نحوه اعمال صلاحیت دادگاه‌ها در رسیدگی به جرایم فضای مجازی

گودرز افتخارجهرمی*

ابراهیم اسلامی*

چکیده:

با پیشرفت فناوری اطلاعات و ارتباطات، تحولاتی اساسی در زیست انسانی صورت گرفته است. آن دسته از رفتارهای انسانی که به شکل سنتی جرم تلقی می‌شد، امروز به شکل ترجمهٔ ایده‌های مجرمانه به زبان خاص رایانه و یا از طریق فضای مجازی تحقق می‌یابد. به این ترتیب، فضای جدیدی به نام فضای سایبر ایجاد شده است که در آن مرز و محدوده به شکل سنتی معنی ندارد. یکی از مهم‌ترین پرسشها در این قلمرو آن است که در هنگام ارتکاب یک جرم سایبری صلاحیت محکمه رسیدگی‌کننده را با استناد به کدام یک از اصول حقوقی آیین دادرسی می‌توان شناخت. اقدامات مجرمانه در این فضا اصول و قواعد صلاحیتی سنتی را به چالش کشیده است. پرسش اصلی این مقاله آن است که در صورت وقوع یک جرم سایبری چگونه و تا چه حد دادگاه‌های یک کشور می‌توانند اعمال صلاحیت نمایند. همچنین در صورتی که میان صلاحیت‌های متفاوت نسبت به یک جرم سایبری تعارض حاصل شود، برای رفع آن بر اساس کدام یک از اصول حاکم بر صلاحیت دادگاه‌ها باید عمل کرد. پاسخ به این پرسش‌ها نیازمند موشکافی دقیق موازین بین‌المللی ناظر بر صلاحیت محاکم و رویه بین‌المللی کشورهای پیشرو در زمینه مبارزه با جرایم سایبری است که در این مقاله به بازخوانی این مقررات

* استاد دانشکده حقوق دانشگاه شهید بهشتی G_Eftekhar@sbu.ac.ir

* دانشجوی دکتری حقوق بین الملل دانشگاه شهید بهشتی، عضو هیأت علمی دانشگاه آزاد رودهن و دادرس دادگاه‌های تجدیدنظر استان تهران (کیفری استان) (نویسنده مسئول)
eeslami56@yahoo.com

و مطالعه این دست رویه‌ها و در پایان به ارایه راه‌حل پیشنهادی در حل تعارض صلاحیت‌های دادگاه‌ها پرداخته خواهد شد.

واژگان کلیدی: جرم سایبری، صلاحیت، عنصر خارجی، دادگاه صالح، تعارض صلاحیت.

مقدمه

با پیشرفت فناوری اطلاعات و ارتباطات، تحولاتی اساسی در زیست انسانی صورت گرفته است. آن دسته از رفتارهای انسانی که به شکل سنتی جرم تلقی می شد، امروز به شکل ترجمه ایده‌های مجرمانه به زبان خاص رایانه و یا از طریق فضای سایبری تحقق می‌یابد. به این ترتیب، فضای جدیدی به نام فضای سایبر[1] ایجاد شده است که در آن مرز و محدوده به شکل سنتی معنی ندارد. چه بسا جرایمی در هزاران کیلومتر دورتر از محل اقامت قربانیان علیه ایشان طراحی و اجرا می‌شود یا آنکه ابزارهای عادی زندگی روزمره وسیله اقدامات مجرمانه علیه اشخاص قرار می‌گیرد. بررسی مسأله چگونگی و مبنای اعمال صلاحیت محاکم بر جرایم سایبری و نیز تعارض در صلاحیت محاکم از اهمیت بسزایی برخوردار است. در این مقاله امکان حل چنین تعارضی با اتکاء به اصول سنتی حل تعارض یا شکل گیری اصول نوین بر پایهٔ موازین بین‌المللی مورد ارزیابی قرار خواهد گرفت.

جامعه بین‌المللی هموار تلاش کرده است تا به‌واسطه انعقاد معاهدات دو یا چند جانبه زمینه همکاری در رسیدگی به جرایم سایبری را فراهم نماید. بنابراین می‌توان گفت که نظام کنونی حاکم بر جرایم سایبری تا حدود زیادی متکی بر همکاری بین-المللی است. با وجود این، این انتقاد نیز مطرح شده است که «یک نظام حقوقی کارآمد جهت رسیدگی به جرایم سایبری نباید تا بدین حد متکی به همکاری باشد. زیرا همیشه تضمین وجود ندارد که فارغ از اعمال قدرت قاهره قضایی، تعقیب و رسیدگی فرامرزی به جرایم سایبری مفید اثری واقعی باشد».[2] از این رو، این پرسش اساسی قابل طرح است که یک کشور تا چه حد می‌تواند مدعی اعمال صلاحیت بر جرایم سایبری باشد؟

برخی از جرایم وجود دارند که از نگاه یک دولت در قلمروی حاکمیت آن دولت اتفاق افتاده‌اند در حالی که بخشی از عناصر مادی این جرایم عملاً در کشور دیگری ارتکاب یافته است. از این رو، دست‌کم ممکن است دو دولت مدعی اعمال صلاحیت

[1]. فضای سایبر یا فضای مجازی یا فضای رایانه‌ای عبارت از مجموعه محیط‌هایی، همچون اینترنت است که اشخاص در آنها بدون حضور فیزیکی در کنار یک دیگر، از طریق رایانه‌ها یا دیگر وسایل ارتباطی، ارتباط برقرار می‌کنند. در خصوص مفهوم فضای سایبر؛ بنگرید به:
هیأت مولفان و ویراستاران مایکروسافت، فرهنگ تشریحی کاربران کامپیوتر انتشارات مایکروسافت، ترجمه فرهاد قلی‌زاده نوری، تهران، نشر علوم روز، ۱۳۸۰، ص. ۸۶.

[2]. Bert-Japp Koops, and Susan Brenner, Cybercrime and Jurisdiction: A Global Survey, T.M.C. Asser Press, 2006, p. 2.

باشند. بر این اساس، پرسش اصلی مقاله حاضر آن است که اگر جرمی سایبری به صورت کلی یا جزئی در قلمرو کشوری دیگر ارتکاب یافته باشد، محدودیت‌های مربوط به ادعای اعمال صلاحیت محاکم کدامند و کدام اصول در تعیین و تشخیص صلاحیت و نیز حل تعارض صلاحیت‌ها قابل اعمال است؟

در این مقاله، پس از بررسی کلیات صلاحیت محاکم در جرایم سایبری و مفهوم جرم سایبری با استفاده از روش توصیفی-تحلیلی، به بررسی قابلیت اعمال اصول صلاحیت به طور سنتی در مورد جرایم سایبری پرداخته خواهد شد. در نهایت بحث تعارض‌های صلاحیتی نیز مورد بررسی قرار می گیرد.

۱. چیستی و چگونگی صلاحیت محاکم در جرایم سایبری

هیأت عمومی دیوان عالی کشور در تاریخ ۱۳۹۱/۱۲/۱ با صدور رأی وحدت رویه شماره ۷۲۹ اعلام داشت: «نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز مستفاده از ماده ۲۹ مورد تأیید قانون‌گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه، هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضایی مختلف صورت گرفته باشد، دادگاهی که بانک افتتاح‌کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشته شده در حوزه آن قرار دارد، صالح به رسیدگی است». همانطور که ملاحظه می‌شود تعیین صلاحیت محکمه در پرونده‌هایی که هر دو طرف دعوی در یک کشور هستند، در رویه قضایی کشور ما نیز ایجاد اختلاف نظر کرده است و به طریق اولی هنگامی که یک عنصر خارجی در معادله حقوقی وارد می‌شود حل مسأله دادگاه صالح به مراتب پیچیده‌تر می‌شود. در رویه محاکم سایر کشورها، به ویژه کشورهایی که طلایه‌دار تکنولوژی فناوری ارتباطات هستند نیز همین موضوع به صورتی بسیار پیچیده‌تر مطرح شده است. جهت ورود به اصل موضوع دو نمونه از رویه دولت‌ها را مورد بررسی قرار خواهیم داد. در پرونده «*الکسی ایوانوف* و *وسیلی گورشکوف*»[1]، دو هکر تبعه روسیه، از چند شرکت آمریکایی اخاذی کرده بودند. این پرونده نمونه بارزی است که ضرورت بحث پیرامون تعیین دادگاه صالح و اعمال صلاحیت بر جرایم سایبری را روشن می‌کند. در این پرونده، پلیس فدرال آمریکا جهت تأمین دلیل و دستگیری مظنونین از شیوه بدیعی استفاده کرد که پیش از این در سایر کشورها مورد استفاده قرار نگرفته بود. مأموران امریکایی خود را به عنوان تاجر به هکرها معرفی کرده و آنها را

1. Alexey Ivanov and Vasiliy Gorshkov

به بهانه انجام مصاحبه در خصوص کار در یک شرکت امنیت شبکه به شهر سیاتل[1] دعوت کردند. سپس در محل مصاحبه از آنها خواسته شد تا مهارت خود در مقابله با حملات جاسوسی به سیستم‌های رایانه‌ای به نمایش بگذارند. این امر مستلزم استفاده هکرها از رمز ورود به رایانه‌های شخصی شان بود. با تدابیر فنی که از قبل پیش‌بینی شده بود، رمز ورود آنها به دست آمد. با به دست آمدن رمز ورود، مأمورین فدرال از طریق شبکه اینترنت وارد رایانه شخصی این دو متهم شده و جهت تأمین دلیل و ایراد اتهام علیه آنها نسخه‌ای از اطلاعات موجود در رایانه‌ایشان را تهیه نمودند.[2] متعاقب پیگیری مقامات قضایی و طرح پرونده علیه آنها و ایراد اتهام، دادگاه هر دو متهم را به دلیل نقض قوانین داخلی روسیه مجرم شناخت. در واکنش به این اقدام ایالات متحده، مقامات دولت روسیه مدعی شدند که اول- مدارک و ادله اثبات جرم به صورت غیرقانونی تحصیل شده و دوم و مهم‌تر اینکه، مقامات قضایی آمریکایی با چنین اقدامی در واقع مرزهای صلاحیتی را نادیده گرفته‌اند. افزون بر این، مقامات روس با طرح اتهام هک علیه مأمورین آمریکایی نیز مخالفت خود را با اقدام آنان ابراز کردند که این امر نیز به نوبه خود مسأله اعمال صلاحیت و رسیدگی به این موضوع را به میان آورد.[3] این پرونده به خوبی نشان می‌دهد که نه تنها پدیده مرز در مفهوم سنتی کمرنگ شده است بلکه نظریه‌های سنتی صلاحیت و اصول حاکم بر آن نیز تا حدودی به چالش کشیده شده است. بنابراین، باید دید مبانی صلاحیتی رسیدگی به جرایم سایبری و اصول حاکم بر آن چیست. از این گذشته، با اعمال نظریه‌ها و نیز اصول سنتی صلاحیت بر جرایم سایبری فرامرزی، امکان دارد که اختیار اعمال صلاحیت توسط کشوری که به واقع مستحق و ذینفع اعمال صلاحیت است، سلب شود و در مقابل، کشور دیگری با اتکاء به مبانی غیرواقعی اعمال صلاحیت کند.

در رویه بین‌المللی کشورها پرونده مشهور دیگری نیز قابل ذکر است. پرونده شرکت ارائه خدمات اینترنتی «کامپیوسرو»[4] از نمونه هایی است که اختلاف صلاحیت محاکم در آن به خوبی مشاهده می‌شود.[5] در این پرونده نماینده دادستان شهر مونیخ

1. Seattle
2. Jody Westby, International Guide to Combating Cybercrime, American Bar Association Publishing, 2003, p. 115.
3. Koops and Brenner, Op. cit., pp.322-323.
4. Compu Serve
۵. شرکت کامپیوسرو در شهر کلمبوس، در ایالت اوهایو آمریکا، قرار دارد و تأمین‌کننده خدمات اینترنتی است. این شرکت نخستین شرکتی بود که خدمات تجاری اینترنتی را در ایالات متحده آمریکا ارایه می‌کرد.

اتهاماتی را علیه «*فلیکس سام*»[1]، مدیر اجرایی این شرکت طرح کرد در حالی که هم متهم و هم شرکت تبعه ایالات متحده بودند. این شرکت متهم به انتشار پورونوگرافی کودکان و مطالبی در زمینه بنیادگرایی بود. دادستان مدعی بود که این شرکت باید دسترسی به چنین مطالبی را مسدود می‌کرد. لیکن محتوای تارنما لزوماً از سوی خود شرکت در صفحات قرار نمی‌گرفت بلکه کاربران نیز می‌توآن استند مطالبی را در این صفحات بارگذاری کنند. دادگاه بدوی *فلیکس سام* را مجرم تشخیص داده و وی را به دوسال حبس تعلیقی محکوم کرد. لیکن با درخواست تجدیدنظر و پس از یک سال، تبرئه شد.[2]

در این پرونده، رسیدگی به اتهام مدیر یک شرکت اینترنتی آمریکایی در آلمان در واقع این رویه را ایجاد کرد که امکان اعمال صلاحیت کیفری محاکم یک کشور بر اتباع کشور دیگر بر اساس مبانی غیرواقعی صلاحیت وجود دارد. مسلم است آثار چنین رویه‌ای خطرناک است زیرا تأمین‌کنندگان خدمات اینترنتی و حتی کاربران آنها را در قبال اعمالی که در یک حوزه حاکمیتی و تحت شمول قوانین یک کشور ارتکاب یافته، با خطر محاکمه در دادگاه‌های تمامی کشورهای جهان مواجه می‌شوند.

این دو رویه قضایی از جانب پرچمداران تکنولوژی ارتباطات یعنی ایالات متحده و آلمان، مؤید آن است که اتکاء به اصول سنتی حاکم بر اعمال صلاحیت در تشخیص دادگاه صالح تردید ایجاد کرده است و حتی به احتمال زیاد موجب تضییع حقوق متهم می‌شود. لیکن باید توجه داشت که عدم تبعیت از چنین اصولی نیز مشکلات خاص خود را دارد. از جمله تأثیر بر روابط بین‌المللی دولت‌ها به دلیل عدم تبعیت از اصول سنتی اعمال صلاحیت بر جرایم فرامرزی. دو اصل کلاسیک حقوق بین‌الملل که در این ارتباط مطرح می‌شود اصل برابری حاکمیت دولت‌ها و اصل استقلال حاکمیت در حقوق بین‌الملل است. یکی از مهم‌ترین تجلی‌های این دو اصل، استقلال قضایی و صلاحیت تشخیص اعمال صلاحیت قضایی توسط محاکم ملی کشورهاست. از دیگر سو به سبب ذات جرایم سایبری و ماهیت فراملی آنها اختلاف در تشخیص صلاحیت می‌تواند به روابط بین‌المللی دولت‌ها خدشه وارد سازد. از دیگر سو، برخی جرایم سایبری از حد جرایم داخلی با ماهیت فراملی فراتر رفته و با خدشه به نظم عمومی بین‌المللی فی‌نفسه جنایتی بین‌المللی را شکل می‌دهند. پدیده اخیر را می‌توان در تروریسم سایبری به

1. Felix Somm
2. Akdeniz, Yaman, Internet Child Pornography and the Law: National and International Responses, Ashgate, 2008, pp. 229-231.

روشنی ملاحظه کرد. تروریسم سایبری با تهدید حاکمیت کشور یا تعدادی کشورها، صلح و امنیت بین‌المللی را تهدید کرده و مقابله با آن نیازمند همکاری و تعامل جهانی است. از این رو لازم است انواع صلاحیت و مبانی اعمال صلاحیت ملی و بین‌المللی در جرایم سایبری را با دقتی دو چندان مورد مداقه و بررسی قرار داد.

۱-۱. مفهوم صلاحیت دادگاه‌ها و سیر تکامل آن

نقطه شروع اعمال صلاحیت قضایی و به ویژه اعمال صلاحیت کیفری بر جرایم فرامرزی «اصل برابری حاکمیت دولت‌ها» است که در موازین بین‌المللی تأکید فراوانی بر آن شده است. همانطور که گفته شد، این اصل قدیمی‌ترین و بنیادی‌ترین اصل حقوق بین‌الملل است که سابقه آن به لحاظ تاریخی به ابتدایی‌ترین دوره روابط میان جوامع سازمان‌یافته در تاریخ باز می گردد. به لحاظ سنتی، حضور فیزیکی مأموران یک کشور در سرزمین کشور دیگر، به جهت انجام عملیات در سرزمین کشور اخیر ممنوع است. رأی صادره از دیوان بین‌المللی دادگستری در پرونده کانال کورفو (۱۹۴۹) که بیان کننده قواعد ناشی از عرف بین‌المللی است، مؤید این ادعاست. دیوان در رأی خود، ورود کشتی‌های جنگی دولت انگلستان به سرزمین آلبانی به منظور بازرسی و پاک‌سازی کانال کورفو از مین‌های دریایی را مصداقی از مداخله قلمداد کرد و آن را مجاز ندانست.[1] بنابراین، دولت‌ها نباید «به هیچ شکل یا دلیلی در امور داخلی و خارجی دولت‌های دیگر مداخله نمایند،»[2] حتی اگر خسارتی هم در بر نداشته باشد. در این پرونده اساساً خسارتی به دولت آلبانی وارد نشده بود لیکن دیوان استدلال کرد که دولت انگلستان با این اقدام، حاکمیت دولت آلبانی را نقض کرده است.

از دیرباز، واژه «صلاحیت» دربرگیرنده سه اختیار اصلی حاکمیتی در هر کشور بوده و در این سه معنی استعمال شده است. این سه اختیار عبارتند از: صلاحیت قانون‌گذاری، صلاحیت قضایی و صلاحیت اجرای قهری قوانین و احکام قضایی. صلاحیت قانون‌گذاری به اختیار کشور در وضع قوانین و مقررات در خصوص فعل یا ترک فعل، وضعیت یا روابط اشخاص، اعمال اداری، مقررات اداری یا احکام دادگاه‌ها

1 . Corfu Channel Case, ICJ Reports, 1949, pp. 34-35.

۲. همچنین بنگرید به:

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965; See also the Military and Paramilitary Activities in and against Nicaragua case, ICJ Reports 1986, p. 202.

اشاره دارد. در حقیقت می‌توان آن را «حق هر کشور نسبت به وضع قانون»[1] توصیف کرد که بر رفتارها، روابط و وضعیت یا منافع اشخاص نسبت به اشیاء قابل اعمال است. صلاحیت قضایی عبارت است از اختیار کشور بر این که «اشخاص حقیقی و حقوقی را تابع فرایند دادگاه‌ها یا محاکم اداری خود کند.»[2] به این ترتیب دولت می‌تواند اشخاص را تحت تعقیب قرار داده یا آنان را محاکمه نماید. صلاحیت اجرای قهری قوانین عبارت است از اختیار کشورها برای تشویق یا اجبار به اجرای قوانین و مقررات و یا مجازات اشخاص در صورت عدم اجرای قوانین یا مقررات، خواه از طریق دادگاه‌ها یا به وسیله اقدامات اجرایی، اداری، انتظامی یا هرگونه اقدام غیرقضایی.[3] موضوعات مرتبط با اجرای قهری قانون و عدالت کیفری در چارچوب این بعد از اختیارات انحصاری دولت قرار می‌گیرند. از نظر سنتی، بنا بر اصل صلاحیت سرزمینی کشورها، صلاحیت کیفری همواره با قلمرو جغرافیایی گره خورده است. بنابراین، کشورها مکلف‌اند از اعمال قهری قوانین و مقررات خود در سایر کشورها خودداری نمایند.[4] به موجب اصول مسلم و مستقر حقوق بین‌الملل از جمله برابری حاکمیت کشورها و استقلال حاکمیت هیچ کشوری مجاز نیست در قلمرو کشور دیگر مبادرت به اقداماتی از جمله دستگیری افراد، ابلاغ احضاریه، تحقیقات پلیسی یا وصول مالیات کند مگر با رضایت دولتی که این اعمال در سرزمین آن انجام می‌شود.[5] موضوع اعمال فراسرزمینی قوانین و مقررات توسط ایالات متحده همواره مورد اعتراض کشورها به ویژه کشورهای اروپایی بوده است.

می‌توان گفت که بدون اعمال صلاحیت قضایی یا اجرای قهری قوانین، صلاحیت قانون‌گذاری یا تجویزی کمابیش یک مفهوم نظری و بلااثر در عرصه اجتماعی است و از سوی دیگر، بدون اعمال صلاحیت قانون‌گذاری، اعمال صلاحیت‌های دیگر امکان‌پذیر

1. Boleslaw Boczek, International Law: A Dictionary, Scarecrow Press, 2005, p.77.
2. Cedric Ryngaert, Jurisdiction in International Law, Oxford University Press, 2008, p.10.
3. Uta Kohl, Jurisdiction and the Internet: Regulatory Competence over Online Activity, Cambridge University Press, 2007, p.18.
۴. حتی برای مثال، در جایی که اتباع یک دولت در خارج از قلمرو آن محاکمه می‌شوند، اصل بنیادین این است که این کشور نمی‌تواند در رسیدگی‌های قضایی کشور حاکم دیگر به نیابت از تبعه خود مداخله نماید. همین طور، کشورها نمی‌توانند در قلمرو کشور دیگر از طریق اجرای قهری قوانین ملی خود بدون رضایت این دولت اقدامی را انجام دهند. بنگرید به:
Antonio Cassese, International Law, Oxford University Press, 2005, p. 53.
5. Ian Brownlie, Principles of Public International Law, Oxford University Press, 6th ed., 2003, p.306.

نیست. با وجود این باید یادآور شد که، ادعای مشروع تجویز صلاحیت محاکم نمی‌تواند دلیل کافی برای اعمال صلاحیت قضایی یا اجرای قهری قوانین و مقررات باشد. در طول تاریخ حقوق بین‌الملل، هر سه چهره صلاحیت عمدتاً مبتنی بر مرزهای سرزمینی بوده است. به عبارت دیگر، کشورها قوانینی را وضع می‌کردند که حوزه شمول جغرافیایی آن قواعد محدود به اعمالی می‌شد که در قلمرو سرزمین تحت حاکمیت‌شان رخ داده است یا اعمالی که به نحوی از انحاء به سرزمین یک کشور تسری پیدا می‌کرد. بنابراین، کشورها نمی‌توانند قوانین کیفری خود را نسبت به بزهی اعمال نمایند که خارج از قلمرو سرزمینی آنها رخ داده است.[1] ریشه‌های چنین رویکردی را می‌توان در گذشته‌های دور جستجو کرد. قبل از پیشرفت‌های شگرف قرن بیستم در حوزه فناوری، «... جرم از حیث مقیاس کوچک بوده و شامل اقدامات خلاف قانونی بود که به وسیله یک شخص یا اشخاصی که با هم مرتبط بودند علیه یک یا چند قربانی صورت می‌گرفت.»[2] این رویکرد ساده‌انگارانه و محلی به ماهیت جرم، رسیدگی به جرایم برای مقامات محلی را ساده کرده بود زیرا انگیزه‌ها و انواع جرایم محدود و معلوم بود. پیدایش فناوری حمل و نقل و ارتباطات راه دور در قرن گذشته و توسعه روابط انسانی ورای مرزهای کشورها، منجر به وقوع انواع جدیدی از جرایم شد که نیازمند واکنش نظام‌های حقوقی در قبال آنها بود. این فرایند موجب تکامل اصول سنتی حاکم بر صلاحیت در قوانین داخلی کشورها و در نتیجه بالا رفتن توانایی این اصول در مواجهه با جرایم جدید شد. به دیگر سخن با توسعه حمل و نقل و ارتباطات بین‌المللی، افراد می‌توآن استند بعد از ارتکاب جرم در یک کشور با استفاده از این فناوری‌ها به سرعت از کشور محل ارتکاب جرم بگریزند و یا اینکه فناوری‌های جدید این امکان را به وجود آورد که مجرم بدون این که کشور محل اقامت و سکونت خود را ترک نماید جرم یا جرایمی را علیه قربانیانی مرتکب شود که در کشوری دیگر سکونت دارند.

این تحولات باعث شد تا اصول نوینی در قوانین ناظر بر صلاحیت محاکم در کشورها پدیدار شوند تا دولت‌ها با استعانت از این اصول بتوانند مدعی صلاحیت فراسرزمینی شده و به وظیفه ذاتی خود که حمایت از شهروندان در برابر جرایم است، جامه عمل بپوشانند. این اصول بر اساس ماهیت پیوند بین جرم و کشور مورد بحث شکل گرفته و اعمال می‌شوند. امروزه، چهار اصل شناخته‌شده وجود دارد که دولت‌ها بر

1. Koops and Brenner, Op. cit., p. 4.
2. Marc Goodman, and Susan Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", International Journal of Law and Information Technology, Vol. 10, No.2, 2002, p.157.

اساس آن مدعی صلاحیت فراسرزمینی در مورد اعمال مجرمانه با وصف بین‌المللی شده و چنین صلاحیتی را اعمال می‌کنند.[1] اصل بنیادین در تشخیص این نوع از صلاحیت آن است که جرایم صرفاً در حوزه شمول صلاحیت سرزمینی یک کشور رخ نمی‌دهد. گاهی جرم، و در بحث ما جرم سایبری، جنبه فراسرزمینی دارد. در چنین مواردی، حقوق بین‌الملل برخی مبانی صلاحیت فراسرزمینی در موضوعات کیفری را پذیرفته است. مبنای مشترکی که در حقوق داخلی و موافقت‌نامه‌های بین‌المللی می‌توان یافت، شرط «ارتباط کافی» یا «پیوند واقعی» بین جرم و دولت مدعی صلاحیت است.

به طور خلاصه و با عنایت به قوانین مدرن کشورها از جمله قوانین کیفری ایران، می‌توان گفت که اعمال صلاحیت فراسرزمینی تابع اصول زیر است: اصل تابعیت فعال، اصل تابعیت منفعل، اصل صلاحیت جهانی و اصل حمایتی. ذکر این نکته لازم است که استناد به این اصول و صلاحیت فراسرزمینی از سوی کشورها - خواه بر مبنای حقوق داخلی یا موافقت‌نامه‌های بین‌المللی- به خودی خود بر اعتبار اصل استقلال حاکمیت و اصل عدم مداخله تاثیرگذار نیست. انجام تحقیقات کیفری در قلمرو کشور دیگر (به موجب اصل حمایتی یا اصل تابعیت منفعل) مستلزم رضایت کشور ذیربط است.[2] بنابراین، ادعای اعمال صلاحیت فراسرزمینی توسط کشور ذینفع هرچند با اصل عدم مداخله و استقلال حاکمیت ارتباط دارد لیکن به هیچ عنوان ناقض این دو اصل بنیادین حقوق بین‌الملل نیست و با مراعات این دو اصل از مجرای جلب رضایت کشورهاست که قابلیت اعمال پیدا می‌کند. از سوی دیگر، اصل حاکمیت سرزمینی قوانین کماکان برای رسیدگی به غالب جرایم مورد استناد قرار می‌گیرد.[3] در این مقاله تلاش می‌کنیم تا همه اصول حاکم بر اعمال صلاحیت در مورد جرایم سایبری و میزان موفقیت آنها در مقابله با این جرایم مورد بررسی قرار دهیم، لیکن بدیهی است قبل از آن لازم است تا مفهوم جرم سایبری به مثابه جرمی فراملی و فراسرزمینی مورد توجه قرار گیرد.

۱-۲. جرم سایبری به مثابه جرم فراملی

جرم سایبری به خودی خود نمی‌تواند فراملی باشد زیرا امکان دارد تمام عناصر جرم و آثار آن محدود به قلمرو یک کشور معین باشد. در این صورت جرم محصور در محدوده ملی یک کشور خاص است. اما در مواردی ممکن است یک یا چند عنصر از

1. Ian Walden, Computer Crimes and Digital Investigations, Oxford University Press, 2007, p. 304.
2. Ian Brownlie, Op. cit., p .306.
3. Goodman and Brenner, Op. cit., pp. 19-20.

جرم، مربوط به دو یا چند کشور باشد و یا اینکه آثار جرم به یک کشور خاص محدود نشود. در این گونه موارد لازم است بحث صلاحیت فراملی مطرح و اصول حاکم بر اعمال آن بررسی شود.جرم سایبری مفهومی است که تعاریف متفاوتی از آن ارایه شده است. جرم سایبری، از نظر لغوی، عبارت است از جرمی که به فضای سایبر، رایانه‌ها، شبکه‌های مجازی و اینترنت پیوند می‌خورد. به طور کلی، می‌توان حوزه‌های وقوع جرایم سایبری را به ترتیب زیر طبقه‌بندی کرد:

(الف) هرزنامه‌ها، انتشار بیش از حد ایمیل، افترا، اظهارات تنفرآمیز و نقض قوانین کپی رایت؛

(ب) دسترسی غیرمجاز، سرقت داده‌ها، هک کردن رایانه، قطع خدمات، و حملاتی که از کدهای نادرست استفاده می‌کنند؛

(ج) کلاهبرداری مالی؛

(د) تسهیل ارتکاب جرایم سنتی از جمله پورنوگرافی آنلاین کودکان، قماربازی آنلاین، جاسوسی[1] و تروریسم.[2]

در صورتی که جرم سایبری در قلمرو یک کشور ارتکاب یابد و هیچ عنصر خارجی در آن دخیل نباشد و هیچ اثر فرامرزی نداشته باشد، طبیعتاً از حیث اعمال صلاحیت مشکلی وجود ندارد. اما مشکل آنجاست که جرم، جنبه فراملی دارد. در حقیقت «در دنیای سایبر، هیچ قلمرو یا مرز مشخصی وجود ندارد.»[3] فاصله مرتکب با تمام دنیا فقط به اندازه فشار دادن سرانگشت بر یک کلید است. «حدود ۸۰ درصد جرایم سایبری که ماموران داخلی کشف می‌کنند مربوط به بیش از یک کشور است.»[4] از نظر برخی، اکثر قربانیان مرتکبان جرایم سایبری در قلمرو «خارج از مرزهای ملی» هستند. در برخی کشورها، بیشترین جرایم سایبری گزارش‌شده ابتدا خارج از قلمرو سرزمینی شروع شده است. در عین حال برخی معتقدند در اکثر موارد کشورها به عنوان مجرا یا کانال

۱. در این خصوص بنگرید به:
میرمحمد صادقی، حسین، «جرم جاسوسی»، ماهنامه دادرسی، شماره ۱۸، اسفند ۱۳۷۸، صص. ۵۵-۵۲.

2. Adel Azzam Saqf Al Hait, "Jurisdiction in Cybercrimes: A Comparative Study", Journal of Law, Policy and Globalization, Vol. 22, 2014, p. 75.

3. Laura Barnett, International Dimensions of Domestic Criminal Law: Extraterritoriality and Extradition, Canada Library of Parliament, 2008, p.1. availabale at:
http://www.parl.gc.ca/information/library/PRBpubs/prb0117-e.htm

4. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, United Nations, Vienna, 2013, p.184.

سایبری ارتکاب جرم عمل می‌کنند و از این طریق درگیر یک جرم سایبری می‌شوند. از نظر کشورها، استفاده از سامانه‌های خدمات‌رسانی اینترنتی و تاثیر فزاینده رسانه‌های اجتماعی، از جمله عوامل افزایش شمار جرایم سایبری فراملی است. حتی از نظر برخی کشورها، مرتکبان کاملاً از مسایل صلاحیتی آگاه هستند و برای اخفای ادله مربوط به اعمال غیرقانونی خود عمداً از منابع اینترنتی، مثل خدمات ایمیل، که در خارج واقع شده‌اند، استفاده می‌کنند. اما ذکر این نکته لازم است که کشورها ارزیابی یکسانی در خصوص جرایم سایبری ندارند. برای نمونه از نظر یک کشور از آمریکای جنوبی بخش قابل توجهی از جرایم سایبری گزارش‌شده جرایم فراملی دارای منشاء داخلی بودند.[1] بنابراین، برای درک اینکه در چه مواردی جرم سایبری دارای جنبه فراملی است، باید در خصوص مفهوم فراملی بودن جرم بحث شود.

به موجب حقوق موضوعه بین‌المللی مندرج در کنوانسیون ملل متحد در مورد جرم سازمان‌یافته، یک جرم در صورتی ماهیتاً فراملی است که: (الف) در بیش از یک کشور ارتکاب یابد؛ (ب) در یک کشور به وقوع بپیوندد اما بخش قابل توجه برنامه‌ریزی یا کنترل آن در کشور دیگری انجام شود؛ (ج) جرم در یک کشور ارتکاب یابد اما مربوط به یک گروه مجرمانه سازمان‌یافته باشد که در بیش از یک کشور به اقدامات مجرمانه مبادرت می‌کنند؛ یا (د) جرم در یک کشور ارتکاب یابد اما در کشور دیگر آثار چشمگیری داشته باشد.[2] جنبه فراملی زمانی بیشتر معنا پیدا می‌کند که رسیدگی به جرم با توجه به ملاحظات صلاحیت و ادله کیفری بررسی شود.[3] بدین ترتیب هر گاه یک یا چند عنصر از عناصر فوق وجود داشته باشند، یا ارتکاب جرم در کشوری دیگر آثار چشمگیری به همراه داشته باشد، یک جنبه فراملی وجود خواهد داشت. جنبه‌های فرامرزی ادله از دو جهت قابل بررسی است: (الف) نقش فزاینده ادله الکترونیکی در تمامی جرایم و نه فقط جرایمی که در مقوله جرایم سایبری جای می‌گیرند؛ و (ب) استفاده روز افزون از محاسبات توده‌ای متضمن ذخیره داده‌های موازی و مخدوش. به‌ویژه، جابه‌جایی پویای داده‌ها به صورت خودکار در مراکز خدمات داده‌های متمرکز که از نظر فیزیکی در کشورهای متفاوتی قرار دارند، می‌تواند در تشخیص محل داده‌ها،

1. Ibid.
2. Article 3(2) of United Nations Convention against Transnational Organized Crime, Singed 15 November 2000, entered into force on 29 September 2003.
3. United Nations Office on Drugs and Crime, Op. cit., p .188.

چالش‌هایی را ایجاد کند.[1] بنابراین، این مسأله که ادله فراسرزمینی را چگونه می‌توان از اشخاص و تأمین‌کنندگان خدمات به دست آورد، باید مورد بررسی قرار گیرد.

۲. اصول حاکم بر اعمال صلاحیت دادگاه‌ها در رسیدگی به جرایم سایبری

براساس یافته‌های تحقیقات سازمان ملل متحد در خصوص اعمال صلاحیت و رسیدگی به جرایم سایبری در نظام‌های حقوقی داخلی، حدود یک‌سوم کشورهای پاسخ‌دهنده، چارچوب حقوقی داخلی خود برای جرایم ارتکابی خارج از کشور را کارآمد دانسته‌اند، ۴۰ درصد دیگر آن را تاحدودی کارآمد ارزیابی کرده و ۲۵ درصد معتقد به ناکارآمدی آن بوده‌اند. در منطقه آمریکا، چارچوب‌های حقوقی داخلی ناکافی ارزیابی شد. در مقایسه با ۶۷ درصد کشورها در آفریقا، آسیا و اقیانوسیه، در منطقه آمریکا تنها ۴۰ درصد کشورها گزارش دادند که چارچوب حقوقی داخلی‌شان کارآمد یا تا حدودی کارآمد است. همه کشورهای منطقه اروپا معتقد بودند که قوانین داخلی‌شان کارآمد یا تا حدودی کارآمد است[2]. کشورهایی که قوانین داخلی خود را برای جرایم سایبری فرامرزی کارآمد نمی‌دانستند، دلایلی را مطرح می‌کردند. خلاءهای مشترک شامل نقص مقررات کیفری در خصوص اقدامات ارتکابی خارج از حوزه صلاحیت سرزمینی و همچنین در برخی موارد عدم قابلیت اجرای قوانین استرداد[3] و معاضدت قضایی متقابل نسبت به جرایم سایبری بود.[4] کشورهایی که به پرسش‌نامه پاسخ دادند، اعلام داشتند که مبنای صلاحیت در خصوص جرایم سایبری فرامرزی اساساً مبتنی بر اصولی از قبیل سرزمینی بودن و تابعیت مرتکب است. بنابراین، از نظر کشورها لازم است که اقدام سایبری دارای آثار داخلی، از قبیل بزه‌دیدگی اتباع یا آثار یا خسارتی درون قلمروی سرزمینی ایشان باشد. از نظر برخی کشورها اگر جرم کاملاً خارج از قلمرو سرزمینی ارتکاب یابد و هیچ اثری درون سرزمین ایشان نداشته باشد، جرم‌انگاری و تعقیب می‌تواند چالش‌برانگیز باشد. رویکرد اسناد جهانی و منطقه‌ای در مورد اعمال صلاحیت بر جرایم سایبری شایسته مداقه و بررسی است. این اسناد از جمله «کنوانسیون شورای

1. United Nations Office on Drugs and Crime, Op. cit., p .188.
2. Ibid, pp. 190-191.
۳. در مورد استرداد به طور کلی بنگرید به: آزمایش، علی، تقریرات درس حقوق بین‌الملل کیفری دوره کارشناسی ارشد، دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی، نیمسال اول، سال تحصیلی ۱۳۸۳- ۱۳۸۲؛ و آخوندی، محمود، « استرداد بزهکاران»، مجله حقوقی و قضائی دادگستری، سال سوم، شماره هشتم، پائیز ۱۳۷۲، صص ۱۱- ۹۳.
4. United Nations Office on Drugs and Crime, Op. cit., p.190.

اروپا در مورد جرایم سایبری»[1] معمولاً تصریح می‌کنند که کشورهای عضو این معاهده باید اقدامات قانون‌گذاری و تدابیر دیگری را اتخاذ کنند تا برای جرایمی که بر طبق این سند پیش‌بینی شده است، اشکال معینی از صلاحیت را اعمال نمایند.

۲-۱. اصل صلاحیت سرزمینی

بر اساس این اصل، یک کشور باید اقدامات مجرمانه‌ای را که در قلمرو سرزمینی‌اش رخ داده تحت تعقیب قرار دهد، حتی در مواردی که مرتکب جرم یک تبعه خارجی است. افزون بر این، صلاحیت سرزمینی شامل مواردی است که یکی از عناصر تشکیل‌دهنده جرم، و به ویژه آثار آن، در درون قلمرو سرزمینی رخ می‌دهد. بنابراین نه تنها کشوری که عمل مجرمانه در آن آغاز شده است، بلکه کشوری که جرم در آن پایان یافته نیز می‌توانند به اعمال صلاحیت قضایی و محاکمه مرتکب بپردازند.[2]

۲-۱-۱. اسناد بین‌المللی ناظر بر صلاحیت سرزمینی

تمام اسناد بین‌المللی یا منطقه‌ای راجع به جرم سایبری که متضمن شرط صلاحیت می‌باشند، اصل صلاحیت سرزمینی را به رسمیت شناخته و کشورهای عضو را ملزم می‌نمایند تا صلاحیت خود را نسبت به جرایم برشمرده‌شده در این اسناد که در قلمرو جغرافیایی آن کشور ارتکاب یافته است، اعمال نمایند. فعالیت‌های مجرمانه در کشتی‌ها و هواپیماها نیز تابع یک سلسله اسناد الزام‌آور و غیرالزام‌آور است. بر اساس اصل صلاحیت سرزمینی، بسیاری از اسناد بین‌المللی و منطقه‌ای که بر جرم‌انگاری اعمال مجرمانه پرداخته‌اند، مقرر داشته‌اند که لازم نیست تمام عناصر جرم در درون قلمرو کشور عضو به وقوع پیوندد تا صلاحیت سرزمینی کشور عضو اعمال شود. گزارش تفسیری کنوانسیون شورای اروپا در مورد جرم سایبری تصریح دارد که به موجب اصل سرزمینی بودن، یک کشور عضو در صورتی صلاحیت سرزمینی خود را اعمال می‌کند که هم شخصی که به یک سیستم رایانه‌ای حمله می‌کند و هم سیستم قربانی در درون قلمرو آن کشور قرار دارند و سیستم رایانه‌ای که مورد حمله قرار گرفته در درون قلمرواش قرار داشته باشد ولو این که حمله‌کننده خارج از قلمرو آن کشور عضو باشد.[3]

1. Council of Europe Cybercrime Convention
2. Lotus case, PCIJ, Series A, No. 10, 1927, p. 23-30.
3. Council of Europe Explanatory Report to Convention on Cybercrime, Council of Europe Treaty Series Explanatory Reports (CETSER), 2001, 23 November 2001, Para. 223.

همچنین، قسمت سوم از بند چهارم ماده ۴۰ پیش‌نویس سند امنیت سایبری بازار مشترک کشورهای شرق و جنوب آفریقا مقرر می نماید: «جرم در جایی وقوع یافته است که عنصر مادی جرایمی که بر طبق این قانون جرم‌انگاری شده است ... به وقوع پیوسته است.»[1]

بر اساس دستور العمل اتحادیه اروپا در مورد استثمار کودکان، اعمال صلاحیت نسبت به جرایمی که تمام یا بخشی از آن در قلمرو اتحادیه اروپا رخ دهد، الزامی است. این دستور العمل تصریح دارد که این روش اعمال صلاحیت شامل مواردی است که جرم به وسیله فناوری اطلاعات و ارتباطات ارتکاب یافته باشد، منصرف از این که ابزارهای مربوط به فناوری مورد استفاده در کشور عضو مستقر باشد یا بیرون از اتحادیه باشد.[2] تصمیم اتحادیه اروپا در مورد حمله علیه سیستم‌های اطلاعاتی، شامل حملات فیزیکی در قلمرو یک دولت (اعم از این که علیه سیستم اطلاعاتی در همان قلمرو باشد یا خیر) و نیز حملات علیه سیستم‌های اطلاعاتی در آن قلمرو خواهد بود، خواه مرتکب به‌طور فیزیکی در آن قلمرو حضور داشته باشد یا نباشد.[3]

۲-۱-۲. قوانین و مقررات ملی ناظر بر صلاحیت سرزمینی

رویکردهای نوین قانون‌گذاری داخلی بر اسناد منطقه‌ای و بین‌المللی نیز تأثیر داشته است. در بسیاری از کشورها مقرراتی وجود دارد با این نگرش که لازم نیست کل جرم در قلمرو کشور ارتکاب یابد تا صلاحیت سرزمینی اعمال شود. با وجود این، برای تعیین و شناسایی وجود پیوند یا رابطه سرزمینی، سازوکارها و معیارهای قانونی در کشورها متفاوت است. در برخی از کشورها، بر «فعل یا ترک فعل»ی تأکید شده است که لزوماً باید در سرزمین ارتکاب یافته باشد. در برخی موارد دیگر، بر محل «سیستم های رایانه‌ای و داده‌ها» تمرکز و تأکید شده است.[4] از نظر برخی از کشورها، صلاحیت سرزمینی شامل جرایمی می‌شود که در جایی دیگری شروع شده، ادامه پیدا کرده یا کامل شده است، اما به طور جزئی یا کلی علیه اموالی است که درون سرزمین آن دولت

1. COMESA Draft Model Bill, Article, 40(f) (iii).
2. Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (EU Directive on Child Exploitation) , 2011/92/E,U 23 November 2001, Article 17.
3. European Union Council Framework Decision on attacks against information systems (EU Decision on Attacks against Information Systems), 2005/222/JHA, 24 February 2005, Article 10.
4. United Nations Office on Drugs and Crime, Op. Cit., p.192.

قرار دارد یا سبب صدمه به شخص یا اشخاصی شده است که درون قلمرو آن دولت حضور دارند. به زعم قوانین برخی دیگر از کشورها، صلاحیت در جایی اعمال می‌شود که «سِرور یا سخت‌افزار به کار گرفته شده برای ارتکاب جرم» خارج از قلمرو آن کشور واقع شده است، اما نوعی اثر در آن کشور داشته است یا عنصری داخلی در ارتکاب جرم وجود دارد.[1] رویه قضایی کشورها نیز نشان می‌دهد که دادگاه‌های ملی در مواردی مدعی اعمال صلاحیت شده‌اند که عناصر جرم، به جز نتیجه آن، در درون قلمرو است. در مقابل، کیفرخواست‌هایی نیز در مواردی صادر شده است که نتیجه جرم داخل قلمرو دولت بوده، اما فعل یا ترک فعل مجرمانه و محل مرتکبان در خارج از کشور بوده است.[2] این موارد در خصوص پرونده‌های قماربازی اینترنتی و پورنوگرافی کودکان به وفور مشاهده می‌شود.

ذکر این نکته نیز لازم است که بر اساس تحقیق سازمان ملل متحد، شمار اندکی از کشورهای منطقه اروپا و آمریکا گزارش دادند که قوانین داخلی در خصوص برخی از جرایم سایبری ارتکابی خارج از کشور، از قبیل قطع خدمات، ارسال هرزنامه و فیشینگ[3] یا جعل عنوان الکترونیک[4]، کافی نبوده‌اند. در نهایت، اصل تابعیت ممکن است بر اصل سرزمینی بودن محدودیت‌هایی وارد کند. حتی در مواردی که امکان اعمال صلاحیت سرزمینی وجود دارد- مثلاً زمانی که فعل یا ترک فعل مجرمانه فرامرزی لیکن دارای آثاری در سرزمین کشور متبوع بزه‌دیده باشد- از نظر برخی از کشورها اگر مرتکب تبعه خارجی باشد، وضعیت مبهم خواهد بود. در این موارد قوانین دادرسی برخی از کشورها رسیدگی را تنها زمانی مجاز دانسته‌اند که شرایطی دیگر (پیوندهای دیگری میان سرزمین و مرتکبین) وجود داشته باشد. از نظر برخی از کشورها جرم‌انگاری و تعقیب مظنونین خارجی منوط به آن است که جرم بر منافع و امنیت داخلی لطمه ملموسی وارد کرده باشد. در این دست جرایم، قاطبه کشورها قائل به اعمال صلاحیت سرزمینی هستند زیرا امنیت و منافع ملی ایشان دچار خطر شده است.[5] قوانین برخی دیگر از کشورها منصرف از محل وقوع جرم، اعمال صلاحیت بر

1. Ibid.
2. US v. Tsastsin et al, United States District Court, Southern District of New York, No. S2. 11 Cr. 878, 1 March 2001.
3. phishing
۴. فیشینگ عبارتست از از اقدام بزهکار سایبری در معرفی خود به عنوان یک مرجع معتبر عموماً مالی جهت کسب اطلاعات و کدهای ارتباطی کاربر با بانک یا مؤسسات مالی به هدف بردن اموال کاربر.
5. United Nations Office on Drugs and Crime, Op. cit., pp.192-193.

مرتکبین با هر تابعیتی را امکان‌پذیر می‌دانند - البته مادام که بتوان رابطه‌ای، همچون حضور متهم، ابزار یا داده‌هایی که در جرم مورد استفاده قرار گرفته یا ایراد خسارت در درون قلمروشان را احراز کرد.[1] در باب حضور متهم در سرزمین باید به قاعده عرفی «محاکمه کن یا مسترد کن» اشاره کرد. بنا بر این قاعده، دولت‌ها در صورت وقوع یک جرم دارای ابعاد بین‌المللی مکلف هستند متهم را محاکمه کنند و در غیر این صورت مکلف به استرداد متهم به کشوری هستند که زیان‌دیده از جرم در آن حضور دارد.

در قانون داخلی ایران در رسیدگی به جرایم سایبری اصل صلاحیت سرزمینی در بندهای (الف) و (ب) ماده ۲۸ قانون جرائم رایانه‌ای به رغم وجود مقررات عام راجع به صلاحیت سرزمینی (ماده ۳ قانون مجازات اسلامی ۱۳۹۲)، به صلاحیت مذکور اشاره شده است. بر اساس بند (الف) ماده ۲۸ می‌توان گفت مراکز داده‌ای که در قلمرو حاکمیت زمینی ، دریایی و هوایی ایران به ارائه خدمات می‌پردازند ، جزء قلمروی حاکمیتی ایران محسوب می‌شوند. مطابق بند ۱ ماده ۱ آئین‌نامه مرکز خدمات داده اینترنتی مصوب ۱۳۸۳ کمیسیون تنظیم مقررات و ارتباطات رادیویی ، مرکز خدمات داده اینترنتی مجتمع ایمن و مقاوم در برابر تهدید و خطا و دارای ارتباطات پرسرعت و پایدار به منظور میزبانی تجهیزات ، سرویس‌ها و کاربردهای اطلاعاتی است. بند (ب) ماده ۲۸ نیز وب‌سایت‌های دارای نام‌دامنه مرتبه‌بالای کد کشوری را در حکم قلمروی ایران دانسته است. قانون جرائم رایانه‌ای برای تعیین محل وقوع جرائم سایبری ضابطه دقیق و شفافی ارائه نداده است اما برای تعیین دقیق محل وقوع جرم در فضای سایبر معیارهایی وجود دارد که از آن جمله نظریه محل استقرار سیستم های رایانه‌ای است که مطابق آن کشوری صالح به رسیدگی به جرم سایبری است که سیستم‌های رایانه‌ای در قلمرو حاکمیتی آن استقرار دارد. منظور از سیستم‌های رایانه‌ای، هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری – نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده‌پیام عمل می‌کند (بند «و» ماده ۲ قانون تجارت الکترونیک مصوب ۱۳۸۲).[2]

۱. در این خصوص برای نمونه بنگرید به:

Computer Crimes Act of Malaysia, (1997), Article 9; Computer Misuse Act of Singapore (Revised, 2007), Article 11; Computer Misuse Act of Trinidad and Tobago (2000), Article 12.

۲. البوعلی، امیر، صلاحیت محاکم در جرائم سایبری ، انتشارات جنگل، ۱۳۹۲، ص. ۵۶.

۲-۲. اعمال صلاحیت بر مبنای اصل تابعیت

یکی از مبانی اعمال صلاحیت تابعیت متهم است.[1] بر اساس این نظریه دولت‌ها بر اتباع خود اعمال صلاحیت می‌کنند. در اعمال اصل تابعیت، اصولاً دو جنبه تابعیت فعال و منفعل مورد توجه رویه قضایی بوده است. تابعیت فعال، به اعمال صلاحیت بر مبنای تابعیت مرتکب، منصرف از محل وقوع جرم، اشاره دارد. تابعیت منفعل، زمانی موجد صلاحیت می‌شود که کشور بر مبنای تابعیت بزه‌دیده، منصرف از محل وقوع جرم، صلاحیت می‌یابد. در حقیقت، در صلاحیت بر مبنای تابعیت، کشور متبوع مرتکب یا بزه‌دیده است که مدعی اعمال صلاحیت می‌شود. افزون بر آن، گاهی صلاحیت بر مبنای محل اقامت عادی مجرم تعیین می‌شود. برای درک موازین بین‌المللی حاکم بر اعمال صلاحیت بر مبنای تابعیت ضرورت دارد که ابتدا رویکرد اسناد بین‌المللی مورد مطالعه قرار گیرد.

۲-۲-۱. اسناد بین‌المللی مرتبط با اعمال صلاحیت بر مبنای تابعیت

در مواردی که اسناد بین‌المللی یا منطقه‌ای راجع به جرم سایبری، اصل سرزمینی بودن را مورد شناسایی قرارداده‌اند به کرات اصل تابعیت فعال را نیز متذکر شده‌اند. به موجب این اصل، در صورت وقوع جرم توسط اتباع در سرزمین بیگانه، کشور متبوع فرد مکلف به تضمین اعمال صلاحیت است. بر اساس برخی از اسناد بین‌المللی، لازم است که رفتار تبعه در کشوری که عمل ارتکاب‌یافته نیز جرم‌انگاری شده باشد.[2] در مقابل، تنها شمار محدودی از اسناد، عمدتاً اسناد مربوط به حقوق کودک، صلاحیت بر مبنای اصل تابعیت منفعل را پیش‌بینی کرده‌اند. دستورالعمل اتحادیه اروپا در مورد استثمار کودکان و برخی از اسناد ملل متحد دولت‌ها را ملزم می نمایند تا نسبت به جرم ارتکابی خارج از قلمرو، علیه اتباع خود یا شخصی که در این کشورها اقامتگاه عادی دارد، اعمال صلاحیت کنند.[3] کنوانسیون شورای اروپا در خصوص حمایت از کودک مقرر می دارد که کشورهای عضو معاهده باید تلاش کنند تا چنین صلاحیتی را اعمال نمایند.[4] این دسته از مقررات، اختیار صلاحیتی را به کشورها می دهند تا حمایت از

1. Malcolm Shaw, International Law, Cambridge, 2003, p.579.
2. COMESA Draft Model Bill, Art.40(c); Commonwealth Model Law, Art. 4(d); Council of Europe Cybercrime Convention, Art. 22(1)(d); and League of Arab States Model Law 2004, Article 30(1)(d).
3. EU Directive on Child Exploitation, Article 17(2) (a).
4. Council of Europe Child Protection Convention, Article 25(2).

کودکان متبوع خود در خارج را تضمین نمایند. ریشه این نوع صلاحیت به مبانی حقوق بشری حمایت از حقوق کودک به عنوان اعضاء آسیب‌پذیر یک کشور باز می‌گردد.

۲-۲-۲. رویکرد قوانین و مقررات داخلی به اعمال صلاحیت بر مبنای تابعیت

برخی از کشورها به استفاده از اصل تابعیت فعال برای اعمال صلاحیت نسبت به جرایم ارتکابی اتباع خود، منصرف از محل ارتکاب، اشاره دارند. از نظر برخی از کشورها، برای اعمال اصل تابعیت فعال، لازم است که عمل در کشور محل ارتکاب نیز جرم تلقی شود.[۱] برخی از کشورها نیز بر مبنای اصل صلاحیت منفعل نسبت به جرایمی که به اتباعشان لطمه می‌زنند، منصرف از محل وقوع آن، اعمال صلاحیت می‌کنند. در تحقیق سازمان ملل متحد در مورد جرایم سایبری به این نکته اشاره شده است که یکی از کشورهای اروپایی گزارش کرده است که بسیاری از پرونده‌های مربوط به جرایم سایبری در آن کشور دارای عناصر فرامرزی است و در برخی از پرونده ها، بزه‌دیدگانی که تابعیت این کشور را داشتند در خارج بودند. برخی کشورها نیز برای کاهش مشکلات صلاحیتی قانونی کیفری را تصویب کرده‌اند که متضمن اصل تابعیت منفعل در مواردی است که مرتکب تبعه خارجی است که در خارج مرتکب جرمی شده که به یک تبعه خارج از آن قلمرو صدمه می‌زند.[۲]

ماده ۵ قانون مجازات اسلامی ۱۳۹۲ چنین صلاحیتی را به صراحت به رسمیت شناخته است. در خصوص اصل صلاحیت شخصی دادگاه‌های ایران مقرره‌ای وجود ندارد اما نظر به صدر ماده ۲۸ قانون جرائم رایانه‌ای که صلاحیت پیش‌بینی‌شده در دیگر قوانین را پذیرفته است (قانون مجازات اسلامی مصوب ۱۳۹۲) ، برای تعیین مواردی که دادگاه‌های ایران به موجب اصل صلاحیت شخصی صلاحیت رسیدگی به جرائم سایبری را دارند باید به مقررات عام موجود در این خصوص توجه نمود.[۳]

۲-۳. سایر مبانی اعمال صلاحیت

افزون بر دو مورد پیشین، موارد دیگری نیز وجود دارد که منجر به اعمال صلاحیت دادگاه‌ها می‌شوند. گاهی کشور بر مبنای «اصل حمایت» اعمال صلاحیت می‌کند. بر اساس این اصل، صلاحیت در جایی ایجاد می‌شود که عمل مجرمانه ارتکابی در خارج از قلمرو کشور مدعی صلاحیت، به امنیت کشور ذینفع یا منافع حیاتی آن

1. United Nations Office on Drugs and Crime, Op. Cit., p.193.
2. Ibid.
۳. زیبر، اولریش، جرائم رایانه‌ای، ترجمه محمدعلی نوری و همکاران، چاپ دوم، گنج دانش، ۱۳۹۰ .ص ۴۵.

لطمه می‌زند.[1] بنابراین، به موجب این اصل دولت‌ها بر کسانی اعمال صلاحیت می‌کنند که اقدامات‌شان، امنیت یا منافع حیاتی کشور را تهدید می‌کند، منصرف از این که عمل مجرمانه در کجا صورت گرفته است. این قسم از صلاحیت کیفری به ویژه پس از عملیات ۱۱ سپتامبر ۲۰۰۱ توسط ایالات متحده مورد استناد قرار گرفته و در قلمرو جرایم تروریستی با اقبال کشورها مواجه شده است. بدین ترتیب در موارد متعددی ایالات متحده با استناد به اصل حمایت از منافع ملی اقدام به اعمال صلاحیت کرده و متهمینی که مظنون به ارتکاب جرایم تروریستی سایبری یا راه‌اندازی سایت‌های حامی فعالیت های تروریستی بوده‌اند را صرف‌نظر از محل اقامت یا تابعیت‌شان تحت تعقیب قرار داده است.

همچنین گاهی، یک کشور با توسل به «دکترین آثار جرم» مدعی اعمال صلاحیت می‌شود. صلاحیت نسبت به یک رفتار صورت گرفته در خارج از قلمرو زمانی ایجاد می‌شود که آثار چشمگیری در درون قلمرو ایجاد کند.[2]

در نهایت، گاهی نیز کشورها با استناد به «اصل صلاحیت جهانی»، مدعی اعمال صلاحیت می‌شوند. صلاحیت بر هر شخص متهم به ارتکاب برخی از جنایات بین‌المللی، از قبیل دزدی دریایی، جنایات جنگی و نقض‌های شدید کنوانسیون‌های ژنو، منصرف از قلمرو یا تابعیت اشخاص مرتبط، ایجاد می‌شود.[3] این اصل معمولاً به وضعیت‌هایی محدود می‌شود که کشور صالح به رسیدگی نمی‌خواهد یا نمی‌تواند جرم یا جرایم ارتکابی را تحت تعقیب قرار دهد.

اصل حمایتی، در برخی کنوانسیون‌های بین‌المللی از جمله کنوانسیون جامعه کشورهای عربی، پیش‌بینی شده است. برای نمونه این کنوانسیون تصریح می‌نماید که کشورهای طرف باید صلاحیت خود ر انسبت به جرایمی تسری دهند که بر منافع مهم آن کشور تاثیر می‌گذارد.[4] اسناد بین‌المللی موجود در اروپا، از جمله تصمیم شورای اروپا در مورد حملات علیه سیستم‌های اطلاعاتی، متضمن مبنای صلاحیتی دیگری نیز

1. Bruno Simma, and Andreas Mueller, Exercise and the Limits of Jurisdiction, In: James Crawford, and Martin Koskenniemi, The Cambridge Companion to International Law, Cambridge University Press, 2012, pp.134- 143.
2. Thomas Schultz, "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", European Journal of International Law, Vol. 19, No.4, 2008, p.812.
3. Cassese, Op. cit. pp. 451-452.
4. League of Arab States Convention, Article 30 (1) (e).

هستند که جرایمی را در بر می‌گیرد که به نفع یک شخص حقوقی ارتکاب یافته که دفتر مرکزی‌اش در آن قلمرو واقع شده است.[1] در نهایت، بنا بر اصل «مسترد کن یا محاکمه کن»، برخی از اسناد، صلاحیت را در مواردی پیش‌بینی کرده‌اند که مرتکب در قلمرو آن کشور حضور دارد و پس از درخواست استرداد، دولت مرتکب را، صرفاً بر مبنای تابعیتش، به کشور دیگری مسترد نمی‌کند.[2]

در مورد سایر مبانی صلاحیتی، از قبیل صلاحیت جهانی، برخی از کشورها به وضعیت‌هایی اشاره می‌کنند که شخص خارجی مرتکب جرمی شود که در قلمرو کشور خودش کشف شده، اما هیچ درخواستی برای استرداد وی نشده است. از نظر برخی از کشورها صلاحیت جهانی به جنایات بین‌المللی محدود می‌شود و جرایم سایبری را در بر نمی‌گیرد. با این حال، برخی دیگر نیز بر این باورند که جرایم شدید سایبری، از قبیل پورنوگرافی کودکان، به طور مسلم می‌تواند مشمول صلاحیت جهانی قرار گیرد.[3]

در قانون داخلی کشور ایران در راستای اصل حمایت مقرره‌هایی پیش‌بینی شده است که توجه به آنها واجد اهمیت می‌باشد. به عنوان مثال قانون‌گذار با توجه به مشکلاتی که در زمینه اعمال اصل صلاحیت سرزمینی وجود داشت، برای تکمیل اصل صلاحیت سرزمینی و جلوگیری از بی‌کیفر ماندن کسانی که در خارج از قلمرو ملی مرتکب جرم سایبری می‌شوند اصول دیگری را در قانون جرائم رایانه‌ای مطرح نمود که جنبه فرا سرزمینی دارد و شامل صلاحیت واقعی و صلاحیت جهانی می‌گردد.[4]

1. European Union Council Framework Decision on attacks against information systems (EU Decision on Attacks against Information Systems), 2005/222/JHA, 24 February 2005, Article 10(1)(c); EU Directive on Child Exploitation, Article 17(2)(b); European Union Council Framework Decision combating fraud and counterfeiting of non-cash means of payment (EU Decision on Fraud and counterfeiting) 2001/413/JHA, 28 May 2001, Article 9(1)(c); and EU Directive Proposal on Attacks against Information Systems, Article 13(1)(c).

2. COMESA Draft Model Bill, Art. 40(d); Council of Europe Cybercrime Convention, Article 22(3); Council of Europe Child Protection Convention, Article 25(7); EU Decision on Attacks against Information Systems, Article10(3); EU Decision on Fraud and Counterfeiting, Article 10(1) and League of Arab States Convention, Article 30(2).

3. United Nations Office on Drugs and Crime, Op. cit., pp.194-195.

۴. پوربافرانی ، حسن ، «تحول اصل صلاحیت واقعی در لایحه جدید مجازات اسلامی با نگاهی تطبیقی»، فصلنامه دیدگاه‌های حقوق قضایی ، شماره ۵۸، تابستان ۹۱، ص۸۶.

اصل صلاحیت واقعی به معنای توسعه صلاحیت تقنینی و قضایی یک کشور نسبت به جرائمی است که در خارج از قلمرو حاکمیت آن کشور واقع شده و به منافع اساسی آن کشور صدمه وارد می‌کند. در بند (ج) ماده ۲۸ قانون جرائم رایانه‌ای ایران به اصل مذکور اشاره شده است. براساس این بند علاوه بر موارد پیش‌بینی‌شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود: ... ج)جرم توسط هر ایرانی یا غیر ایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای مورداستفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد و موسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه تارنماهای دارای دامنه مرتبه‌بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد ...)[۱]

در خصوص اصل صلاحیت واقعی، قانون جرائم رایانه‌ای به صرف بیان منافع مورد حمایت در فضای سایبر اکتفا کرده و به شرط خاصی اشاره ننموده است. این درحالی است که قانون مجازات اسلامی مصوب ۱۳۹۲ شروطی از قبیل حصری بودن جرائم موضوع اصل صلاحیت واقعی و رعایت قاعده احتساب مجازات‌های قبلی در جرائم تعزیری موضوع این اصل را پذیرفته که قواعد راجع به صلاحیت واقعی در حقوق ایران را به قواعد پذیرفته شده در حقوق بین الملل نزدیک‌تر کرده است.[۲]

راجع به اصل صلاحیت جهانی قابل ذکر است که علاوه بر جرائمی که نظم عمومی داخلی کشورها را مختل می‌کند، جرائمی وجود دارد که به نظم جهانی خدشه وارد می‌کند و جامعه جهانی در پی محاکمه مرتکبان این جرائم می‌باشد. از این رو جرائم مذکور را جرائم بین‌المللی می‌نامند. برای رسیدگی به این جرائم، اصل صلاحیت جهانی وضع شده است که جرائم سایبری هم از همین خصیصه برخوردار می‌باشد.[۳] قانون‌گذار ایران در بند (د) ماده ۲۸ قانون جرائم رایانه‌ای، جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال را موضوع اصل صلاحیت جهانی قرار داده است. به موجب این بند ، دادگاه‌های ایران در «جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیرایرانی باشد»،

۱. جلالی فراهانی، امیرحسین، درآمدی بر آئین دادرسی کیفری جرائم سایبری، تهران، خورسندی، ۱۳۸۹، ص. ۹۲.

۲. جلالی فراهانی، امیرحسین، صلاحیت کیفری سایبری در پرتو قوانین داخلی، در: حقوق فن آوری اطلاعات و ارتباطات (مجموعه مقالات)، انتشارات روزنامه رسمی جمهوری اسلامی ایران، چاپ نخست، ۱۳۸۸، ص. ۵۳.

۳. خالقی، علی، آئین دادرسی کیفری، چاپ نوزدهم، موسسه مطالعات و پژوهش‌های شهر دانش، ۱۳۹۱، ص. ۶۶.

صالح به رسیدگی هستند. قانون‌گذار ایران برای تأکید بر اصل صلاحیت جهانی و تقویت این اصل در حقوق ایران هر گونه پیوند میان ایران و جرم موضوع اصل صلاحیت جهانی، از قبیل تابعیت مرتکب یا بزه‌دیده را نادیده گرفته است. بند مذکور، جرم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال را موضوع اصل صلاحیت جهانی قرار داده است، اما به شرط دیگری برای اعمال این اصل که همان رعایت قاعده منع محاکمه مجدد است، اشاره ننموده است. چه‌بسا که جرائم سایبری دیگری نظیر انتشار ویروس نیز قابلیت آن را دارد که موضوع اصل صلاحیت جهانی قرار گیرد که مورد توجه قرار نگرفته است.[۱]

۳. تعارض صلاحیت‌ها در رسیدگی به جرایم سایبری

تعارض صلاحیت موضوعی است که هم اسناد بین‌المللی و هم قوانین داخلی به آن پرداخته‌اند. در این قسمت به بررسی تعارض‌های صلاحیتی و نحوه رفع تعارض‌ها پرداخته می‌شود. در برخی موارد دولت‌های متعدد با استناد به طیف زیادی از منابع صلاحیتی نسبت به یک جرم سایبری خاص اعمال صلاحیت می‌کنند. برخی از اسناد بین‌المللی و منطقه‌ای چالش صلاحیت «متقارن» را مورد توجه قرار داده‌اند. برای نمونه، برخی از این اسناد تصریح می‌کنند که اگر جرمی تحت صلاحیت بیش از یک دولت باشد و هنگامی که هر یک از دولت‌های مربوطه بتواند به طور معتبر بر مبنای کشف وقایع و ادله وقوع جرم، آن جرم را تحت تعقیب قرار دهد، کشورها باید به منظور تصمیم‌گیری در خصوص صلاحیت مناسب برای تعقیب و رسیدگی با هم همکاری و مشورت نمایند.[۲] به ویژه هدف اسناد اروپایی «متمرکز کردن رسیدگی‌ها در یک کشور واحد» است.[۳] کنوانسیون اتحادیه عرب شیوه مفصلی را به صورت سلسله مراتبی در خصوص برتری ادعاهای صلاحیتی متعارض به شرح زیر بیان می دارد:

(الف) کشوری که امنیت یا منافع‌شان به وسیله جرم مختل شده است؛

(ب) کشوری که جرم در قلمروی آن ارتکاب یافته است؛

(ج) کشور متبوع مرتکب.

---

۱. فروغی، فضل‌اله، و امیر البوعلی، «صلاحیت کیفری مراجع قضایی در فضای سایبر»، مجله تحقیقات حقوقی دانشگاه شهید بهشتی، شماره ۵۸، تابستان ۹۱، ص. ۸۵.

2. Council of Europe Child Protection Convention, Article 25(8); Council of Europe Cybercrime Convention, Article 22(5); EU Decision on Attacks against Information Systems, Article 10(4) and COMESA Draft Model Bill, Article 40(e).

3. EU Decision on Attacks against Information Systems, Article 10(4).

در صورتی که بر اساس این ترتیب، نتوان راه‌حلی را پیدا کرد، اولویت با کشوری است که زودتر درخواست کرده است.[1] کشورها، به طور کلی، قانون مشخصی ندارند که تعارض صلاحیتی در پرونده های جرایم سایبری را حل کند.[2] با وجود این، برخی از کشورها برنامه هایی را در خصوص تعارضات احتمالی صلاحیت در قوانین خاص جرایم سایبری پیش‌بینی کرده‌اند. با وجود این، در مطالعه میدانی سازمان ملل متحد روشن شده است که به نظر برخی از کشورها در جرایم سایبری فرامرزی «طیف گسترده جرایم سایبری و شیوه‌های توسعه قواعد حقوقی صلاحیت، پذیرش انحصاری بودن صلاحیت را دشوار کرده است.»[3]

برخی از کشورها به منظور اجتناب از تحقیقات مضاعف و تعارض‌های صلاحیتی، تلاش می‌کنند تا اختلافات صلاحیتی را با استناد به مشاوره‌های رسمی و غیررسمی با دیگر کشورها حل کنند. از نظر یکی از کشورهای اروپایی «اکثر مواقع می‌توان از طریق مشاوره‌های قبلی غیررسمی یا مبادله همزمان اطلاعات از وقوع تعارض صلاحیت‌ها جلوگیری کرد. همچنین عملیات(های) تحقیقاتی مشترک می‌تواند مؤثر باشد ... .»[4] مکاتبات به طور دوجانبه یا از طریق کانال‌هایی که نهادهایی از قبیل اینترپل، یوروپل و یوروجاست فراهم می‌کنند، انجام می‌شود. از نظر برخی از کشورها، به‌ویژه در قاره آمریکا، از آن‌جا که رسیدگی به این جرایم بسیار دشوار است، لذا رسیدگی‌ها اساساً تنها زمانی شروع می‌شوند که ادله قوی وجود داشته باشد که یا مجرم یا بزه‌دیده، تبعه کشور اعمال‌کننده صلاحیت است. تمام دیگر موارد از طریق اینترپل به کشورهای منشاء وقوع جرم گزارش می‌شوند.[5] افزون بر این، یادآوری اصل منع محاکمه مجدد در این خصوص حایز اهمیت است و رسیدگی‌ها تنها در صورتی شروع می‌شوند که هیچ رسیدگی در کشور محل وقوع جرم صورت نگرفته باشد. برخی از کشورها قبل از این که از ادعای صلاحیت خود منصرف شوند تضمیناتی را لازم می‌دانند، مبنی بر این که دیگر کشور مدعی صلاحیت در خلال تحقیقات و رسیدگی به معیارهای حقوق بشری پایبند باشد.[6]

1. League of Arab States Convention, Article 30(3).
2. United Nations Office on Drugs and Crime, Op. cit., p. 195.
3. Ibid.
4. Ibid.
5. Ibid.
6. Ibid.

در کشور ایران در خصوص تعارض صلاحیت‌ها راجع به جرایم سایبری، قانون جرائم رایانه‌ای و دیگر مقررات جاری ایران در مورد حالتی که چند کشور به دنبال اعمال صلاحیت نسبت به یک جرم سایبری باشند، راه‌حلی ارائه نداده‌اند که از این حیث باید به راه‌حل‌های پیشنهادی در بخش نتیجه‌گیری توجه گردد.[1]

[1]. جلالی فراهانی، امیرحسین، درآمدی بر آئین دادرسی کیفری جرائم سایبری، خورسندی، ۱۳۸۹، ص. ۹۳.

نتیجه

تحلیل مقررات اسناد بین‌المللی و منطقه‌ای و قوانین و رویه کشورها حاکی از آن است که چالش‌های صلاحیتی در خصوص جرایم سایبری با تضمین صراحت و اجرای ابتکاری اصول موجود قابل حل است. از نظر برخی از صاحب‌نظران «اقدامات و مبادلات در فضای سایبری از یک سو مستلزم رعایت اصل صلاحیت سرزمینی در خصوص بزه ارتکابی در قلمرو داخلی یک کشور و از سوی دیگر متضمن آن است که اگر مجرمین به فعالیتی در یک کشور مبادرت می‌نمایند که سبب آثار فراملی در کشور دیگر شده است، کشور اخیر نیز حق اعمال صلاحیت دارد.[1] در نتیجه، دو دسته صلاحیت سرزمینی و صلاحیت مبتنی بر تابعیت تقریباً همواره قابلیت تضمین اعمال صلاحیت کیفری را فراهم می‌نمایند زیرا رابطه کافی یا پیوند واقعی بین جرم سایبری و دست کم یک دولت قابل احراز است. بنابراین، به نظر می‌رسد با عنایت به رویه بین‌المللی دولت‌ها در حال حاضر نیازی به نوع دیگری از صلاحیت نسبت به «فضای سایبری» نیست. اکثریت قابل توجهی از جرایم سایبری مشمول صلاحیت سرزمینی یا صلاحیت مبتنی بر تابعیت هستند و بنابراین به طور واقعی با کشورهای مشخصی مرتبط هستند. نکته قابل توجه آن است که در دنیای امروز، داده‌ها به طور فزاینده‌ای در جریان هستند و از طریق مراکز جهانی داده‌ها پخش می‌شوند، و لذا این واقعیت در حال حاضر بیشتر چالشی برای گردآوری ادلّه ایجاد کرده است تا برای ایجاد و اعمال صلاحیت.

از منظر حقوق بین‌المللی بشر، موضوع صلاحیت فراسرزمینی می‌تواند به چندگانگی محتوای اینترنت مربوط باشد. در دل مباحث صلاحیتی، تفسیر محل عناصر جرم و آثار جرم در چارچوب مرزهای جغرافیایی وجود دارد. این که آیا باید این موضوع از منظر «اعمال»، «رفتار»، «اوضاع و احوال»، «داده‌ها» یا «سیستم‌های رایانه‌ای» بررسی کرد، دارای اهمیت فراوان است.

در نهایت می‌توان این طور نتیجه گرفت که برای حل تعارض‌های صلاحیتی در جرایم سایبری باید به اصول مطلوب و قابل‌قبولی در ایجاد یک «پیوند واقعی» میان جرم، مجرم، بزه‌دیده و حسب مورد ابزار جرم با کشور مدعی اعمال صلاحیت استناد شود و یا با فراهم شدن الحاق کشورها به کنوانسیون جرایم سایبری به رفع تعارض‌ها در زمینه صلاحیت اقدام گردد.

1. David Post, "Against Cyber anarchy", Berkeley Technology Law Journal, Vol. 17, 2002, pp. 1365-1387.

منابع

- آخوندی، محمود، «استرداد بزهکاران»، مجله حقوقی و قضائی دادگستری، سال سوم، شماره هشتم، پائیز ۱۳۷۲.
- آزمایش، علی، «تقریرات درس حقوق بین‌الملل کیفری دوره کارشناسی ارشد»، دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی، نیمسال اول، سال تحصیلی ۱۳۸۳- ۱۳۸۲.
- البوعلی، امیر، صلاحیت محاکم در جرائم سایبری، انتشارات جنگل، ۱۳۹۲.
- پوربافرانی، حسن، تحول اصل صلاحیت واقعی در لایحه جدید مجازات اسلامی با نگاهی تطبیقی، فصل‌نامه دیدگاه‌های حقوق قضایی، شماره ۵۸، تابستان ۹۱.
- جلالی فراهانی، امیرحسین، درآمدی بر آئین دادرسی کیفری جرائم سایبری، خورسندی، ۱۳۸۹.
- ـــــــــــــــــــ، «صلاحیت کیفری سایبری در پرتو قوانین داخلی»، در: حقوق فن آوری اطلاعات و ارتباطات (مجموعه مقالات)، انتشارات روزنامه رسمی جمهوری اسلامی ایران، ۱۳۸۸.
- خالقی، علی، آئین دادرسی کیفری، موسسه مطالعات و پژوهش‌های شهر دانش، چاپ ۱۹، ۱۳۹۱.
- زیبر، اولریش، جرائم رایانه‌ای، ترجمه محمدعلی نوری، و دیگران، گنج دانش، چاپ دوم، ۱۳۹۰.
- فروغی، فضل‌اله، و امیر البوعلی، «صلاحیت کیفری مراجع قضایی در فضای سایبر»، مجله تحقیقات حقوقی، شماره ۵۸، تابستان ۹۱.
- میرمحمد صادقی، حسین، «جرم جاسوسی»، ماهنامه دادرسی، اسفند ۱۳۷۸.
- هیأت مولفان و ویراستاران مایکروسافت، فرهنگ تشریحی کاربران کامپیوتر انتشارات مایکروسافت، ترجمه فرهاد قلی‌زاده نوری، نشر علوم روز، ۱۳۸۰.

- Adel Azzam Saqf Al Hait, "Jurisdiction in Cybercrimes: A Comparative Study", Journal of Law, Policy and Globalization, Vol. 22, 2014.
- Ahlstrom and Others v. Commission of European Communities, ECR 5193, 1988, Case 131/85.

- Antonio Cassese, International Law, Oxford University Press, 2005.
- Bert-Japp Koops, and Susan Brenner, Cybercrime and Jurisdiction: A Global Survey, T.M.C. Asser Press, 2006.
- Bruno Simma, and Andreas Mueller, Exercise and the Limits of Jurisdiction, In: James Crawford, and Martin Koskenniemi (eds), The Cambridge Companion to International Law, Cambridge University Press, 2012.
- Council of Europe Explanatory Report to Convention on Cybercrime, Council of Europe Treaty Series Explanatory Reports (CETSER), 2001, 23 November 2001.
- David Post, "Against Cyber anarchy", Berkeley Technology Law Journal, Vol. 17, 2002.
- Ian Brownlie, Principles of Public International Law, Oxford University Press, 6th ed., 2003.
- Ian Walden, Computer Crimes and Digital Investigations, Oxford University Press, 2007.
- Malcolm Shaw, International Law, Cambridge, 2003.
- Marc Goodman, and Susan Brenner, "The Emerging Consensus on Criminal Conduct in Cyberspace", International Journal of Law and Information Technology, Vol. 10, No.2, 2002.
- Restatement of Foreign Relations Law of the United States the Third, 1987.
- US v. Tsastsin et al, United States District Court, Southern District of New York, No. S2. 11 Cr. 878, 1 March 2001.