوق بشر. آنچه بیش از هر چیز در این زمینه مورد نیاز است، شفافیت در موضع رسمی دولت‌هاست. در وهلهٔ بعـد اسـتفاده از این روش در رویهٔ عملی دولت‌ها از بیشترین اهمیت برخـوردار اسـت. بـدون بـه‌اشـتراک‌گـذاری

مواضع شفاف دولت‌ها و تجربیات عملی آنها با جامعهٔ بین‌المللی، دستیابی به توافق در خصوص دسترسی مستقیم به داده‌های فرامرزی نامحتمل به نظر می‌رسد.

اصلاح سازکارهای معاضدت قضای راه‌حل دوم است که همخوانی بیشتری با حاکمیت ملی دولت‌ها دارد. این راه‌حل به نظر آسان نمی‌آید؛ زیرا دولت‌ها با وجود نیاز به روش‌های همکاری کارآمدتر، از مذاکره در مورد چگونگی اصلاح این سازکار سنتی اجتناب می‌نمایند. دلیل خودداری دولت‌ها از توافق در مورد قواعد روشن‌تر برای همکاری بین‌المللی به درستی روشن نیست. ممکن است یکی از دلایل این امر فقدان آمارهای معتبر در زمینهٔ جرایم سایبری و سازکارهای مختلف همکاری در زمینهٔ ادلهٔ الکترونیکی باشد. آگاهی دولت‌ها از این ضرورت نیازمند ادامهٔ تلاش‌های سازمان‌های بین‌المللی و ابتکار عمل آنهاست. دولت ایران نیز در صورتی‌که موفق به اعتمادسازی بین‌المللی در زمینهٔ دسترسی مستقیم به داده‌ها نشود، تلاش برای انعقاد معاهدات معاضدت قضایی دو یا چندجانبه بر اساس مقتضیات همکاری در زمینهٔ دسترسی به ادلهٔ الکترونیکی، بهترین رویکرد ممکن برای این دولت خواهد بود. می‌توان مهم‌ترین اقدامات لازم برای اصلاح فرایندهای معاضدتی در زمینهٔ دسترسی فرامرزی را به این صورت خلاصه نمود: نخست ایجاد چارچوب‌های واحد برای تنظیم درخواست‌های همکاری: این چارچوب‌ها ممکن است شامل نوع داده‌های قابل درخواست، جرایم موضوع درخواست و معیارهای وجود سوءظن کیفری موجه باشند؛ دوم شفاف‌سازی معیارهای قانونی پذیرش درخواست‌های همکاری: انتشار شفاف معیارهای مزبور از جمله معیارهای ارزیابی سوءظن کیفری موجه و معیارهای ارزیابی ارتباط دولت درخواست‌کننده با داده‌ها می‌تواند بر امکان پذیرش درخواست‌ها و سرعت همکاری بیفزاید؛ سوم تعیین بازهٔ زمانی برای رسیدگی و اجرای درخواست‌ها: تسریع در فرایندهای معاضدتی مستلزم تعیین یک معیار زمانی مناسب در معاهدات همکاری است که شرایط استثنایی نظیر تحقیقات کیفری پیچیده نیز در تعیین آن مورد توجه قرار گرفته باشد؛ چهارم توجیه قانونی دسترسی به داده‌ها: منافع قانونی در دسترسی به داده‌ها و دلایل لزوم این دسترسی باید در درخواست‌های همکاری به روشنی تبیین شود تا دولت مورد درخواست ارتباط میان دولت درخواست‌کننده و داده‌های مورد نظر را ارزیابی نماید؛ پنجم استفاده از فناوری‌های ارتباطی نوین در همکاری‌ها: جایگزینی مجاری رسمی دیپلماتیک با سیستم‌های ارتباطی دیجیتال بر سرعت

همکاری‌ها خواهد افزود. دولت‌ها می‌توانند درگاه‌های اینترنتی ویژه‌ای را برای تبادل درخواست‌های همکاری و ارائهٔ داده‌های درخواست شده ایجاد نمایند؛ ششم تأمین نیروی انسانی آموزش‌دیده برای تنظیم درخواست‌های همکاری و رسیدگی به درخواست‌های دریافتی.

در هر صورت، تسهیل دسترسی به داده‌های فرامرزی و ارتقای همکاری‌ها در این زمینه از هر روشی که صورت گیرد، باید بر اصولی چون دسترسی موجه و متناسب به داده‌ها، شفافیت فرایندهای همکاری، سرعت عمل و رعایت حقوق بشر از جمله آزادی بیان و حریم خصوصی مبتنی باشد. برای دستیابی به یک مبنای مشترک میان دولت‌ها و فائق شدن بر موضع مبهم حقوق بین‌الملل، سازکارهای دسترسی به داده‌های فرامرزی بایستی به بحث گذارده شوند تا دولت‌ها دیدگاه‌ها، ارزیابی‌های حقوقی و تجربیات عملی خود را به اشترک بگذارند. سازمان‌هایی بین‌المللی می‌توانند نقش مؤثری در ترویج این گفتگوها بر عهده بگیرند.

فهرست منابع

الف) منابع فارسی

کتاب

۱. عقیقی، نگار، ***صلاحیت در فضای مجازی از منظر حقوق بین‌الملل***، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش، ۱۳۹۶.

۲. خانعلی پور، سکینه، ***بازاندیشی معیارهای صلاحیت کیفری سایبری***، مجموعه مقالات همایش جنبه‌های حقوقی فناوری اطلاعات ایران، تهران: دانشگاه علم و فرهنگ، ۱۳۹۷.

مقاله

۳. سیفی، سید جمال و نگار عقیقی، **اصول حاکم بر اعمال صلاحیت تجویزی در فضای مجازی**، ویژه‌نامهٔ مجلهٔ تحقیقات حقوقی، ۱۳۸۹، شمارهٔ ۸.

۴. فروغی، فضل‌الله و امیر البوعلی، **صلاحیت کیفری مراجع قضایی در فضای سایبری**، ویژه‌نامهٔ مجلهٔ تحقیقات حقوقی، ۱۳۸۹، شمارهٔ ۵۸.

ب) منابع انگلیسی

Books

5. Cassese, A. *International Law*. First Ed. Oxford: Oxford University Press, 2001.
6. Gercke, M. *Understanding Cybercrime: Phenomena, Challenge and Legal Response.* First Ed. Vienna: International Telecommunication Union, 2012.
7. United Nation Office of Drugs and Crime. *Comprehensive Study on Cybercrime.* First Ed. Vienna: UNODC Publications, 2012.
8. Walden, I. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent in: *Privacy and Security for Cloud Computing*, Edited by Siani Pearson. First Ed. New York: Springer.
9. Walden, I. *Computer Crimes and Digital Investigations*. Second Ed. Oxford: Oxford University Press, 2007.

Articles

10. Bradshaw, S., and C. Millard and I. Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud

Computing Services," *International Journal of Law and Information Technology* 19, 2011.
11. Daskal, J., "Borders and Bits," *Vanderbilt Law Review* 71, 2018.
12. Goldsmith J. L., "The Internet and the Legitimacy of Remote Cross-Border Searches," *The University of Chicago Legal Forum* 103, 2001.
13. Kerr, O. S., "Fourth Amendment Seizures of Computer Data," *Yale Law Journal* 119, 2010.
14. Kuner, C., "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)," *International Journal of Law and Information Technology* 18, 2010.
15. O'Floinn, M., "It Wasn't All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe," *Computer Law & Security Review* 29, 2013.
16. Seitz, N., "Transborder Search: A New Perspective in Law Enforcement," *Yale Journal of Law and Technology* 7, 2004.
17. Schiff Berman, P., "Legal Jurisdiction and the Deterritorialization of Data," *Vanderbilt Law Review* 71, 2018.
18. Swire, p. & Hemmings, J. D., "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," *New York Annual Survey of American Law 71*. 2015.
19. Trudel, P., "Jurisdiction over the Internet: A Canadian Perspective," *The International Lawyer* 32, 1998.
20. Westmoreland, K. and Kent, G., "Foreign Law Enforcement Access to User Data: A Survival Guide and Call for Action," *Canadian Journal of Law and Technology* 13, 2015.

Internet Sites

21. Andrew K. Woods, **Data Beyond Borders: Mutual Legal Assistance in the Internet Era**, 2015: 3, available at:
https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub (last visited on 10/10/2018).
22. Benson, K., and R. Dowsley, and H. Shacham, **Do you know where your cloud files are?**, Proceedings of the 3rd ACM Workshop on Cloud Computing Security (October 2010), available at:
http://iks.ira.uka.de/fileadmin/User/Dowsley/pdf/BenDowSha11.pdf (last visited on 11/10/2018).

23. Cybercrime Convention Committee (T-CY), 2013, **Transborder Access to Data (Article 32)**, Council of Europe (December 2014), available at: https://rm.coe.int/16802e726a (last visited on 11/9/2018).
24. Council of Europe Cybercrime Convention Committee (T-CY), **Trans-border Access and Jurisdiction: What Are the Options**, Council of Europe (December 2012), 9, available at: https://rm.coe.int/16802e79e8 (last visited on 11/10/2018).
25. Council of Europe Cybercrime Convention Committee (T-CY), T**-CY Assessment report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime**, Council of Europe (December 2014), 31, available at: https://rm.coe.int/16802e726c(last visited on 11/9/2018).
26. European Committee of Crime Problem, **Explanatory Report to the Convention on Cybercrime**, Council of Europe (November 2001), 53, available at: https://rm.coe.int/16800ce5b (last visited on 11/9/2018).
27. Facebook Company, **Information for Law Enforcement Authorities**, Facebook Website, available at: http://www.facebook.com/safety/groups/law/guidelines/(last visited on 11/10/2018).
28. Giles, K., **Russia's Public Stance on Cyberspace Issues**, 4th International Conference on Cyber Conflict (January 2012), available at: https:// www.researchgate.net/ publication/ 261044707_ Russia's_public_stance_on_cyberspace_issues (last visited on 11/9/2018).
29. New Zealand Law Commission, **Search and Surveillance Powers**, lawcom.govt.nz (June 2007), 226, available at: http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R97.pdf (last visited on 11/9/2018).
30. Peterson, Z.N.J., and Gondree, M., and Beverly, R., 2011. **A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud**, Usenix (June 2011), available at: https:// www.usenix.org/ legacy/events/ hotcloud11/ tech/final_files/ Peterson.pdf (last visited on 11/10/2018).
31. Schwerha, J. J., **Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from Cloud Computing Providers**, Council of Europe Project on Cybercrime Discussion (January 2010), available at: https://rm.coe.int/16802fa3dc (last visited on 11/10/2018).