معاضدت قضایی متقابل درزمینهٔ جرایم سایبری

توقان نظامی نرج‌آباد* ـ دکتر لیلا رئیسی**

چکیده:

تعقیب و پی‌جویی جرایم سایبری مستلزم دسترسی به داده‌های مربوط به فعالیت‌های مجرمانهٔ سایبری است. درعین‌حال ممکن است داده‌های رایانه‌ای موردنظر که درواقع ادلّهٔ بالقوهٔ جرم هستند بر روی سیستم یا سروری مستقر در قلمروی دولتی دیگر قرار داشته باشند. در این صورت دسترسی مأمورین تحقیق به آن داده‌ها می‌تواند موجب نقض حاکمیت دولت مزبور گردد مگر اینکه ازطریق همکاری بین‌المللی با آن دولت صورت گیرد. همکاری دراین‌زمینه اغلب در چهارچوب معاضدت قضایی صورت می‌گیرد. معاضدت قضایی روشی مرسوم و شناخته‌شده برای همکاری بین‌المللی در امور کیفری است اما ویژگی‌های فضای سایبری و داده‌های رایانه‌ای، معاهدات قضایی درزمینهٔ جرایم سایبری را تحت تأثیر قرار داده است. این مقاله درصدد روشن ساختن چگونگی این تأثیرات و ابعاد مختلف آن است. ویژگی‌های فضای سایبری و داده‌های رایانه‌ای موجب اهمیت یافتن استفاده از معاضدت قضایی درزمینهٔ مبارزه با جرایم سایبری و نیز ایجاد اشکال جدیدی از معاضدت قضایی شده و همچنین همکاری بین‌المللی ازطریق معاضدت قضایی را با مشکلاتی مواجه ساخته است.

کلیدواژه‌ها:

جرایم سایبری، معاضدت قضایی، داده‌های رایانه‌ای، ادلّهٔ الکترونیکی، دسترسی به داده‌های فرامرزی.

مجلهٔ پژوهشهای حقوق جزا و جرم‌شناسی، شمارهٔ ۱۵، نیمسال اول ۱۳۹۹
صفحهٔ ۲۷۸-۲۵۵، تاریخ وصول: ۱۳۹۸/۰۲/۱۱، تاریخ پذیرش: ۱۳۹۸/۱۰/۲۵

* دانشجوی دوره دکترای حقوق، دانشکده علوم انسانی و حقوق، دانشگاه آزاد واحد اصفهان (خوراسگان)، اصفهان، ایران Email: toghan_nezami@yahoo.com

** دانشیار دانشکده علوم انسانی و حقوق، دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)، اصفهان، ایران، نویسنده مسئول Email: raisi.leila@gmail.com

مقدمه

مجرمان سایبری نیازی به حضور در محل ارتکاب جرم ندارند و فواصل مکانی و مرزهای ملّی مانعی برای ارتکاب جرایم سایبری محسوب نمی‌شوند. امروزه با انتقال داده‌ها ازطریق شبکه‌های ارتباطی نظارت‌های مرزی کارایی خود را از دست داده‌اند. ازآنجاکه جامعهٔ مدرن به‌شدت به جریان فرامرزی و آزاد اطلاعات وابسته است جرایم سایبری به‌راحتی در مقیاسی بین‌المللی ارتکاب می‌یابند. ممکن است ورود به سیستم رایانه‌ای، سوءاستفاده از داده‌ها و حصول نتایج مجرمانه در کشورهای مختلفی صورت پذیرند. هکرها می‌توانند از گوشه‌ای دورافتاده از جهان، سیستم‌های رایانه‌ای در آن‌سوی جهان را مختل سازند. عناصر فرامرزی جرایم سایبری و به‌خصوص ادلّهٔ الکترونیکی، چالش‌های حقوقی جدیدی را ایجاد کرده و همکاری دولت‌ها را اجتناب‌ناپذیر ساخته‌اند.[۱] یکی از مقتضیات اصلی تعقیب این جرایم عکس‌العمل سریع و به‌موقع است اما روش‌های سنتی همکاری بین‌المللی در امور کیفری غالباً برآورندهٔ این مقتضیات نیستند.[۲] درواقع سرعت و انعطاف‌پذیری جرایم سایبری بیش از هر جرم فرامرزی دیگری سبب تحوّل همکاری‌های بین‌المللی در امور کیفری شده است. مبارزه با جرایم سایبری مستلزم ایجاد شبکهٔ پیشرفته‌ای از همکاری‌های بین‌الدولی است تا انجام سریع تحقیقات کیفری را میسر سازد. جلوگیری از خسارات هنگفت اقتصادی، نقض حقوق افراد و ایجاد پناهگاه‌های امن مجرمین سایبری انگیزه اصلی این همکاری‌هاست. چهارچوب‌های همکاری بایستی ضرورت‌های تجارت و روابط بین‌الملل و احترام به حقوق و آزادی‌های فردی را توأمان مدّنظر قرار داده و سعی در ایجاد تعادل میان آنها نماید.

معاضدت قضایی نوعی همکاری بین‌المللی است که در آن دولتی بنا به درخواست دولت دیگر، از اختیارات شکلی خود نظیر تفتیش و توقیف، اخذ شهادت، ضبط عایدات جرم و کنترل ارتباطات راه دور در راستای تعقیب جرم استفاده می‌کنند. همکاری از این طریق اغلب در

---

۱. دراین‌زمینه نک:

Michael A. Sussmann, "The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium," *Duke Journal of Comparative & International Law* 9 (1998): 451.

۲. گزارش تفسیری کنوانسیون جرایم سایبری ضرورت سرعت عمل در همکاری بین‌المللی برای تعقیب جرایم سایبری را موردِتأکید قرار داده: «داده‌های رایانه‌ای بسیار آسیب‌پذیرند و به‌راحتی می‌توان آنها را حذف و ردیابی مرتکبان را غیرممکن نمود. برخی از انواع داده‌های رایانه‌ای تنها برای مدت کوتاهی ذخیره می‌شوند. درصورت عدمِ‌جمع‌آوری فوری ادلّه ممکن است خسارات شدیدی به اشخاص و دارایی‌ها وارد آید. در این‌گونه موارد ارائهٔ درخواست و رسیدگی به آن باید به‌سرعت انجام گیرد.»

چهارچوب معاهدات دوجانبهٔ معاضدت قضایی صورت می‌گیرد. درواقع دوجانبه‌گرایی گرایش اصلی دولت‌ها در انعقاد این معاهدات است چراکه آنها ترجیح می‌دهند در روابط خود با هر یک از دولت‌های خارجی بر اساس مقتضیات دوجانبه عمل نمایند. البته معاهدات معاضدت قضایی در سطح منطقه‌ای نیز منعقد می‌شوند. امروزه شبکهٔ گسترده‌ای از معاهدات معاضدت قضایی در میان دولت‌های جهان وجود دارد. البته همکاری ازطریق معاضدت قضایی همیشه مستلزم وجود معاهده یا توافق بین‌المللی نیست. بیشتر دولت‌ها حتی درصورت فقدان معاهدهٔ معاضدت قضایی، درخواست‌های دادگاه‌ها و یا نهادهای دیپلماتیک خارجی را اجرا می‌نمایند.

علاوه‌بر معاهدات دوجانبه و منطقه‌ای معاضدت قضایی، برخی از کنوانسیون‌های بین‌المللی نیز چهارچوب‌هایی را برای معاضدت قضایی میان اعضاء پدید آورده‌اند که در رابطه با برخی از جرایم سایبری نیز قابل‌اِعمالند. کنوانسیون ملل متحد برای مبارزه با جرایم سازمان‌یافتهٔ فرامرزی و کنوانسیون‌های آمریکایی و اروپایی معاضدت متقابل در امور کیفری ازجملهٔ این کنوانسیون‌ها هستند. علی‌رغم تلاش‌های گستردهٔ سازمان‌های بین‌المللی مختلف برای ارتقای همکاری‌های بین‌المللی درزمینهٔ جرایم سایبری تاکنون تنها دو کنوانسیون در این رابطه به‌تصویب رسیده است: کنوانسیون شورای اروپا درزمینهٔ جرایم سایبری (کنوانسیون بوداپست–۲۰۰۱) و کنوانسیون اتحادیهٔ عرب برای مبارزه با جرایم فناوری اطلاعات.[3] این دو سند حاوی مقرراتی درزمینهٔ جرم‌انگاری، اختیارات شکلی، صلاحیت‌های قضایی، استرداد و همچنین معاضدت قضایی می‌باشند.

باتوجه‌به اهمیت حیاتی سرعت عمل در تعقیب جرایم سایبری و ماهیت خاص ادلّهٔ الکترونیکی، جمع‌آوری این ادلّه مستلزم به‌کارگیری اختیارات تعقیبی ویژه‌ای است و لذا اشکال جدیدی از معاضدت قضایی دراین‌زمینه به‌وجود آمده است. انجام این معاهدات مستلزم آن است که اختیارات شکلی ویژه‌ای به‌صورت هماهنگ در قوانین داخلی دولت‌ها پیش‌بینی شود. به‌عبارت‌دیگر هماهنگی قوانین کیفری شکلی برای استفاده از سازکار معاضدت قضایی درزمینهٔ جرایم سایبری ضروری است.

با وجود اهمیت فزایندهٔ معاضدت قضایی برای تعقیب جرایم سایبری، همکاری بین‌المللی ازطریق این سازکار با مشکلاتی مواجه است که کندی فرایندهای همکاری مهم‌ترین آنهاست چراکه تحقیقات کیفری در فضای سایبر مستلزم جمع‌آوری سریع ادلّهٔ الکترونیکی

3. League of Arab States Convention on Combating Information Technology Offences (2010)

می‌باشد و کندی فرایندهای همکاری، تعقیب مؤثر جرم را ناممکن می‌سازد. عوامل متعددی در ایجاد این مشکل نقش دارند: معاهدات معاضدت قضایی هنوز فراگیر نیستند و در میان بسیاری از دولت‌ها چهارچوب مشخصی برای معاضدت قضایی وجود ندارد. به‌علاوه معیارهای قانونی و روندهای اجرایی از شفافیت لازم برخوردار نیستند. این مقاله می‌کوشد تا نشان دهد که ویژگی‌های خاص داده‌های رایانه‌ای چگونه بر معاضدت‌های قضایی تأثیر گذاشته‌اند.

۱- اهمیت معاضدت قضایی درزمینهٔ جرایم سایبری

باتوجه‌به ویژگی اصلی جرایم سایبری یعنی امکان ارتکاب آن در فضای مجازی از هر نقطهٔ مکانی و جنبهٔ بین‌المللی آن، مقابلهٔ کارآمد با این جرایم نیازمند همکاری‌های کیفری بین‌المللی است.[۴] اگرچه فرامرزی بودن جرایم سایبری مانع بزرگی در تعقیب این جرایم است اما ازآنجاکه که مجرمین سایبری همواره ردپایی از خود در محیط سایبری باقی می‌گذارند در موقعیت متزلزلی قرار دارند[۵] چراکه ادلّهٔ جرایم آنان علی‌رغم فرامرزی بودن، ازطریق همکاری بین‌المللی قابل‌دسترسی هستند. حدود ۷۰ درصد همکاری‌های بین‌المللی درزمینهٔ جرایم سایبری در چهارچوب معاهدات قضایی صورت می‌گیرد[۶] که امروزه به دو دلیل اهمیت فزاینده‌ای یافته است: نخست ماهیت فرامرزی جرایم سایبری و داده‌های رایانه‌ای و دوم گسترش استفاده از رمزنگاری داده‌ها[۷] در ارتباطات اینترنتی به‌دلیل ضرورت حفظ حریم خصوصی کاربران. امروزه بین ۳۰ تا ۷۰ درصد جرایم سایبری دارای ابعاد فرامرزی هستند.[۸] ادلّهٔ الکترونیکی به ورای مرزهای ملّی منتقل می‌شوند و درنتیجه در قلمروی دولت تعقیب‌کننده قابل‌دسترسی نیستند. این درحالی است که امور کیفری در زمرهٔ امور حاکمیتی قرار دارند و مطابق اصول عدم‌مداخله و تساوی حاکمیت‌ها هیچ دولتی نمی‌تواند در قلمروی دیگر دولت‌ها به انجام تحقیقات کیفری بپردازد مگر به‌موجب معاهده یا شکل دیگری از

---

۴. بهزاد رضوی‌فرد، «محدودیت‌ها و راهبردهای صلاحیت در جرایم سایبری»، *مجله حقوقی دادگستری* ۹۸ (۱۳۹۶)، ۹۷.

۵. حسنعلی مؤذن‌زادگان، «دادرسی الکترونیکی در رویارویی با جرایم رایانه‌ای»، *مجله حقوقی دادگستری* ۱۰۰ (۱۳۹۶)، ۱۸۵.

6. Steven Malby, et al., *Comprehensive Study on Cyber-Crime* (Vienna: UNODC, 2013), 201.

۷. در رمزنگاری از الگوریتم‌های ریاضی برای پنهان کردن محتوای داده‌های رایانه‌ای استفاده می‌شود و آگاهی از محتوای رمزنگاری‌شده تنها با استفاده از کلید رمز ممکن می‌باشد. رمزنگاری برای حفظ محرمانگی نامه‌های الکترونیکی، داده‌های سرّی و معاملات تجاری الکترونیکی حائز اهمیت است.

8. Malby, et al., op. cit., xxiv.

اعلام رضایت آن دولت.[۹] دستیابی به یا شبکه برای کشف، تعقیب و تحصیل دلیل ممکن است پردازش داده‌ها در کشور دیگر محسوب شود که خود تعرض به حاکمیت دولت‌ها خواهد بود.[۱۰] درنتیجه درصورت فرامرزی بودن ادلّهٔ الکترونیکی، تعقیب جرم تنها ازطریق همکاری با دولت محل ذخیرهٔ داده‌ها ممکن می‌باشد.

با استفادهٔ فزاینده از رمزنگاری ارتباطات آنلاین، معاضدت قضایی اهمیتی بیشتری یافته چراکه بررسی محتوای ارتباطات اینترنتیِ رمزنگاری‌شده مستلزم دسترسی به داده‌های اولیه‌ای است که بر روی ابرهای رایانه‌ای[۱۱] قرار دارند و توسط شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی رمزنگاری شده‌اند. این داده‌ها اغلب در سِرورهای خارجی ذخیره می‌شوند و بنابراین دولت تعقیب‌کنندهٔ جرم برای دسترسی به آنها بایستی با دولت محل استقرار سِرورها و یا دولت متبوع شرکت ارائه‌دهندهٔ خدمات اینترنتی همکاری نماید.[۱۲] برای دهه‌ها تلفن فناوری ارتباطی اصلی بود و دولت‌ها در تحقیقات کیفری از شنود تلفنی استفاده می‌کردند. حتی پس از گسترش ارتباطات اینترنتی، دولت‌ها همچنان می‌توانستند ازطریق شرکت‌های داخلی ارائه‌دهندهٔ خدمات اینترنتی به محتوای ارتباطات دسترسی یابند. بااین‌حال تهدیدات امنیتی، لزوم حفاظت از حریم خصوصی کاربران و مقتضیات تجارت الکترونیک در دههٔ اخیر شرکت‌های خدمات اینترنتی را به رمزنگاری ارتباطات اینترنتی واداشته به‌طوری‌که امروزه تجارت الکترونیک کاملاً به رمزنگاری داده‌ها وابسته است. ازاین‌رو مأموران تحقیق می‌باید پیش از آنکه داده‌ها توسط شرکت‌های مزبور رمزنگاری شوند به آنها دست یابند که این دسترسی غالباً ازطریق معاضدت قضایی صورت می‌گیرد.

ضرورت دسترسی به داده‌های فرامرزی موجب شده تا برخی دولت‌ها[۱۳] شرکت‌های

---

۹. دراین‌زمینه نک:

Elcio Ricardo de Carvalho and et al., "Challenges and Best Practices in Cybercrime Investigation," 2008, http://www.unafei.or.jp/english/pdf/RS_No79/No79_15RC_Group2.pdf (Accessed November 10, 2018).

۱۰. حسین میرمحمدصادقی، «راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران»، *دیدگاه‌های حقوقی* ۴۳-۴۲ (۱۳۸۶)، ۱۲۳.

۱۱. ابر رایانه‌ای سیستمی متشکل از یک رایانهٔ مرکزی است که کاربران می‌توانند داده‌های خود را از سراسر جهان به‌وسیلهٔ اینترنت بر روی آن ذخیره کنند و کاربران می‌توانند بدون ذخیره‌سازی داده‌ها در رایانه‌های شخصی یا سازمانی، در هر زمان ازطریق اینترنت به داده‌های مزبور دسترسی یابند.

12. Peter Swire, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud," *International Data Privacy Law* 2 (2012): 200.

۱۳. ازجمله آلمان، استرالیا، اندونزی، برزیل، تایلند، تایوان، چین، روسیه، سوئد، فرانسه، قزاقستان، کانادا، ←

خدمات اینترنتی را ملزم نمایند تا داده‌های کاربران داخلی را پیش از انتقال به سرورهای خارجی در داخل ذخیره نمایند تا دسترسی مستقیم به آنها ممکن باشد. شرکت‌ها برای ارائهٔ خدمات اینترنتی در قلمروی این دولت‌ها می‌باید از سِرورهای داخلی استفاده نمایند. چنین رویکردی که داخلی‌سازی داده‌ها نامیده می‌شود پیامدهای اقتصادی نامطلوبی در پی دارد. تجارت اینترنتی شدیداً به ارتباط آسان با مشتریان خارجی و بازاریابی بین‌المللی ازطریق اینترنت وابسته است.[۱۴] ازاین‌رو داخلی‌سازی داده‌ها هزینهٔ هنگفتی را بر تجارت اینترنتی تحمیل خواهد کرد.[۱۵] همچنین به‌لحاظ فنی موجب افزایش هزینهٔ خدمات اینترنتی می‌شود و نیز حریم خصوصی و حق آزادی بیان کاربران را در معرض تهدید قرار می‌دهد.[۱۶] ضرورت دسترسی به داده‌های فرامرزی همچنین سبب شده تا برخی دولت‌ها در تحقیقات کیفری خود درصدد اِعمال فراسرزمینی قوانینشان برآیند.[۱۷] به‌علاوه باعث شده تا دولت‌ها با استفاده از ابزارهای فنی جدید تحقیقات خود را از راه دور انجام دهند و به جمع‌آوری داده‌ها از قلمروی دیگر دولت‌ها بپردازند. به‌عنوان مثال اف‌بی‌آی با استفاده از یک برنامهٔ ردیابی به نام «فانوس جادویی» مجرمین سایبری را ردیابی می‌کند. این برنامه با نصب یک ویروس بر روی رایانهٔ مظنونان، کل داده‌های آنها را ضبط و منتقل می‌نماید.[۱۸] این بدان‌معناست که اف‌بی‌آی نیازی به دسترسی مستقیم به رایانهٔ مظنونان در هر کجای دنیا که باشند، ندارد و این امر می‌تواند

کرهٔجنوبی، مالزی، نیجریه، ویتنام و هند.

Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64 (2015): 682.

14. Peter Swire and Justin D. Hemmings, "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," *New York Annual Survey of American Law* 71 (2017): 713.

۱۵. برای مثال نک:

Leviathan Security Group, "Quantifying the Cost of Forced Localization," 2015, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying™he+Cost+of+Forced+Localization.pdf (Accessed November 10, 2018), 13-14.

۱۶. دولت‌های آلمان، استرالیا، اندونزی، برزیل، تایلند، تایوان، چین، روسیه، سوئد، فرانسه، قزاقستان، کانادا، کرهٔجنوبی، مالزی، نیجریه، ویتنام و هند قوانینی را درزمینهٔ داخلی‌سازی داده‌ها وضع نموده‌اند: Chander and Uyên P. Lê, op.cit. 682.

۱۷. برای مثال درمورد اِعمال فراسرزمینی قوانین توسط دولت برزیل نک:

Hogan Lovells Client Alert, "Marco Civil da Internet: Brazil's New Internet Law Could Broadly Impact Online Companies' Privacy and Data Handling Practices," 2014, http://ehoganlovells.com/cv/92a5426dc5d9947a6ef3abd4eb988b549ae2472b (Accessed November 10, 2018).

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

منجر به نقض حاکمیت دولت محل استقرار سیستم‌های هدف گردد. روشن است که اجرای فرامرزی قوانین داخلی موجب ایجاد اختلافات بین‌المللی خواهد شد. به‌علاوه در چنین شرایطی شرکت‌های خدمات اینترنتی ناگزیر از رعایت قوانین دولت‌های مختلف خواهند بود. امروزه داخلی‌سازی داده‌ها و اِعمال فراسرزمینی قوانین داخلی بزرگ‌ترین خطراتی هستند که اینترنت آزاد و ساختار جهانی آن را تهدید می‌نمایند. قطعاً ناکارآمدی سازکارهای همکاری درزمینهٔ جرایم سایبری از مهم‌ترین علل اتخاذ چنین رویکردهایی هستند. چنانچه دولت‌ها بتوانند ازطریق سازکارهای کارآمد معاضدت قضایی به‌نحو مؤثری به داده‌های فرامرزی دسترسی یابند گرایش آنان به داخلی‌سازی داده‌ها و اِعمال فراسرزمینی قوانینشان کاهش خواهد یافت.

۲- انواع معاضدت‌های قضایی درزمینهٔ جرایم سایبری

تعقیب جرایم سایبری و جمع‌آوری ادلّهٔ الکترونیکی مستلزم استفاده از اختیارات تعقیبی ویژه‌ای است که در قوانین کیفری شکلی پیش‌بینی می‌شوند. ضرورت استفاده از اختیارات مزبور سبب ایجاد انواع جدیدی از معاضدت‌های قضایی درزمینهٔ ادلّهٔ الکترونیکی شده است. در معاضدت قضایی دولت تعقیب‌کننده از دولت مقابل می‌خواهد تا از اختیارات تعقیبی خود به‌منظور تعقیب جرم موردنظر استفاده نماید. ازاین‌رو دولت درخواست‌شونده تنها درصورتی قادر به اجرای درخواست خواهد بود که از اختیارات قانونی لازم برخوردار باشد. به عبارتی در معاضدت قضایی دولت‌ها همان اختیاراتی را می‌توانند به‌کار بندند که در تحقیقات داخلی مجاز به به‌کارگیری آن هستند.[۱۹] به‌طور مثال چنانچه دولتی از اختیار قانونی برای حفاظت فوری از داده‌های رایانه‌ای برخوردار نباشد دیگر دولت‌ها نیز نمی‌توانند انجام آن را از وی درخواست نمایند.

ادلّهٔ الکترونیکی می‌توانند به‌صورت از راه دور در سِرور یا رایانه‌ای در سوی دیگر کرهٔ زمین ذخیره شوند. به‌طور مثال برخی از شرکت‌های تجاری داده‌های مربوط به شعبات و

---

۱۹. در برخی موارد دولت‌ها انجام اقداماتی را از یکدیگر درخواست می‌نمایند که در قانون دولت درخواست‌شونده پیش‌بینی نشده‌اند. غالب معاهدات معاضدت قضایی دولت‌ها را صراحتاً ملزم به اجرای چنین درخواست‌هایی نمی‌نمایند. البته مطابق بند ۱ مادهٔ ۱۰ تحقیقات اروپایی (European Investigation Order) درصورتی‌که اقدام درخواست‌شده در قانون دولت موردِدرخواست پیش‌بینی نشده باشد، بایستی از اقدامات جایگزین استفاده گردد.
(Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, Art. 10, Para. 1.)

نمایندگی‌های خارجی خود را در مقر اصلی شرکت ذخیره می‌نمایند. مثلاً با اینکه شرکت آمریکا آنلاین[۲۰] خدمات اینترنتی خود را در ایالات‌متحده، اروپا و آسیا ارائهٔ می‌نماید، داده‌های کاربران خود را در مقر شرکت در رِستونِ ویرجینیا[۲۱] ذخیره می‌کند.[۲۲] بنابراین چنانچه دو فرد در ژاپن از خدمات این شرکت برای نامه‌نگاری اینترنتی استفاده کنند تمام داده‌های مربوط به ارتباطات آنان در ایالات‌متحده ذخیره می‌گردد. درنتیجه چنانچه مقامات ژاپنی به‌منظور تعقیب جرمی سایبری درصدد کنترل ارتباطات مزبور برآیند بایستی با مقامات آمریکایی همکاری نمایند. گذشته از این گاهی داده‌ها تعمّداً در کشور دیگری ذخیره می‌گردند تا دسترسی مقامات داخلی به آنها میسر نباشد. مجرمان سایبری با استفاده از ابرهای رایانه‌ای می‌توانند داده‌های خود را به‌راحتی به سِرورهای خارجی منتقل کنند. در چنین شرایطی دولت‌ها برای دسترسی به داده‌ها بایستی تفتیش و توقیف آنها را از دولت محل ذخیره درخواست نمایند.[۲۳] چنانچه داده‌ها در معرض حذف یا دستکاری باشند تسریع در اجرای تقاضای توقیف حیاتی خواهد بود. معاضدت قضایی برای تفتیش و توقیف داده‌ها پرکاربردترین نوع معاضدت درزمینهٔ تعقیب جرایم است چراکه دسترسی کامل به داده‌ها و بررسی دقیق آنها را میسر می‌گرداند.[۲۴]

به‌دلیل حجم بالای پرونده‌ها، پیچیدگی‌های فنی، حجم بالای داده‌ها، گسترش تدابیر امنیتی برای حفظ حریم خصوصی کاربران و امکان اختلال در فعالیت‌های سایبری قانونی، تفتیش و توقیف داده‌ها در بیشتر موارد غیرممکن است.[۲۵] عمدهٔ زیرساخت‌های اینترنتی و داده‌های ارتباطاتی در کنترل شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی و اشخاص قرار دارد. ازاین‌رو دولت محل ذخیرهٔ داده‌ها بنا به درخواست دولت تعقیب‌کننده بایستی حکمی موسوم به دستور ارائهٔ داده‌ها[۲۶] را صادر نماید که به‌موجب آن ارائه‌دهندگان خدمات اینترنتی و یا سایر اشخاصی که داده‌های موردنظر را در اختیار دارند، ملزم به بازیابی و ارائهٔ آنها می‌باشند.

---

20. America Online
21. Reston, Virginia
22. Micheal A. Sussmann, "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium," *Duke Journal of Computer & International Law* 9 (1998): 471.

۲۳. معاضدت متقابل برای تفتیش و توقیف داده‌های رایانه‌ای در مادهٔ ۳۱ کنوانسیون بوداپست و مادهٔ ۳۹ کنوانسیون اتحادیهٔ عرب پیش‌بینی شده است.

24. Kate Westmoreland and Gail Kent, "International Law Enforcement Access to User Data: A Survival Guide and Call for Action," *Canadian Journal of Law and Technology* 13 (2015): 203.
25. Lucie Angers, "Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation," In *Crime and Technology: New Frontiers for Regulations, Law Enforcement and Research* (Springer: New York, 2004): 46.
26. Production Order

یکی از ویژگی‌های ادلّهٔ الکترونیکی قابلیت دستکاری، انتقال و حذف فوری آنها از راه دور است.[۲۷] ممکن است این تغییرات درنتیجهٔ اقدامات مرتکبین برای از بین بردن ادلّه ایجاد گردد و یا نتیجهٔ اقدامات معمول شرکت‌های خدمات اینترنتی نظیر حذف داده‌های ترافیکی[۲۸] باشد. روش‌های سنتی جمع‌آوری ادلّهٔ فرامرزی بسیار کند هستند چراکه طی شدن روندهای قانونی و تکمیل فرایندهای دیپلماتیک معمول بسیار زمان‌بر است. به‌علاوه ممکن است مأمورین تحقیق بلافاصله پس از ارتکاب یک جرم سایبری منشأ آن را شناسایی نمایند اما قادر به جمع‌آوری و ارائهٔ فوری اطلاعات موردنیاز به دولت محل ذخیرهٔ داده‌ها نباشند. هرچه انجام این کار به زمان بیشتری نیاز داشته باشد احتمال حذف یا دستکاری داده‌ها بیشتر خواهد بود.[۲۹] صدور حکم تفتیش و توقیف و یا صدور دستور ارائهٔ داده‌ها فرایندهایی زمانبرند که ممکن است داده‌ها در خلال آنها حذف یا دستکاری گردند. ازاین‌رو مقامات دولت ذی‌صلاح بایستی بنا به درخواست دولت تعقیب‌کننده با صدور حکمی ارائه‌دهندگان خدمات اینترنتی را ملزم به ذخیره‌سازی داده‌های موردنظر نمایند. درغیراین‌صورت ممکن است حذف و دستکاری داده‌ها انجام تحقیقات کیفری را با مانع مواجه سازد. دستور حفاظت سریع از داده‌های ذخیره‌شده[۳۰] دستوری موقتی است و تا زمانی اجرایی می‌باشد که دولت درخواست‌شونده درمورد تفتیش و توقیف داده‌ها تصمیم‌گیری نماید. به‌طورکلّی حفاظت سریع از داده‌های ذخیره‌شده یک اقدام موقتی برای تضمین حفظ داده‌ها تا زمان صدور حکم قضایی مناسب است. حفاظت از داده‌ها را نباید با الزام به حبس داده‌ها[۳۱] یکسان دانست. حبس داده‌ها یک الزام قانونی است که به‌موجب آن ارائه‌دهندگان خدمات اینترنتی می‌باید داده‌های مربوط به همهٔ کاربران را جمع‌آوری و برای یک دورهٔ زمانی مشخص ذخیره نمایند تا دسترسی به داده‌ها امکان‌پذیر باشد.[۳۲]

---

۲۷. دراین‌زمینه نک:

M. Kettle and O. Bowcott, "Computer Crime: The Age of Digital Sleuth," *The Guardian,* December 12, 1997, 19.

۲۸. داده‌های ترافیکی داده‌هایی هستند که اینترنت از آنها برای شناسایی و تعیین موقعیت مبدأ و مقصد یک ارتباط اینترنتی استفاده می‌کند و برقراری ارتباط و جابه‌جایی داده‌های محتوایی را در مسیر میان آنها میسّر می‌سازد. مأموران تحقیق از داده‌های ترافیکی برای ردیابی ارتباطات اینترنتی استفاده می‌کنند.

29. Clifford Stoll and John. W. D. Connolly, "The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage," *Physics Today* 43 (1990): 75.

۳۰. معاضدت متقابل درزمینهٔ حفاظت سریع از داده‌های رایانه‌ای در مادهٔ ۱۷ کنوانسیون بوداپست و مادهٔ ۲۴ کنوانسیون اتحادیهٔ عرب پیش‌بینی شده است.

31. Data Retention

32. Council of Europe, "Explanatory Report to the Council of Europe Convention," 2001, ←

امروزه تعقیب جرایم سایبری در بسیاری از موارد مستلزم ردیابی ارتباطات اینترنتی مظنونین ازطریق داده‌های ترافیکی است. این درحالی است که ممکن است داده‌های ترافیکی در طی ارتباطات موقتی ایجاد شده و از بین بروند. این داده‌ها پس از اتمام فرایند برقراری ارتباط موردنیاز نیستند و شرکت‌های خدمات اینترنتی به دلایل اقتصادی آنها را حذف می‌کنند. درنتیجه ردگیری ارتباطات اینترنتی مستلزم جلوگیری از حذف داده‌های ترافیکی مربوطه می‌باشد. ازاین‌رو چنانچه برای برقراری ارتباط اینترنتی از خدمات یک شرکت خارجی استفاده شود، دولت تعقیب‌کنندهٔ جرم باید از دولت متبوع یا مقر آن شرکت درخواست نماید تا مانع از حذف داده‌های ترافیکی مربوط شود.[۳۳]

ازآنجاکه ممکن است داده‌ها در مسیر انتقالشان از مبدأ به مقصد از سِرورهای مستقر در کشورهای مختلف عبور نمایند، حفاظت از داده‌های ترافیکی بایستی در تمامی این کشورها صورت گیرد. ازاین‌رو تقاضا برای افشای فوری داده‌های ترافیکی جمع‌آوری‌شده[۳۴] جهت شناسایی مسیر انتقال داده‌ها ضروری می‌باشد.[۳۵] افشای داده‌های ترافیکی تا حدّی ضروری است که برای ردیابی ارتباطات اینترنتی کافی باشد.[۳۶] این اقدام یکی از ابزارهای مهم همکاری درزمینهٔ جرایم سایبری است چراکه امروزه شرکت‌های خدمات اینترنتی در حوزه‌های قضایی مختلف پراکنده‌اند و ردیابی موفقیت‌آمیز یک ارتباط اینترنتی معمولاً مستلزم همکاری تمامی ارائه‌دهندگان خدمات اینترنتی در زنجیرهٔ انتقال داده‌هاست.[۳۷]

ممکن است دسترسی به داده‌های محتوایی[۳۸] ارتباطات اینترنتی برای تعقیب جرم ضروری باشد. در این صورت دولت ذی‌صلاح بایستی بنا به درخواست دولت تعقیب‌کننده، داده‌های محتوایی ارتباطات موردنظر را شنود نماید.[۳۹] بدیهی است که دسترسی به داده‌های

---

https://rm.coe.int/16800cce5b (Accessed November 10, 2018), 25

۳۳. معاضدت متقابل درزمینهٔ جمع‌آوری آنی داده‌های ترافیکی در مادهٔ ۳۳ کنوانسیون بوداپست و مادهٔ ۴۱ کنوانسیون اتحادیهٔ عرب پیش‌بینی شده است.

34. Expedited Disclosure of Preserved Traffic Data

35. Council of Europe, "International Co-operation under the Convention on Cybercrime," 2009, https://rm.coe.int/1680304352 (Accessed November 10, 2018), 8.

۳۶. نک: بند ۱ مادهٔ ۳۰ کنوانسیون بوداپست.

۳۷. معاضدت متقابل درزمینهٔ افشای داده‌های ترافیکی در بند ۱ مادهٔ ۳۰ کنوانسیون بوداپست و مادهٔ ۳۸ کنوانسیون اتحادیهٔ عرب پیش‌بینی شده است.

۳۸. داده‌های محتوایی (Content Data) داده‌هایی هستند که محتوای یک ارتباط اینترنتی را تشکیل می‌دهند.

۳۹. معاضدت متقابل درزمینهٔ کنترل داده‌های محتوایی در مادهٔ ۳۴ کنوانسیون بوداپست و مادهٔ ۴۲ کنوانسیون اتحادیهٔ عرب پیش‌بینی شده است.

محتوایی بیشتر از دسترسی به داده‌های ترافیکی و داده‌های مربوط به اشتراک اینترنتی[۴۰]، حریم خصوصی و حقوق فردی اشخاص را در معرض تهدید قرار می‌دهد؛ بنابراین برخی از دولت‌ها حکم شنود داده‌های محتوایی را تنها در رابطه با جرایم خاصی صادر می‌نمایند که در قوانین داخلی فهرست شده‌اند و یا حد معینی از مجازات را در پی دارند.[۴۱و۴۲] این درحالی است که شنود داده‌های محتوایی اغلب باید به‌سرعت و پیش از بررسی قابل‌شنود بودن ارتباطات موردنظر انجام گیرد زیرا ممکن است فرصت شنود داده‌ها در خلال بررسی این موضوع از بین برود.

یکی از موانع شنود داده‌های محتوایی استفادهٔ مرتکبین از فناوری رمزنگاری است. مرتکبان با استفاده از این فناوری می‌توانند دسترسی مأمورین به داده‌های محتوایی را دشوار سازند. ممکن است داده‌هایی که ازطریق معاضدت قضایی در دسترس مأمورین خارجی قرار می‌گیرند، داده‌هایی رمزنگاری‌شده باشند که در این صورت کارایی چندانی برای آنان نخواهند داشت و ازآنجاکه دولت محل ذخیرهٔ داده‌ها از موقعیت بهتری برای دستیابی به داده‌های اصلی برخوردار است، می‌باید درزمینهٔ رمزگشایی داده‌ها با مقامات خارجی همکاری نماید.

۳- مشکلات معاضدت قضایی درزمینهٔ جرایم سایبری

عدم‌هماهنگی میان قوانین دولت‌ها مشکل اصلی همکاری بین‌المللی در امور کیفری است. عدمِ‌اجماع جهانی درمورد تعریف قانونی جرایم سایبری، عدم‌کفایت اختیارات قانونی برای تحقیق و دسترسی به سیستم‌های رایانه‌ای و عدمِ‌انسجام میان قوانین مختلف آیین دادرسی ملّی مانع جدّی در مسیر همکاری‌های بین‌المللی به‌منظور تعقیب درباره جرایم سایبری محسوب می‌شوند.[۴۳] برای مثال فقدان مقررات حفاظت از داده‌ها موجب می‌شود تا پیش از آنکه حکم توقیف داده‌ها توسط شرکت‌های خدمات اینترنتی اجرا شود، داده‌ها در معرض خطر

---

۴۰. داده‌های مربوط به اشتراک اینترنتی (Subscriber Data) داده‌هایی هستند که نشانی‌های اینترنتی را به اشخاصی که از آنها استفاده می‌کنند، مربوط می‌سازند. به‌وسیلهٔ این داده‌ها می‌توان به هویت کاربر خدمات اینترنتی، موقعیت جغرافیایی یا آدرس پستی وی، نوع خدمات و امکانات فنی مورداستفاده و مدت زمان استفاده پی برد.

۴۱. به‌طور مثال نک: بند ۱ مادهٔ ۲۱ کنوانسیون بوداپست.

42. Anger, op.cit. 47.

۴۳. آرامش شهبازی، «بایسته‌های حقوقی همکاری بین‌المللی در مبارزه با جرایم سایبری» (مقالهٔ ارائه‌شده در همایش جنبه‌های حقوقی فناوری اطلاعات و ارتباطات ایران، تهران، ۵ و ۶ اسفند ۱۳۹۶).

حذف یا دستکاری قرار گیرند.

هنوز در میان برخی از دولت‌ها هیچ توافقی درزمینهٔ معاضدت قضایی وجود ندارد؛ به عبارتی رژیم‌های معاهداتی معاضدت قضایی هنوز فراگیر نیستند. البته ممکن است دولت‌ها درخواست‌های معاضدت قضایی یکدیگر را تنها بر اساس اصل همکاری و برای رعایت نزاکت بین‌المللی اجرا نمایند. بااین‌حال همکاری بین‌المللی در امور کیفری، بدون وجود یک چهارچوب حقوقی از پیش تعیین‌شده و الزام‌آور، کند و پرهزینه است و به‌دلیل فقدان تعهدات قانونی، تضمینی برای موفقیت‌آمیز بودن آن وجود ندارد.[۴۴]

سازکارهای کنونی معاضدت قضایی پیش از پیدایش اینترنت شکل گرفته‌اند و تناسبی با واقعیت‌های جهان امروز ندارند. نظام فعلی معاضدت قضایی به انحاء مختلف موردانتقاد قرار گرفته و به‌صورت یک نظام پیچیده و تاریخ‌گذشته، کند، فرمالیستی و نامنطبق با مقتضیات فضای سایبری، وابسته به بروکراسی اداری، زمانبر و ناکارآمد توصیف شده است.[۴۵] معاضدت قضایی سنتاً مستلزم طی مراحل دیپلماتیک، قضایی و اداری متعدد است و امکان واکنش سریع را از بین می‌برد. تعداد زیاد درخواست‌ها نیز مزید بر علت شده، به‌خصوص که اغلب سرورها و زیرساخت‌های شبکهٔ جهانی اینترنت در آمریکای شمالی و اروپا مستقر هستند[۴۶] و این امر موجب شده تا این دولت‌ها شمار فزاینده‌ای از درخواست‌های معاضدت را دریافت کنند. به‌طور مثال دولت بریتانیا با حجم عظیم درخواست‌های معاضدت روبه‌روست.[۴۷] میانگین مدت زمان اجرای درخواست‌های معاضدت ۱۵۰ روز است.[۴۸] این درحالی است که شناسایی منشأ یک جرم سایبری در بهترین حالت در هنگام اتصال مرتکب به اینترنت میسر است.[۴۹] از طرفی باتوجه‌به ناپایداری ادلّهٔ الکترونیکی، کندی فرایندهای معاضدتی ممکن است موجب تأخیر در تعقیب جرم شود و یا اساساً آن را غیرممکن سازد. قوانین داخلی دولت‌ها نیز به‌ندرت این واقعیت را موردتوجه قرار داده‌اند. در معاهدات بین‌المللی نیز هیچ مهلتی برای رسیدگی به درخواست‌های معاضدت تعیین نشده است. البته برخی از کنوانسیون‌ها استفاده از روش‌های

44. Andrew K. Woods, "Data beyond Borders: Mutual Legal Assistance in the Internet Era," 2015, https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub (Accessed November 10, 2018), 3.
45. R. E. Bell, "The Prosecution of Computer Crime," *Journal of Financial Crime* 9 (2002): 316.
۴۶. رضوی‌فرد، پیشین، ۹۳.
47. Ibidem.
48. Malby, et al., op.cit. 206.
49. Tonya L. Putnam and David D. Elliott, "International Responses to Cyber Crime," In *The Transnational Dimension of Cyber Crime and Terrorism,* ed. Abraham D. Sofaer et al. (Stanford: Hoover Institution, 2001), 62.

ارتباطی سریع نظیر پست الکترونیک، دورنما یا سیستم‌های آنلاین را درموارد اضطراری پیش‌بینی کرده‌اند که البته بایستی متعاقباً به‌صورت رسمی تأیید شود.[۵۰] ایجاد شبکه‌های ارتباطی ۲۴ ساعته نیز احتمالاً سبب افزایش سرعت همکاری‌ها شده است.[۵۱]

بروکراسی، کمبود منابع مالی و نیروی انسانی، ناآگاهی از ضوابط و معیارهای قانونی دولت مقابل، عدمِشفافیت دولت‌ها در بررسی و اجرای درخواست‌ها، عدم‌کفایت ادلّه برای اثبات ضرورت دسترسی به داده‌ها و فقدان یک چهارچوب استاندارد واحد برای تنظیم درخواست‌ها ازجمله عوامل کندی فرایندهای معاضدتی هستند. در شرایطی که جرایم سایبری به‌سرعت جابه‌جایی داده‌ها ارتکاب می‌یابند، تأخیر در دسترسی مأمورین به داده‌ها به این معناست که مجرمان سایبری می‌توانند داده‌ها را حذف یا پنهان کنند، روش‌های ارتکاب جرم را تغییر دهند و رد پای خود را پیش از انتقال داده‌ها از بین ببرند. این شرایط می‌تواند دولت‌ها را به‌سوی اقداماتی نظیر داخلی‌سازی داده‌ها و محدودسازی دسترسی به سرورهای خارجی سوق دهد.

مشکل دیگر مربوط است به تفتیش و توقیف بانک‌ها و حامل‌های داده. ممکن است دولت‌ها تفتیش یا توقیف داده‌ها را از یکدیگر تقاضا نمایند. بااین‌حال ممکن است قانون دولت درخواست‌شونده، تفتیش و توقیف را تنها در رابطه با اشیاء مادی امکان‌پذیر بداند که در این صورت بانک‌های داده و سیستم‌های حامل باید توقیف شوند. ظرفیت فنی بانک‌های داده و سیستم‌های حامل برای ذخیره‌سازی داده‌ها اغلب بسیار بیشتر از حجم داده‌های موردنظر دولت درخواست‌کننده می‌باشد؛ بنابراین بایستی قواعد روشنی در رابطه با باقی داده‌های ذخیره‌شده بر روی آنها وضع گردد تا تنها داده‌های موردنظر تفتیش و توقیف گردند و اختلالی در فعالیت‌های سایر کاربران به‌وجود نیاید.

۴- همکاری مستقیم با شرکت‌های خارجی ارائه‌دهندهٔ خدمات اینترنتی

شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی طیف گسترده‌ای از داده‌های مربوط به کاربران را

---

۵۰. نک: بند ۳ مادهٔ ۲۵ کنوانسیون بوداپست، بند ۳ مادهٔ ۳۲ کنوانسیون اتحادیهٔ عرب درزمینهٔ مبارزه با جرایم فناوری اطلاعات و بند (c) مادهٔ ۴۳ پیش‌نویس مقررات مدل بازار مشترک آفریقای شرقی و جنوبی درزمینهٔ امنیت سایبری.

۵۱. اولین شبکهٔ ارتباطی ۲۴/۷ توسط گروه ۸ ایجاد شد که عضویت در آن به دولت‌های عضو گروه محدود نمی‌باشد. اعضای کنوانسیون بوداپست و اینترپل نیز شبکه‌های ارتباطی مشابهی را ایجاد نموده‌اند. کنوانسیون اتحادیهٔ عرب نیز اعضاء را متعهد به ایجاد چنین شبکه‌ای کرده است.

جمع‌آوری و حفظ می‌کنند. این داده‌ها می‌توانند شامل نام، نشانی، اطلاعات کارت‌های اعتباری، آی‌پی آدرس‌ها، محتوای نامه‌های الکترونیکی، داده‌های مربوط به موقعیت جغرافیایی و سوابق جستجو در اینترنت باشد. ممکن است این داده‌ها به‌عنوان ادلّهٔ جرم در جریان تعقیب جرایم سایبری مورداستفاده قرار گیرند. این شرکت‌ها درموارد بسیاری، داده‌های کاربرانشان را بنا به تقاضای دولت‌های خارجی در اختیار آنان قرار می‌دهند. البته این درصورتی است که شرکت‌های مزبور بر اساس قوانین دولت متبوعشان ـ علی‌الخصوص قوانین مربوط به حریم خصوصی ـ و همچنین تعهدات قراردادیشان در قبال کاربران، مجاز به انجام چنین کاری باشند. باتوجه‌به کندی و زمانبر بودن فرایندهای معاضدت قضایی، همکاری مستقیم با شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی می‌تواند بر سرعت فرایند تعقیب جرم بیفزاید. بااین‌حال همکاری مستقیم با شرکت‌های خدمات اینترنتی در هیچ‌یک از اسناد بین‌المللی موجود موردتوجه قرار نگرفته است. تنها استثناء دراین‌زمینه پیش‌نویس مقررات مدل بازار مشترک آفریقای شرقی و جنوبی درزمینهٔ امنیت سایبری است که ارائهٔ داوطلبانهٔ اطلاعات توسط ارائه‌دهندگان خدمات اینترنتی را پیش‌بینی کرده است.[۵۲] تنها ۱۰ درصد از دولت‌های جهان برای دستیابی به داده‌های رایانه‌ای به‌طور مستقیم با ارائه‌دهندگان خدمات اینترنتی ارتباط برقرار می‌کنند.[۵۳]

البته این نوع همکاری را نمی‌توان همکاری میان دولت‌ها قلمداد نمود؛ بااین‌حال همکاری دولت‌های خارجی با شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی مستلزم موافقت دولت‌های متبوع این شرکت‌هاست که می‌توانند با وضع قوانینی این اختیار را به شرکت‌های مزبور اعطاء نمایند. دسترسی به داده‌ها ازطریق شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی یکی از متداول‌ترین شیوه‌های دسترسی به داده‌های فرامرزی است. به‌طور مثال شرکت گوگل[۵۴] در نیمهٔ اول سال ۲۰۱۴، مستقیماً تعداد ۱۹۱۵۹ درخواست همکاری درزمینهٔ دسترسی به داده‌های کاربرانش را از دولت‌های خارجی دریافت نموده است.[۵۵] البته دسترسی به برخی از انواع داده‌ها نظیر داده‌های محتوایی مستلزم همکاری مستقیم با دولت متبوع شرکت‌های

---

۵۲. نک: بند (b) مادهٔ ۱۷ پیش‌نویس مقررات مدل بازار مشترک آفریقای شرقی و جنوبی درزمینهٔ امنیت سایبری.

53. United Nation Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), 220.

54. Google

55. Westmoreland, op.cit. 227-228.

خدمات اینترنتی است و دولت‌های خارجی نمی‌توانند دسترسی به آنها را مستقیماً از این شرکت‌ها درخواست نمایند. به‌عنوان مثال مطابق قوانین دولت ایالات‌متحده افشای محتوای یک ارتباط الکترونیکی توسط ارائه‌دهندگان خدمات اینترنتی جرم محسوب می‌شود.[۵۶] این درحالی است که برخی دیگر از انواع داده‌ها نظیر داده‌های مربوط به اشتراک اینترنتی، بر اساس قوانین داخلی مربوط به حریم خصوصی، مستقیماً ازطریق شرکت‌های مزبور قابل‌دسترسی هستند.[۵۷] قوانین دولت‌ها در رابطه با نوع داده‌هایی که می‌توان آنها را خارج از چهارچوب معاضدت قضایی رسمی در اختیار مقامات خارجی قرار داد، متفاوت هستند.[۵۸] برای مثال برخی دولت‌ها تنها می‌توانند داده‌های ترافیکی و داده‌های مربوط به اشتراک اینترنتی کاربران را از این طریق در اختیار مقامات دولت‌های خارجی قرار دهند. برخی دیگر از دولت‌ها، داده‌های مربوط به اشترک اینترنتی را بر اساس عمل متقابل به اشتراک می‌گذارند و شماری از دولت‌ها نیز فقط داده‌هایی را به اشتراک می‌گذارند که توسط پلیس و از طریقی به غیر از اقدامات قهری و بدون حکم دادگاه به‌دست آمده باشند. اگرچه به‌تدریج شرکت‌های غیرآمریکایی بیشتری به ارائهٔ خدمات اینترنتی در سطح جهانی می‌پردازند، اما بااین‌حال امروزه شرکت‌های آمریکایی بخش عمدهٔ بازار جهانی خدمات اینترنتی را در اختیار دارند و ازاین‌رو قوانین و مقررات دولت ایالات‌متحده درزمینهٔ دسترسی به داده‌های کاربران شاکلهٔ حقوقی این نوع دسترسی را تشکیل می‌دهد. این نوع همکاری به‌ویژه درمواردی صورت می‌گیرد که قربانی و مظنون از اتباع دولت درخواست‌کننده باشند و جرم نیز در قلمروی همان دولت ارتکاب یافته و حقوق هیچ‌یک از اتباع دولت متبوع شرکت ارائهٔ‌دهندهٔ خدمات اینترنتی تحت تأثیر قرار نگرفته باشد.[۵۹] برقراری ارتباط با ارائه‌دهندگان خدمات فرامرزی اینترنتی ازطریق مجاری غیررسمی صورت می‌گیرد و درصورتی‌که ارائه‌دهندگان خدمات اینترنتی از همکاری خودداری کنند، مقامات اجرای قانون برای کسب مجوز قانونی لازم و دستیابی به داده‌های موردنظر از مجاری رسمی استفاده می‌کنند. سازکارهای همکاری مستقیم دولت‌ها با شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی را می‌توان در معاهدات معاضدت قضایی متقابل

56. Council of Europe Cybercrime Convention Committee, "Trans-Border Access and Jurisdiction: What Are the Options," 2012, https://rm.coe.int/16802e79e8 (Accessed November 10, 2018), 13.
57. Christopher Hooper, "Cloud Computing and Its Implications for Cybercrime Investigations in Australia," *Computer Law & Security Review* 29 (2013): 155.
58. Council of Europe Cybercrime Convention Committee, "T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime," 2014, https://rm.coe.int/16802e726c (Accessed November 10, 2018), 8,
59. Swire and Hemmings, op.cit. 720.

پیش‌بینی نمود. این نوع همکاری مستلزم آن است که دولت‌ها قوانین هماهنگی را درزمینهٔ تعهدات شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی در قبال درخواست‌های دولت‌های خارجی وضع نمایند. همچنین ازآنجاکه در این سطح از همکاری رفتار متقابل از اهمیت اساسی برخوردار است، دولت‌های طرف همکاری می‌باید ضوابط قانونی مشابهی را برای تضمین حقوق بشر و حفظ حریم خصوصی، شفافیت، حاکمیت قانون و تناسب میان جرم و اقدامات تعقیبی اِعمال نمایند.

۵- تسهیل و ارتقای فرایندهای همکاری

اصلاح قوانین داخلی می‌تواند منجر به تسریع فرایندهای معاضدتی شود. به‌طور مثال می‌توان قوانین را طوری اصلاح نمود که شرکت‌های ارائهٔ خدمات اینترنتی قانوناً بتوانند داده‌های غیرمحتوایی را بدون نیاز به حکم دادگاه در اختیار دولت‌های خارجی قرار دهند چراکه دسترسی به داده‌های غیرمحتوایی کمتر منجر به نقض حریم خصوصی و حقوق کاربران می‌شود. دولت‌ها حتی می‌توانند تصمیم‌گیری درمورد دسترسی دولت‌های خارجی به داده‌های محتوایی کاربران خارجی غیرمقیم را به شرکت‌های خدمات اینترنتی محوّل نمایند. البته چنین تصمیمی می‌تواند از دامنهٔ اختیارات دولت‌ها بکاهد و تهدیدی برای حاکمیت آنها تلقی شود.

کمبود نیروی انسانی عامل مهم کندی رسیدگی به درخواست‌های معاضدت است. تعداد کارکنان معاونت بین‌الملل وزارت دادگستری ایالات‌متحده که رسیدگی به درخواست‌های معاضدت دولت‌های خارجی را برعهده دارد، در پنج سال گذشته ثابت بوده درحالی‌که تعداد این درخواست‌ها به‌طور تصاعدی افزایش یافته است.[۶۰] این مشکل مختص ایالات‌متحده نیست. شمار قابل‌توجهی از درخواست‌های معاضدت به‌صورت ناقص و بدون توجه به معیارهای دولت درخواست‌شونده تنظیم می‌شوند. بسیاری از مقامات مسئول از نحوهٔ صحیح تنظیم درخواست‌ها آگاهی ندارند. ازاین‌رو شاید آموزش مقامات زودبازده‌ترین راهکار برای کارآمدسازی فرایندهای معاضدتی باشد. این آموزش‌ها علاوه‌بر ضوابط قانونی دولت‌های خارجی بایستی مقتضیات حقوق بشری را نیز شامل گردند. برگزاری برنامه‌های آموزشی بین‌المللی می‌تواند بسیار مؤثر باشد. سازمان‌هایی نظیر اینترپل و دفتر مواد مخدر و جرم ملل

60. U.S. President's Review Group, "Liberty and Security in a Changing World: Report and Recommendations of the on Intelligence and Communications Technologies," 2013, Recommendation No. 34, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (Accessed November 5, 2018).

متحد می‌توانند با تدوین پروتکل‌های آموزشی نقش مهمی دراین‌زمینه ایفاء نمایند.

منافع قانونی دولت درخواست‌کننده در دسترسی به داده‌های موردنظر بایستی در درخواست‌های معاضدت قضایی تبیین شوند و صرف تأکید بر وجود ارتباط میان داده‌ها و تعقیب جرم کافی نمی‌باشد. در این راستا بایستی واقعیات پرونده در درخواست‌ها منعکس شود تا دولت درخواست‌شونده لزوم دسترسی به داده‌ها را باتوجه‌به آن ارزیابی نماید. عمدهٔ دولت‌ها از معیارهای قانونی مشخصی برای ارزیابی سوءظن کیفری موجود استفاده می‌کنند. این معیارها برای تعیین حدود به‌کارگیری اختیارات تعقیبی نظیر تفتیش و توقیف داده‌ها به‌کار می‌روند. دولت درخواست‌کننده بایستی از معیارهای قانونی دولت مقابل مطلع باشد تا درخواست خود را مطابق آن تنظیم نماید. به این منظور طرفین معاهدات معاضدت قضایی بایستی معیارهای قانونی خود برای پذیرش درخواست‌های معاضدت را منتشر نمایند. این معیارها بایستی به‌روشنی تبیین گردند و سازمان‌های بین‌المللی نظیر اینترپل و دفتر مواد مخدر و جرم ملل متحد آنها را جمع‌آوری نموده و در دسترس دولت‌ها قرار دهند.

یکی از علل تأخیر در رسیدگی به درخواست‌های معاضدت، تنظیم نادرست آنهاست. ترویج یک چهارچوب استاندارد برای تنظیم درخواست‌ها احتمالاً ساده‌ترین راهکار برای کارآمدسازی فرایندهای معاضدت است. چنین چهارچوبی می‌تواند شامل معیارهایی در رابطه با نوع داده‌های قابل‌درخواست، جرایم موضوع درخواست و دلایل وجود سوءظن موجه باشد.

معاهدات معاضدت قضایی بهترین ابزار برای تعیین چهارچوب همکاری‌ها و تضمین رعایت معیارهای طرفین هستند. ازاین‌رو دولت‌ها باید اهتمام ویژه‌ای به انعقاد این معاهدات داشته باشند. معاهدات معاضدت قضایی موجود نیز بایستی اصلاح شوند تا به چهارچوب‌های کارآمدتر و شفاف‌تری تبدیل شوند. معاهدات مزبور بایستی به‌منظور انطباق با مقتضیات فضای سایبر و ادلّهٔ الکترونیکی بروزرسانی شوند. بیشتر معاهدات موجود اغلب بر دسترسی به ادلّهٔ فرامرزی به‌دست‌آمده از ابزارهای ارتباط از راه دور سنتی تمرکز دارند. همکاری برای دسترسی به داده‌ها بایستی به‌طور صریح در این معاهدات پیش‌بینی شود. دامنهٔ کاربرد معاهدات مزبور بایستی طوری تعریف شود که با پیشرفت روش‌های ارتباطی نیازی به اصلاح آنها وجود نداشته باشد. همچنین دولت‌ها بایستی ملزم به انتشار منظم گزارشی از درخواست‌های معاضدت باشند که جزئیات مربوط به داده‌های موردِدرخواست، دولت‌های درخواست‌کننده و هدف از دسترسی به داده‌ها در آن منعکس گردد.

معاهدات معاضدت قضایی بایستی مهلتی را جهت رسیدگی به درخواست‌ها تعیین کنند و

یا دست‌کم معیاری را دراین‌زمینه تعریف نمایند. به‌طور مثال طرفین می‌توانند توافق کنند که به اغلب درخواست‌ها ظرف یک ماه رسیدگی نمایند. البته چهارچوب‌های زمانی شامل موارد استثنائی نظیر تحقیقات کیفری پیچیده که به زمان بیشتری نیاز دارند، نخواهد شد اما بازهٔ زمانی سی‌روزه می‌تواند به‌عنوان مبنای اصلی تعیین گردد. طرفین بایستی درخواست‌ها را طوری تنظیم کنند که رسیدگی به آنها در مهلت تعیین‌شده ممکن باشد. در حالت ایده‌آل دولت‌ها می‌توانند یک سیستم پیگیری آنلاین ایجاد نمایند تا دولت‌های درخواست‌کننده به‌وسیلهٔ آن در جریان روند رسیدگی قرار گیرند. معاهدات معاضدت قضایی همچنین بایستی حاوی مقررات روشنی در رابطه با حفظ حقوق بشر باشند. معاهدات معاضدت قضایی می‌باید اشتراک‌گذاری داده‌ها را درمواردی‌که به‌رغم وجود مجرمیت متقابل ممکن است منجر به نقض حقوق بشر شود، منع نمایند و احتمال نقض حقوق بشر را به‌عنوان مبنای رد درخواست به‌رسمیت بشناسند. چنانچه دولت درخواست‌شونده به شواهد قانع‌کننده‌ای دست یابد که نشان دهد دسترسی دولت درخواست‌کننده به داده‌های موردنظر می‌تواند منجر به نقض حقوق کاربران شود، بایستی از اجرای درخواست خودداری نماید. ازآنجاکه تصویب معاهدات بین‌المللی توسط قوهٔ مقننه ضروری است، اصلاح آنها اغلب دشوار می‌باشد؛ اما دولت‌ها می‌توانند ازطریق انعقاد موافقت‌نامه‌های اجرایی و الحاق آنها به معاهدات موجود به اهداف موردنظر دست یابند. هرچند نیازی به‌تصویب این موافقت‌نامه‌ها توسط قوهٔ مقننه وجود ندارند اما این اسناد به‌موجب حقوق بین‌الملل لازم‌الاجرا هستند و تعهدات الزام‌آوری به‌وجود می‌آورند.

معاضدت قضایی اساساً یک سازکار دولتی است و اصلاح آن بایستی توسط دولت‌ها صورت گیرد. بااین‌حال درصورتی‌که دستورالعمل‌های قانونی روشنی درزمینهٔ معاضدت‌های قضایی وجود نداشته باشد، شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی می‌توانند گام‌های مهمی برای اصلاح شرایط بردارند. نخست اینکه آنها می‌توانند دولت‌های درخواست‌کننده را در جریان مقتضیات قانونی افشای داده‌ها قرار دهند، مقتضیاتی که در غیاب یا سکوت چهارچوب‌های معاهداتی توسط قانون داخلی تعیین می‌شوند. این شرکت‌ها اغلب به‌وسیلهٔ دولت‌های میزبان خود ملزم به ارائهٔ داده‌ها نمی‌شوند و دولت‌های متبوع این شرکت‌ها هم آنها را از افشای برخی انواع داده‌ها نظیر داده‌های مربوط به اشتراک اینترنتی منع نمی‌کنند. امروزه شرکت‌های ارائهٔ خدمات اینترنت درمورد افشای داده‌ها به‌صورت موردی و بر اساس

تحلیل اسنادی نظیر اعلامیهٔ جهانی حقوق بشر و اصول جی‌ان‌آی[۶۱] تصمیم‌گیری می‌نمایند. دسترسی به داده‌های محتوایی مستلزم ارائهٔ درخواست معاضدت قضایی است و دولت‌های خارجی نمی‌توانند آن را مستقیماً از شرکت‌های خدمات اینترنتی درخواست نمایند. درحالی‌که داده‌های غیرمحتوایی مستقیماً ازطریق این شرکت‌ها و بر اساس قوانین داخلی و موازین حقوق بشر قابل‌دسترسی هستند. دولت‌های درخواست‌کننده بایستی توسط شرکت‌های خدمات اینترنتی در جریان این قوانین قرار گیرند. درصورت وجود معاهدهٔ معاضدت قضایی میان طرفین همکاری برای دسترسی به داده‌های محتوایی بایستی در چهارچوب معاهدهٔ مزبور صورت گیرد اما چنانچه دسترسی به داده‌ها مستقیماً ازطریق شرکت‌های خدمات اینترنتی ممکن باشد آنها بایستی سیاست شفاف و منسجمی را درزمینهٔ افشای داده‌ها اتخاذ نمایند چراکه در بسیاری از موارد دولت‌ها برای دسترسی به داده‌هایی درخواست معاضدت می‌نمایند که مستقیماً ازطریق شرکت‌ها و مطابق سیاست‌های آنان قابل‌دسترسی هستند.

شماری از شرکت‌های بزرگ خدمات اینترنتی سالانه جزئیات مربوط به دسترسی دولتی به داده‌های کاربرانشان را منتشر می‌کنند. این گزارش‌ها اطلاعات مهمی را درمورد نحوهٔ مدیریت داده‌های کاربران در اختیار آنان قرار می‌دهند.[۶۲] بااین‌حال گزارش‌های مزبور مشخص نمی‌کنند که درکدام موارد دسترسی به داده‌ها بنا به درخواست دولت‌های خارجی صورت گرفته است. در احکامی که شرکت‌های خدمات اینترنتی را ملزم به ارائهٔ داده‌ها می‌نمایند اغلب اشاره‌ای به دولت درخواست‌کننده نمی‌شود. درنتیجه این شرکت‌ها نمی‌توانند تصویر روشنی از دسترسی دولت‌های خارجی به داده‌ها ارائه نمایند. انتشار گزارش‌های شفاف درمورد دسترسی دولت‌ها به داده‌های کاربران به سیاست‌گذاران در کارآمدسازی فرایندهای معاضدتی یاری خواهد نمود. امروزه ارزیابی معاضدت‌های قضایی درزمینهٔ دسترسی به

۶۱. اصول جی‌ان‌آی (Global Network Initiative Principles) که توسط سازمان «ابتکار عمل در شبکهٔ جهانی» تدوین شده‌اند، راهبردها و دستورالعمل‌هایی را درزمینهٔ حفاظت از آزادی بیان و حریم خصوصی کاربران در اختیار شرکت‌ها و دست‌اندرکاران فناوری اطلاعات قرار می‌دهند. سازمان مزبور سازمانی غیردولتی است که با هدف جلوگیری از سانسور دولتی اینترنت و حمایت از حقوق کاربران تأسیس شده و تأمین مالی آن توسط مجموعه‌ای از شرکت‌های چندملیتی، سازمان‌های غیرانتفاعی و دانشگاه‌ها صورت می‌گیرد.

۶۲. در همین راستا شرکت‌های گوگل، یاهو، فیس‌بوک، توئیتر، مایکروسافت، اپل و ... سالانه آمار درخواست‌های دولتی برای دسترسی به داده‌های کاربرانشان را منتشر می‌سازند. نک:

Christopher Wolf, "An Analysis of Service Provider Transparency Reports on Government Request for Data," 2013, https://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Papers-Analysis-of-Transparency-Reports.pdf (Accessed November 10, 2018).

داده‌های فرامرزی به‌دلیل عدم‌انتشار اطلاعات دشوار است. حتی بسیاری از دولت‌ها شرکت‌های ارائهٔ خدمات اینترنتی را از انتشار اطلاعات مربوط منع می‌کنند.[۶۳]

در درازمدت انعقاد یک معاهدهٔ جهانی درزمینهٔ دسترسی دولت‌ها به داده‌های فرامرزی می‌تواند به‌عنوان یک جایگزین دیگر برای معاهدات معاضدت قضایی موردتوجه قرار گیرد. چنین معاهده‌ای در مقایسه با معاهدات عمدتاً دوجانبهٔ معاضدت قضایی مزایایی به همراه دارد. دولت‌ها می‌توانند در چهارچوب چنین معاهده‌ای قواعد جهانی دسترسی به داده‌های فرامرزی را تعیین نمایند و آن را جایگزین ترتیبات متشتت معاضدت قضایی سازند. تدوین چنین معاهده‌ای مستلزم گفتگویی جهانی درزمینهٔ چگونگی ایجاد یک رژیم کارآمد همکاری در عین حفظ حقوق بشر، شفافیت و حاکمیت ملّی می‌باشد. البته دستیابی به چنین معاهده‌ای بسیار زمانبر خواهد بود. به‌علاوه ازآنجاکه معاهدات دوجانبه بهتر می‌توانند تضمین‌کنندهٔ منافع طرفین باشند، ممکن است چنین معاهده‌ای منافع برخی دولت‌ها را تأمین ننماید. همچنین ممکن است تلاش برای دستیابی به چنین معاهده‌ای انگیزهٔ دولت‌ها را برای سرمایه‌گذاری در رژیم کنونی معاضدت قضایی و اصلاح آن کاهش دهد. به‌علاوه یک معاهدهٔ جهانی با عضویت گستردهٔ دولت‌ها ممکن است در مقایسه با چهارچوب‌های فعلی معاضدت قضایی حمایت کمتری از حقوق بشر به‌عمل آورد چراکه دولت‌ها دیدگاه‌های متفاوتی نسبت به حقوق بشر دارند و توافق آنها درمورد تضمینات فراگیر حقوق بشری دشوار خواهد بود.

راهکار جایگزین دیگر عبارتست از ایجاد یک نهاد بین‌المللی مستقل برای رسیدگی هماهنگ، شفاف و سریع به درخواست‌های دسترسی به داده‌های فرامرزی. البته ممکن است دامنهٔ صلاحیت چنین نهادی توسط قوانین ملّی محدود شود. به‌طور مثال نهاد مزبور نمی‌تواند درمواردی‌که دسترسی به داده‌ها مستلزم حکم دادگاه است ـ نظیر داده‌های محتوایی ـ تصمیم‌گیری نماید. چنین نهادی می‌باید علاوه‌بر ضوابط حقوق داخلی دولت‌ها، موازین حقوق بشر را نیز در افشای داده‌ها رعایت نماید. البته دولت‌ها تمایل چندانی به تفویض اختیارات حاکمیتی خود به نهادی بین‌المللی ندارند و بعید به‌نظر می‌رسد که با مداخلهٔ چنین نهادی در روند تحقیقات کیفری خود موافقت نمایند. بااین‌حال حتی توافقی محتاطانه دراین‌زمینه گامی

---

۶۳. برای مثال طبق گزارش شرکت وُدافن (Vodafone) انتشار اطلاعات مربوط به دسترسی دولت‌ها به داده‌های کاربران در یک‌سوم از دولت‌های میزبان این شرکت جرم تلقی می‌شود.
"Respecting Our Customers' Rights to Privacy and Freedom of Expression Is One of Our Highest Priorities," Vodafone, Accessed November 10, 2018, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html.

مهم به‌سوی کارآمدسازی معاضدت‌های قضایی درزمینهٔ جرایم سایبری خواهد بود.

نتیجه

معاضدت قضایی متقابل سازکاری است برای استفادهٔ دولت‌ها از اختیارات تعقیبی یکدیگر. بی‌مرزی فضای سایبری سبب شده تا ادلّهٔ الکترونیکی اغلب ماهیتی فرامرزی داشته باشند. به‌علاوه لزوم حفاظت از حریم خصوصی کاربران و حفظ محرمانگی داده‌ها موجب اهمیت یافتن استفاده از معاضدت قضایی برای دسترسی به داده‌های فرامرزی شده است. ادلّهٔ الکترونیکی به‌راحتی حذف یا دستکاری می‌شوند و لذا بسیار ناپایدارند؛ درنتیجه واکنش سریع مأموران تحقیق در دسترسی به آنها ضروری است. از همین رو به موازات ایجاد اختیارات شکلی نوین برای تعقیب جرایم سایبری، اشکال نوینی از معاضدت قضایی نیز برای تعقیب بین‌المللی این جرایم به‌وجود آمده است. بسته به نوع داده‌های موضوع همکاری، نقش آنها در ارتباط اینترنتی و ارتباط آنها با حریم خصوصی کاربران، انواع مختلفی از معاضدت قضایی تعریف شده است.

رویه‌های معمول معاضدت قضایی برای دسترسی به اسناد کاغذی طراحی شده‌اند و برای تعقیب جرایم سایبری ناکافی‌اند. فرایند اجرای درخواست‌های معاضدت بسته به شرایط ممکن است هفته‌ها، ماه‌ها و یا حتی سال‌ها به طول بینجامد. درحالی‌که که فرصت طلایی برای ردگیری جرایم سایبری اندک است چراکه داده‌های ترافیکی و دیگر منابع اطلاعاتی موقتاً در سِرورها ذخیره می‌شوند و درصورت عدمِ‌توقیف سریع قابلِ‌بازیابی نیستند. کمبود معاهدات همکاری، عدمِ‌هماهنگی قوانین شکلی، عدمِ‌شفافیت دولت‌ها در بررسی و اجرای درخواست‌های معاضدت و فقدان یک چهارچوب استاندارد واحد برای تنظیم درخواست‌ها از دیگر مشکلات مهم دراین‌زمینه هستند. مشکلات موجود در سازکارهای معاضدت قضایی درزمینهٔ ادلّهٔ الکترونیکی، دولت‌ها را به سمت اقداماتی نظیر داخلی‌سازی داده‌ها سوق می‌دهد که می‌توانند به تحدید اینترنت آزاد و بروز اختلافات بین‌المللی منجر شوند.

دو رویکرد جایگزین برای غلبه بر این چالش‌ها قابل‌طرح است. رویکرد نخست عبارتست از تلاش برای اصلاح فرایندهای سنتی معاضدت قضایی ازطریق راهکارهای ارائه‌شدهٔ معاهداتی و غیرمعاهداتی. رویکرد دوم ایجاد یک رژیم همکاری نوین است که در آن مقامات بدون نیاز به کسب مجوز از دولت محل ذخیرهٔ داده‌ها از اختیار دسترسی فرامرزی به داده‌های غیرمحتوایی ازطریق شرکت‌های خدمات اینترنتی برخوردار باشند. البته دسترسی فرامرزی مستقیم به داده‌های محتوایی هم مستلزم شفافیت دولت‌ها درمورد قوانین و رویه‌هایشان است و هم مستلزم شفافیت شرکت‌های ارائه‌دهندهٔ خدمات اینترنتی درمورد دسترسی دولت‌ها به داده‌های کاربرانشان.

فهرست منابع

الف. منابع فارسی

رضوی‌فرد، بهزاد. «محدودیت‌ها و راهبردهای صلاحیت در جرایم سایبری». *مجله حقوقی دادگستری* ۹۸ (۱۳۹۶): ۱۰۲-۸۳.

شهبازی، آرامش. «بایسته‌های حقوقی همکاری بین‌المللی در مبارزه با جرایم سایبری». مقالهٔ ارائه‌شده در همایش جنبه‌های حقوقی فناوری اطلاعات و ارتباطات ایران، تهران، ۵ و ۶ اسفند ۱۳۹۶.

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

مؤذن‌زادگان، حسنعلی. «دادرسی الکترونیکی در رویارویی با جرایم رایانه‌ای». *مجله حقوقی دادگستری* ۱۰۰ (۱۳۹۶): ۱۹۶-۱۶۹.

میرمحمدصادقی، حسین. «راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران». *دیدگاه‌های حقوقی* ۴۳-۴۲ (۱۳۸۶): ۱۲۶-۱۰۱.

ب. منابع خارجی

Angers, Lucie. “Combating Cyber-Crime: National Legislation as a Pre-Requisite to International Cooperation.” In *Crime and Technology: New Frontiers for Regulations, Law Enforcement and Research*, edited by Ernesto U. Savona. 39-54. Springer: New York, 2004.

Bell, R. E. “The Prosecution of Computer Crime.” *Journal of Financial Crime* 9 (2002): 308-325.

Chander, Anupam, and Uyên P. Lê. “Data Nationalism.” *Emory Law Jou*rnal 64 (2015): 682-713.

Council of Europe Cybercrime Convention Committee. “Trans-Border Access and Jurisdiction: What Are the Options?” 2012. https://rm.coe.int/16802e79e8 (Accessed November 10, 2018).

Council of Europe. “Explanatory Report to the Council of Europe Convention.” 2001. https://rm.coe.int/16800cce5b (Accessed November 10, 2018).

Council of Europe. “International Co-operation under the Convention on Cybercrime.” 2009. https://rm.coe.int/1680304352 (Accessed November 10, 2018).

Council of Europe. “T-CY Assessment REPORT: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime.” 2014. https://rm.coe.int/16802e726c (Accessed November 10, 2018).

de Carvalho, Elcio Ricardo, Mirza Abdullahel Baqui, Rita Chun-fa Lam, Yoichi Omura, Hiroyuki Ito, Gilbert Caasi Sosa, Napoleon Bonaparte, Jesus Rodriguez Almeida, Yunsik Jang, Shintaro Naito, Ryuji Tatsuya, Tetsuya Sugano, Tetsuya Sugano, Koji Yamada, Haruhiko Higuchi. “Challenges and Best Practices in Cybercrime Investigation.” 2008. http://www.unafei.or.jp/english/pdf/RS_No79/No79_15RC_Group2.pdf (Accessed November 10, 2018).

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters.

Gabuardi, Carlos A. “Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America.” *Mexican Law Review* I (2009): 155-176.

Hooper, Christopher. “Cloud Computing and Its Implications for Cybercrime Investigations in Australia.” *Computer Law & Security Review* 29 (2013): 152-163.

Kettle, M., and O. Bowcott. “Computer Crime: The Age of Digital Sleuth.” *The Guardian*, December 12, 1997.

Lee-Makiyama, Hosuk. “A Multilateral Legal Assistance Protocol: Preventing Fragmentation and Re-dearterialisation of Internet.” 2013. http://www.ecipe.org/app/uploads/2014/12/PB9.pdf (Accessed November 10, 2018).

Leviathan Security Group. “Quantifying the Cost of Forced Localization.” 2015. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying™he+Cost+of+Forced+Localization.pdf (Accessed November 10, 2018), 13-14.

Lovells, Hogan, and Client Alert. “Marco Civil da Internet: Brazil’s New Internet Law Could Broadly Impact Online Companies’ Privacy and Data Handling Practices.” 2014. http://ehoganlovells.com/cv/92a5426dc5d9947a6ef3abd4eb988b549ae2472b (Accessed November 10, 2018).

Malby, Steven, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus and Eva Ignatuschtschenko. *Comprehensive Study on Cyber-Crime*. Vienna: UNODC, 2013.

Putnam, Tonya L., and David D. Elliott. “International Responses to Cyber Crime.” In *International Dimension of Cyber Crime and Terrorism*, edited by Abraham D. Sofaer and Seymour E. Goodman, 36-67. Stanford: Hoover Institution, 2001.

Stoll, Clifford, & John. W. D. Connolly. “The Cuckoo’s Egg: Tracking a Spy through the Maze of Computer Espionage.” *Physics Today* 43 (1990): 75-76.

Sussmann, Micheal A. “The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium.” *Duke Journal of Computer & International Law* 9 (1998): 451-489.

Swire, Peter, and Justin D. Hemmings. “Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program.” *New York Annual Survey of American Law* 71 (2017): 687-800.

Swire, Peter. “From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud.” *International Data Privacy Law* 2 (2012): 200-206.

U.S. President’s Review Group. “Liberty and Security in a Changing World: Report and Recommendations of the on Intelligence and Communications Technologies.” 2013. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (Accessed November 5, 2018).

UN General Assembly Resolution A/RES/55/63, Combating the Criminal Misuse of Information Technologies, 22 January, 2001.

United Nation Office on Drugs and Crime (UNODC). *Comprehensive Study on Cybercrime*. New York: United Nations, 2013.

Vodafone . “Respecting Our Customers’ Rights to Privacy and Freedom of Expression Is One of Our Highest Priorities.” Accessed November 10, 2018. http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html.

Westmoreland, Kate, and Gail Kent. “International Law Enforcement Access to User Data: A Survival Guide and Call for Action.” *Canadian Journal of Law and Technology* 13 (2015): 225-254.

Wolf, Christopher. “An Analysis of Service Provider Transparency Reports on Government Request for Data.” 2013. https://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Papers-Analysis-of-Transparency-Reports.pdf (Accessed November 10, 2018).

Woods, Andrew K. “Data beyond Borders: Mutual Legal Assistance in the Internet Era.” 2015. https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1517&context=law_facpub (Accessed November, 2018).