مجله حقوقی بین‌المللی/ شماره ۶۰/ بهار ـ تابستان ۱۳۹۸/ صفحات ۲۱۰ ـ ۱۸۵

دسترسی به اطلاعات دیتاسنتر دولت خارجی در تقابل با اصول صلاحیت کیفری سرزمینی و اعمال حاکمیت در حقوق بین‌الملل

جواد صالحی*

شناسه دیجیتال اسناد (DOI) : 10.22066/cilamag.2019.35082

تاریخ دریافت: ۱۳۹۶/۰۷/۱۵ تاریخ پذیرش: ۱۳۹۶/۱۲/۲۷

چکیده

سرویس رایانش ابری یکی از امکانات نوظهور فضای سایبری است. بر این اساس، دیتای شخصی در حساب کاربری یا صفحه کاربر در شبکه‌های اجتماعی افراد در سایبر تولید و تبادل می‌شود. سپس این دیتا به دیتاسنترهای فراسرزمینی در اختیار و کنترل شرکت‌های سرویس‌دهنده خدمات الکترونیک منتقل و ذخیره می‌شود. وقوع جرم و انتقال دیتای مجرمانه آن نیز از این فرایند مستثنا نیست. تحقیقات کیفری از قلمرو سرزمینی در این حوزه، در تعارض با اعمال صلاحیت سرزمینی و اعمال حاکمیت دولت خارجی است. از حیث نظری، شرکت سرویس‌دهنده در قلمرو درون‌سرزمینی، اطلاعات کاربران خویش را با توجیه حفظ حریم خصوصی در اختیار مقامات تحقیق قرار نمی‌دهد. دولت محل استقرار دیتاسنتر نیز اعمال صلاحیت کیفری دولت متقاضی دریافت دیتای مجرمانه را با توجیه اعمال حاکمیت درون‌سرزمینی و مداخله در امور حاکمیتی وی نمی‌پذیرد. این وضعیت در رویه‌قضایی نیز در رابطه با پرونده مایکروسافت، منجر به تعارض اعمال اصل صلاحیت سرزمینی با اعمال حاکمیت دولت خارجی محل استقرار دیتاسنتر شده است. پیامد صدور قرار الزام شرکت *مایکروسافت*، با توجیه درون‌سرزمینی‌بودن مرکز فعالیت وی، بر افشای اطلاعات ذخیره‌شده در دیتاسنتر مستقر در ایرلند، توسعه صلاحیت کیفری فراتر از مرزهای سرزمینی و مداخله در امور حاکمیتی دولت ثالث است. تحقیقات کیفری به اتکای مجوزهای قضایی درون‌سرزمینی برای دسترسی به دیتای ذخیره‌شده در قلمرو دولت خارجی با بن‌بست بایسته‌های حقوق بین‌الملل کیفری مواجه است. راهکار برون‌رفت از این وضعیت، توسل به معاهده همکاری حقوقی متقابل است. اما این همکاری نیز مستلزم مراعات و تفکیک صلاحیت کیفری درون‌سرزمینی و برون‌سرزمینی و همین طور، احترام به اعمال حاکمیت دولت خارجی در قلمرو سرزمینی خویش است.

* استادیار دانشگاه پیام نور، تهران javadsalehi@pnu.ac.ir

واژگان کلیدی
رایانش ابری، دیتاسنتر، اصل صلاحیت سرزمینی، اصل حاکمیت، جرایم سایبری

مقدمه

ظهور ابزارهای جدید اطلاعاتی و ارتباطی در عصر حاضر، موجد روش‌هایی جدید برای برقراری ارتباط، تولید و ذخیره دیتا شده است.[۱] اینترنت شرایطی را برای بشریت فراهم آورده است که از حیث قلمرو و اهمیت در طول حیات بشری بی‌سابقه است.[۲] توسعه سرویس‌های جامعه اطلاعاتی، بخش بزرگی از فعالیت‌های اجتماعی افراد را از دنیای واقعی به دنیای مجازی منتقل کرده است. سایبر، فضای سیال است که حد و مرزی ندارد. اگرچه برخی معتقدند که مرزهای فضای سایبر همان مرزهای سابق میان کشورهاست،[۳] واقعیت این است که مرزهای جغرافیایی دنیای واقعی در سایبر مشهود است و ورود و خروج افراد در آن محدودیت ندارد. بنابراین سایبر، فرامرزی و بدون جغرافیاست. تحت این شرایط، چالش‌های جدید امنیت ارتباطات الکترونیک و فعالیت در فضای مجازی در کنار مزایای آن امری بدیهی است،[۴] چرا که فضای سایبر، مالک خصوصی و دولتی ندارد؛ لذا تابع قانونگذاری عمومی نیست.[۵] با توسل به سایبر، از هر منطقه‌ای امکان ارتکاب جرم در منطقه دیگر وجود دارد.[۶] به همین دلیل، جرایم سایبری نسبت به دیگر جرایم فیزیکی از رقم سیاه بالاتری برخوردارند.[۷] ابزارهای اینترنتی جدید نه فقط برای تبادل اطلاعات، خرید الکترونیکی یا تراکنش‌های قانونی بانکی به کار می‌رود، بلکه به همین نحو، مجرمان بنا به مقتضیات خود، از آن برای سرقت، کلاهبرداری و ... استفاده می‌کنند. با وجود این،

۱. شهبازی‌نیا، مرتضی و محبوبه عبداللهی؛ «دلیل الکترونیک در نظام ادله اثبات دعوا،» *فصلنامه حقوق*، مجله دانشکده حقوق‌وعلوم‌سیاسی، دوره ۴۰، شماره ۴، زمستان ۱۳۸۹، ص ۱۹۳.

2. Nunziato, Dawn, *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*, Stanford University Press, 2009, p. 2.

۳. افضلی، رسول؛ محمدباقر قالیباف و میثم احمدی فیروزجائی؛ «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی»، *پژوهش‌های جغرافیای انسانی*، دوره ۴۵، شماره ۱، بهار ۱۳۹۲، ص ۲۳۵.

۴. برای مطالعه بیشتر در این زمینه ن.ک: جواد صالحی؛ «ممنوعیت بازرسی تلفن همراه و بایسته‌های آن؛ جلوه‌ای از حریم خصوصی متهم در رویه‌قضایی و دستاوردهای آن»، *فصلنامه پژوهش حقوق کیفری دانشگاه علامه طباطبایی*، شماره ۲۱، زمستان ۱۳۹۶، ص ۲۲۸.

۵. جوان جعفری، عبدالرضا؛ «جرایم سایبر و رویکرد افتراقی حقوق کیفری»، *مجله دانش و توسعه*، شماره ۳۴، اسفند ۱۳۸۹، ص ۱۷۱.

۶. جهانشیری، جواد؛ محمدرضا حسینی و احمد ابراهیمی؛ «تبیین فرآیند تحقیقات مقدماتی در جرایم سایبری»، *فصلنامه پژوهش‌های اطلاعاتی و جنایی*، دوره ۱۰، شماره ۳، پیاپی ۳۹، پاییز ۱۳۹۴، ص۱۷.

۷. ترابی، کریم و حمید محمدی؛ «بررسی چگونگی پیشگیری کیفری و اجتماعی از جرایم الکترونیکی با تأکید بر نقش نیروی انتظامی و تجارت الکترونیک»، *فصلنامه کارآگاه*، سال دهم، شماره ۳۴، بهار ۱۳۹۵، ص ۴۸.

رشد جرایم سایبری متکی به پیشرفت و گسترش رایانه‌ها و ورود به ابعاد مختلف زندگی مدرن امروز است. جرایم سایبری اعمال غیرقانونی است که در آن رایانه، ابزار یا هدف است.[۸] بر این اساس، جرایم الکترونیکی در فضا و بستری ارتکاب می‌یابد که امکان شناسایی و مقابله با آن بسیار دشوار است. با وجود این، ضروری است به همان نحوی که مجرمان در تطبیق خود با فضای مجازی از آخرین فناوری روز برای نیل به اهداف مجرمانه خویش استفاده می‌کنند، مقامات تحقیقات کیفری نیز در بهره‌گیری از نرم‌افزارهای ردیابی[۹] و هک‌کردن صفحات شخصی مجازی مجرمان، به‌روز عمل کنند، بدون اینکه مجرمان فضای سایبر آن‌ها را شناسایی کنند. مبارزه مؤثر با جرایم سایبری در گرو راهبردهای پیشگیرانه، حمایت از بزه‌دیده و تعقیب کیفری مرتکب آن است،[۱۰] ولی تحقیقات کیفری سایبری در رابطه با اطلاعات موجود در فضای مجازی تحت وب با چالش‌هایی مواجه است، درعین‌حال که این رقابت میان مجرمان و مقامات تحقیقات کیفری در پیشی‌گرفتن از یکدیگر در دسترسی به آخرین نرم‌افزارهای فناوری مدرن برای دستیابی به دیتای شخصی طرف مقابل، مستوجب نگرانی‌هایی در بروز اشتباه در عملکرد مقام تحقیقات کیفری و فراهم‌شدن شرایط نقض حریم خصوصی سایر افراد در سایبر و رایانش ابری[۱۱] است.

رایانش ابری یک طرح محاسباتی جدید شامل سه مدل ارائه خدمت تحت عناوین نرم‌افزار، بستر و زیرساخت است[۱۲] که با فراهم‌شدن این امکان، زین‌پس کاربر از رایانه شخصی برای ویرایش اسناد، اشتراک‌گذاری و پشتیبان‌گیری از داده‌ها با مزایای بهینه، ازجمله خدمات بر خط، پردازش سریع، سرعت شبکه و توزیع داده‌ها با هزینه کم استفاده می‌کند.[۱۳] این مزایا همان امتیازاتی است که مجرمان نیز برای اهداف پلید خود از آن بهره می‌گیرند. با وجود این، نقش دولت برای پیشگیری از جرم یا مبارزه با آن در رایانش ابری با مدیریت امور محقق است. حقوق

۸. لک، بهزاد؛ «شناسایی و پیشگیری از کمین سایبری در فضای مجازی»، *فصلنامه کارآگاه*، شماره ۱۸، بهار ۱۳۹۱، ص ۹۱.

۹. ن.ک: جواد صالحی؛ «استفاده غیرمجاز پلیس از دستگاه ردیاب؛ جلوه‌ای از نقض حریم خصوصی در رویه‌قضایی دیوان عالی ایالات متحده و دستاوردهای آن»، *فصلنامه پژوهش حقوق کیفری دانشگاه علامه طباطبایی*، دوره ۳، شماره ۸، پاییز ۱۳۹۳، ص ۱۴۶.

۱۰. پورقهرمانی، بابک؛ «مطالعه تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست»، *پژوهشنامه حقوق کیفری*، سال هشتم، شماره ۱۵، بهار- تابستان ۱۳۹۶، صص ۲۲-۷.

11. Cloud-computing

۱۲. رضایی، سعید، محمدعلی دوستاری و مجید بیات؛ «مروری بر کنترل دسترسی مبتنی بر ویژگی در محیط‌های ابری»، *دوفصلنامه منادی امنیت فضای تولید و تبادل اطلاعات*، جلد ۹، شماره ۱، ۱۳۹۵، ص ۵۳.

۱۳. محمدی، زینب و نیما جعفری نویمی‌پور؛ «خدمات ابری معتبر و نامعتبر؛ بررسی روش‌های موجود و ارائه راهکارهای جدید»، *فصلنامه منادی امنیت فضای تولید و تبادل اطلاعات*، جلد ۹، شماره ۱، ۱۳۹۵، ص ۳۳.

کیفری برای دولت، کاربردی ابزاری دارد[۱۴] و از آن می‌تواند برای تحقق نظم اقتصادی، سیاسی، سایبری و حریم خصوصی افراد[۱۵] در چارچوب نظام کیفری و جرم‌انگاری نقض این ارزش‌ها بهره گیرد.[۱۶] اما ورود دیتا به فضای مجازی تحت وب (ابر)، میان حق بر حریم خصوصی دیتای کاربران و بایسته‌های امنیت ملی دولت محل استقرار دیتاسنتر ذخیره‌کننده اطلاعات کاربران، تنش ایجاد می‌کند. حریم خصوصی جایی است که فرد در آن احساس امنیت می‌کند[۱۷] و اطلاعات خود را در آن قرار می‌دهد. دیتاسنتر از این حیث حریم خصوصی است. محل استقرار دیتاسنتر ذخیره‌کننده اطلاعات ارسالی به ابررایانش، فراسوی مرزهای دولت متبوع شرکت سرویس‌دهنده و کاربر فضای مجازی آن است. از یک طرف، دیتای ذخیره‌شده کاربر، جلوه‌ای از حریم خصوصی وی است و از طرف دیگر، دیتاسنتر با الزامات امنیت ملی دولت میزبان گره خورده است. ازاین‌رو دیتاسنتر، یک عامل خارجی دخیل در جرم سایبری است. جرم سایبری با برجاگذاشتن تمام عناصر و آثار خود در قلمرو سرزمینی یک کشور، دیگر فراملی نیست. هریک از دولت‌ها مجبور به اعمال حاکمیت خویش در محیط اینترنت است، تا زمانی که از قلمرو سرزمینی به اطلاعات آن دسترسی دارد. اما در فضای ابررایانش، عنصر خارجی دیتاسنتر در ارکان یا آثار آن دخالت می‌کند. این وضعیت، تحقیق و تعقیب جرم و مجازات عامل آن را با پیچیدگی‌هایی مواجه می‌کند که باید برای آن چاره‌اندیشی کرد.

کشف جرم، تحقیق و جمع‌آوری دلایل مجرمانهٔ فراسرزمینی از مصائب دولت سرزمینی تعقیب‌کننده جرم است. گمنامی مجرم در فضای مجازی و عدم دسترسی به وی و دیتای مجرمانهٔ تبادل‌شدهٔ وی در قلمرو سرزمینی نیز در قلمرو جرایم سایبری، مزید بر علت است. تعقیب جرایم فراملیتی با چالش نحوه جمع‌آوری، نگهداری و ارسال دلایل در قلمرو سرزمینی دولت خارجی برای استناد در قلمرو داخلی روبه‌روست، حال آنکه با ناهماهنگی قوانین در نظام‌های حقوقی کشورها مواجه است. برای عبور از این تنگنا پیشنهاد شده است تا با تصویب اسناد در سطح جهانی و منطقه‌ای، با گسترش روزافزون هرزه‌نگاری در فضای سایبر به‌عنوان

---

۱۴. افراسیابی، محمداسماعیل و فهیم مصطفی‌زاده؛ «بررسی رویکرد ابزارگرا به حقوق کیفری ایران در پرتو قانون اساسی»، *فصلنامه دیدگاه‌های حقوقی*، دوره ۱۹، شماره ۶۸، زمستان ۱۳۹۳، ص ۲۴.

۱۵. حبیب‌زاده، محمدجعفر و سلمان عمرانی؛ «تحلیل ساختاری رابطه حقوق کیفری و دانش سیاسی»، *فصلنامه مطالعات حقوقی دولت اسلامی*، دوره دوم، شماره ۳، بهار ۱۳۹۲، ص۵۰.

۱۶. رحمانیان، حامد و محمدجعفر حبیب‌زاده؛ «ابزارگرایی کیفری؛ قلمرو، مفهوم، شاخص‌ها، پژوهش حقوق کیفری»، سال دوم، شماره ۵، زمستان ۱۳۹۲، ص ۶۶.

۱۷. خان‌محمدی، کریم و علی اکبر شامی؛ «اخلاق اسلامی حریم خصوصی در شبکه‌های اجتماعی سایبر (با تأکید بر واتس آپ)»، *اسلام و مطالعات اجتماعی*، دوره ۴، شماره ۲، پیاپی ۱۴، پاییز ۱۳۹۵، ص ۸۵.

یکی از جرایم بین‌المللی مبارزه شود.[۱۸] اما اگر این اسناد، منجر به تغییر در قوانین داخلی و همکاری بین‌المللی میان تمام دولت‌ها نشود، به‌خودی‌خود فایده‌ای ندارد. یکسان‌نبودن نظام‌های حقوقی کیفری کشورها مانع جدی پیش روی تحقیقات کیفری در قلمرو جرایم فراملی ولو در بستر موافقت‌نامه‌های بین‌المللی مرتبط فی‌مابین دولت‌هاست. دولت‌ها بر حسب فرهنگ، عقاید و باورهای مذهبی یا غیرمذهبی ملت، برخی از رفتارها را جرم‌انگاری می‌کنند. مقامات قانونی در کشورهای مختلف در انجام تحقیقات برحسب قوانین آیین دادرسی کیفری داخلی از تکنیک‌ها و شگردهای خاص در جمع‌آوری دلایل مجرمانه استفاده می‌کنند. ممکن است این قوانین با استانداردهای حقوق‌بشری یا اصول پیشرفته دادرسی عادلانهٔ مورد پذیرش نظام‌های حقوقی پیشرفته منافات داشته باشد. بااین‌همه، ناگزیر تنها گزینه برای رفع موانع، معاهدات همکاری متقابل دولت‌هاست. دولت‌های عضو معاهدات همکاری حقوقی متقابل با اشراف به قوانین داخلی خویش به خواسته‌های طرف‌های مقابل در انجام تحقیقات کیفری توجه مقتضی نموده و با تصویب یا اصلاح قوانین آیین دادرسی کیفری هماهنگ، زمینه را برای همکاری متقابل فراهم می‌کنند.

این نوشتار در صدد است که با بررسی مباحث ابررایانش، جلوه‌ای مدرن از فضای سایبر در چالش با انتقال و ذخیره فراسرزمینی اطلاعات کاربران اینترنت (الف)، الزام مایکروسافت به افشای اطلاعات دیتاسنتر فراسرزمینی در چالش با اصول حاکمیت و سرزمینی‌بودن قوانین (ب)، چالش‌های نظام عدالت کیفری در فضای ابررایانش بر اساس آموزه‌های حقوق بین‌المللی کیفری (ج) به این سؤال‌ها پاسخ دهد که آیا دادستان و دادگاه کیفری برای تکمیل تحقیقات کیفری در قلمرو جرایم سایبری می‌توانند به شخص حقوقی مستقر در قلمرو سرزمینی خویش، دستور افشای اطلاعات ذخیره‌شده در دیتاسنترهای فراسرزمینی را بدهند؟ آیا الزام شخص حقوقی به افشای دیتای موجود در قلمرو سرزمین دولت دیگر، نقض اعمال حاکمیت دولت ثالث در برخورداری از صلاحیت کیفری سرزمینی نیست؟

الف. ابررایانش، جلوه‌ای مدرن از فضای سایبر در چالش با انتقال و ذخیره فراسرزمینی اطلاعات کاربران اینترنت

تحول در زیرساخت‌های فناوری اطلاعات، مرهون ظهور پدیده رایانش ابری است. فضای سایبر، مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی بدون درنظرگرفتن

۱۸. تقی‌پور، علیرضا و مرتضی زرینه؛ «پاسخ کیفری در قبال هرزه‌نگاری سایبری در اسناد بین‌المللی و قانون جرایم رایانه‌ای مصوب ۱۳۸۸»، *مجله حقوقی دادگستری*، سال ۸۱، شماره ۹۹، پاییز ۱۳۹۶، صص ۸۲-۵۹.

جغرافیای فیزیکی است.[۱۹] فضای سایبر، بستری است که داده‌های الکترونیکی در آن ذخیره و پردازش می‌شود و در اختیار کاربر آن قرار می‌گیرد. کاربر اینترنت به‌محض ساخت یک حساب کاربری ایمیل در *گوگل*، ارسال یا دریافت ایمیل، از این طریق وارد فضای ابررایانش می‌شود. زمانی که کاربر اینترنت به اطلاعات، نرم‌افزارها و اپلیکیشن‌های ذخیره‌شده در فضای مجازی تحت وب دسترسی پیدا می‌کند نیز به همین نحو است.[۲۰] ابر[۲۱] دربرگیرنده مرکز دیتای سخت‌افزار و نرم‌افزاری تأمین‌کنندهٔ سرویس پردازشی است و زمینه دسترسی کاربران به حجم عظیمی از منابع محاسباتی به‌صورت مجازی‌شده را فراهم می‌کند تا نرم‌افزارهای تحت وب توسط سرویس‌دهندگانی مانند *گوگل* یا *مایکروسافت* از طریق سرویس رایانش ابری برای آن‌ها قابل بهره‌برداری باشند. تحت این شرایط، اطلاعات در ابر به‌جای دستگاه رایانه ذخیره می‌شود. دیتا و اطلاعات، دارایی باارزشی است که باید با دقت از آن نگهداری شود. وابستگی به اطلاعات و سرعت تغییر فناوری، بسیاری از سازمان‌ها را مجبور کرده است که از سامانه اطلاعاتی با برنامه‌های امنیتی مناسب محافظت کنند.[۲۲] رایانش ابری، الگویی کم‌هزینه با کارایی بالا برای عرضه خدمات رایانشی در پاسخ به نیازهای کاربر خدمات نوین حوزه فناوری اطلاعات است.

دیتای شخصی کاربران الکترونیک شرکت *مایکروسافت* در فضای ابر قابل دسترسی است. اما این دیتا پس از پردازش در دیتاسنتر ایرلند ذخیره می‌شود؛ حال آنکه مرکز فعالیت شرکت *مایکروسافت* در *نیویورک* است و کاربران الکترونیک وی از سرتاسر جهان هستند. اگرچه بهتر است محل استقرار دیتاسنتر برای بهبود کیفیت و سرعت ارتباطات شبکه اینترنت، نزدیک به محل فعالیت شرکت سرویس‌دهنده باشد، این الزاماً به معنای وحدت محل استقرار شرکت *مایکروسافت* و محل استقرار دیتاسنتر نیست.[۲۳] فضای ابر به کاربر مجازی اجازه دسترسی به اطلاعات الکترونیک را در هر جای دنیا می‌دهد، اما محل فیزیکی ذخیره این اطلاعات در نهایت، دیتاسنتر مستقر در یک مکان خاص است. با وجود این، پس از ذخیره در دیتاسنتر فراسرزمینی، دسترسی به این اطلاعات به‌طور مطلق برای کاربر آن ممکن است. برای شرکت ارائه‌دهنده خدمات ابررایانش نیز به استناد پروتکل‌های متفاوت و بسته به نرم‌افزارها و اپلیکیشن‌های مورد استفاده نیز تا حدودی ممکن‌الحصول است. اما این دسترسی برای دولت متبوع کاربر، یا دولت

۱۹. عاملی، سعیدرضا؛ *رویکرد قضایی به آسیب‌ها، جرایم و قوانین و سیاست‌های فضای مجازی*، امیرکبیر، ۱۳۹۰، ص ۲۳.

20. Koba, Mark, Cloud Computing 101: Learning the Basics , 2011. Available at: http://www.cnbc.com/id/43077233.

21. Cloud

۲۲. ملکان، اسفندیار و رسول سلمانی؛ «ویروس‌های کامپیوتری، تهدیدی برای امنیت سیستم اطلاعات حسابداری»، *پژوهش حسابداری*، دوره ۲، شماره ۴، شماره پیاپی ۷، زمستان ۱۳۹۱، ص ۳۹.

23. *Microsoft Corp. v. United States* (2014), In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, Case No. 14-2985-cv, Available at: http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html., p. 2.

محل استقرار مرکز فعالیت شرکت ارائه‌کننده خدمات الکترونیک با ممنوعیت مواجه است. در چنین فضایی اگرچه پلیس می‌تواند با بهره‌مندی از آموزه‌های جرم‌شناسی سایبری، تحلیل مسائل مجرمانه و ناهنجار فضای مجازی، بزهکار سایبری را شناسایی کند،[۲۴] در این مسیر با چالش‌هایی مواجه است که دامنه آن به فراسوی مرزهای سرزمینی در نحوه جمع‌آوری اطلاعات از فضای ابررایانش و ذخیره‌شده در دیتاسنتر فراسرزمینی می‌رسد. اگرچه این مسئله در ایران فاقد سابقه قانونی و رویه‌قضایی است، از چالش‌های نوظهور برخی از سیستم‌های قضایی است که در این حوزه پیشرو هستند. ایالات متحده بر اساس مقررات قانونی ارتباطات ذخیره‌شده[۲۵] می‌تواند محتویات ارتباطات ذخیره‌شده در قلمرو سرزمینی خویش را تحت شرایطی در اختیار بگیرد. اما قانون مذکور در خصوص دسترسی به دیتای ذخیره‌شده در دیتاسنتر فراسرزمینی ساکت است. بر اساس نظریه اصل حاکمیت داخلی نسبت به امور شرکت سرویس‌دهندهٔ ارتباطات الکترونیک در قلمرو سرزمینی می‌توان شرکت *مایکروسافت* را ملزم به افشای دیتای شخصی کاربران خویش کرد.[۲۶] اما این نظریه تنها نسبت به دیتای ذخیره‌شده در دیتاسنتر درون‌سرزمینی کاربرد دارد. اگر دیتا در دیتاسنتر مستقر در قلمرو فراسرزمینی ذخیره شده باشد، قاعده سرزمینی‌بودن قوانین کیفری حاکم است. بر این اساس باید قائل به محدودیت حاکمیت قانون نسبت به دیتاسنتر درون‌سرزمینی بود. اگر دیتاسنتر در خارج از قلمرو سرزمینی دولت متقاضی اطلاعات آن مستقر باشد، ممنوعیت‌های فراسرزمینی اعمال صلاحیت کیفری در تعقیب، تحقیق و جمع‌آوری دلایل مجرمانه پیش می‌آید.

صلاحیت قضایی دولت تعقیب‌کنندهٔ جرم، مبنای تحقیقات کیفری در قلمرو جرایم ارتکابی در فضای ابر است. عرصه فضای مجازی، جهانی است. در این عرصه کدام دولت دارای صلاحیت قضایی تعقیب و تحقیق جرایم است؟ در جامعه بین‌الملل، حق مالکیت و افشای دیتای ذخیره‌شده در دیتاسنترهای فراسرزمینی با کدام دولت است؟ این در حالی است که این دیتا در کنترل کاربر آن و شرکت سرویس‌دهنده آن است. چه ابزاری برای الزام شرکت سرویس‌دهنده خدمات الکترونیک به افشای دیتای فراسرزمینی به دولتی وجود دارد که تحت تأثیر عوارض منفی دیتا و کاربر مجرم آن قرار گرفته است؟ پاسخ به این ابهامات در قلمرو حقوق بین‌الملل کیفری، به لحاظ اعمال صلاحیت کیفری سرزمینی و اعمال حاکمیت درون‌سرزمینی دولت‌ها، محدودیت‌های دارد که تحت تأثیر جهان‌شمولی اینترنت قرار گرفته است و از اهمیت زیادی در مناسبات

۲۴. مسعودیان، محسن؛ «نقش پلیس در پیشگیری از جرایم سایبری و تأمین امنیت در فضای مجازی»، *فصلنامه انتظام اجتماعی*، دوره ۴، شماره ۱، بهار ۱۳۹۱، ص ۱۰۳.

25. Stored Communications Act

26. Center for Democracy and Technology, "Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?", 2014, Available at: https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrantcompel-a-us-provider-to-disclose-data-stored-abroad/.

بین‌المللی برخوردار است.[۲۷] اعطای صلاحیت الزام شخص حقوقی به افشای اطلاعات کاربران به دولت سرزمینی شرکت‌های پشتیبانی اینترنت به معنای دادن حق قانونی بر نقض حریم خصوصی کاربران فضای مجازی تحت وب از سرتاسر دنیاست.[۲۸] ذخیره اطلاعات کاربران *مایکروسافت* در فضای مجازی تحت وب با کنترل و مدیریت شرکت *مایکروسافت* صورت می‌گیرد که در قلمرو سرزمینی ایالات متحده فعالیت می‌کند. از حیث فنی، شرکت *مایکروسافت* می‌تواند در قلمرو سرزمینی محل فعالیت به این اطلاعات دسترسی یابد، آن‌ها را استخراج کند و در اختیار دولت سرزمینی مرکز فعالیت قرار دهد، بدون اینکه برای انجام آن‌ها نیازی به مجوزی از ایرلند، دولت سرزمینی محل استقرار دیتاسنتر داشته باشد.[۲۹] این استدلال از لحاظ نظری اگرچه ممکن به نظر می‌رسد، دقت در آن حاکی از اعمال صلاحیت فراسرزمینی و مداخله در امور کشور ثالث بدون رعایت تشریفات مقتضی است که با ممنوعیت‌های جدی و در تعارض با رویه دیوان بین‌المللی دادگستری در قضیه کانال *کورفو*[۳۰] است. رویه *دیوان بین‌المللی دادگستری* در قضیه کانال *کورفو* حاکی از ممنوعیت مداخله کشورها در امور داخلی و خارجی دیگر دولت‌هاست، چرا که این رویه منجر به نقض حاکمیت آن‌ها می‌شود که در آموزه‌های حقوق بین‌الملل عمومی ممنوع و موجب مسئولیت بین‌المللی دولت مداخله‌کننده است.

استانداردها و فرایند جمع‌آوری دلایل از فضای مجازی تحت وب و ملاک پذیرش یا عدم پذیرش دلایل جمع‌آوری‌شده در دادگاه‌های داخلی قاعده‌مند نشده است. اگرچه دولت‌ها برای مبارزه با به‌کارگیری نامناسب فناوری‌های نوین و سوءاستفاده از وسایل ارتباطی در نقض حریم خصوصی افراد در فضای سایبر رهنمون شده‌اند،[۳۱] واقعیت این است که ماهیت گسترده و فرامرزی‌بودن محیط سایبری باعث شده است تا کنون اقدام مؤثری از سوی دولت‌ها در مقابله با جرایم سایبری صورت نگیرد.[۳۲] در بسیاری از کشورها هنوز قوانین مناسب تحقیق و تعقیب جرایم

---

۲۷. ضیایی، یاسر و احسان شکیب‌زاده؛ «قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران»، *مجله حقوقی بین‌المللی*، دوره ۳۴، شماره ۵۷، پاییز- زمستان ۱۳۹۶، ص ۲۲۸.

28. Wilson, Mark, Twitter Moves Non-US Accounts to Ireland, and Away from the NSA , Available at: http://yro.slashdot.org/story/15/04/18/0633204/twitter-moves-non-us-accounts-to-ireland-and-away-from-the-nsa. 2015.

29. *United States v. Microsoft Corp*, Brief of Government in Support of the Magistrate Judge s Decision to Uphold a Warrant at 12, In Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 15 F. Supp. 3d 466. 2014.

30. International Court of Justice, *United Kingdom of Great Britain and Northern Ireland v. Albania, Corfu Channel Case*, ICJ Reports, http://www.icj-cij.org/en/case/1., 1949, pp. 34-35.

۳۱. پاکزاد، بتول و محمدحسین آزادی‌خواه؛ «مبانی جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته»، *مطالعات حقوق کیفری و جرم‌شناسی*، دوره ۳، شماره ۲، شماره پیاپی ۷، پاییز- زمستان ۱۳۹۵، ص ۲۰۷.

۳۲. اسلامی، ابراهیم؛ «جایگاه حمایت از بزه‌دیدگان جرایم سایبری در مقررات کیفری حقوق داخلی و حقوق بین‌الملل»، *پژوهش‌نامه حقوق اسلامی*، سال ۱۷، شماره ۱، شماره پیاپی ۴۳، بهار- تابستان ۱۳۹۵، ص ۱۵۷.

فضای مجازی تصویب نشده است.[۳۳] تا کنون مرجع قضایی بین‌المللی فضای سایبر برای رسیدگی به این جرایم، و دادگاهی که بتواند به تمام جرایم ارتکابی در این حوزه رسیدگی کند پیش‌بینی نشده است،[۳۴] در حالی که وقتی که فضای مجازی زندگی افراد را احاطه کرده است، تطبیق اجزا و تجهیزات فنی شبکه مجازی تحت وب با مفاهیم قوانین جزایی حوزه رایانه[۳۵] در اولویت است. مجرمان نیز از این تحول و درهم‌آمیختگی فضای واقعی و مجازی نیز برخوردار شده‌اند. آن‌ها برای احتراز از ریسک تعقیب و دستگیری نیز محیط مجرمانه خود را از فضای فیزیکی به فضای مجازی منتقل کرده‌اند، به این امید که با حفظ گمنامی، هم بخش اعظمی از جامعه را در دام خود گرفتار کنند و هم معادله فایده ـ هزینهٔ اعمال مجرمانه خویش را به نفع خود تعدیل کرده و افزایش دهند؛ حال آنکه دسترسی قانونی به اطلاعات مجازی مُبیّن اعمال مجرمانه مرتکبین آن، و مقدمه اثبات جرایم سایبری است.[۳۶] اصل بر درون‌مرزی‌بودن قلمرو حقوق کیفری است.[۳۷] تحقیقات پلیسی و قضایی نیز تابع تشریفات و مقررات درون‌سرزمینی است.

ب. الزام مایکروسافت به افشای اطلاعات دیتاسنتر فراسرزمینی در چالش با اصول حاکمیت و سرزمینی‌بودن قوانین

دولت‌ها با توسل به صلاحیت سرزمینی، مرتکبان جرایم ارتکاب‌یافته در قلمرو خویش را مجازات می‌کنند تا بدین وسیله اقتدار خویش را اثبات کنند.[۳۸] تحت این شرایط، تسرّی قوانین فراسرزمینی کشورها و تأثیر آن بر صلاحیت بین‌المللی کشورها با چالش‌هایی روبه‌روست. در نظام حقوق بین‌الملل، از حیث تاریخی، انعقاد معاهده *وستفالی* (۱۶۴۸) مؤید ظهور اصل حاکمیت دولت در

33. Martini, Ben and Kim-Kwang Raymond Choo, An Integrated Conceptual Digital Forensic Framework for Cloud Computing , *Digital Investigation*, vol. 9, No. 2, Available at: http://www.sciencedirect.com/science/article/pii/S174228761200059X., 2012, pp. 71-80.

۳۴. فروغی، فضل‌الله و امیر البوعلی؛ «صلاحیت کیفری مراجع قضایی در فضای سایبر»، *مجله تحقیقات حقوقی*، شماره ۵۸، تابستان ۱۳۹۱، ص ۳۳۹.

۳۵. میرمحمدصادقی، حسین و افشین آذری‌متین؛ «راهبرداهای کیفری در بانکداری نوین؛ با تأکید بر امضای الکترونیکی»، *فصلنامه راهبرد*، سال ۲۶، شماره ۸۲، بهار ۱۳۹۶، ص ۴۹.

36. Hooper, Christopher, Martini, Ben & Choo, Kim Kwang Raymond, Cloud Computing and Its Implications for Cybercrime Investigations Australia's *Computer Law and Security Report*, vol. 29, No. 2, 2013, pp. 152-163.

۳۷. طهماسبی، جواد؛ «اصل صلاحیت شخصی مبتنی بر تابعیت بزه‌دیده در قوانین کیفری ایران»، *مجله حقوقی دادگستری*، سال ۸۱، شماره ۹۷، بهار ۱۳۹۶، ص ۱۱۵.

۳۸. فرجیها، محمد و امین آقایی؛ «جنبه‌های منفی و مثبت اصل صلاحیت شخصی در حقوق جزای بین‌الملل»، *فصلنامه مطالعات بین‌المللی پلیس*، شماره ۹، بهار ۱۳۹۱، ص ۷۴.

قلمرو سرزمینی خویش است.[۳۹] اصل برابری حاکمیت دولت‌ها از قدیمی‌ترین و بنیادی‌ترین اصول حقوق بین‌الملل در اعمال صلاحیت کیفری بر جرایم فرامرزی است؛[۴۰] کما اینکه هر دولتی با حمایت کیفری از تبعه داخلی، ولو در هر جای دنیا به دفاع از اعمال حاکمیت خود می‌پردازد. بااین‌همه، هیچ دولتی بر فضای مجازی اعمال حاکمیت انحصاری ندارد.[۴۱] رویه‌قضایی ایالات متحده حاکی از بی‌توجهی به این الزامات است. دادستان در پرونده ایالات متحده علیه *مایکروسافت* موفق به اخذ دستور قضایی برای دسترسی به اطلاعات کاربری شهروندان از *مایکروسافت* شده است، درحالی‌که دیتاسنتر شرکت *مایکروسافت* در *دوبلین*[۴۲] ایرلند مستقر است. دادگاه ایالات متحده در صدور دستور قضایی، به لزوم همکاری *مایکروسافت* در افشای اطلاعات کاربران خود از سرتاسر جهان، فاقد صلاحیت است. اگرچه محل فعالیت شرکت *مایکروسافت* در قلمرو سرزمینی ایالات متحده است، اطلاعات حساب کاربری و محتویات ایمیل کاربران این شرکت در دیتاسنتر ایرلند، ذخیره و نگهداری می‌شود که یک واحد سیاسی مستقل از ایالات متحده در جامعه بین‌الملل است.

محدودیت‌های صلاحیت سرزمینی نباید مانع تحقیقات کیفری دولت شود.[۴۳] بر این اساس، دادگاه می‌تواند شرکت *مایکروسافت* را ملزم به افشای حساب کاربری و محتویات ایمیل تبعه خارجی ذخیره‌شده در دیتاسنتر *مایکروسافت*، ولو مستقر در صندوق امانات بانک کشور خارجی نماید، به‌صرف اینکه مرکز فعالیت *مایکروسافت* درون‌سرزمینی است. دولت نیز معتقد است که قانونگذار در ماده ۴۱ قانون آیین دادرسی کیفری، شرکت‌های عامل را مخاطب قرار داده است که اطلاعات الکترونیک را ثبت و جمع‌آوری می‌کنند، صرف‌نظر از اینکه این اطلاعات را در کجا ذخیره و نگهداری می‌کنند. تکلیف *مایکروسافت* در افشای اطلاعات ایمیل کاربر خویش، ارتباطی به محل نگهداری اطلاعات،[۴۴] ولو خارج از قلمرو سرزمینی ایالات متحده ندارد. بر این اساس، ایالات متحده متقاضی دریافت اطلاعات از عامل مستقر در خاک سرزمین خویش (شرکت *مایکروسافت*) است، صرف‌نظر از اینکه وی این اطلاعات را در ایرلند، یکی از کشورهای عضو

۳۹. ضیایی، یاسر؛ «مبانی نظری صلاحیت فراسرزمینی دولت از منظر حقوق بین‌الملل عمومی»، *مجله حقوقی دادگستری*، شماره ۷۶، زمستان ۱۳۹۰، ص ۲۳.

۴۰. افتخارجهرمی، گودرز و ابراهیم اسلامی؛ «نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرایم فضای مجازی»، *مجله حقوقی دادگستری*، دوره ۷۸، شماره ۸۸، زمستان ۱۳۹۳، ص ۴۲.

41. Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, p. 16.

42. Dublin

43. Narayanan, Vineeth, Harnessing the Cloud: International Law Implications of Cloud-Computing , *Chicago Journal of International Law*, No. 12, 2012, pp. 472-4

44. *United States v. Microsoft Corp*, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 15 F. Supp. 3d, Available at: https://www.casemine.com/judgement/us/5914fab5add7b049349a9a00., 2014, para. 471.

اتحادیه اروپا ذخیره و نگهداری کرده باشد. این استدلال‌ها در مرحله بدوی مقبولیت پیدا می‌کند. اما قرار الزام به همکاری در تحقیقات کیفری با اعتراض *مایکروسافت* در مرحله تجدیدنظر نقض می‌شود.[۴۵] ماده ۴۱ قانون آیین دادرسی کیفری فدرال، مستند شعبه بدوی در الزام *مایکروسافت* به افشای اطلاعات ایمیل کاربر خویش است،[۴۶] حال آنکه مقررات این قانون درون‌سرزمینی است و نسبت به خارج از قلمرو سرزمینی ایالات متحده کاربرد ندارد. دادگاه نمی‌تواند شرکت سرویس‌دهنده ارتباطات الکترونیک را ملزم به بازرسی و افشای اطلاعات ذخیره‌شده‌ای بنماید که در دیتاسنتر خارج از کشور، ضبط و نگهداری می‌شوند. ثبت و افشای اطلاعات دیتاسنتر مستقر در خاک ایرلند، تابع قوانین ایرلند است. اگرچه شرکت سرویس‌دهندهٔ *مایکروسافت* در سرزمین ایالات متحده مشغول به فعالیت است، این شرکت، خود برای استفاده از دیتاسنتر مستقر در ایرلند نیز تابع تشریفات مبتنی بر مقررات ایرلند است. این شرکت در رابطه با فعالیت‌های خویش در سرزمین ایالات متحده دارای مسئولیت حقوقی و کیفری مطابق با قوانین ایالات متحده است، ولی این به معنای چشم‌پوشی از تعهدات ایجادشده برای وی در زمان بهره‌برداری از امکانات سایر کشورها در راستای تحقق اهداف سازمانی خویش نیست. الزام *مایکروسافت* به تبعیت از قوانین ایرلند در برخورداری از امکان ذخیره دیتای کاربران خویش در دیتاسنتر این کشور از اهمّ این تعهدات است.

نظام عدالت کیفری دارای نهادهایی است که در تلاش برای مقابله با جرم هستند.[۴۷] روش‌های تحقیقات کیفری جدید با ابزارهای هک اینترنتی صورت می‌گیرد که حق بر حریم خصوصی[۴۸] و آگاهی از اطلاعات سرنوشت‌ساز افراد را به‌راحتی نقض می‌کند. با وجود این، ماهیت جهانی اینترنت یا اطلاعات تبادل‌شده در بستر آن و ذخیره آن در دیتاسنترهای فراسرزمینی، چیزی را به نفع تحقیقات کیفری داخلی عوض نمی‌کند. اگر حتی بستر مبادلات الکترونیک و مرکز ذخیره اطلاعات آن درون‌سرزمینی باشد، دولت و دادگاه کیفری وی نیز بدون رعایت تشریفات قانونی، مجاز به دسترسی و افشای اطلاعات آن نیستند. در جایی که دولت ثالث به‌عنوان دولت دارنده دیتاسنتر اطلاعات الکترونیک ذخیره‌شده دخیل است، این وضعیت تشدید می‌شود. دولت سرزمینی

45. *Microsoft Corp. v. United States*, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained, No. 829 F.3d, 2016, para. 197.

46. Kerr, Orin, What Legal Protections Apply to E-mail Stored Outside the U.S.? Volokh Conspiracy , 2014, Available at: http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mailstored-outside-the-u-s/.

۴۷. جعفری، فریدون، رؤیا موسوی و امیر اسلامیه همدانی؛ «مطالعه تطبیقی حق برخورداری از وکیل در مرحله تعقیب در حقوق داخلی ایران و اسناد و رویه‌های محاکم کیفری بین‌المللی»، *پژوهش‌های حقوق تطبیقی*، دوره۲۰، شماره ۴، شماره پیاپی ۹۴، زمستان ۱۳۹۵، ص ۲۷.

۴۸. صالحی، جواد؛ «مؤلفه‌های امنیت اجتماعی در قوانین کیفری»، *مجله پژوهش‌های حقوقی*، سال نهم، شماره ۱۷، بهار- تابستان ۱۳۸۹، ص ۱۰۲.

و دادگاه کیفری آن برای صدور مجوز قانونی بر مشروعیت دسترسی غیرمجاز از طریق هک‌کردن اطلاعات ذخیره‌شده در فضای ابررایانش با بن‌بست مواجه است. حفظ نظام اسلامی یکی از مصالح اجتماعی است[۴۹] که در قلمرو جرایم امنیتی داخلی و خارجی معنا و مفهوم می‌یابد. نقض حریم خصوصی با علم اجمالی با وجود مُنکر امری مجاز در قلمرو قاعده حفظ نظام توسط نهادهای اطلاعاتی است،[۵۰] اما به‌جز معدودی ازجمله، هرزه‌انگاری و جاسوسی سایبری که یکی از اصطلاحات جدید در حوزه امنیت سایبری است،[۵۱] سایر جرایم معمولی سایبری از چنین ظرفیتی برخوردار نیستند. بنابراین رویکرد دادگاه سرزمینی در صدور مجوز دسترسی غیرقانونی به اطلاعات ذخیره‌شده در فضای ابررایانش، به‌جز در موارد استثنایی جرایم علیه امنیت عمومی، نقض بایسته‌های حقوق بین‌المللی است. اگرچه غرض از جرم‌انگاری، تعقیب و مجازات فاعل آن، بیش از هر چیز در دیدگاه رایج حفظ نظم و دفاع از منافع عمومی جامعه است،[۵۲] این به معنای توسل به هر ابزاری برای تحقق آن در کلیه جرایم نیست. فعالیت اطلاعاتی و ضداطلاعاتی جزء جدانشدنی حکومت‌ها برای حفظ امنیت است.[۵۳] از یک طرف پیشرفت‌های فناوری‌های ارتباطی و اطلاعاتی، شناسایی موقعیت‌های پیش‌جنایی و پیشگیری از بزهکاری احتمالی سایبری را تسهیل کرده است تا جایی که با کاربست گسترده ابزارهای فاوا می‌توان امنیت حداکثری این فضا را تأمین کرد.[۵۴] دسترسی به ارتباطات الکترونیک مجرمان در فضای مجازی بدون مداخله فیزیکی در تجهیزات مورد استفاده مجرمان از راه دور، دستیابی به اطلاعات حذف یا فرمت‌شده از سیستم‌های رایانه‌ای مجرمان برای جمع‌آوری ادله مجرمانه، نمونه‌هایی از تحقیقات کیفری در حوزه سایبری است. از طرف دیگر، پیشرفت‌های فناوری اطلاعات و ارتباطات الکترونیک، شهروندان را در معرض خطر نقض حریم خصوصی اطلاعاتی توسط سازمان‌های دولتی و

---

۴۹. مهرا، نسرین و کامران محمودیان اصفهانی؛ «الزامات حقوق‌بشری کشف جرم در نظام حقوقی ایران»، *مطالعات حقوق عمومی*، دوره ۴۷، شماره ۲، تابستان ۱۳۹۶، ص ۳۳۶.

۵۰. درگاهی، مهدی؛ «میان‌کنش قاعده حفظ نظام و حریم خصوصی افراد»، *پژوهش‌های حفاظتی ـ امنیتی*، سال پنجم شماره ۱۹، پاییز ۱۳۹۵، ص ۸۳.

۵۱. صدیق، میرابراهیم؛ «انقلاب سایبری و تحول در پدیده جاسوسی»، *فصلنامه مطالعات راهبردی*، سال نوزدهم، شماره ۱، شماره پیاپی ۷۱، بهار ۱۳۹۵، ص ۷۲.

۵۲. نوبهار، رحیم و فاطمه صفاری؛ «رعایت مصالح بزه‌دیده در جرم‌انگاری»، *مجله حقوقی دادگستری*، سال ۸۰، شماره ۹۳، بهار ۱۳۹۵، ص ۲۱۹.

۵۳. علی‌اکبریان، حسنعلی؛ «بررسی حکم شرعی رفتار حکومت در جمع‌آوری اطلاعات از حوزه حریم خصوصی اشخاص»، *فصلنامه کاوشی نو در فقه*، سال بیست‌ویکم، شماره ۳، پاییز ۱۳۹۳، ص ۲۲.

۵۴. فرهادی آلاشتی، زهرا و عبدالرضا جوان جعفری بجنوردی؛ «بررسی تعارض رهیافت‌های تدابیر موقعیت‌مدار نظارت سایبری، با حریم خصوصی کاربران»، *فصلنامه مجلس و راهبرد*، سال بیست‌وسوم، شماره ۸۷، پاییز ۱۳۹۵، ص ۷۵.

غیردولتی قرار داده است،[۵۵] مگر اینکه چارچوب‌های آن بر اساس آموزه‌های حقوق کیفری با اولویت حفظ امنیت ملی مراعات شود. بهره‌گیری از آخرین فناوری اطلاعاتی برای دستیابی به اهداف حفظ نظم و امنیت عمومی در تحقیقات کیفری توجیه می‌شود، اما این رویکرد، تنها نسبت به فضاهای عمومی تحت حاکمیت دولت و کنترل نامحسوس رفتارهای اجتماعی در دسترسی به فضاهای عمومی مجازی قابل پذیرش است.

ج. چالش‌های نظام عدالت کیفری در فضای ابررایانش بر اساس آموزه‌های حقوق بین‌المللی کیفری

رسیدگی به جرایم رایانه‌ای در قلمرو سرزمینی ایران بر اساس بندهای (الف) و (ب) ماده ۲۸ قانون جرایم رایانه‌ای، مبتنی بر صلاحیت سرزمینی است. ولی این مقدار قانونگذاری، ضابطه‌ای برای تشخیص محل وقوع جرایم رایانه‌ای تلقی نمی‌شود،[۵۶] مگر اینکه به حداقل آن یعنی محل استقرار و استفاده از سامانه رایانه‌ای در قلمرو حاکمیتی ایران اکتفا شود. ازاین‌رو ممکن است دولتی بر جرم و فاعل آن صلاحیت داشته باشد، اما این مسئله مجوزی برای وی در گسترش صلاحیت سرزمینی و جمع‌آوری دلایل مثبت جرم نیست، درحالی‌که دلایل جرم در قلمرو سرزمینی کشور دیگر است. صلاحیت کیفری برون‌مرزی مبتنی بر عامل فراملیتی است. بسیاری از دولت‌ها تمایل دارند که قلمرو قوانین کیفری خود را به خارج از مرزهای داخلی بسط دهند[۵۷] اما این رویکرد دولت‌ها در اعمال صلاحیت کیفری فراسرزمینی تابع محدودیت‌های حقوق بین‌الملل عمومی و مسئولیت‌آور است.[۵۸] ازاین‌رو چاره‌اندیشی دولت‌ها برای پرهیز از نقض آموزه‌های حقوق بین‌الملل ضروری است. وضع قانون و قاعده‌مندکردن رفتار، چیزی غیر از اعمال صلاحیت بر رفتاری است که منشأ آن، خارج از قلمرو سرزمینی دولت است. اگر رفتار فردی در قلمرو سرزمینی یک دولت باعث ایراد ضرر به اتباع یا منافع دولت دیگری می‌شود، ضروری است که سیستم قضایی هر دو کشور در زمینه جمع‌آوری دلایل و تعقیب و مجازات فرد خاطی دخیل باشند. ضرورت مبارزه با جرایم فراملی، دولت‌ها را ترغیب به همکاری متقابل برای سرکوب جرم کرده است، مشروط بر اینکه مقررات مربوط به صلاحیت کیفری و منافع

---

۵۵. تقوی‌فرد، محمدتقی، محمدرضا تقوا، مهدی فقیهی و محمدجواد جمشیدی؛ «مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب»، *مجلس و راهبرد*، سال ۲۴، شماره ۸۹، بهار ۱۳۹۶، ص ۳۰۱.

۵۶. البوعلی، امیر؛ «صلاحیت محاکم در جرایم سایبری»، جنگل، ۱۳۹۲، ص ۵۶.

57. Colangelo, Anthony J., "Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law , *Harvard International Law Journal*, 2007, No. 48, p. 121.

58. Lawson, Rick, The Concept of Jurisdiction and Extraterritorial Acts of State , in Gerard Kreijen et al (eds), *State, Sovereignty, and International Governance*, Oxford University Press, 2002, p. 281.

درون‌حاکمیتی آن‌ها از سوی طرف مقابل رعایت شود. این وضعیت در خصوص جرایم اینترنتی نیز صادق است. مبارزه با این وضعیت در گرو سازوکارهای فرامرزی ازجمله همکاری قضایی دوجانبه و استرداد مجرمین است.[۵۹] اما این سازوکارها با توجه به تفاوت در نوع جرم‌انگاری‌ها در فضای مجازی و اعمال صلاحیت کیفری دولت‌ها با پیچیدگی‌هایی توأم هستند.[۶۰]

استرداد مجرمین به‌عنوان یکی از بهترین گزینه‌های تحقق اعمال صلاحیت درون‌سرزمینی دولت متبوع ذی‌صلاح تجربه شده است، اما این گزینه در خصوص جمع‌آوری اطلاعات الکترونیک از سرورهای فراسرزمینی کاربرد ندارد. تأسیس نهاد استرداد مجرم، برای پرهیز از خدشه به حق حاکمیت کشورها و به‌مخاطره‌انداختن روابط مسالمت‌آمیز آن‌ها[۶۱] است، اما نسبت به اتباع داخلی یا در جرایم تأثیرگذار در نظم عمومی دولت سرزمینی، بنا به حق اولویت دولت سرزمینی رعایت نمی‌شود. صرف‌نظر از اینکه قاعده سنتی «استرداد یا محاکمه» در قلمرو جرایم دارای ماهیتِ بین‌المللی که مجازات عامل آن، صرف‌نظر از محل وقوع جرم یا محل دستگیری وی، خواسته جامعه بین‌المللی است، در تمام جرایم سایبری نیز موضوعیت ندارد. قاعده استرداد یا محاکمه در حقوق بین‌الملل، به تعهد حقوقی دولت‌ها مطابق بایسته‌های حقوق بین‌الملل عمومی اشاره دارد که دولت‌ها بر این اساس مکلف‌اند متهمان به ارتکاب جرایم شدید و مهمّ بین‌المللی را محاکمه کنند یا آنان را برای محاکمه به دولت متقاضی استرداد تحویل دهند.[۶۲] بر این اساس، حقوق کیفری مدرن، به همبستگی و پیوستگی بین قوانین کشورها نیاز دارد. بر این اساس، قانون فراملیتی، محصول همکاری دولت‌هاست و اجرای آن توسط عوامل غیردولتی[۶۳] یا نهادی مرکب از اعضا صورت می‌گیرد. تجربه و دستاوردهای نظام حقوقی کشورها و قوانین داخلی آن‌ها در شکل‌گیری قانون فراملیتی تأثیرگذار است. با وجود این، صلاحیت کیفری دولت‌های همکاری‌کننده و عضو در قانون فراملیتی، متکی به رفتار اشخاص است.[۶۴] گاهی عنصر مادی رفتار آن‌ها به

59. Weber, Alamie M., The Council of Europe`s Convention on Cybercrime , *Barkeley Technology Law Journal*, No. 18, 2014, p. 123.

60. Urbas, Gregor, Cybercrime, Jurisdiction and Extradition: the Extended Reach of Cross-Border Law Enforcement , *Journal of Internet Law*, No. 16, 2012, p. 8.

۶۱. ورویی، اکبر و محمد رضوی؛ «بررسی وضعیت حقوقی استرداد مجرمین در قلمرو حقوق کیفری بین‌المللی»، *فصلنامه دانشکده علوم و فنون مرز*، شماره ۲، تابستان ۱۳۹۴، ص ۹۶.

۶۲. اردبیلی، محمدعلی و ندا میرفلاح نصیری؛ «اجرای کنوانسیون‌های بین‌المللی متضمن قاعده استرداد یا محاکمه در ایران»، *مجله حقوقی دادگستری*، سال ۸۱، شماره ۹۸، تابستان ۱۳۹۶، ص ۱۰.

63. Orentlicher, Diane F., Whose Justice? Reconciling Universal Jurisdiction with Democratic Principles in Thomas J Biersteker et al (eds), *International Law and International Relations*, Routledge, 2007, p. 207.

64. Lowe, Vaughan, Jurisdiction in Malcolm Evans (ed), *International Law*, Oxford University Press, 2nd ed, 2003, p. 329.

خارج از مرزهای سرزمینی کشانده می‌شود.[۶۵] در این شرایط، در مواردی که مفهوم سنتی حاکمیت دولت مدنظر قرار می‌گیرد، اعمال قانون فراملیتی کیفری با چالش تداخل صلاحیت کیفری مواجه است.[۶۶] اعمال صلاحیت کیفری ملی در خارج از قلمرو سرزمینی، در تعارض با اصل حاکمیت دولت خارجی قرار می‌گیرد. دولت سرزمینی و دولت خارجی هریک واحد مجزای سیاسی در جامعه بین‌المللی هستند. اعمال صلاحیت دولت سرزمینی خارج از قلمرو حاکمیتی وی، مداخله در اعمال حاکمیت دولت خارجی است، حال آنکه اعمال قوانین برون‌مرزی دولت‌ها بر اساس آموزه‌های حقوق بین‌المللی تا جایی مشروعیت دارد که منجر به نقض حاکمیت سایر دولت‌ها نشود.[۶۷]

دادستان و ضابطین قضایی تحت حاکمیت قوانین و صلاحیت کیفری دولت متبوع خویش هستند، ولی در جرایم فراملی، محل وقوع جرم یا فاعل آن در خارج از قلمرو سرزمینی است. در این شرایط، نظام حقوقی بیگانه و لزوم احترام به حاکمیت سرزمینی وی، مانع از دسترسی به مجرم یا جمع‌آوری دلایل مجرمانه است. مجرم یا دلایل مجرمانه در اختیار دولت فراسرزمینی محل وقوع جرم است. فقدان معاهده یا قرارداد همکاری حقوقی متقابل با وی، مانع از انجام تحقیقات کیفری فراسرزمینی دادستان و ضابطین قضایی داخلی است. معاهدات همکاری حقوقی متقابل میان دولت‌ها موجد اعمال پروسه‌های اجباری فراملیتی است. در مرحله اول، دولت‌های عضو در این معاهدات، استانداردهای بین‌المللی را در قوانین کیفری داخلی وارد می‌کنند و در مرحله دوم، فرایندهای معمول در نظام‌های حقوقی ولو متفاوتِ دیگر دولت‌های عضو را به رسمیت می‌شناسند. انتظار این است که دولت‌ها پس از عضویت در این معاهدات، زمینه را برای کسب و پذیرش دلایل مجرمانهٔ جمع‌آوری‌شده توسط مقامات قانونی دولت سرزمینی در مراجع قضایی نظام‌های حقوقی سایر دولت‌های عضو مهیا کنند. بازرسی، جمع‌آوری و نحوه ثبت و ضبط دلایل مجرمانه، اعتبار شهادت شاهد، شرایط شاهد و نحوه استماع اظهارات وی، صدور اخطاریه‌ها و قرارهای قضایی بر احضار، جلب و دستگیری مظنون یا متهم، اعزام متهم یا شاهد در بازداشت به سرزمین دیگر دولت عضو معاهده، از موضوعات قابل بحث در تنظیم پیش‌نویس معاهده‌های همکاری حقوقی متقابل است.[۶۸]

65. Zerk, Jennifer A., Extraterritorial Jurisdiction: Lessons for the Business and Human Rights Sphere from Six Regulatory Areas , Working Paper, 2010, No. 59, *Harvard Corporate Social Responsibility Initiative*, p. 13.

66. Ireland-Piper, Danielle, Extraterritoriality and Sexual Offences Outside Australia , *Bond Law Review*, No. 22(2), 2010, p. 31.

67. Perrin, Benjamin, Taking a Vacation from the Law? Extraterritorial Criminal Jurisdiction and Section 7(4.1) of the Criminal Code , *Canadian Criminal Law Review*, No. 13, 2009, p. 180.

68. Richardson, L. Song, Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem , *Berkeley Journal of International Law*, No. 26, 2008, pp. 62-110.

با وجود این، رژیم معاهدات همکاری حقوقی دوجانبه،[۶۹] مقامات اروپایی را از تبادل اطلاعات ذخیره‌شدهٔ کاربران در سرورهای سرزمینی خویش منع می‌کند. حتی اگر دادگاه ایالات متحده، الزام شرکت *مایکروسافت* بر افشای اطلاعات کاربران را تأیید کند، باز هم قوانین اتحادیه اروپا مانع انتقال اطلاعات به سرزمین ایالات متحده است.[۷۰] پس از افشای اطلاعات سازمان امنیت ملی ایالات متحده توسط *ادوارد اسنودن*،[۷۱] شرکت‌های ارائه خدمات ابررایانش از سوی دولت‌های اروپایی تحت فشار قرار گرفتند که اطلاعات شهروندان اروپایی را خارج از قلمرو سرزمینی ایالات متحده و در سرزمین کشورهای اروپایی نگهداری کنند.[۷۲] اطلاعات کاربران *مایکروسافت* به‌خاطر ذخیره در دیتاسنتر فراسرزمینی، تحت حمایت قوانین ایرلند از اعضای اتحادیه اروپا و خارج از حکومت قوانین و قلمرو اعمال حاکمیت ایالات متحده است.[۷۳] اتحادیه اروپا از کشورهای عضو خواسته است در راستای تحقق عدالت کیفری، تقاضای دریافت اطلاعات مجرمانه الکترونیکی را تنها از مجاری قانونی بپذیرند.[۷۴] همکاری دولت‌های اروپایی در عرصه اجرایی یا قضایی برای دسترسی سریع و مطمئن به اطلاعات الکترونیک ذخیره‌شدهٔ کاربران اینترنت در سرورهای سرزمینی باید در پرتو الزامات حقوق‌بشری در احترام به حریم خصوصی افراد صورت‌گیرد.[۷۵] بر این اساس، عملکرد دادگاه بدوی در صدور رأی الزام شرکت *مایکروسافت* به افشای اطلاعات سرورهای ایرلند، اِعمال صلاحیت فرامرزی و نقض بایسته‌های حقوق بین‌الملل است.[۷۶] اصل عدم مداخله در امور داخلی کشورها مُبین این مفهوم است که عملکرد دادگاه بدوی منجر به گسترش صلاحیت ایالات متحده در امور داخلی ایرلند و نادیده‌گرفتن اعمال حاکمیت ایرلند در منافع خود است. درعین‌حال، امکان دسترسی *مایکروسافت* به اطلاعات از مرکز فعالیت در قلمرو ایالات متحده بدون نیاز به تقاضای رسمی از دولت ایرلند از غیرقانونی‌بودن این عمل

69. Mutual Legal Assistance Treaty (MLAT)

70. *Microsoft Corp. v. United States*, Albrecht brief, amici in the case, *Electronic Frontier Foundation*, Available at: https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland., 2014, p. 6.

71. Edward Snowden

72. Roberts, Paul, In Wake of Snowden, U.S. Cloud Providers Face Calls to Wall off Data . 2014. Available at: http://www.itworld.com/article/2699656/security/inwake-of-snowden--u-s--cloud-providers-face-calls-to-wall-off-data.html.

73. *Microsoft Corporation v. United States*, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, No. 14-2985, 2017 WL 362765, Available at: http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2017-01-24.html, 2017, p. 39.

74. Council of Europe, Cybercrime Convention Committee (T-CY), Trans-Border Access to Data and Jurisdiction: Options for Further Action by the T-CY, Doc. No. T-CY, 2014, pp. 13-14.

75. Daskal, Jennifer & Andrew K. Woods, Cross-Border Data Requests: A Proposed Framework, Just Security, 2015. Available at: https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework.

76. *Microsoft Corp. v. United States*, Colangelo brief, Amici in the Case, Electronic Frontier Foundation, Available at: https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland., 2014, pp. 10-11.

غیرقانونی‌بودن این عمل نمی‌کاهد.[۷۷] *مایکروسافت* عامل دولت ایرلند در جمع‌آوری اطلاعات کاربران و ذخیره آن‌ها در سرورهای ایرلند است. الزام *مایکروسافت* به افشای اطلاعات در کنترل دولت خارجی به‌واسطه اصل صلاحیت سرزمینی مرکز فعالیت *مایکروسافت*، دورزدن قوانین دولت ایرلند و زیرپاگذاشتن اصل عدم مداخله در امور سایر کشورهاست.

نتیجه

گسترش روزافزون دستاوردهای فناوری در ابعاد مختلف زندگی بشر باعث شده است که ضرورت حمایت از کاربران آن، از چالش‌های اساسی دستگاه قانونگذاری و سیستم عدالت کیفری باشد. رایانش ابری، یک فناوری اطلاعات در فضای سایبر است. استفاده مجاز و غیرمجاز از این بستر برای همگان فراهم است. مخترعین این فضا در صدد بهره‌برداری مجاز بشریت از دستاوردهای آن بوده‌اند تا به رفاه اجتماعی و زدوده‌شدن آسیب‌های اجتماعی کمک بیشتری شود. اما واقعیت این است که در هر حوزه‌ای که بشر پیشرفت کرده، با خلأهایی جدی مواجه بوده است که تا مدت‌ها از همین خلأهای پیش‌بینی‌نشده، صدماتی را متحمل شده تا اینکه بالاخره برای رفع این نقیصه‌ها چاره‌اندیشی کرده است. این وضعیت در رابطه با شکل‌گیری روابط اجتماعی در بستر فضای سایبر و احتمالاً سوءاستفاده از آن برای مجرمان بین‌المللی نیز مصداق دارد. بر این اساس انتظار می‌رود تحقیقات کیفری در سایبر نیز به منظور دسترسی به حساب کاربری یا محتویات ایمیل و اسناد ذخیره‌شده در ابرایانش جریان داشته باشد. قوه مقننه در این مسیر به انطباق یا نوآوری قوانین با دستاوردهای جدید فناوری رسوخ کرده و در زندگی بشریت و سیستم عدالت کیفری به ایجاد رویه‌قضایی منطبق با آن می‌پردازد. اما تردیدی نیست که سرعت فناوری و چالش‌های ناشی از آن به‌مراتب از عملکرد این دو نهاد بیشتر است. یکی از این چالش‌ها، نحوه حمایت یا دسترسی به دیتای شخصی کاربران فضای مجازی است، درحالی‌که سرور ذخیره‌کنندهٔ آن در خارج از قلمرو سرزمینی متبوع است. دسترسی و جمع‌آوری دلایل الکترونیک از فضای مجازی با توسل به نرم‌افزارهای هک شبکه مجازی از قلمرو سرزمینی هر کشوری از مزیت‌های پیش روی دولت‌ها در کشف، تعقیب و مجازات جرایم فرامرزی سایبری است. اما این رویکرد، هم با عدم تمایل دولت دارندهٔ دیتاسنتر به مداخله و نفوذ سایر دولت‌ها به مرزهای الکترونیک وی و هم با ممنوعیت حقوق بین‌الملل کیفری مواجه است. این ممنوعیت، مبتنی بر اصول سرزمینی‌بودن صلاحیت کیفری و اعمال حاکمیت درون‌سرزمینی است. اگرچه فضای مجازی فاقد مرز فیزیکی است، دسترسی به منابع اطلاعاتی دولت‌های خارجی از طرق غیرمجاز در قلمرو

77. Taddese, Yamri, Focus: Cloud services create challenges for e-discovery, 2015, http://www.lawtimesnews.com/author/yamri-taddese/focus-cloud-services-create-challenge-for-e-discovery-12360.

سرزمینی، مداخله در امور حاکمیتی آن‌ها و موجد مسئولیت بین‌المللی دولت است.

با چنین پیش‌فرضی *مایکروسافت* با ذخیره اطلاعات ایمیل کاربران خویش در دیتاسنترهای مستقر در سرتاسر دنیا به افزایش کیفیت ارتباطات کمک کرده است. دیتاسنتر ایرلند را شرکت *مایکروسافت* اجاره کرده است و تحت کنترل عملیاتی وی است. درعین‌حال، اطلاعات ذخیره‌شده در فضای مجازی، قابل دسترسی برای شرکت سرویس‌دهنده در هر سرزمینی است اما این مسئله نافی نقض مقررات محل استقرار فیزیکی دیتاسنتر نیست. از این منظر، اطلاعات ذخیره‌شده در دیتاسنتر، خارج از قلمرو سرزمینی محل استقرار و فعالیت شرکت سرویس‌دهنده است. شرکت *مایکروسافت* تابع مقررات محل استقرار مرکز و فعالیت خویش است، اما خروج اطلاعات از دیتاسنتر قلمرو سرزمینی دیگر، تابع مقررات دولت حاکم آن (ایرلند) است. ایالات متحده با توسل به قوانین داخلی در صدد انجام تحقیقات کیفری درون‌سرزمینی برآمده است، اما دامنه این تحقیقات به فراسوی مرزهای آن کشیده شده است. بر این اساس، با ممنوعیت فراسرزمینی‌بودن قوانین کیفری داخلی و مداخله در امور حاکمیتی دولت ثالث مواجه شده است. عملکرد دادگاه داخلی ایالات متحده با صدور قرار الزام شرکت *مایکروسافت* بر افشای اطلاعات کاربری و دیتای ذخیره‌شدهٔ احد از کاربران به درخواست دادستان ولو به اتکای قوانین داخلی در واقع، مداخله در امور حاکمیتی ایرلند است، چرا که قانون ارتباطات ذخیره‌شده، مصوب و مجری در قلمرو ایالات متحده، نسبت به اطلاعات ذخیره‌شده در دیتاسنتر مستقر در قلمرو فراسرزمینی کاربرد ندارد، هرچند ایجاد صلاحیت فرامرزی برای دولت، مبنایی برای جمع‌آوری دلایل الکترونیک با اتکا به امکانات فنی غیرمجاز هک و فضای ابررایانش از درون سرزمین خویش بدون مداخله یا ورود فیزیکی به سرزمین دیگر باشد.

اگرچه در بادی امر به نظر می‌رسد که محل فعالیت شرکت سرویس‌دهنده، موجد صلاحیت برای دادگاه ایالات متحده در صدور مجوز دسترسی به اطلاعات ذخیره‌شده تحت کنترل و مدیریت شرکت *مایکروسافت* است، این صلاحیت بر اساس محل استقرار فیزیکی دیتاسنتر متفاوت می‌شود. اگر صلاحیت سرزمینی بر اساس محل فعالیت شرکت *مایکروسافت* در نظر گرفته شود، دولت حق الزام شرکت *مایکروسافت* به افشای اطلاعات کاربران را دارد، درحالی‌که قلمرو فیزیکی فعالیت این شرکت، سرزمین ایالات متحده است، مشروط به اینکه دیتاسنتر ذخیره‌کننده اطلاعات الکترونیک نیز درون‌سرزمینی باشد. دولت‌ها با اتکا به اصل صلاحیت، قدرت خود را بر تصویب و اجرای قوانین داخلی توجیه می‌کنند که قلمرو آن درون‌سرزمینی و بر اساس اصل اعمال حاکمیت است. اما در برخی موارد، بنا به اصول دیگر، ازجمله اصل صلاحیت شخصی، صلاحیت واقعی یا صلاحیت جهانی، دامنه این اعمال حاکمیت گسترده می‌شود که وجه اشتراک آن‌ها در شرط دسترسی به متهم یا دلایل مجرمانه وی در قلمرو سرزمینی یا استرداد

مجرم و تبادل اطلاعات مؤید اتهامات وی در پرتو همکاری‌های قضایی متقابل بین‌المللی با سایر دول است. اگر چنین شرایطی وجود نداشته باشد، امکان دسترسی به مجرم یا اطلاعات مجرمانه وی ممکن نیست، ولو اینکه دولت سرزمینی به تصور خود از طرق غیررسمی یا نفوذ غیرمجاز به فضاهای خصوصی مجازی، امکان دسترسی به آن را داشته باشد. اگرچه راهکار اخیر با توجیه حفظ امنیت ملی برای جلوگیری از هرزه‌نگاری‌های گسترده و سازمان‌یافته یا جاسوسی سایبری و موارد مشابه در حد رفع خطر و برچیده‌شدن دامنه آن منطقی است، تمام جرایم سایبری چنین ظرفیتی را ندارند. اما به نظر می‌رسد این وضعیت، چیزی غیر از توسل به دستگاه قضایی بر صدور قرار الزام شخص حقوقی به افشای اطلاعات کاربران خود از سرتاسر جهان است که در دیتاسنتر مستقر در قلمرو فراسرزمینی دادگاه صادرکننده قرار قضایی ذخیره شده است، بدون اینکه مشخص باشد کاربر مدنظر، از اتباع داخلی دولت متقاضی اطلاعات وی است.

از این حیث، عملکرد شعبه بدوی مصداق نفوذ به حریم خصوصی کاربران اینترنت شرکت *مایکروسافت* است. تقاضای دادستان و رسیدگی آن در دادگاه بخش ایالات متحده، فاقد مبنای صلاحیت سرزمینی در امور کیفری است چرا که محل نگهداری اطلاعات الکترونیکی، خارج از حوزه قضایی سرزمینی ایالات متحده است، درحالی‌که شخص حقوقی نسبت به اطلاعات ذخیره‌شدهٔ کاربران مالکیتی ندارد. *مایکروسافت* تنها عامل پشتیبان و ارائه‌کننده خدمات اینترنت به کاربران و متعهد به حفاظت و عدم افشای این اطلاعات از مرحله تولید، انتقال تا ذخیره در دیتاسنتر است. ایرلند، دولت محل استقرار دیتاسنتر شرکت *مایکروسافت*، عضو اتحادیه اروپاست. استانداردهای حمایت از حریم خصوصی در اتحادیه اروپا به‌مراتب سخت‌گیرانه‌تر از آن است که ایالات متحده بتواند با توسل به مقررات داخلی خویش، شرکت *مایکروسافت* را ملزم به افشای اطلاعات کاربران اینترنت از سرورهای ذخیره‌کننده ایرلند کند. اطلاعات حساب کاربری و محتویات ایمیل به‌طور فیزیکی در سرور شرکت *مایکروسافت* در صندوق امانات بانک خارجی ذخیره شده است و بدون تأیید دولت ایرلند، امکان استخراج از سرور وجود ندارد. ازاین‌رو ایالات متحده نمی‌تواند بدون طی‌کردن روند معمول همکاری‌های بین‌المللی از طریق معاهدات همکاری قضایی متقابل، به محتویات الکترونیک فراسرزمینی دسترسی پیدا کند. اگرچه این وضعیت از سرعت انجام تحقیقات کیفری می‌کاهد، همکاری‌های بین‌المللی کشورها در مبارزه با جرایم اینترنتی را تقویت می‌کند تا از طریق آن بر سرعت انجام تحقیقات کیفری جرایم بین‌المللی افزوده شود. بااین‌حال، همکاری‌های قضایی فرامرزی با چالش‌هایی در سطح ملی و بین‌المللی مواجه است. موفقیت در همکاری در سطح ملی منوط به توانایی و امکانات در اختیار دستگاه قضایی و نیروهای پلیس است. مشابهت‌داشتن جرم تحت تعقیب دولت متقاضی با سیاهه جرم‌انگاری‌های دولت سرزمینی در اکثر موارد مدنظر است. اگرچه در معاهدات بین‌المللی برخی از

جرایم به‌عنوان جرایم مشترک مدنظر دولت‌ها در همکاری‌های قضایی قرار می‌گیرند تا دولت‌های امضاکنندهٔ این معاهدات مکلف به قانونگذاری داخلی باشند، تفاوت در میزان مجازات از چالش‌های اصلی میان دولت متقاضی و دولت سرزمینی است. میزان اهمیت جرم، منوط به میزان مجازات آن است. در چنین شرایطی اجماع نظر میان دو دولت متقاضی و سرزمینی راجع به جرم تحت تعقیب، به اندازه‌ای اقناع‌کننده نیست که حس مشترک ضرورت تعقیب و مجازات عامل آن را به وجود آورد.

منابع:

الف. فارسی

ـ کتاب

- البوعلی، امیر؛ *صلاحیت محاکم در جرایم سایبری*، جنگل، ۱۳۹۲.
- عاملی، سعیدرضا؛ *رویکرد قضایی به آسیب‌ها، جرایم و قوانین و سیاست‌های فضای مجازی*، امیرکبیر، ۱۳۹۰.

ـ مقاله

- اردبیلی، محمدعلی و ندا میرفلاح نصیری؛ «اجرای کنوانسیون‌های بین‌المللی متضمن قاعده استرداد یا محاکمه در ایران»، *مجله حقوقی دادگستری*، سال ۸۱، شماره ۹۸، تابستان ۱۳۹۶.
- اسلامی، ابراهیم؛ «جایگاه حمایت از بزه‌دیدگان جرایم سایبری در مقررات کیفری حقوق داخلی و حقوق بین‌الملل»، *پژوهش‌نامه حقوق اسلامی*، سال ۱۷، شماره ۱، شماره پیاپی ۴۳، بهار_ تابستان ۱۳۹۵، ۱۳۹۵.
- افتخارجهرمی، گودرز و ابراهیم اسلامی؛ «نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرایم فضای مجازی»، دوره ۷۸، *مجله حقوقی دادگستری*، شماره ۸۸، زمستان ۱۳۹۳.
- افراسیابی، محمد اسماعیل و فهیم مصطفی‌زاده؛ «بررسی رویکرد ابزارگرا به حقوق کیفری ایران در پرتو قانون اساسی»، دوره ۱۹، *فصلنامه دیدگاه‌های حقوقی*، شماره ۶۸، زمستان ۱۳۹۳.
- افضلی، رسول؛ محمدباقر قالیباف و میثم احمدی فیروزجائی؛ «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی»، *پژوهش‌های جغرافیای انسانی*، دوره ۴۵، شماره ۱، بهار ۱۳۹۲.
- پاکزاد، بتول و محمدحسین آزادی‌خواه؛ «مبانی جرم‌انگاری ارسال پیام‌های الکترونیکی ناخواسته»، *مطالعات حقوق کیفری و جرم‌شناسی*، دوره ۳، شماره ۲، پاییز_ زمستان ۱۳۹۵.
- پورقهرمانی، بابک؛ «مطالعه تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست»، *پژوهشنامه حقوق کیفری*، شماره ۱۵، بهار_ تابستان ۱۳۹۶.
- ترابی، کریم و حمید محمدی؛ «بررسی چگونگی پیشگیری کیفری و اجتماعی از جرائم الکترونیکی با تأکید بر نقش نیروی انتظامی و تجارت الکترونیک»، *فصلنامه کارآگاه*، شماره ۳۴، بهار ۱۳۹۵.
- تقوی‌فرد، محمدتقی، محمدرضا تقوا، مهدی فقیهی و محمدجواد جمشیدی؛ «مقایسه تطبیقی قوانین حمایت از حریم خصوصی اطلاعاتی در ایران و کشورهای منتخب»، *مجلس و راهبرد*،

سال ۲۴، شماره ۸۹، بهار ۱۳۹۶.

- جعفری، فریدون، رؤیا موسوی و امیر اسلامیه همدانی؛ «مطالعه تطبیقی حق برخورداری از وکیل در مرحله تعقیب در حقوق داخلی ایران و اسناد و رویه‌های محاکم کیفری بین‌المللی»، *پژوهش‌های حقوق تطبیقی*، دوره ۲۰، شماره ۴، زمستان ۱۳۹۵.
- جوان جعفری، عبدالرضا؛ «جرایم سایبر و رویکرد افتراقی حقوق کیفری»، *مجله دانش و توسعه*، شماره ۳۴، زمستان ۱۳۸۹.
- جهانشیری، جواد؛ محمدرضا حسینی و احمد ابراهیمی؛ «تبیین فرآیند تحقیقات مقدماتی در جرایم سایبری»، *فصلنامه پژوهش‌های اطلاعاتی و جنایی*، شماره۳، پاییز ۱۳۹۴.
- حبیب‌زاده، محمدجعفر و سلمان عمرانی؛ «تحلیل ساختاری رابطه حقوق کیفری و دانش سیاسی»، *فصلنامه مطالعات حقوقی دولت اسلامی*، شماره ۲، بهار ۱۳۹۲.
- رحمانیان، حامد و محمدجعفر حبیب‌زاده؛ «ابزارگرایی کیفری؛ قلمرو، مفهوم، شاخص‌ها»، *پژوهش حقوق کیفری*، شماره ۵، زمستان ۱۳۹۲.
- خان‌محمدی، کریم و علی اکبر شامی؛ «اخلاق اسلامی حریم خصوصی در شبکه‌های اجتماعی سایبر (با تأکید بر واتس‌آپ)»، *اسلام و مطالعات اجتماعی*، دوره ۴، شماره ۲، پیاپی ۱۴، پاییز ۱۳۹۵.
- رضایی، سعید؛ محمدعلی دوستاری و مجید بیات؛ «مروری بر کنترل دسترسی مبتنی بر ویژگی در محیط‌های ابری، فصلنامه منادی امنیت فضای تولید و تبادل اطلاعات»، جلد ۹، شماره ۱، ۱۳۹۵.
- درگاهی، مهدی؛ «میان‌کنش قاعده حفظ نظام و حریم خصوصی افراد»، *پژوهش‌های حفاظتی ـ امنیتی*، سال ۵، شماره ۱۹، ۱۳۹۵.
- شهبازی‌نیا، مرتضی و محبوبه عبداللهی؛ «دلیل الکترونیک در نظام ادله اثبات دعوا»، *فصلنامه حقوق، مجله دانشکده حقوق و علوم سیاسی*، دوره ۴۰، شماره ۴، زمستان ۱۳۸۹.
- صالحی، جواد؛ «مؤلفه‌های امنیت اجتماعی در قوانین کیفری»، *مجله پژوهش‌های حقوقی*، شماره ۱۷، تابستان ۱۳۸۹.
- ـــــــــــ؛ «استفاده غیرمجاز پلیس از دستگاه ردیاب؛ جلوه‌ای از نقض حریم خصوصی در رویه‌قضایی دیوان عالی ایالات متحده و دستاوردهای آن»، *فصلنامه پژوهش حقوق کیفری دانشگاه علامه طباطبایی*، شماره ۸، پاییز ۱۳۹۳.
- ـــــــــــ؛ «ممنوعیت بازرسی تلفن همراه و بایسته‌های آن؛ جلوه‌ای از حریم خصوصی متهم در رویه‌قضایی و دستاوردهای آن»، *فصلنامه پژوهش حقوق کیفری دانشگاه علامه*

طباطبایی، شماره ۲۱، زمستان ۱۳۹۶.

- صدیق، میرابراهیم؛ «انقلاب سایبری و تحول در پدیده جاسوسی»، *فصلنامه مطالعات راهبردی*، سال ۱۹، شماره ۱، پیاپی شماره ۷۱، بهار ۱۳۹۵.
- ضیایی، یاسر؛ «مبانی نظری صلاحیت فراسرزمینی دولت از منظر حقوق بین‌الملل عمومی»، *مجله حقوقی دادگستری*، شماره ۷۶، زمستان ۱۳۹۰.
- ضیایی، یاسر و احسان شکیب‌زاده؛ «قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران»، *مجله حقوقی بین‌المللی*، دوره ۳۴، شماره ۵۷، پاییز_ زمستان ۱۳۹۶.
- طهماسبی، جواد؛ «اصل صلاحیت شخصی مبتنی بر تابعیت بزه‌دیده در قوانین کیفری ایران»، *مجله حقوقی دادگستری*، شماره ۹۷، بهار ۱۳۹۶.
- علی‌اکبریان، حسنعلی؛ «بررسی حکم شرعی رفتار حکومت در جمع‌آوری اطلاعات از حوزه حریم خصوصی اشخاص»، *فصلنامه کاوشی نو در فقه*، سال ۲۱، شماره ۳، پاییز ۱۳۹۳.
- فرجیها، محمد و امین آقایی؛ «جنبه‌های منفی و مثبت اصل صلاحیت شخصی در حقوق جزای بین‌الملل»، *فصلنامه مطالعات بین‌المللی پلیس*، شماره ۹، بهار ۱۳۹۱.
- فروغی، فضل‌الله و امیر البوعلی؛ «صلاحیت کیفری مراجع قضایی در فضای سایبر»، *مجله تحقیقات حقوقی*، شماره ۵۸، تابستان ۱۳۹۱.
- فرهادی آلاشتی، زهرا و عبدالرضا جوان جعفری بجنوردی؛ «بررسی تعارض رهیافت‌های تدابیر موقعیت مدار نظارت سایبری، با حریم خصوصی کاربران»، *فصلنامه مجلس و راهبرد*، سال ۲۳، شماره ۸۷، پاییز ۱۳۹۵.
- لک، بهزاد؛ «شناسایی و پیشگیری از کمین سایبری در فضای مجازی»، *فصلنامه کارآگاه*، شماره ۱۸، بهار ۱۳۹۱.
- محمدی، زینب و نیما جعفری نویمی‌پور؛ «خدمات ابری معتبر و نامعتبر؛ بررسی روش‌های موجود و ارائه راهکارهای جدید»، *فصلنامه منادی امنیت فضای تولید و تبادل اطلاعات*، جلد ۹، شماره ۱، ۱۳۹۵.
- مسعودیان، محسن؛ «نقش پلیس در پیشگیری از جرایم سایبری و تأمین امنیت در فضای مجازی»، *فصلنامه انتظام اجتماعی*، دوره ۴، شماره ۱، بهار ۱۳۹۱.
- ملکان، اسفندیار و رسول سلمانی؛ «ویروس‌های رایانهی تهدیدی برای امنیت سیستم اطلاعات حسابداری»، *پژوهش حسابداری*، شماره ۷، زمستان ۱۳۹۱.
- مهرا، نسرین و کامران محمودیان اصفهانی؛ «الزامات حقوق بشری کشف جرم در نظام حقوقی ایران»، *مطالعات حقوق عمومی*، دوره ۴۷، شماره ۲، تابستان ۱۳۹۶.

- میرمحمدصادقی، حسین و افشین آذری متین؛ «راهبرداهای کیفری در بانکداری نوین؛ با تأکید بر امضای الکترونیکی»، *فصلنامه راهبرد*، شماره ۸۲، بهار ۱۳۹۶.
- نوبهار، رحیم و فاطمه صفاری؛ «رعایت مصالح بزه‌دیده در جرم‌انگاری»، *مجله حقوقی دادگستری*، سال ۸۰، شماره ۹۳، بهار ۱۳۹۵.
- وروایی، اکبر و محمد رضوی؛ «بررسی وضعیت حقوقی استرداد مجرمین در قلمرو حقوق کیفری بین‌المللی»، *فصلنامه دانشکده علوم و فنون مرز*، شماره ۲، تابستان ۱۳۹۴.

ب. انگلیسی

- Books

- Nunziato, Dawn, *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age*, Stanford University Press, 2009.
- Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

- Articles

- Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad? *Center for Democracy and Technology*, 2014.
- Colangelo, Anthony J., "Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law", *Harvard International Law Journal*, No. 48. 2007.
- Daskal, Jennifer & Andrew K. Woods, Cross-Border Data Requests: A Proposed Framework , *Just Security*, 2015.
- Hooper, Christopher, Martini, Ben & Choo, Kim Kwang Raymond, Cloud Computing and its Implications for Cybercrime Investigations , *Australia' Computer Law and Security Report*, vol. 29, No. 2. 2013.
- Ireland-Piper, Danielle, "Extraterritoriality and Sexual Offences Outside Australia , *Bond Law Review*, No. 22(2). 2010.
- Kerr, Orin, What Legal Protections Apply to E-mail Stored Outside the U.S.? Volokh Conspiracy *Washington Post*, 2014.
- Koba, Mark, Cloud Computing 101: Learning the Basics , 2011.
- Lawson, Rick, The Concept of Jurisdiction and Extraterritorial Acts of State , in Gerard Kreijen et al (eds), *State, Sovereignty, and International Governance*, Oxford University Press. 2002.
- Lowe, Vaughan, Jurisdiction in Malcolm Evans (ed), *International Law*, Oxford University Press, 2nd ed. 2003.
- Martini, Ben and Kim-Kwang Raymond Choo, An Integrated Conceptual Digital Forensic Framework for Cloud Computing *Digital*

Investigation, vol. 9, No. 2. 2012.
- Narayanan, Vineeth, Harnessing the Cloud: International Law Implications of Cloud-Computing ,*Chicago Journal of International Law*, No. 12. 2012.
- Orentlicher, Diane F., "Whose Justice? Reconciling Universal Jurisdiction with Democratic Principles" in Thomas J. Biersteker et al (eds), *International Law and International Relations*, Routledge. 2007.
- Perrin, Benjamin, Taking a Vacation from the Law? Extraterritorial Criminal Jurisdiction and Section 7(4.1) of the Criminal Code , *Canadian Criminal Law Review*, No. 13. 2009.
- Richardson, L. Song, Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem , *Berkeley Journal of International Law*, No. 26. 2008.
- Roberts, Paul, In Wake of Snowden, U.S. Cloud Providers Face Calls to Wall off Data , 2014.
- Taddese, Yamri, Focus: Cloud Services Create Challenges for E-Discovery, 2015.
- Urbas, Gregor, Cybercrime, Jurisdiction and Extradition: the Extended Reach of Cross-Border Law Enforcement ,*Journal of Internet Law*, No. 16. 2012.
- Weber, Alamie M., The Council of Europe`s Convention on Cybercrime , *Barkeley Technology Law Journal*, No. 18. 2014.
- Wilson, Mark, Twitter Moves Non-US Accounts to Ireland, and Away from the NSA , 2015.
- Zerk, Jennifer A., Extraterritorial Jurisdiction: Lessons for the Business and Human Rights Sphere from Six Regulatory Areas ,Working Paper, No 59, *Harvard Corporate Social Responsibility Initiative*. 2010.

- International Jurisprudence and Instruments

- Council of Europe, Cybercrime Convention Committee (T-CY), Trans-Border Access to Data and Jurisdiction: Options for Further Action by the T-CY, Doc. No. T-CY, 2014.
- International Court of Justice, *United Kingdom of Great Britain and Northern Ireland v. Albania, Corfu Channel Case*, ICJ Reports, http://www.icj-cij.org/en/case/1. 1949.
- *Microsoft Corp. v. United States*, Albrecht brief, amici in the case, Electronic Frontier Foundation, Available at: https://www.eff.org/ cases/re-warrant-microsoft-email-stored-dublin-ireland. 2014.
- *Microsoft Corp. v. United States*, Colangelo brief, Amici in the Case, Electronic Frontier Foundation, Available at: https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland. 2014.
- *Microsoft Corp. v. United States*, In the Matter of a Warrant to Search a

Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, Case No. 14-2985-cv, Available at: http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html.2014.

- *Microsoft Corp. v. United States*, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained, No. 829 F.3d. 2016.
- *Microsoft Corporation v. United States*, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, No. 14-2985, 2017 WL 362765, Available at: http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2017-01-24.html.
- *United States v. Microsoft Corp*, Brief of Government in Support of the Magistrate Judge s Decision to Uphold a Warrant at 12, In the Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 15 F. Supp. 3d 466. 2014.
- *United States v. Microsoft Corp*., In the Matter of a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 15 F. Supp. 3d, Available at: https://www.casemine.com/judgement/us/5914fab5add7b049349a9a00. 2014.