مقاله

شاپا

مجلهٔ

پژوهشهای حقوقی

فصلنامه علمی ـ ترویجی

شماره ۳۴

هزار و سیصد و نود و هفت ـ تابستان

شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

http://jlr.sdil.ac.ir/article_67524.html

صلاحیت سرزمینی دادگاه‌های ایران نسبت به جرایم ارتکابی در فضای سایبر

نجمه غفاری الهی کاشانی*

چکیده:

ماهیت خاص فضای سایبر و جرایم ارتکابی در آن باعث شد که قانون‌گذار علی‌رغم وجود مقررات عام در خصوص صلاحیت، در مورد جرایم رایانه‌ای نیز به طور خاص به وضع قاعده بپردازد. به طوری که ابتدا در فصل یکم بخش آیین دادرسی قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۰۳/۰۵ به موضوع صلاحیت پرداخته و سپس بر اساس ماده ۶۹۸ قانون دادرسی کیفری مصوب ۱۳۹۲، با نسخ موارد مربوط به دادرسی در قانون مذکور و اعمال تغییرات جزئی، مقررات مربوط به آیین دادرسی جرایم رایانه‌ای و از جمله بحث صلاحیت را به قانون آیین دادرسی کیفری مصوب ۱۳۹۲/۱۲/۰۴ الحاق نمود. با وجود این بخش آیین دادرسی جرایم رایانه‌ای در قانون آیین دادرسی کیفری، حاوی مقررات ضعیف و مجملی در باب صلاحیت سرزمینی که مهم‌ترین اصل صلاحیتی در عرصهٔ حقوق جزای بین‌الملل محسوب می‌شود، می‌باشد. به طوری که در این بخش برای تعیین قلمرو حاکمیت ایران و محل وقوع جرایم سایبری که دو رکن اصلی برای اعمال صلاحیت سرزمینی محسوب می‌شود، ضابطهٔ دقیقی ارائه نشده است. در مقاله حاضر با ابهام‌زدایی از عبارات مجمل مقررات مربوط به جرایم رایانه‌ای در باب اصل صلاحیت سرزمینی و ارائهٔ راهکارهایی در خصوص خلأهای موجود در این زمینه، ملاحظه می‌شود که چه زمانی دادگاه‌های ایران بر اساس اصل صلاحیتی مذکور نسبت به جرایم سایبری صالح به رسیدگی خواهند بود.

کلیدواژه‌ها:

جرم سایبری، صلاحیت سرزمینی، قلمرو حاکمیت در فضای سایبر، محل وقوع جرم سایبری، آیین دادرسی جرایم رایانه‌ای.

مجلهٔ پژوهشهای حقوقی (فصلنامه علمی - ترویجی)، شمارهٔ ۳۴، تابستان ۱۳۹۷
صفحهٔ ۱۸۵-۲۱۸، تاریخ وصول: ۱۳۹۲/۰۹/۳۰، تاریخ پذیرش: ۱۳۹۲/۱۱/۲۸

* دانشجوی دکترای رشته حقوق کیفری، دانشکده حقوق و علوم سیاسی دانشگاه تهران
Email: n8.ghaffari@yahoo.com

مقدمه

اصل صلاحیت سرزمینی مهم‌ترین اصلی است که کشورها برای اعمال صلاحیت در عرصهٔ حقوق جزای بین‌الملل به آن استناد می‌کنند. اصل مذکور به این معناست که «کلیه جرایم ارتکابی در قلمرو حاکمیت یک کشور به موجب قوانین جزایی همان کشور مورد تعقیب و مجازات قرار می‌گیرند.»[۱] در خصوص اعمال اصل صلاحیت سرزمینی دلایلی ذکر شده که استناد به آن را توجیه می‌کند: «حق حاکمیت دولت ایجاب می‌کند که اوامر و نواهی آن بر تمام اموری که در قلمرو آن در جریان است حکومت و آنها را اداره نماید. به علاوه، حمایت از نظم عمومی به وسیله این اصل بهتر و کامل‌تر صورت می‌گیرد و قانون محل وقوع جرم بهتر می‌تواند لطمه واردشده به این نظم را ارزیابی و نحوه ترمیم آن را تعیین نماید؛ و بالاخره اینکه در این محل، جمع‌آوری آثار و دلایل جرم، استماع شهادت شهود، اخذ نظر کارشناس و احیاناً ملاقات زیان‌دیده آسان‌تر و کم‌هزینه‌تر خواهد بود.»[۲]

برای اعمال اصل صلاحیت سرزمینی توسط دادگاه‌های ایران، ابتدا باید قلمروی حاکمیت کشور را ترسیم کرد و سپس محل وقوع جرم را تعیین نمود. تعیین دو رکن مذکور در فضای واقعی جزء در برخی از صور مشکل ارتکاب جرم، ساده به نظر می‌رسد اما فضای سایبر با ویژگی فرامرزی‌اش این مفاهیم را به چالش کشیده است. ویژگی‌هایی از قبیل بی‌حدومرز بودن فضای سایبر و غیرملموس بودن موضوعات در آن، ترسیم قلمرو حاکمیت کشورها و تعیین محل وقوع جرم در فضای مذکور را دشوار نموده است. دولت‌ها در فضای واقعی در قلمروی سرزمینی خود به اعمال حاکمیت می‌پردازند اما از آنجایی که در فضای سایبر مفهوم قلمرو فیزیکی رنگ باخته، تردیدهایی در خصوص اعمال حاکمیت در آن به وجود آمده است. تعیین محل وقوع جرم در فضایی که افراد و اشیاء از موقعیت فیزیکی برخوردار نیستند، از مسائلی است که ذهن را درگیر می‌کند؛ زیرا به نظر نمی‌رسد در اینجا بتوان به صرف مؤلفه‌های تعیین ارتکاب جرم در فضای واقعی اکتفاء کرد. با توجه به وجود چنین ابهاماتی در اعمال اصل صلاحیت سرزمینی در فضای سایبر، قانون‌گذار ایران مقررات عام موجود در این خصوص را کافی ندانسته و به طور خاص نیز مقرراتی را در این باب وضع نموده است. با

---

۱. مهدی مومنی، *مبانی حقوق جزای بین‌الملل* (تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۱)، چاپ هشتم، ۴۹.

۲. علی خالقی، *جستارهایی از حقوق جزای بین‌الملل* (تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۰)، چاپ دوم، ۳۸.

توجه به ماهیت پیچیدهٔ جرایم سایبری بررسی قواعد راجع به صلاحیت سرزمینی در آن ضروری به نظر می‌رسد. چه در غیر این صورت شاهد تشتت آراء و حتی در مواردی بی‌کیفر ماندن مرتکبین جرایم سایبری خواهیم بود. آنچه ضرورت بررسی فوق را بیشتر نمایان می‌سازد روند رو به افزایش ارتکاب جرایم مذکور در ایران است. چراکه امروزه بسیاری از افراد برای رسیدن به امیال سوء خود ابزارهای سنتی ارتکاب جرم را کنار گذاشته و از فضای سایبر بهره می‌گیرند.

۱- قلمرو حاکمیت و تعیین محل وقوع جرم در فضای سایبر

در بند نخست این قسمت، قلمروی حاکمیت در فضای سایبر را تعیین می‌نماییم، در بند دوم به بررسی نظریاتی که در خصوص تعیین محل وقوع جرایم سایبری مطرح شده می‌پردازیم و در بند سوم موضع حقوق ایران را نسبت به محل وقوع جرم سایبری تحلیل خواهیم نمود.

۱-۱- مفهوم قلمرو حاکمیت در فضای سایبر

قلمروی حاکمیت یک کشور در فضای واقعی شامل قلمروی زمینی، دریایی و هوایی آن کشور می‌باشد اما این قلمرو در فضای سایبر رنگ و بوی دیگری به خود می‌گیرد به طوری که جلوه‌های قلمرو حاکمیتی در این فضا منطبق با ویژگی‌های خاص آن است. برای مثال مراکز داده به عنوان مراکزی که به ارائهٔ خدمات میزبانی در اینترنت می‌پردازند، از جلوه‌های قلمرو حاکمیتی در فضای سایبر محسوب می‌شوند. در فصل اول کنوانسیون جرایم سایبری مصوب هشتم نوامبر ۲۰۰۱، ارائه‌دهندگان خدمات این‌گونه تعریف شده است: «هر نهاد عمومی یا خصوصی که برای کاربران خدمات خود این امکان را فراهم می‌کند که از طریق سیستم‌های رایانه‌ای ارتباط برقرار کنند و هر نهادی که داده‌های رایانه‌ای را برای چنین خدمات ارتباطی یا کاربران چنین خدماتی پردازش و ذخیره می‌نماید.»[۳] به موجب این ماده ارائهٔ خدمات اینترنتی به دو صورت ارائهٔ خدمات دسترسی و میزبانی انجام می‌پذیرد. در قانون مجازات اسلامی در بخش جرایم رایانه‌ای، تعریفی از ارائه‌دهندگان خدمات اینترنتی ارائه نشده و در مواد ۷۴۹ و ۷۵۱ این قانون صرفاً به تکلیف ارائه‌دهندگان خدمات دسترسی و میزبانی در پالایش محتوای مجرمانه اشاره شده است؛ اما منظور از خدمات میزبانی ارائهٔ فضا

3. “Convention on Cyber Crime, Budapest, 23.XI.2001. Chapter I, Article 1,” Council of Europe, accessed July 14, 2018, http//conventions.coe.int/Treaty/en/Treaties/html/185.htm.

به کاربران برای ذخیره اطلاعات آنها در اینترنت است. «بنابراین به اشخاصی که تجهیزات و امکانات لازم را برای ذخیره و عرضه محتوا تهیه کرده و در اختیار کاربران اینترنت قرار می‌دهند، در اصطلاح ارائه‌کننده خدمات میزبانی یا «هاست» می‌گویند.»[۴] در «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای» مصوب جلسه شماره ۴۸۸ شورای عالی انقلاب فرهنگی به تاریخ ۱۳۸۰/۰۸/۱۵ و آیین‌نامه «تأمین، توزیع و عرضه خدمات اینترنت و اینترانت ملی» مصوب جلسه شماره ۱۴ مورخ ۱۳۸۵/۰۵/۰۱ کمیسیون تنظیم مقررات ارتباطات به ارائه‌دهندگان خدمات میزبانی اشاره‌ای نشده است؛ اما از ارائه‌دهندگان این خدمات در آیین‌نامه «مرکز خدمات داده‌اینترنتی (IDC)» مصوب ۱۳۸۳ کمیسیون تنظیم مقررات و ارتباطات رادیویی با عنوان مرکز خدمات داده‌اینترنتی یاد شده است که همچنان که گفته شد از جلوه‌های قلمرو حاکمیتی در فضای سایبر محسوب می‌شود.

بر اساس بند ۱ ماده ۱ آیین‌نامه مذکور، این مرکز، مجتمع ایمن و مقاومی در برابر تهدید و خطا و دارای ارتباطات پرسرعت و پایدار به منظور میزبانی تجهیزات، سرویس‌ها و کاربردهای اطلاعاتی است. مراکز داده جزء قلمروی حاکمیتی کشوری محسوب می‌شوند که در آن به ارائه خدمات می‌پردازند. برای مثال اگر محتویات مجرمانه‌ای از طریق یک مرکز داده که در ایران مستقر است ذخیره شده باشد و در فضای سایبر قرار بگیرد، کشور ایران می‌تواند به استناد صلاحیت سرزمینی که بر قلمرو حاکمیتی خود دارد به جرم ارتکابی رسیدگی نماید.

نام‌های دامنه از دیگر جلوه‌های قلمروی حاکمیتی در فضای سایبر به حساب می‌آید. سایت‌ها بر روی اینترنت با آدرس‌های اینترنتی هویت می‌یابند. آدرس‌های اینترنتی شامل زنجیره‌ای از اعداد هستند که اگرچه به راحتی توسط رایانه قابل شناسایی است اما به خاطر سپردن آنها برای کاربران دشوار است. یک راه برای آسان کردن یادآوری و شناسایی این آدرس‌ها آن است که بین آدرس‌های عددی و حروف الفبایی معادل آنها که نام‌های دامنه نامیده می‌شوند، ارتباط ایجاد کنیم.[۵] نام‌های دامنه «از سوی سازمان پشتیبانی نام‌های دامنه که وابسته به آیکان است به سایت‌ها و قلمروهای فعالیت در فضای مجازی و شبکه جهانی

---

۴. احمد، خرم‌آبادی، *حقوق کیفری فناوری اطلاعات، مسؤولیت کیفری ارائه‌دهندگان خدمات اینترنتی* (اصفهان: دادیار، ۱۳۹۱)، ۵۳.

5. IDA MADIEHA AZMI, "Domain Names and Cyberspace: the Application of Old Norms to New *Problems*," *International Journal of Law and Information Technology* 8 (2000): 194.

اینترنت اختصاص داده می‌شود.»[۶] آنچه در اینجا مدنظر ماست قسمت پایانی نام دامنه است که پسوند ir. (مثلاً در نام دامنه www.ut.ac.ir) نمونه‌ای از آن محسوب می‌شود.

محققین و دانشمندان برای شناسایی و درک بهتر نام‌های سطح بالای دامنه در اینترنت آنها را بر اساس دو محدودهٔ سازمانی و جغرافیایی نام‌گذاری کرده‌اند.[۷] در محدوده سازمانی، اختصاص نام دامنه بر اساس نوع فعالیتی است که سایت‌ها به آن می‌پردازند. برای مثال به سایت‌هایی که به فعالیت تجاری می‌پردازند پسوند com. اختصاص داده می‌شود و یا پسوند edu. به سایت‌هایی اختصاص می‌یابد که به فعالیت‌های آموزشی می‌پردازند. همچنین می‌توان به پسوندهایی از قبیل mil.، org.، net. و ... اشاره کرد. این پسوندها موضوع بحث ما نیستند و از جلوه‌های قلمروی حاکمیت محسوب نمی‌شوند. در محدوهٔ جغرافیایی، نام‌های دامنه بر اساس موقعیت جغرافیایی کشوری که محتویات سایت‌ها مربوط به امور داخلی آن کشور است، اختصاص داده می‌شود. برای مثال نام دامنه ir. به سایت‌هایی که حاوی مسائل مربوط به امور داخلی ایران است اختصاص داده می‌شود یا پسوند us. به کشور آمریکا اختصاص دارد. در خصوص ماهیت این نام‌های دامنه که دامنه مرتبه بالای کد کشوری نامیده می‌شوند، دو استدلال قابل طرح است. بر اساس یک استدلال با توجه به اینکه مثلاً در سایت‌هایی با پسوند fr. تنها مطالب مربوط به کشور فرانسه گنجانیده شده‌اند، نام‌های دامنه کد کشوری بالا، جزء قلمروی حاکمیتی کشورها محسوب می‌شوند؛ اما بر اساس استدلالی دیگر «انطباق این نام‌ها با حوزهٔ حاکمیتی کشورها یک امر تصادفی بیش نیست و نمی‌توان از آن استیلاء و حاکمیت استنتاج کرد. بلکه همان‌طور که در عمل مشاهده می‌شود، اختیار عمل این نام‌ها به عهده مرجعی مافوق کشورها به نام شرکت تخصیص نام‌ها و شماره‌های اینترنتی (ICANN) است که از سال ۱۹۹۸ رسماً عهده‌دار این مسؤولیت شده است.»[۸] با نگاهی به بند ب ماده ۶۶۴ قانون آیین دادرسی کیفری درمی‌یابیم که قانون‌گذار ایران استدلال نخست را پذیرفته و وب‌سایت‌های دارای دامنه بالای کد کشوری را در حکم قلمروی سرزمینی خود دانسته است. چنان که به موجب بند مذکور دادگاه‌های ایران در مورد

---

۶. محمدرضا حافظنیا، *جغرافیای سیاسی فضای مجازی* (تهران: سمت، مرکز تحقیق و توسعه علوم انسانی، ۱۳۹۰)، چاپ اول، ۱۰۱.

۷. مهدی ابراهیمی، *اینترنت* (تهران: کتابدار، ۱۳۸۰)، چاپ دوم، ۴۳.

۸. امیرحسین جلالی فراهانی، *درآمدی بر آیین دادرسی کیفری جرایم سایبری* (تهران: خرسندی، ۱۳۸۹)، چاپ اول، ۶۰.

جرمی که «... از طریق تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یابد.» صالح به رسیدگی خواهند بود.

۱-۲- تعیین محل وقوع جرم در فضای سایبر

یکی از ارکان اعمال اصل صلاحیت سرزمینی تعیین محل وقوع جرم است. از آنجا که در اغلب جرایمی که در فضای واقعی ارتکاب می‌یابند ارکان مادی جرم و نتایج حاصل از آن در مکان واحد محقق می‌گردند، محل وقوع جرم، محل حضور مرتکب جرم می‌باشد؛ اما این ضابطه به تنهایی در تمامی اشکال جرایم راه‌گشا نیست و باید به دنبال ضوابطی دقیق‌تر در این زمینه بود زیرا در مواردی مشاهده می‌شود که بین جرم ارتکابی و نتیجه حاصل از آن فاصله وجود دارد. در واقع در این جرایم نتیجهٔ جرم در محلی متفاوت از محل ارتکاب جرم محقق شده است. به همین دلیل اصل صلاحیت سرزمینی را به دو اصل صلاحیت سرزمینی ذهنی و اصل صلاحیت سرزمینی عینی تقسیم نموده‌اند. مطابق اصل صلاحیت سرزمینی ذهنی، کشوری که بخشی از عناصر متشکله یک جرم در قلمروی سرزمینی آن ارتکاب یافته است صلاحیت رسیدگی به آن جرم را دارد. «اصل صلاحیت سرزمینی عینی نیز مبتنی بر نتایج زیان‌بار عملی است که از خارج از قلمروی سرزمینی آن کشور سرچشمه گرفته است.»[۹] جرایم سایبری با توجه به ماهیت غیرفیزیکی و فرامرزی‌شان صلاحیت سرزمینی را بیشتر به چالش کشیده‌اند به طوری که حتی اگر جرم سایبری علیه قطعه‌های سخت‌افزاری یک رایانه که از ماهیت فیزیکی برخوردارند ارتکاب یابد و آنها را از کار بیاندازد «باز هم به طور قطع نمی‌توان نظر داد که محل وقوع جرم سایبر همان محل وجود قطعه‌های سخت‌افزاری آسیب‌دیده خواهد بود؛ زیرا در قریب به اتفاق این‌گونه جرایم، عمل مجرمانه در مکان دیگری انجام گرفته و فقط نتیجه مجرمانه روی قطعه‌های سخت‌افزاری پدیدار شده است.»[۱۰]

کنوانسیون جرایم سایبری در ماده ۲۲ به اصل صلاحیت سرزمینی اشاره کرده و مقرر داشته است: «هریک از اعضاء باید مقرراتی را که برای اعمال صلاحیت بر جرایم مصرح در کنوانسیون لازم است، وضع کنند؛ زمانی که: الف ـ جرم در قلمرو سرزمینی آنها ارتکاب یابد؛ ب ـ جرم بر روی کشتی که پرچم آن کشور را برافراشته است، ارتکاب یابد؛ ج ـ جرم در

9. Uta Kohl, "Eggs, Jurisdiction and the *Internet*," *International and Comparative Law Quarterly* 51 (2002): 571.

۱۰. مرتضی یوسفی، «بررسی و تبیین جایگاه فضای سایبر به عنوان عامل ارتکاب جرم» (پایان‌نامه کارشناسی ارشد در رشته حقوق جزا و جرم‌شناسی، قم: دانشکده پردیس قم دانشگاه تهران، ۱۳۸۷)، ۱۲۰.

سطح هواپیمایی که بر اساس قانون آن کشور ثبت شده است، ارتکاب یابد. د ـ ...»[11] لکن کنوانسیون ضابطه‌ای را برای تعیین محل ارتکاب جرم ارائه نکرده است. لذا نظریات مختلفی در خصوص محل ارتکاب جرایم سایبری توسط حقوقدانان مطرح شده است. برای مثال گفته شده، محلی که عمل مجرمانه از آنجا شروع شده، موقعیت فیزیکی ابزاری که برای ارتکاب عمل مجرمانه به کار گرفته می‌شود، محلی که هدف و نشانه اعمال مجرمانه است، محلی که محتویات یک وب‌سایت در آنجا در دسترس قرار می‌گیرد یا به عبارت دیگر محلی که محتویات یک وب‌سایت در آن منتشر می‌شود و در نهایت محلی که عمل مجرمانه بر آن تأثیر می‌گذارد، محل ارتکاب جرایم سایبری محسوب می‌شوند.[12] مطابق نظریه‌ای دیگر در جایی که جرایم سایبری بر روی داده‌ها ارتکاب یافته است، مکانی که این داده‌ها دستخوش حمله‌های مجرمانه قرار گرفته‌اند محل وقوع جرم محسوب می‌شود.[13] در این بند به بررسی مهم‌ترین نظریه‌های مطرح‌شده در خصوص محل ارتکاب جرایم سایبری می‌پردازیم و در قسمت بعد موضع حقوق ایران را در این باره ملاحظه خواهیم کرد.

۱-۲-۱- نظریه محل استقرار سیستم‌های رایانه‌ای[14]

بر اساس بند «و» ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲/۱۰/۱۷ سیستم رایانه‌ای «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری ـ نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده‌پیام» عمل می‌کند.» در فصل اول کنوانسیون جرایم سایبری نیز سیستم‌های رایانه‌ای این‌گونه تعریف شده است: «هر دستگاه یا مجموعه‌ای از دستگاه‌های به هم مرتبط که یک یا بیش از یکی از آنها مطابق یک برنامه به پردازش خودکار داده‌ها می‌پردازند.»[15] بنابراین منظور از سیستم‌های رایانه‌ای تنها رایانه‌های شخصی نمی‌باشد، بلکه شامل رایانه‌های سرور که در زمینه دسترس‌پذیری داده‌ها و ارائهٔ

11. "Convention on Cyber Crime, Budapest, 23.XI.2001. Chapter II, Section 3, Article 22," Council of Europe, accessed July 14, 2018, http//conventions.coe.int/Treaty/en/Treaties/html/185.htm.

12. Bernhard Maier, "How Has the Law Attempted to Tackle the Borderless Nature of the *Internet*," *International Journal of Law and Information Technology* 18 (2010): 171.

۱۳. شاهپور دولتشاهی، *صلاحیت قضایی در محیط مجازی، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات* (تهران: دانشگاه شهید بهشتی، دانشکده ادبیات و علوم انسانی، معاونت پژوهشی، ۱۳۸۳)، ۱۵۳.

14. Computer System.

15. "Convention on Cyber Crime, Budapest, 23.XI.2001. Chapter I, Article 1," Council of Europe, accessed July 14, 2018, http//conventions.coe.int/Treaty/en/Treaties/html/185.htm.

خدمات میزبانی فعالیت می‌کنند، نیز می‌شوند. به موجب این نظریه محل ارتکاب جرم در کشوری است که سیستم‌های رایانه‌ای در آن مستقر هستند.

در این قسمت محل استقرار رایانه‌های سرور که یکی از سیستم‌های رایانه‌ای به حساب می‌آید به عنوان محل وقوع جرم مورد بررسی قرار می‌گیرد. علت بررسی رایانه‌های سرور در اینجا به این خاطر است که رایانه‌های شخصی که از دیگر سیستم‌های رایانه‌ای محسوب می‌شوند، در قالب سایر نظریات از جمله نظریه محل حضور بارگذار و پیاده‌ساز مورد تجزیه و تحلیل قرار خواهند گرفت.

بر اساس نظریه سرور، دادگاه‌هایی که رایانه‌های سرور در حوزه آنها مستقر هستند صلاحیت رسیدگی به جرایمی را دارند که در آنها ارتکاب می‌یابند. نظر به اینکه سرورها از موقعیت فیزیکی برخوردار هستند با توسل به این نظریه می‌توان از سد موانعی که به دلیل ماهیت غیرفیزیکی جرایم سایبری در اعمال اصل صلاحیت سرزمینی وجود دارد، عبور کرد؛ اما نکاتی در خصوص عملکرد حقیقی سرورها در فضای سایبر وجود دارد که در انتخاب این نظریه به عنوان ضابطه منطقی در تعیین محل وقوع جرم تردید ایجاد می‌کند. در ذیل به برخی از این نکات اشاره می‌شود:

نکته اول این است که در جایی که یک کاربر محتویات مجرمانه‌ای نظیر هرزه‌نگاری کودکان را در قالب یک فایل در وب‌سایت خود قرار می‌دهد و در واقع آن محتویات را در یک سرور ذخیره می‌کند، چه زمانی عمل مجرمانه در فضای سایبر ارتکاب می‌یابد؟ زمانی که داده‌ها در سرور استقرار می‌یابند یا زمانی که این داده‌ها وارد رایانه پیاده‌ساز می‌شوند و در صفحه نمایشگر رایانه او مشاهده می‌شوند؟ در صورتی که کشورها پاسخ دوم را برای اعمال صلاحیت انتخاب کنند، نظریهٔ سرور ضابطهٔ مناسبی برای تعیین محل وقوع جرم نخواهد بود؛

نکته دوم اینکه ممکن است بخش‌های اساسی یک صفحه وب از طریق سرورهای مختلف که در نقاط مختلف جهان مستقر هستند فراهم شوند. در نتیجه محتمل است که بخش‌هایی از وب‌سایت که دربرگیرنده مطالب قانونی است در سرور واقع در کشور الف قرار داشته باشد و بخشی از آن وب‌سایت که حاوی مطالب مجرمانه است در سرور واقع در کشور ب قرار داشته باشد؛

نکته سوم اینکه یک صفحه وب ممکن است به وب‌سایت‌های دیگری که در کشورهای مختلف قرار دارد، پیوند داشته باشد. در این صورت غیرمنطقی است که بگوییم صفحه وبی که به وب‌سایت‌های حاوی مطالب مجرمانه مانند قماربازی و هرزه‌نگاری که در سرورهای

بیست کشور مختلف قرار دارد، لینک شده است، موضوع قانون هریک از این کشورها و صلاحیت دادگاه‌های آنها باشد؛[۱۶]

نکته چهارم به یکی از خدمات اینترنت که به انباشت موقت از آن یاد می‌شود، مربوط می‌گردد. منظور از انباشت موقت برنامه‌ای است که توسط آن اطلاعاتی که کاربران به آن مراجعه می‌کنند برای مدتی مشخص در رایانه‌های سرور این خدمات ذخیره می‌گردد. «در نتیجه بسیار محتمل است که محتوای در دسترس قرارگرفته، یک کپی و نه اصل آن باشد که این خود تعیین سرور اصلی از میان چندین سرور کپی‌کننده را با مشکلات اجرایی بسیاری مواجه می‌سازد.»[۱۷]

۱-۲-۲- نظریه محل حضور بارگذار و پیاده‌ساز

بارگذار کسی است که اطلاعات مورد نظر خود را در فضای سایبر قرار می‌دهد و پیاده‌ساز کسی است که آن اطلاعات را دریافت می‌کند. نیازی هم نیست که این دو از هویت یکدیگر آگاه باشند. مطابق نظریه محل بارگذاری، محل حضور فردی که یک وب‌سایت یا اطلاعات محتوی مطالب مجرمانه را در فضای سایبر قرار می‌دهد، محل وقوع جرم محسوب می‌شود و مطابق نظریه محل پیاده‌سازی، محلی که پیاده‌ساز در آن مطالب مجرمانه را دریافت می‌کند، محل ارتکاب جرم محسوب می‌شود؛ اما این نظریه نیز معایبی دارد که تمسک به آن را در اعمال اصل صلاحیت سرزمینی دشوار می‌کند. برای مثال ممکن است عمل بارگذاری یک فایل مجرمانه در چندین کشور انجام پذیرد. به این شکل که فراهم‌کننده مطالب مجرمانه در کشور الف حضور داشته باشد و فراهم‌کننده خدمات میزبانی در کشور ب قرار داشته باشد. در این صورت عمل بارگذاری در کشور الف شروع شده و در کشور ب اتمام یافته است. در این میان ممکن است عمل بارگذاری در کشورهایی هم که اطلاعات از طریق آن انتقال یافته است، صورت بپذیرد. در نتیجه امکان دارد تعداد زیادی از کشورها بر اساس نظریه بارگذاری در خصوص آن محتویاتِ مجرمانه ادعای صلاحیت داشته باشند و در نتیجه تعارض صلاحیت‌ها ایجاد شود؛[۱۸] یا در همین مثالی که ذکر شد کشوری هم که کاربر در آنجا مطالب مجرمانه را پیاده‌سازی کرده است، می‌تواند بر اساس نظریه محل حضور پیاده‌ساز ادعای

16. Darrel C. Menthe, "Jurisdiction in Cyberspace: A Theory of International *Spaces*," *Michigan Telecommunications and Technology Law Review* 69 (1998): 80.

۱۷. جلالی فراهانی، پیشین، ۷۲.

18. Susan W. Brenner, and Bert Jaap Koops, "Approaches to Cybercrime *Jurisdiction*," *Journal of High Technology* 5 (2004): 15.

صلاحیت کند. توضیح اینکه تعارض صلاحیت‌ها ممکن است به دو شکل منفی و مثبت در فضای سایبر ظهور کند. تعارض منفی صلاحیت‌ها در خصوص جرایم سایبری زمانی اتفاق می‌افتد که هیچ کشوری ادعای اعمال صلاحیت بر آنها را نداشته باشد. در خصوص جرایمی مانند هک کردن، رایانه‌های مشخصی هدف قرار می‌گیرند. در این موارد کشورها می‌توانند برمبنای موقعیت رایانه یا محلی که جرم در آن تأثیر می‌گذارد اعمال صلاحیت کنند؛ اما در خصوص جرم انتشار ویروس و جرایم مرتبط با محتوا وضعیت متفاوت است. ماهیت این جرایم به گونه‌ای است که در یک مکان مشخص ارتکاب نمی‌یابند، بلکه به طور هم‌زمان در محل‌های متفاوت ارتکاب می‌یابند. در چنین شرایطی اگر شخصی در کشوری که قانونی در خصوص جرایم سایبری ندارد و در واقع پناهگاه امنی برای جرایم سایبری محسوب می‌شود، مرتکب جرم شود، در حالی که او از تابعیت آن کشور نیز برخوردار است، احتمال بروز تعارض منفی صلاحیت‌ها وجود دارد. البته ظهور تعارض منفی صلاحیت‌ها در اینجا امری حتمی نیست چون بر اساس عوامل دیگری مانند تأثیر در قلمروی سرزمینی یک کشور یا گذر کردن داده‌ها از یک قلمرو سرزمینی می‌توان در خصوص جرایم مذکور اعمال صلاحیت نمود مگر اینکه این کشورها تصور کنند که به اندازهٔ کافی به آنها ضرر وارد نشده یا کشورهای دیگر قطعاً در خصوص این جرایم اعمال صلاحیت خواهند کرد.[۱۹] با توجه به ویژگی فرامرزی جرایم سایبری امکان بروز تعارض مثبت صلاحیت در آنها به مراتب بیشتر از تعارض منفی صلاحیت است. مثلاً می‌توان حالتی را تصور نمود که در آن یک فرد ایرانی در فرانسه از طریق سرورهای واقع در کشور آمریکا رایانه‌ای در هلند را هک کند. در این صورت به نظر می‌رسد حداقل چهار کشور آلمان، فرانسه، آمریکا و هلند بتوانند در خصوص جرم ارتکابی اعمال صلاحیت کنند. کنوانسیون جرایم سایبری که مهم‌ترین سند بین‌المللی در زمینه جرایم سایبری محسوب می‌شود در مورد تعارض مثبت صلاحیت‌ها راه‌حل بسیار ضعیفی ارائه نموده است. به موجب بند ۵ ماده ۲۲ این کنوانسیون:

«در صورتی که بیش از یک عضو نسبت به یک جرم سایبری که در کنوانسیون مقرر شده ادعای صلاحیت داشته باشد، اعضاء باید در صورت اقتضاء به شور نشسته و مناسب‌ترین کشور را برای اعمال صلاحیت و تعقیب مرتکب تعیین نمایند.»[۲۰] به نظر می‌رسد راه‌حل

19. Ibid, 40.
20. "Convention on Cyber Crime, Budapest, 23.XI.2001. Chapter II, Section 3, Article 22," Council of Europe, accessed July 14, 2018, http//conventions.coe.int/Treaty/en/Treaties/html/185.htm.

ارائه‌شده در کنوانسیون فاقد هرگونه ضمانت اجرایی می‌باشد. چراکه ممکن است کشورها از اعمال حاکمیت خود دست نکشند و حاضر به مشورت برای تعیین دادگاه صالح نگردند. در نتیجه هریک از کشورها خود را صالح به رسیدگی می‌دانند و در صورت دسترسی به مرتکب وی را محاکمه خواهند نمود. در چنین حالتی احتمال محاکمه مجدد مرتکبین جرایم سایبری بیشتر می‌شود که این خلاف عدالت می‌باشد. حتی در فرض پذیرفتن این راه‌حل توسط اعضاء، باز این سؤال مطرح می‌شود که بر اساس چه معیارهایی می‌توان از میان کشورهای مدعی صلاحیت یکی از آنها را برای رسیدگی به جرم ارتکابی برگزید؟ نه‌تنها در قانون جرایم رایانه‌ای که در سایر قوانین جاری ایران نیز در خصوص این تعارض‌ها راه‌حلی ارائه نگردیده است.

نکته دیگر اینکه اگرچه بارگذار باید نسبت به مطالبی که در فضای سایبر در دسترس تمام نقاط جهان قرار می‌گیرد، هشیار باشد،[۲۱] لکن در نظر گرفتن محل پیاده‌سازی داده‌ها به عنوان محل ارتکاب جرم مستلزم این است که فرد بارگذار مطالبی را که می‌خواهد در فضای سایبر قرار دهد مطابق قوانین تمام کشورهایی نماید که این مطالب ممکن است در آنها پیاده‌سازی شود. این ناعادلانه به نظر می‌رسد که یک بارگذار به صرف دسترسی مطالبش در کشورهایی که او کوچک‌ترین شناختی نسبت به قوانین آنها ندارد موضوع این قوانین قرار بگیرد و در صورت نقض آنها مجرم شناخته شده و در دادگاه‌های کشورهای مذکور محاکمه شود.

با توجه به معایبی که برشمرده شد سیستمی پیشنهاد شده است که در آن برای اعمال صلاحیت سرزمینی دو نظریه محل بارگذاری و پیاده‌سازی و نظریه محل استقرار سرور در کنار هم قرار می‌گیرند. به موجب این دیدگاه اگر عمل بارگذاری محتویات یک وب‌سایت به طور کامل در قلمروی حکومتی صورت بگیرد که سرور آن وب‌سایت نیز در آن قلمرو قرار دارد، اعمال صلاحیت بر آن وب‌سایت بر اساس نظریه سرور به جای محل حضور بارگذار هیچ تفاوتی جز در نظریه‌پردازی ایجاد نمی‌کند و از این طریق می‌توان از سد معایبی که در بالا ذکر شد عبور کنیم. اما در جایی که محل بارگذاری با محل استقرار سرور متفاوت است برای اعمال نظریه سرور باید اثبات شود که عمل بارگذاری، در قلمروی سرزمینی حکومتی که سرور در آن قرار دارد تأثیر گذاشته است. این تأثیر باید به اندازه‌ای باشد که امکان اعمال

21. Oren Bigos, "Jurisdiction over Cross-Border Wrongs on the *Internet*," *International and Comparative Law Quarterly* 54 (2005): 619.

صلاحیت سرزمینی عینی یا صلاحیت محل تحقق اثر جرم را که در آینده به تبیین آن خواهیم پرداخت، فراهم کند.[۲۲]

۱-۲-۳- نظریه محل وب‌سایت

این نظریه محل استقرار وب‌سایت را محل ارتکاب جرم می‌داند. منظور از محل استقرار وب‌سایت، محل استقرار ارائه‌دهندگان خدمات دسترسی به اینترنت[۲۳] می‌باشد. مطابق نظریه فوق موقعیت فیزیکی ارائه‌دهندگان خدمات اینترنتی که امکان اتصال کاربران را به اینترنت فراهم می‌کنند محل وقوع جرم محسوب می‌شود.

اگرچه این نظریه از محاسنی از قبیل سهولت دسترسی به مدارک ناشی از جرم و شناسایی ایجادکنندگان وب‌سایت برخوردار است اما ممکن است که کاربران در هنگام اتصال به اینترنت از خدمات ارائه‌دهندگان اینترنتی که در دیگر نقاط جهان قرار دارند استفاده کنند.[۲۴] در این حالت چنانچه کاربران قربانی جرمی شوند که از طریق یک وب‌سایت که ارائه‌دهندگان آن در کشور دیگری قرار دارند، علیه آنها ارتکاب یافته است، دادگاه صالح به رسیدگی به این جرم ممکن است در کشوری قرار داشته باشد که کیلومترها با کشور بزه‌دیده فاصله دارد که این مسئله از اشکالات این نظریه است.

نکته دیگر اینکه ارتباطات اینترنتی میان افرادی با موقعیت‌ها و هویت‌های ناشناس و نامشخص صورت می‌گیرد. از این رو یک کاربر نمی‌تواند موقعیت فیزیکی ارائه‌دهنده خدماتی که امکان دسترسی او را به یک وب‌سایت فراهم کرده، تعیین کند. ارائه‌دهندگان خدمات اینترنتی نیز نمی‌توانند موقعیت حقیقی افرادی را که با هویت‌های مجعول و ناشناس وارد فضای سایبر می‌شوند شناسایی کنند.[۲۵]

با وجود اشکالاتی که نظریه محل وب‌سایت دارد برخی از محاکم ایالتی کشور آمریکا این نظریه را در مواردی اعمال کرده‌اند، البته این محاکم بین وب‌سایت‌های فعال و منفعل تمایز قائل شده‌اند. محاکم مذکور تنها بر وب‌سایت‌های فعال اعمال صلاحیت کرده‌اند. وب‌سایت‌های فعال وب‌سایت‌هایی هستند که کاربران با آنها روابط متقابل دارند مثلاً کاربران از طریق آنها به انعقاد قرارداد یا انجام دادوستدهای تجاری می‌پردازند. وب‌سایت‌های منفعل

22. Menthe, op.cit., 79.
23. ISP (Internet Service Provider).
۲۴. جلالی فراهانی، پیشین، ۸۲.
25. Allan R. Stein, "The Unexceptional Problem of Jurisdiction in *Cyberspace*," *The International Lawyer* 32 (1998): 1172.

صرفاً اطلاعاتی را در اختیار افرادی که وب‌سایت را ملاحظه می‌کنند قرار می‌دهند. این وب‌سایت‌ها اجازهٔ روابط متقابل بین میزبان وب‌سایت و کاربر را نمی‌دهند.[۲۶]

اما تشخیص وب‌سایت فعال از منفعل همیشه آسان نیست؛ زیرا اولاً تعداد زیادی وب‌سایت وجود دارد که به طور مطلق نمی‌توان گفت که آنها فعال یا منفعل هستند. ثانیاً وب‌سایت‌های بسیاری هستند که ممکن است آنچه به نظر می‌رسند نباشند برای مثال سایت‌هایی مانند چت‌روم‌های آنلاین ممکن است فعال به نظر برسند اما دادگاه‌ها آنها را منفعل توصیف کرده‌اند. ثالثاً معیارهایی که وب‌سایت فعال و منفعل را تعیین می‌کند دائماً در حال تغییر است.[۲۷]

۱-۲-۴- نظریه محل تحقق اثر جرم یا صلاحیت سرزمینی عینی

با توجه به دشواری که در تشخیص وب‌سایت فعال از منفعل وجود داشت رویکرد جدیدی ایجاد شد که در آن به محلی که عمل مجرمانه در آن تأثیر زیان‌بار می‌گذارد توجه شد. زمانی می‌توان به این رویکرد که نظریه محل تحقق اثر جرم نامیده می‌شود استناد کرد که عمل مجرمانه‌ای که در یک حکومت ارتکاب یافته منجر به ایراد صدمه و آسیب در حکومت دیگری گردد.[۲۸] این نظریه که در قوانین کلاسیک جزایی به عنوان اصل سرزمینی عینی شناخته شده است تنها ناظر به جرایم مقید نمی‌باشد چرا که برخی از جرایم مطلق که در فضای سایبر ارتکاب می‌یابند اثرات بسیار زیان‌باری در غیر از محلی که ارتکاب یافته‌اند برجا می‌گذارند و نظریه فوق در خصوص آنها قابل اجراست.[۲۹]

با توجه به اینکه بسیار محتمل است که جرایم سایبری در قلمرو سرزمینی کشورهای متعددی تأثیر بگذارند و در نتیجه همه این کشورها به دنبال اعمال صلاحیت در خصوص این جرایم باشند نظریه دیگری مطرح شد که به موجب آن فقط کشوری که به صورت قابل ملاحظه و چشم‌گیری هدف فعالیت‌های آنلاین قرار گرفته و جرایم سایبری تأثیر زیان‌بار

26. Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in EU, US and China* (New York: Cambridge University Press, 2010), 69.

27. Adam Thierer, and Clyde Wayne Jr Crews, *Who Rules the Net?* (Washington, D.C: CATO Institute, 2003), 104.

28. Stephan Wilske, and Teresa Schiller, "International Jurisdiction in Cyberspace: Which States May Regulate the *Internet?*," *Federal Communications Law Journal* 50 (1997-1998): 130.

۲۹. فضل‌الله فروغی و امیر البوعلی، «صلاحیت کیفری مراجع قضایی در فضای سایبر» *مجله تحقیقات حقوقی* ۵۸ (۱۳۹۱)، ۳۲۰.

قابل توجهی بر آن گذاشته است صلاحیت رسیدگی به جرایم مذکور را داشته باشد.[۳۰] اما این نظریه نیز خالی از اشکال نیست زیرا اولاً تنها کشورهایی که جرم ارتکابی در آنها تأثیر چشم‌گیر گذاشته است می‌توانند اعمال صلاحیت کنند. ثانیاً اتفاق نظر در خصوص ضوابطی که تعیین می‌کنند کدام کشور هدف فعالیت‌های آنلاین قرار گرفته است، دشوار به نظر می‌رسد.[۳۱]

۱-۲-۵- نظریه محل حضور فیزیکی بزه‌دیده

مطابق این نظریه محل حضور فیزیکی بزه‌دیده محل ارتکاب جرم محسوب می‌شود؛ اما این نظریه معیار معقولی در تعیین محل وقوع جرم در جرایم سایبری به خصوص جرایم مرتبط با محتوا نیست. برای مثال در سخنرانی تنفرآمیزی که یهودیان را هدف قرار داده فرض می‌شود که تمام یهودیان بزه‌دیدهٔ آن واقع شده‌اند؛ اما آیا معقول است که بر اساس این نظریه، هر کشوری که مقرراتی در خصوص سخنرانی تنفرآمیز دارد و شهروندان یهودی در قلمرو سرزمینی آن کشور حضور دارند، بتواند اعمال صلاحیت کند؟ مثال دیگر اینکه هرزه‌نگاری کودکان در کشورهای بسیاری جرم‌انگاری شده است. اگر ادعا کنیم که تمام کودکان قربانیان بالقوه این جرایم هستند این نتیجه را در پی دارد که کشور الف که هرزه‌نگاری کودکان را جرم‌انگاری کرده بر اساس این ادعا که هرزه‌نگاری که در کشور ب صورت گرفته، اشخاص هوسران در کشور الف را تحریک کرده، بتواند بر هرزه‌نگاری که در کشور ب تولید شده اعمال صلاحیت بکند. اگر کشور الف واقعاً بتواند اثبات کند که هرزه‌نگاری مجازی کودکان که در کشور ب تولید شده منجر به ارتکاب جرم علیه شهروندانش در قلمرو سرزمینی آن می‌شود و در واقع در قلمروی سرزمینی آن تأثیر می‌گذارد، این کشور اجازه اعمال صلاحیت را خواهد داشت. به عکس اگر پیوندی میان این هرزه‌نگاری و جرایم ارتکابی علیه کودکان در کشور الف وجود نداشته باشد، امکان اعمال صلاحیت کشور الف در این مورد وجود ندارد.[۳۲] بنابراین با توجه به اینکه اغلب جرایم سایبری در سطح وسیعی ارتکاب می‌یابند و تعداد بزه‌دیدگان آنها بسیار زیاد است، تمسک به این نظریه احتمال بروز تعارض صلاحیت‌ها را بیشتر می‌کند.

30. Uta Kohl, *Jurisdiction and the Internet (Regulatory Competence over Online Activity)* (New York: Cambridge University Press, 2007), 26.
31. Adithya S V Vidyasagar, "Jurisdictional Issues in Cyber *Space*," *Acta Iuridica Olomucensis* 5 (2010): 40.
32. Brenner, op.cit., 17, 18.

۱-۲-۶- نظریه محل حضور فیزیکی مرتکب جرم

محل حضور مرتکب جرم رایج‌ترین شیوه در تعیین محل وقوع جرایم در فضای واقعی محسوب می‌شود؛ اما این ضابطه در جرایم سنتی که محل حضور مرتکب و نتیجه در یک مکان محقق نمی‌گردد به چالش کشیده شد و نظریه صلاحیت سرزمینی عینی در جهت حل این معضل مطرح گردید. با توجه به اینکه احتمال وجود فاصله بین دو محل مذکور در جرایم سایبری با توجه به ویژگی‌های خاص آن به مراتب بیشتر است توسل به این نظریه مطلوب به نظر نمی‌رسد.

اشکال توسل به نظریه فوق خصوصاً در جایی رخ می‌نماید که بزهکار و بزه‌دیدهٔ جرم سایبری در دو قلمرو حاکمیتی متفاوت حاضر باشند و کشوری که بزهکار در آن حضور دارد عمل ارتکابی توسط او را جرم نداند مانند موضوع اسپم (Spam) که در تعداد معدودی از کشورها جرم انگاری شده است.[۳۳]

۱-۳- موضع حقوق ایران نسبت به محل وقوع جرایم سایبری

بعد از بررسی مهم‌ترین نظریات مطرح‌شده در خصوص تعیین محل وقوع جرایم سایبری، اینک موضع حقوق ایران را در این باره ملاحظه می‌نماییم. با بررسی قوانین جاری در این حوزه درمی‌یابیم که در حالت‌های زیر دادگاه‌های ایران صلاحیت سرزمینی در رسیدگی به جرایم سایبری را خواهند داشت، در واقع در صُور زیر کشور ایران محل وقوع جرم سایبری محسوب می‌شود:

الف ـ ذخیره داده‌های مجرمانه در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های دادهٔ مستقر در قلمروی سرزمینی ایران

به نظر می‌رسد بند الف ماده ۶۶۴ قانون آیین دادرسی کیفری، نظریه محل استقرار سیستم‌های رایانه‌ای را پذیرفته که پیشتر به تبیین آن پرداختیم.[۳۴] البته این ماده از سامانه‌های رایانه‌ای سخن گفته که می‌توان آن را معادل سیستم‌های رایانه‌ای دانست. بر اساس ماده مذکور: «علاوه بر موارد پیش‌بینی‌شده در دیگر قوانین، دادگاه‌های ایران صلاحیت رسیدگی به موارد زیر را دارند: الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته‌اند که به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های دادهٔ

۳۳. محمدرضا زندی، «صلاحیت در جرایم سایبری»، *ماهنامه قضاوت* ۶۰ (۱۳۸۸)، ۴۹.

۳۴. صفحه ۱۹۳ همین اثر، نظریه محل استقرار سیستم‌های رایانه‌ای.

موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شود ...» این ماده علاوه بر محل استقرار سیستم‌های رایانه‌ای در قلمروی سرزمینی ایران، محل استقرار سامانه‌های مخابراتی و حامل‌های داده در این قلمرو را نیز محل وقوع جرم دانسته است. به نظر می‌رسد که منظور از سامانه‌های مخابراتی ابزارهایی نظیر تلفن ثابت و همراه، بی‌سیم و ... باشد. منظور از حامل‌های داده نیز به موجب بند ت ماده ۱ «آیین‌نامه ساماندهی و توسعه رسانه‌ها و فعالیت‌های فرهنگی دیجیتال» مصوب ۱۳۸۹/۰۵/۲۴ هیئت وزیران، ابزاری نظیر لوح فشرده است که داده به منظور تبادل یا عرضه بدون استفاده از شبکه، بر روی آن ذخیره می‌گردد؛ بنابراین چنانچه شخصی داده‌های مجرمانه مانند هرزه‌نگاری کودکان که در سرور مستقر در کشور دیگر ذخیره شده را در یک لوح فشرده یا یک کارت حافظه موجود در قلمروی سرزمین ایران ذخیره کند، دادگاه‌های ایران نسبت به جرم این شخص صالح به رسیدگی خواهند بود.

ب ـ ارتکاب جرم از طریق وب‌سایت‌های دارای دامنه مرتبهٔ بالای کد کشوری ایران

مطابق بند ب ماده ۶۶۴ قانون آیین دادرسی کیفری نیز در صورتی که «جرم از طریق تارنماهای دارای دامنهٔ مرتبهٔ بالای کد کشوری ایران ارتکاب یابد.»، دادگاه‌های ایران صالح به رسیدگی خواهند بود. همان‌طور که پیشتر بیان شد[۳۵] ماده فوق وب‌سایت‌های دارای دامنهٔ مرتبهٔ بالای کد کشوری یا همان ir. را در حکم قلمروی سرزمینی ایران دانسته است. لذا چنانچه جرمی از طریق آنها ارتکاب یابد گویی در قلمروی سرزمینی ایران ارتکاب یافته و دادگاه‌های ایران نسبت به آن صالح به رسیدگی خواهند بود.

ج ـ حصول نتیجه جرم در قلمروی حاکمیتی ایران

به نظر می‌رسد بنا بر صدر ماده ۶۶۴ قانون آیین دادرسی کیفری که مقرر می‌دارد: «علاوه بر موارد پیش‌بینی‌شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود: ...» سایر قوانین موجود در خصوص صلاحیت در حوزه جرایم سایبری همچنان مُجراست؛ بنابراین برای تعیین صلاحیت دادگاه‌های ایران در ارتباط با جرایم سایبری می‌توان به مواد ۳ تا ۸ قانون مجازات اسلامی مصوب ۱۳۹۲/۰۲/۰۱ نیز استناد نمود. در ارتباط با اصل صلاحیت سرزمینی در جرایم سایبری می‌توان به ماده ۴ قانون مذکور اشاره نمود که مقرر می‌دارد: «هرگاه قسمتی از جرم یا نتیجهٔ آن در قلمرو حاکمیت ایران واقع شود در حکم جرم

۳۵. صفحه ۱۸۹ همین اثر، مفهوم قلمرو حاکمیت در فضای سایبر.

واقع‌شده در جمهوری اسلامی ایران است.» آن قسمت از ماده که وقوع نتیجهٔ جرم در قلمروی حاکمیت ایران را در حکم جرم واقع‌شده در کشورمان دانسته، به نظریه صلاحیت محل تحقق اثر یا صلاحیت سرزمینی عینی اشاره دارد.

اما عنصر مادی جرایم سایبری نیز همانند جرایم ارتکابی در فضای واقعی، همیشه به شکل ساده، آنی و مباشرت واقع نمی‌شود و امکان ارتکاب این جرایم به صورت مستمر، مرکب، معاونت و ... وجود دارد؛ بنابراین ضروری است که محل ارتکاب جرم سایبری را در این صور مشکل نیز تعیین نماییم تا ملاحظه کنیم که دادگاه‌های ایران در چه صورتی صلاحیت رسیدگی به این فروض را خواهند داشت.

۱-۳-۱- جرایم مستمر

جرم مستمر جرمی است که عنصر مادی آن در طول زمان استمرار می‌یابد. «این استمرار ممکن است مبین قصد مجرمانه فاعل (جرم مستمر پیاپی) و یا ناشی از طبیعت عمل باشد (جرم مستمر دائم). جرایم مستمر دائم جرایمی هستند که عناصر تشکیل‌دهنده آنها در زمانی معلوم و یکباره فراهم می‌آیند، ولی آثار آنها در طول زمان ادامه دارد. ... در ارتکاب جرایم مستمر پیاپی ... سوءنیت فاعل در هر آن تجدید می‌شود. به سخن دیگر، استمرار جرم ناشی از اراده و عزم مرتکب و به گونه‌ای است که در هر لحظه جرم با تمام عناصر تشکیل‌دهنده آن تکرار می‌شود.»[۳۶]

اگرچه در جرایم سایبری با فشار چند دکمه و در کوتاه‌ترین زمان ممکن می‌توان مرتکب جرم شد اما عنصر مادی جرایم مذکور همیشه به صورت آنی واقع نمی‌شوند. برای مثال در انتشار محتویات مستهجن در فضای سایبر با اینکه این محتویات در یک لحظه در فضای سایبر قرار می‌گیرد اما آثار آن در طول زمان ادامه خواهد داشت به طوری که محتویات مذکور در هر لحظه از زمان برای کاربران حاضر در نقاط مختلف جهان قابل دسترس است. در واقع می‌توان انتشار محتویات مستهجن در فضای سایبر را از دستهٔ جرایم مستمر دائمی دانست.

در خصوص دادگاه صالح به رسیدگی جرایم مستمر پیاپی سه نظریه ابراز شده است: «۱- قبول صلاحیت محلی که جرم در آنجا شروع شده است؛ ۲- قبول صلاحیت محلی که استمرار در آنجا قطع شده است؛ ۳- قبول صلاحیت کلیه محل‌هایی که استمرار در آنجا

---

۳۶. محمدعلی اردبیلی، *حقوق جزای عمومی* (تهران: میزان، ۱۳۹۱)، چاپ بیست و هشتم، ۱۶۶.

جریان داشته است؛ با پذیرش این نکته که حق تقدم با دادگاهی است که رسیدگی را زودتر شروع کرده باشد.»[۳۷] دیدگاه سوم منطقی‌تر به نظر می‌رسد بنابراین دادگاهی صالح به رسیدگیِ جرایم مستمر است که حالت استمرار در حوزهٔ آن دادگاه محقق شده باشد. این راه‌حل مربوط به جرم مستمر پیاپی است اما در خصوص جرایم مستمر دائمی که امکان ارتکاب جرایم سایبری به این صورت بیشتر است دادگاه‌های ایران زمانی صلاحیت رسیدگی به این جرایم را دارند که جرم ارتکابی در قلمروی حاکمیتی ایران تأثیر داشته باشد.

۱-۳-۲- جرایم مرکب

جرم مرکب جرمی است که عنصر مادی آن از ترکیب چند عمل تشکیل یافته‌است. در واقع با انجام مجموع اعمالی که قانون‌گذار آنها را به عنوان عنصر مادی یک جرم تبیین کرده، جرم مذکور تحقق می‌یابد. کلاهبرداری که در فضای سایبر ارتکاب می‌یابد از جرایم مرکب محسوب می‌شود. عنصر مادی کلاهبرداری سایبری به موجب ماده ۷۴۱ قانون مجازات اسلامی از دو عمل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه و تحصیل وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تشکیل شده است. در صورتی که یکی از دو عمل مذکور در ماده ۷۴۱ قانون مجازات اسلامی در قلمروی سرزمینی ایران به وقوع بپیوندد دادگاه‌های ایران مطابق ماده ۴ قانون مجازات اسلامی ۱۳۹۲ صالح به رسیدگی می‌باشند؛ بنابراین در مواردی که یکی از اجزای عنصر مادی جرم مرکبِ سایبری، در قلمروی سرزمین ایران واقع شود، دادگاه‌های ایران صلاحیت رسیدگی به آن جرم را خواهند داشت؛ اما در خصوص حالتی که هریک از اجزای جرم کلاهبرداری سایبری در دو محل مختلف در قلمروی سرزمینی ایران ارتکاب یابد، رأی وحدت رویه شماره ۷۲۹-۱۳۹۱/۱۲/۰۱ مقرر داشته: «نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز مستفاد 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 برداشت شده در حوزه آن قرار دارد، صالح به رسیدگی است. بنا به مراتب آرای شعب یازدهم و سی و

۳۷. محمود آخوندی، *آیین دادرسی کیفری* (تهران: سازمان و صلاحیت مراجع کیفری، تهران، وزارت فرهنگ و ارشاد اسلامی؛ سازمان چاپ و انتشارات، ۱۳۹۰)، چاپ سیزدهم، ۲۸۵.

دوم دیوان عالی کشور که بر اساس این نظر صادر شده به اکثریت آراء صحیح و قانونی تشخیص داده و تأیید می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی کشور و دادگاه‌ها لازم‌الاتباع است.» چنان که ملاحظه شد رأی مذکور نسبت به تعیین دادگاه صالح در جرایم سایبری مرکب که یک قسمت از آن در قلمروی سرزمینی ایران و قسمت دیگر در خارج از ایران ارتکاب یافته کاربرد ندارد، بلکه آن ناظر به تعیین صلاحیت محلی داخلی کشورمان است.

۱-۳-۳- جرایم به عادت

«مقصود از جرم به عادت جرمی است که مانند جرم ساده با تشکیل عناصر جرم زاده می‌شود ولی مجازات آن مشروط به آن است که چند بار و به کرات انجام شود و به شکل عادت درآید بی‌آنکه ضرورتاً عنوان خاص تکرار جرم پیدا کند.»[۳۸] در خصوص اینکه این جرایم با چند بار تکرار محقق می‌شوند دیوان کشور ایران حداقل دو بار انجام عمل مجرمانه را ضروری دانسته و تفاوتی نیز از جهت فاصله بین این دو عمل در نظر نگرفته است.[۳۹] در مورد جرایم سایبری به عادت می‌توان به تبصره ۳ ماده ۷۴۲ قانون مجازات اسلامی که برای حرفه قرار دادن اعمال انتشار، توزیع، معامله محتویات مستهجن یا تولید یا ذخیره و نگهداری آنها به قصد تجارت یا افساد حداکثر هر دو مجازات مقرر در ماده مذکور را تعیین نموده و به تبصره ماده ۷۵۳ قانون مذکور که مطابق آن هرکس تولید یا انتشار یا توزیع و در دسترس قرار دادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرایم رایانه‌ای به کار می‌رود یا فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند یا انتشار یا در دسترس قرار دادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی را حرفه خود قرار بدهد به حداکثر هر دو مجازات مقرر در ماده ۷۵۳ محکوم می‌شود، اشاره کرد. لازم به ذکر است که حرفه قرار دادن اعمال فوق که موجب

۳۸. رضا نوربها، *زمینه حقوق جزای عمومی* (تهران: کتابخانه گنج دانش، ۱۳۹۱)، چاپ سی و سوم، ۲۳۱.
۳۹. همانجا.

تشدید مجازات می‌گردد، جرم به عادت محسوب می‌شود. چرا که بر اساس مواد ۷۴۲ و ۷۵۳ قانون مجازات اسلامی به صرف یکبار انجام دادن این اعمال نیز مرتکب مجازات می‌گردد.

دادگاهی صلاحیت رسیدگی به جرایم سایبری به عادت را دارد که حالت به عادت در قلمرو آن حادث شده باشد. برای مثال اگر شخصی به طور مکرر اقدام به انتشار محتویات مستهجن در سامانه‌های رایانه‌ای یا مخابراتی واقع در قلمروی حاکمیتی ایران بنماید، به طوری که حاکی از آن باشد که این عمل را حرفهٔ خود قرار داده است، دادگاه‌های ایران صلاحیت رسیدگی به جرم این شخص را خواهند داشت.

۱-۳-۴- شروع به جرم

«عبور از قصد مجرمانه و عملیات مقدماتی و ورود در مرحله اجرایی جرم را، به نحوی که اعمال انجام‌شده متصل به جرم باشد، شروع به آن جرم گویند مشروط بر آنکه بزه به طور کامل واقع نشود و زیر عنوان جرم تام قرار نگیرد.»[۴۰]

در قانون جرایم رایانه‌ای به شروع به جرم اشاره‌ای نشده است اما شاید دلیل این امر آن بوده است که در قانون جدید مجازات اسلامی که هم‌زمان با قانون جرایم رایانه‌ای تحت بررسی نمایندگان مجلس قرار گرفته بود، حکم کلی شروع به جرم بیان شده است. ضمن اینکه در خود قانون جرایم رایانه‌ای مقرر شده بود که مواد آن به قانون مجازات اسلامی ملحق گردد؛ بنابراین با تصویب قانون مذکور، حکم ماده ۱۲۲ آن در باب شروع به جرم به استناد ماده ۵۵ قانون جرایم رایانه‌ای[۴۱] به این قانون نیز تسری می‌یابد. ماده ۱۲۲ قانون مجازات اسلامی مصوب ۱۳۹۲ مقرر می‌دارد که:

«هرکس قصد ارتکاب جرمی کند و شروع به اجرای آن نماید لکن به واسطه عامل خارج از اراده او قصدش معلق بماند، چنانچه اقدامات انجام‌گرفته جرم باشد به مجازات همان جرم محکوم و در غیر این صورت به شرح زیر مجازات می‌شود:

۱- در جرایمی که مجازات قانونی آنها سلب حیات، حبس دائم یا حبس تعزیری درجه یک تا سه است به حبس تعزیری درجه چهار؛

---

۴۰. همان، ۲۱۹.

۴۱. ماده ۵۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸: «شماره مواد (۱) تا (۵۴) این قانون به عنوان مواد (۷۲۹) تا (۷۸۲) قانون مجازات اسلامی (بخش تعزیرات) با عنوان فصل جرایم رایانه‌ای منظور و شماره ماده (۷۲۹) قانون مجازات اسلامی به شماره (۷۸۳) اصلاح گردد.»

۲- در جرایمی که مجازات قانونی قطع عضو یا حبس تعزیری درجه چهار است به حبس تعزیری درجه پنج؛

۳- در جرایمی که مجازات قانونی آنها شلاق حدی یا حبس تعزیری درجه پنج است به حبس تعزیری یا شلاق یا جزای نقدی درجه شش، تبصره ـ هرگاه رفتار ارتکابی ارتباط مستقیم با ارتکاب جرم داشته باشد، لکن به جهات مادی که مرتکب از آنها بی‌اطلاع است وقوع جرم غیرممکن شود، اقدام انجام‌شده در حکم شروع به جرم است.» بر اساس ماده ۱۹ این قانون، منظور از حبس تعزیری درجه یک حبس بیش از بیست و پنج تا سی سال، حبس تعزیری درجه دو، حبس بیش از پانزده سال تا بیست و پنج سال، حبس تعزیری درجه سه، حبس بیش از ده تا پانزده سال، حبس تعزیری درجه چهار، حبس بیش از پنج تا ده سال و حبس تعزیری درجه پنج، حبس بیش از دو تا پنج سال می‌باشد. اگرچه تشخیص شروع به جرم در جرایم سایبری با توجه به سرعت بسیار بالای ارتکاب آنها دشوار است اما با در نظر گرفتن دو ماده ۱۲۲ و ۱۹ قانون مجازات اسلامی ۱۳۹۲ و مجازات جرایم تام سایبری در قانون جرایم رایانه‌ای می‌توان گفت که شروع به افشاء یا در دسترس قرار دادن داده‌های سری در حال انتقال یا ذخیره‌شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت، دولت، سازمان، شرکت، یا گروه بیگانه یا عاملان آنها (بند ب و ج ماده ۷۳۱ قانون مجازات اسلامی)، شروع به جعل رایانه‌ای و سوءاستفاده از آن (مواد ۷۳۴ و ۷۳۵ قانون مجازات اسلامی)، شروع به کلاهبرداری رایانه‌ای (ماده ۷۴۱ قانون مجازات اسلامی)، شروع به تخریب یا اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند، به قصد به خطر انداختن امنیت و آسایش عمومی (ماده ۷۳۹ قانون مجازات اسلامی) قابل مجازات خواهند بود.

همچنین نظر به اینکه مطابق ماده ۷۸۰ قانون مجازات اسلامی، قوانینی که عنصر مادی جرایمی که از طریق سامانه‌های رایانه‌ای ارتکاب می‌یابند را تشکیل می‌دهند و در قانون جرایم رایانه‌ای به این جرایم اشاره نشده، همچنان قابل اجراست، اگر امکان تحقق شروع به جرم در جرایم مصرح در این قوانین وجود داشته باشد می‌توان به عنوان عنصر قانونی شروع به جرم در جرایم سایبری به آنها نیز استناد کرد. مثلاً فردی که قصد ارتکاب جرم قتل را از طریق فضای سایبر داشته باشد ولی بعد از شروع به اجرای آن، جرم منظور واقع نشود به استناد بند الف ماده ۱۲۲ قانون جدید مجازات اسلامی قابل مجازات است، چنان که ممکن

است شخصی که با هک کردن سیستم رایانه‌ای یک بیمارستان قصد دارد میزان داروی بیماران را تغییر دهد و منجر به مرگ آنان شود در مرحله شروع به جرم متوقف شود.[۴۲]

به هر حال در فرض تحقق شروع به جرایم سایبری و پیش‌بینی مجازات برای آن توسط قانون‌گذار ایران، با توجه به اینکه در بندهای مختلف ماده ۶۶۴ قانون آیین دادرسی کیفری، عنوان مطلق جرم آمده در صورتی که داده‌هایی که برای ارتکاب شروع به جرم به کار رفته، در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمروی حاکمیتی ایران ذخیره شده باشد (بند الف ماده ۶۶۴ قانون آیین دادرسی کیفری) یا شروع به جرم از طریق تارنماهای دارای مرتبه بالای کد کشوری ایران ارتکاب یافته باشد (بند ب ماده ۶۶۴ قانون مجازات اسلامی)، دادگاه‌های ایران صلاحیت سرزمینی در رسیدگی به جرایم مذکور را خواهند داشت.

۱-۳-۵- معاونت در جرم

معاونت به عمل کسی گفته می‌شود که بدون دخالت در عنصر مادی جرم، مباشر را در ارتکاب جرم یاری می‌کند. در خصوص عنصر قانونی معاونت در جرایم سایبری، نظر به ماده ۵۵ قانون جرایم رایانه‌ای که مواد قانون مذکور را جزئی از بخش تعزیرات قانون مجازات اسلامی قلمداد کرده است، باید به احکام کلی مندرج در قانون مجازات اسلامی ۱۳۹۲ رجوع کنیم. ماده ۱۲۶ قانون مذکور در خصوص معاونت در جرم مقرر می‌دارد که: «اشخاص زیر معاون جرم محسوب می‌شوند: الف ـ هرکس دیگری را ترغیب، تهدید، تطمیع، یا تحریک به ارتکاب جرم کند یا با دسیسه یا فریب یا سوءاستفاده از قدرت موجب وقوع جرم گردد؛ ب ـ هرکس وسایل ارتکاب جرم را بسازد یا تهیه کند یا طریق ارتکاب جرم را به مرتکب ارائه دهد؛ پ ـ هرکس وقوع جرم را تسهیل کند. تبصره ـ برای تحقق معاونت در جرم وجود وحدت قصد و تقدم و یا اقتران زمانی بین رفتار معاون و مرتکب جرم شرط است. چنانچه فاعل اصلی جرم، جرمی شدیدتر از آنچه مقصود معاون بوده است مرتکب شود، معاون به مجازات معاونت در جرم خفیف‌تر محکوم می‌شود.» در خصوص مجازات معاونت در جرم نیز ماده ۱۲۷ مقرر می‌دارد: «در صورتی که در شرع یا قانون، مجازات دیگری برای معاون تعیین نشده باشد، مجازات وی به شرح زیر است: الف ـ در جرایمی که مجازات قانونی آنها سلب

42. Marc D Goodman, and Susan W Brenner, "The Emerging Consensus on Criminal Conduct in *Cyberspace*," *International Journal of Law and Information Technology* 10 (2002): 149.

حیات یا حبس دائم است، حبس تعزیری درجهٔ دو یا سه؛ ب ـ در سرقت حدی و قطع عمدی عضو، حبس تعزیری درجهٔ پنج یا شش؛ پ ـ در جرایمی که مجازات قانونی آنها شلاق حدی است سی و یک تا هفتاد و چهار ضربه شلاق تعزیری درجهٔ شش؛ ت ـ در جرایم موجب تعزیر یک تا دو درجه پایین‌تر از مجازات جرم ارتکابی. تبصره ۱- در مورد بند (ت) این ماده مجازات معاون از نوع مجازات قانونی جرم ارتکابی است مگر در مورد مصادرهٔ اموال، انفصال دائم و انتشار حکم محکومیت که مجازات معاون به ترتیب جزای نقدی درجهٔ چهار، شش و هفت است. تبصره ۲- در صورتی که به هر علت قصاص نفس یا عضو اجرا نشود، مجازات معاون بر اساس میزان تعزیر فاعل اصلی جرم، مطابق بند (ت) این ماده اعمال می‌شود.» بنابراین بر اساس ماده ۱۲۷ قانون مجازات اسلامی ۱۳۹۲، مجازات معاونت در جرم به این صورت تعیین می‌شود که اگر برای معاونت در جرم در قانون یا شرع مجازات خاصی مقرر شده باشد همان مجازات ملاک می‌باشد، در غیر این صورت در معاونت در جرایم مستوجب سلب حیات یا حبس دائم مطابق بند الف ماده ۱۲۷، در معاونت در جرایم سرقت حدی و قطع عمدی عضو مطابق بند ب این ماده، در معاونت در شلاق حدی مطابق بند پ آن و در نهایت در معاونت در جرایم تعزیری بر اساس بند ت قانون مذکور حکم به مجازات صادر می‌شود؛ اما در خصوص چگونگی تعیین مجازات معاونت در جرایم سایبری به نظر می‌رسد که در دو بند الف و ب ماده ۷۴۳ قانون مجازات اسلامی که برای معاونت در دستیابی افراد به محتویات مستهجن یا مبتذل یا ارتکاب جرایم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده، مجازات‌های خاصی مقرر شده، مجازات‌های مذکور اعمال خواهد شد، برای تعیین مجازات معاونت در جرم کسی که انتشار یا توزیع یا معامله، تولید یا ذخیره یا نگهداری به قصد تجارت یا افساد محتویات مستهجن را از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حرفهٔ خود قرار دهد و مباشر مطابق تبصره سه ماده ۷۴۲ قانون مجازات اسلامی مفسد فی‌الارض شناخته شود، طبق بند الف ماده ۱۲۷ عمل می‌شود. در مورد مجازات معاونت در سایر جرایم مقرر در فصل جرایم رایانه‌ایِ قانون مجازات اسلامی نیز با توجه به تعزیری بودن آنها بر اساس بند ت ماده ۱۲۷ عمل خواهد شد.

حال این سؤال مطرح می‌شود که در مواردی که معاونت در جرم سایبری در ایران و جرم تام در خارج از ایران واقع می‌شود یا معاونت در جرم سایبری در خارج از کشور و خود جرم در ایران واقع می‌شود، کدام دادگاه صالح است؟ دادگاه ایران یا دادگاه کشور خارجی؟ قانون‌گذار

ایران در پاسخ به این سؤال‌ها راهکار روشنی ارائه ننموده است. به نظر می‌رسد که در خصوص قسمت اول سؤال یعنی در مواردی که معاونت در جرم سایبری در ایران و جرم تام در خارج واقع می‌شود، دادگاه‌های ایران صلاحیت رسیدگی به معاونت در جرم ارتکابی را خواهند داشت. به این دلیل که معاونت در جرم به موجب ماده ۱۲۶ قانون مجازات اسلامی ۱۳۹۲ جرم شناخته شده است و بر اساس بند الف و ب ماده ۶۶۴ قانون آیین دادرسی کیفری، مطلق جرایمی که در قلمروی حاکمیتی ایران ارتکاب می‌یابند در صلاحیت دادگاه‌های ایران خواهند بود. البته باید به این نکته توجه نمود که جرم تام ارتکابی در خارج باید بر اساس قانون مجازات اسلامی جرم شناخته شده باشد در غیر این صورت دادگاه‌های ایران صالح به رسیدگی نمی‌باشند.[۴۳] به علاوه رسیدگی به جرم معاون در دادگاه‌های ایران منوط به آن است که دادگاه خارجی به عمل مباشر رسیدگی کرده و تحقق جرم را احراز نموده باشد؛ اما در مورد صلاحیت دادگاه‌های ایران در حالتی که معاونت در جرم در خارج و خود جرم در قلمروی ایران ارتکاب می‌یابد، اختلاف وجود دارد. اغلب حقوقدانان در این مورد نیز قائل به صلاحیت دادگاه‌های ایران در معاونت در جرم ارتکابی شده‌اند. برای مثال گفته شده: «در صورتی که جرم اصلی در کشور ایران ارتکاب ولی معاونت آن در خارج از کشور انجام یافته باشد، جرم واقع‌شده در ایران محسوب و رسیدگی به اتهام معاون در جرم در صلاحیت دادگاه‌های ایران است.»[۴۴] یا اینکه «به نظر می‌رسد معاونت در جرم‌های واقع‌شده در ایران یا در خارج از آن می‌تواند تابع قوانین کیفری ایران قرار گیرد.»[۴۵] استدلال این گروه از حقوقدانان بیشتر بر پایهٔ عاریه‌ای بودن مجرمیت معاونت در حقوق ایران است. به طوری که به اعتقاد یکی از آنها: «تبعی بودن مجازات معاونت در مسائل مربوط به آیین دادرسی کیفری و صلاحیت دادگاه‌ها هم صدق می‌کند. به این ترتیب مرور زمان معاونت با مرور زمان جرم اصلی آغاز می‌شود. همین‌طور در صورتی که جرم اصلی در کشور ایران انجام یافته ولی معاونت در خارج مصداق کرده باشد، رسیدگی به مسؤولیت جزایی معاون جرم در صلاحیت محاکم ایران خواهد بود.»[۴۶] همچنین ممکن است گفته شود که معاونت در جرم، قسمتی از جرم اصلی به حساب

---

۴۳. مومنی، پیشین، ۱۳۰.

۴۴. ایرج گلدوزیان، *بایسته‌های حقوق جزای عمومی (۳-۲-۱)* (تهران: میزان، بی‌تا)، چاپ بیست و دوم، ۲۱۶.

۴۵. حسین آقایی جنت‌مکان، *حقوق کیفری عمومی، براساس قانون مجازات اسلامی ۱۳۹۰* (تهران: جنگل، ۱۳۹۱)، چاپ اول، ۱۷۶.

۴۶. پرویز صانعی، *حقوق جزای عمومی* (تهران: کتابخانه گنج دانش، ۱۳۷۱)، جلد دوم، چاپ چهارم، ۸۵.

می‌یابد و در نتیجه دادگاه‌های ایران به استناد بخش آخر ماده ۴ قانون مجازات اسلامی ۱۳۹۲ صالح به رسیدگی می‌باشند؛ اما در رد این نظریات گفته شده: «ماده ۴ قانون مجازات اسلامی تاب چنین تفسیری ندارد چرا که معاونت در جرم «قسمتی از جرم» اصلی که در ایران اتفاق افتاده نیست بلکه خود جرم مستقلی است که در خارج از قلمرو حاکمیت ایران اتفاق افتاده است. درست است که معاونت در جرم مجرمیت خود را از جرم اصلی به عاریت می‌گیرد، اما هیچ‌گاه قسمتی از جرم اصلی که توسط مباشر در ایران اتفاق افتاده به شمار نمی‌آید، لذا دادگاه‌های ما به استناد ماده ۴ قانون مجازات اسلامی واجد صلاحیت نیستند اما ممکن است از حیث صلاحیت‌های دیگر مثل اصل صلاحیت شخصی، اصل صلاحیت واقعی و اصل صلاحیت جهانی واجد صلاحیت باشند.»[۴۷] این دیدگاه منطقی‌تر به نظر می‌رسد چراکه علاوه بر دلایل فوق طبق اصل صلاحیت سرزمینی نیز، «همان‌گونه که از وجه تسمیه آن پیداست، محاکم به خاطر جرمی که در قلمروشان اتفاق می‌افتد صلاحیت رسیدگی دارند ولی در معاونت که یک عنوان مستقل از مباشرت یا شراکت می‌باشد، معاونت در خارج از ایران به هیچ‌وجه در ایران اتفاق نمی‌افتد که بخواهیم بر طبق مواد ۳ یا ۴ ق.م.ا مرتکب را در ایران محاکمه نماییم.»[۴۸]

۱-۳-۶- مشارکت در جرم

مشارکت در جرم به حالتی اطلاق می‌شود که در آن دو یا چند نفر با یکدیگر در ارتکاب جرم همکاری می‌کنند به نحوی که همهٔ آنها در عنصر مادی جرم دخالت داشته «... و جرم مستند به رفتار همه آنها باشد خواه رفتار هریک به تنهایی برای وقوع جرم کافی باشد خواه نباشد و خواه اثر کار آنها مساوی باشد خواه متفاوت، ...» (ماده ۱۲۴ قانون مجازات اسلامی ۱۳۹۲)

در خصوص مشارکت در جرایم سایبری می‌توان حالتی را تصور کرد که در جرمی مانند جرم کلاهبرداری سایبری یکی از شرکاء در قلمروی حاکمیتی ایران مرتکب قسمتی از جرم شده و شریک دیگر خارج از این قلمرو مرتکب قسمت دیگر آن شده است. مثلاً تغییر یا محو داده‌ها در قلمروی سرزمینی ایران انجام شده و تحصیل وجوه یا منفعت در خارج از قلمروی سرزمینی ایران واقع شده است. حال در اینجا این مسئله مطرح می‌شود که آیا دادگاه‌های

۴۷. حسن پوربافرانی، *حقوق جزای بین‌الملل* (تهران: جنگل، ۱۳۹۱)، چاپ چهارم، ۲۰.

۴۸. ابوالفتح خالقی و بهزاد جودکی، «دادگاه ذی‌صلاح در بزه معاونت در جرم در قلمروی حقوق جزای بین‌الملل»، *مجله مطالعات حقوقی* ۲ (۱۳۸۹): ۴۴.

ایران صلاحیت رسیدگی به جرم شریکی را که در خارج از قلمروی حاکمیتی ایران مرتکب جرم شده است دارند؟ در پاسخ می‌توان گفت عمل هریک از این شرکاء قسمتی از عنصر مادی جرم را تشکیل می‌دهد، بنابراین دادگاه‌های ایران به استناد ماده ۴ قانون مجازات اسلامی ۱۳۹۲ صالح به رسیدگیِ جرم شریکی که در ایران مرتکب جرم شده، می‌باشند. البته با توجه به اینکه به احتمال بسیار زیاد کشوری نیز که قسمت دیگری از جرم در آن ارتکاب یافته به دنبال اعمال صلاحیت برمبنای اصل صلاحیت سرزمینی می‌باشد، بروز تعارض صلاحیت‌ها اجتناب‌ناپذیر خواهد بود. چراکه در خصوص مثالی که زده شد حداقل دو کشور در پیِ اعمال صلاحیت نسبت به یک جرم می‌باشند.

۲- صلاحیت ذاتی و محلی دادگاه‌های ایران در جـرایم ارتکـابی در فضـای سایبر

در این بند به بررسی این موضوع می‌پردازیم که در صورتی که دادگاه‌های ایران صلاحیت رسیدگی به یک جرم سایبری را داشته باشند این جرم در کدام‌یک از دادگاه‌های مستقر در ایران رسیدگی می‌شود یا به عبارت دیگر کدام‌یک از دادگاه‌های ایران صلاحیت ذاتی و محلی برای رسیدگی به جرم ارتکابی را دارند.

۲-۱- صلاحیت ذاتی

بعد از اینکه مراجع قضایی ایران در رسیدگی به جرایم سایبری صالح شناخته شدند، باید تعیین کنیم که کدام‌یک از دادگاه‌های مستقر در ایران صلاحیت ذاتی در رسیدگی جرایم مذکور را دارند. طبق ماده ۶۶۶ قانون آیین دادرسی کیفری:

«قوه قضائیه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدیدنظر را برای رسیدگی به جرایم رایانه‌ای اختصاص دهد.»

لذا برای تعیین اینکه جرایم سایبری مصرح در قانون جرایم رایانه‌ای در شعب اختصاصی کدام‌یک از دادگاه‌های ایران باید مطرح شود باید به مقررات عام موجود در خصوص صلاحیت ذاتی دادگاه‌های ایران رجوع کرد. در حقوق ایران در مرحلهٔ بدویِ «رسیدگی‌های کیفری اصل بر صلاحیت مراجع عمومی است و هرگاه که قانون‌گذار تکلیف مرجع صالح جهت رسیدگی به جرمی را مشخص نکرده باشد باید بدون شک به صلاحیت دادگاه‌ها و

مراجع تحقیق عمومی حکم کرد.»[۴۹] بنابراین اصل بر این است که جرایم سایبری در مراجع عمومی رسیدگی شوند مگر اینکه برخی از آنها در صلاحیت مراجع اختصاصی قرار بگیرند. در حال حاضر دادگاه‌های کیفری یک و دو، مراجع عام رسیدگی بوده و اصل بر آن است که دادگاه‌های مذکور صالح به رسیدگی باشند. مطابق ماده ۳۰۱ قانون آیین دادرسی کیفری «دادگاه کیفری دو صلاحیت رسیدگی به تمام جرایم را دارد، مگر آنچه به موجب قانون در صلاحیت مرجع دیگری باشد.» مطابق ماده ۳۰۲ قانون آیین دادرسی کیفری نیز جرایم موجب مجازات سلب حیات، جرایم موجب حبس ابد، جرایم موجب قطع عضو یا جنایات عمدی علیه تصمیمات جسمانی با میزان نصف دیه کامل یا بیش از آن، جرایم موجب مجازات تعزیری درجه سه و بالاتر و جرایم سیاسی و مطبوعاتی در صلاحیت دادگاه کیفری یک می‌باشد.

در خصوص مراجع اختصاصی نیز ماده ۶۶۶ قانون آیین دادرسی کیفری به دادگاه‌های اطفال و نوجوانان و نظامی اشاره کرده است. بر اساس ماده ۳۰۴ قانون آیین دادرسی کیفری، دادگاه اطفال و نوجوانان «به کلیه جرایم اطفال و نوجوانان و افراد کمتر از هجده سال تمام شمسی» رسیدگی می‌نماید. در نتیجه در صورت ارتکاب جرایم سایبری توسط اطفال و اشخاص بالغ کمتر از ۱۸ سال دادگاه‌های اطفال و نوجوانان صالح به رسیدگی خواهند بود.

دادگاه‌های نظامی یکی دیگر از مراجع اختصاصی می‌باشند که مطابق ماده ۱ قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۰۹ به وظایف خاص نظامی و انتظامی افراد نظامی رسیدگی می‌کنند؛ اما با توجه به اینکه در این قانون از جرایمی نظیر اختلاس (ماده ۱۱۹ قانون مجازات جرایم نیروهای مسلح)، سرقت (ماده ۸۸ قانون مجازات جرایم نیروهای مسلح) و ... ذکر شده که جرم نظامی صرف محسوب نمی‌شوند و توسط غیرنظامیان نیز قابل ارتکاب هستند، باید گفت «از نقطه‌نظر صلاحیت رسیدگی، مفهوم جرم نظامی مفهومی وسیع بوده و علاوه بر جرم ماهیتاً نظامی یا جرم نظامی در مفهوم خاص خود، شامل جرایم مرتبط با وظایف نظامی و انتظامی هم می‌شود.»[۵۰]

---

۴۹. محمد آشوری، *آیین دادرسی کیفری* (تهران: سمت، ۱۳۸۹)، جلد دوم، چاپ دوازدهم، ۹۲.

۵۰. علی خالقی، *آیین دادرسی کیفری* (تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۱)، چاپ نوزدهم، ۳۲۸.

بنابراین اگر نظامیان مرتکب اعمال تصریح‌شده در ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲[۵۱] شوند، در شعب تخصصی جرایم رایانه‌ای دادگاه‌های نظامی محاکمه خواهند شد.

دادگاه‌های انقلاب و ویژه روحانیت از دیگر مراجع اختصاصی هستند که در ماده ۶۶۶ قانون آیین دادرسی کیفری نامی از آنها برده نشده است. طبق ماده ۳۰۳ قانون آیین دادرسی کیفری، دادگاه‌های انقلاب در جرایم ذیل صالح به رسیدگی می‌باشند: «... الف ـ جرایم علیه امنیت ملی داخلی و خارجی و محاربه یا افساد فی‌الارض، بغی، تبانی و اجتماع علیه جمهوری اسلامی ایران یا اقدام مسلحانه یا احراق، تخریب و اتلاف اموال به منظور مقابله با نظام؛ ب ـ توهین به مقام بنیان‌گذار جمهوری اسلامی ایران و مقام معظم رهبری؛ پ ـ تمام جرایم مربوط به مواد مخدر، روان‌گردان و پیش‌سازهای آن و قاچاق اسلحه، مهمات و اقلام و مواد تحت کنترل؛ ت ـ سایر مواردی که به موجب قوانین خاص در صلاحیت این دادگاه است.» لذا جرایم سایبری از قبیل جاسوسی رایانه‌ای (مواد ۷۳۱ تا ۷۳۳ قانون مجازات اسلامی)، تخریب یا اخلال داده‌های سامانه‌های رایانه‌ای یا مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند به قصد به خطر انداختن امنیت و آسایش عمومی (ماده ۷۳۹ قانون مجازات اسلامی)، انتشار یا توزیع محتویات مستهجن در حد افساد فی‌الارض (تبصره ۳ ماده ۷۴۲ قانون مجازات اسلامی)، هتک حیثیت بنیان‌گذار جمهوری اسلامی ایران و مقام رهبری از طریق سامانه‌های رایانه‌ای یا مخابراتی (مواد ۷۴۴ و ۷۴۵ قانون مجازات اسلامی) در دادگاه انقلاب قابل رسیدگی هستند، لکن در ماده ۶۶۶ قانون آیین دادرسی کیفری به تشکیل شعب تخصصی دادگاه انقلاب برای رسیدگی به جرایم رایانه‌ای اشاره‌ای نشده است. به موجب ماده ۱۳ آیین‌نامه دادسراها و دادگاه‌های ویژه روحانیت مصوب مرداد ماه ۱۳۶۹ و اصلاحی مصوب ۱۳۸۴/۰۹/۰۵ نیز که مقرر داشته: «دادسراها و دادگاه‌های ویژهٔ روحانیت در موارد ذیل صالح

---

۵۱. ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲: «هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوط صورت گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی‌شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند، افشای غیرمجاز اطلاعات یا معدوم کردن آنها یا سوءاستفاده‌های مالی که نظامیان به وسیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مواد مربوط به این قانون می‌باشند.» در صورتی که فضای سایبر بستر یا ابزار ارتکاب اعمال مذکور در این ماده باشد، این اعمال جزء جرایم سایبری محسوب شده و مرتکبین آن مطابق این قانون مجازات خواهند شد.»

به رسیدگی می‌باشند: الف ـ کلیهٔ جرایم روحانیون؛ ...» جرایم سایبری ارتکابی توسط روحانیون در صلاحیت دادسراها و دادگاه‌های ویژه روحانیت می‌باشند.

با وجود اینکه در ماده ۶۶۶ قانون آیین دادرسی کیفری، نامی از دو دادگاه مذکور برده نشده است اما در تبصره بند ط ماده ۳۳ قانون برنامه چهارم توسعه مصوب ۱۳۸۳/۰۶/۱۱ آمده: «قوه قضائیه موظف است شعبه یا شعبی از دادگاه‌ها را برای بررسی جرایم الکترونیکی و نیز جرایم مربوط به تجارت الکترونیکی و تجارت سیار، اختصاص دهد.» در واقع با توجه به اینکه این تبصره دادگاه‌ها را به صورت مطلق ذکر کرده، دادگاه‌های انقلاب و ویژه روحانیت را نیز دربر می‌گیرد.

در رابطه با دادسرای صالح در تحقیقات مقدماتی جرایم سایبری نیز بر اساس ماده ۲۲ قانون آیین دادرسی کیفری که مقرر می‌دارد: «به منظور کشف جرم، تعقیب متهم، انجام تحقیقات، حفظ حقوق عمومی و اقامه دعوای لازم در این مورد، اجرای احکام کیفری ... در حوزهٔ قضایی هر شهرستان و در معیت دادگاه‌های آن حوزه، دادسرای عمومی و انقلاب و همچنین در معیت دادگاه‌های نظامی و دادسرای نظامی تشکیل می‌شود» باید گفت دادسراهای عمومی و انقلاب نسبت به تحقیق و تعقیب در جرایم موضوع صلاحیت دادگاه‌های کیفری یک، دو، انقلاب و اطفال و نوجوانان، دادسرای ویژه روحانیت نسبت به تحقیق و تعقیب در جرایم موضوع صلاحیت دادگاه‌های ویژه روحانیت و دادسرای نظامی نسبت به تحقیق و تعقیب در جرایم موضوع صلاحیت دادگاه‌های نظامی صالح به رسیدگی خواهند بود.

تاکنون از دادگاه‌های صالح در مرحله بدوی رسیدگی به جرایم سایبری سخن گفتیم اما برای تعیین مراجع صالح در مرحله تجدیدنظر نیز باید به قواعد عام موجود رجوع کنیم. به این ترتیب و بر اساس ماده ۴۲۸ قانون آیین دادرسی کیفری «آرای صادره درباره جرایمی که مجازات قانونی آنها سلب حیات، قطع عضو، حبس ابد و یا تعزیر درجه سه و بالاتر است و جنایات عمدی علیه تمامیت جسمانی که میزان دیه آنها نصف دیه کامل یا بیش از آن است و آرای صادره دربارهٔ جرایم سیاسی و مطبوعاتی، قابل فرجام‌خواهی در دیوان عالی کشور است.» در غیر از این موارد بر اساس ماده ۴۲۶ قانون آیین دادرسی کیفری مرجع صالح برای رسیدگی به درخواست تجدیدنظر، دادگاه تجدیدنظر استان خواهد بود. تجدیدنظر از آرای دادگاه‌های نظامی مطابق ماده ۶۳۴ قانون آیین دادرسی کیفری به همان ترتیبی که در بالا آمد حسب مورد در دیوان عالی کشور یا دادگاه تجدیدنظر استان صورت خواهد گرفت و در

نهایت مرجع تجدیدنظر از آرای دادگاه‌های ویژه روحانیت، دادگاه تجدیدنظر ویژه روحانیت می‌باشد. (ماده ۵۰ آیین‌نامه دادسراها و دادگاه‌های ویژه روحانیت الحاقی ۱۳۸۴)

۲-۲- صلاحیت محلی

حال که مشخص شد کدام‌یک از دادگاه‌ها صلاحیت ذاتی در رسیدگی به جرایم سایبری را دارند، باید تعیین کرد که کدام‌یک از آنها صلاحیت محلی رسیدگی به جرایم مذکور را دارند. برای مثال اگر دادگاه‌های انقلاب برای رسیدگی به جرم جاسوسی سایبری صالح شناخته شدند، باید تعیین کنیم که کدام شعبه از دادگاه‌های مذکور صلاحیت محلی در رسیدگی به این جرم را که در قلمروی سرزمینی ایران ارتکاب یافته دارند. مستفاد از ماده ۶۶۵ قانون آیین دادرسی کیفری، ملاک تعیین صلاحیت محلی در جرایم سایبری همچون جرایم سنتی محل ارتکاب جرم می‌باشد. اگرچه تعیین محل ارتکاب جرایم سایبری دشوار است ولی نباید به این بهانه از رسیدگی به جرایم مذکور سر باز زد بلکه همچنان که ماده ۶۶۵ مقرر می‌دارد: «چنانچه جرم رایانه‌ای در صلاحیت دادگاه‌های ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و در صورت اقتضاء صدور کیفرخواست می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.» در خصوص اینکه بین دادسراهای موجود در محل وقوع جرم کدام‌یک نسبت به تحقیقات مقدماتی جرایم سایبری صالح خواهند بود، باید گفت دادسرایی صالح است که در حوزهٔ دادگاه صالح به رسیدگی به جرم قرار دارد. در صلاحیت محلی اصل بر این است که دادگاه محل وقوع جرم صالح به رسیدگی باشد؛ اما این اصل هم استثنائاتی نظیر صلاحیت اضافی و احاله دارد. نظر به اینکه بر اساس ماده ۶۸۷ قانون آیین دادرسی کیفری «در مواردی که در این بخش برای رسیدگی به جرایم رایانه‌ای مقررات خاصی از جهت آیین دادرسی پیش‌بینی نشده است، تابع مقررات عمومی آیین دادرسی کیفری است.» در جرایم سایبری نیز قواعد مربوط به صلاحیت اضافی، احاله و سایر مقررات آیین دادرسیِ مندرج در قانون آیین دادرسی کیفری که در بخش آیین دادرسی جرایم رایانه‌ای پیش‌بینی نشده، قابل اعمال است؛ اما در هر حال باید توجه داشت مقررات مذکور در صورتی در جرایم سایبری مفید فایده است که تمام ارکان جرایم سایبری در قلمروی سرزمینی ایران ارتکاب یافته باشد.

نتیجه

چنان که گذشت ماهیت خاص فضای سایبر و شیوه ارتکاب جرایم در آن، مقررات عام صلاحیت کیفری را به چالش کشیده و موجب شد که قانون‌گذار مقرراتی مطابق با ویژگی‌های فضای مذکور، در این زمینه وضع نماید. اگرچه مقررات مذکور تفاوت اساسی با قواعد عام راجع به صلاحیت کیفری ندارد اما قانون‌گذار برای رفع ابهاماتی که جرایم سایبری در زمینهٔ اعمال صلاحیت ایجاد می‌کرد، ناگزیر از وضع این مواد بوده است. با این وجود قانون آیین دادرسی کیفری در بخش آیین دادرسی جرایم رایانه‌ای به تبیین دقیق اصل صلاحیت سرزمینی نپرداخته است. برای مثال همچنان که گفته شد برای اعمال اصل صلاحیت سرزمینی در زمینهٔ جرایم سایبری ابتدا باید قلمروی سرزمینی ایران و سپس محل وقوع این جرایم را تعیین کنیم. در بخش آیین دادرسی جرایم رایانه‌ای، قلمروی سرزمینی ایران در فضای سایبر به طور دقیق مشخص نشده است. تحلیل‌هایی نیز که وب‌سایت‌های دارای دامنهٔ ir. و مراکز خدمات داده را جزء قلمروی حاکمیتی ایران می‌داند با برداشت از نظریات موجود و مواد مقرر در قانون مذکور، ارائه گردیده است. قانون آیین دادرسی کیفری در خصوص تعیین محل وقوع جرایم سایبری نیز که چالشی‌ترین موضوع در زمینهٔ اعمال صلاحیت سرزمینی محسوب می‌شود، ضابطهٔ دقیق و شفافی ارائه ننموده است. از این رو ناگزیر شدیم که با بررسی نظریاتی که در این خصوص مطرح گشته، ملاحظه نماییم قانون‌گذار ایران بر اساس کدام‌یک از این نظریه‌ها اقدام به وضع قانون نموده است. بدیهی است معضل تعیین محل وقوع جرم در صور مشکل جرایم سایبری بیشتر نمایان می‌شود از این رو بهتر است که قانون‌گذار موضع دقیقی در این خصوص اتخاذ کند. همچنین قانون آیین دادرسی کیفری به اندازهٔ کافی به مباحث مربوط به آیین دادرسی جرایم رایانه‌ای نپرداخته و با وضع ماده ۶۸۷ موضع سکوت خود را توجیه نموده است؛ اما باید توجه داشت که اگرچه بر اساس ماده مذکور، در صورت سکوت قانون‌گذار در بخش آیین دادرسی جرایم رایانه‌ای در خصوص فرایند دادرسی، مقررات آیین دادرسی کیفری قابل اعمال است ولی نباید این مسئله را دور از نظر داشت که مکانیزم‌هایی همچون احاله، صلاحیت اضافی و ... در خصوص صلاحیت محلی داخلی دادگاه‌های کشورمان در نظم داخلی مثمرثمر خواهند بود چراکه در صورت فرامرزی بودن جرایم سایبری اجرای این مکانیزم‌ها مستلزم همکاری کشورهایی خواهد بود که با جرم ارتکابی پیوند دارند.

با وجودی که امکان بروز تعارض صلاحیت‌ها در فضای سایبر با توجه به ویژگی فرامرزی جرایم سایبری بسیار زیاد است اما نه در اسناد بین‌المللی و نه در قوانین موضوعهٔ ایران راه‌حل روشنی برای آن ارائه نشده است. راهی که برای برون‌رفت از تعارض صلاحیت‌ها به نظر می‌رسد، آن است که هر کشور با سنجش تعداد بزه‌دیدگان، دسترسی که به مرتکب و دلایل و مدارک ناشی از جرم دارد، اینکه آیا هدف جرایم سایبری بوده یا خیر، میزان تأثیری که جرم ارتکابی بر آن کشور داشته و سرانجام، توانایی‌های که دستگاه قضایی برای رسیدگی به جرم از آن برخوردار است، خود را صالح به رسیدگی بداند. به این ترتیب «یکی از راه‌های محدود کردن تعارضات بالقوه ارزیابی سودمندی تعقیب به وسیلهٔ مقامات مسؤول است.»[۵۲] البته اجرای این راهکار مستلزم همکاری دولت‌ها با یکدیگر در این زمینه خواهد بود. چراکه اگر کشورها به این عوامل بی‌توجهی کنند و بدون وجود یک رابطهٔ منطقی بین خود و جرم ارتکابی، به اعمال صلاحیت بپردازند، مشکلات ناشی از تعارض صلاحیت‌ها که محاکمهٔ مجدد مرتکبین مهم‌ترین نمونهٔ آن محسوب می‌شود، همچنان پابرجا خواهد بود.

۵۲. محمدحسن دزیانی، «صلاحیت رسیدگی به جرایم در سایبر اسپیس»، *خبرنامه انفورماتیک* ۷۷ (۱۳۸۰)، ۳۵.

فهرست منابع

الف) منابع فارسی

آخوندی، محمود. *آیین دادرسی کیفری*. جلد دوم. چاپ سیزدهم. سازمان و صلاحیت مراجع کیفری. تهران: وزارت فرهنگ و ارشاد اسلامی؛ سازمان چاپ و انتشارات، ۱۳۹۰.

آشوری، محمد. *آیین دادرسی کیفری*. جلد دوم. چاپ دوازدهم. تهران: سمت، ۱۳۸۹.

آقایی جنت‌مکان، حسین. *حقوق کیفری عمومی*. جلد نخست. بر اساس قانون مجازات اسلامی ۱۳۹۰. چاپ اول. تهران: جنگل، ۱۳۹۱.

ابراهیمی، مهدی. *اینترنت*. چاپ دوم، تهران: کتابدار، ۱۳۸۰.

اردبیلی، محمدعلی. *حقوق جزای عمومی*. جلد نخست. چاپ بیست و هشتم. تهران: میزان، ۱۳۹۱.

پوربافرانی، حسن. *حقوق جزای بین‌الملل*. چاپ چهارم. تهران: جنگل، ۱۳۹۱.

جلالی فراهانی، امیرحسین. *درآمدی بر آیین دادرسی کیفری جرایم سایبری*. چاپ اول. تهران: خرسندی، ۱۳۸۹.

حافظنیا، محمدرضا. *جغرافیای سیاسی فضای مجازی*. چاپ اول. تهران: سمت، مرکز تحقیق و توسعه علوم انسانی، ۱۳۹۰.

خالقی، ابوالفتح، و بهزاد جودکی. «دادگاه ذی‌صلاح در بزه معاونت در جرم در قلمروی حقوق جزای بین‌الملل». *مجله مطالعات حقوقی* ۲ (۱۳۸۹): ۵۶-۳۷.

خالقی، علی. *آیین دادرسی کیفری*. چاپ نوزدهم. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۱.

خالقی، علی. *جستارهایی از حقوق جزای بین‌الملل*. چاپ دوم. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۰.

خرم‌آبادی، احمد. *حقوق کیفری فناوری اطلاعات، مسؤولیت کیفری ارائه‌دهندگان خدمات اینترنتی*. چاپ اول. اصفهان: دادیار، ۱۳۹۱.

دزیانی، محمدحسن. «صلاحیت رسیدگی به جرایم در سایبر اسپیس». *خبرنامه انفورماتیک* ۷۷ (۱۳۸۰).

دولتشاهی، شاهپور. *صلاحیت قضایی در محیط مجازی، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات*. تهران: دانشگاه شهید بهشتی، دانشکده ادبیات و علوم انسانی، معاونت پژوهشی، ۱۳۸۳.

زندی، محمدرضا. «صلاحیت در جرایم سایبری». *ماهنامه قضاوت* ۶۰ (۱۳۸۸): ۴۹-۴۸.

صانعی، پرویز. *حقوق جزای عمومی*. جلد دوم. چاپ چهارم. تهران: کتابخانه گنج دانش، ۱۳۷۱.

فروغی، فضل‌الله، و امیر البوعلی. «صلاحیت کیفری مراجع قضایی در فضای سایبر». *مجله تحقیقات حقوقی* ۵۸ (۱۳۹۱): ۳۵۷-۳۱۱.

گلدوزیان، ایرج. *بایسته‌های حقوق جزای عمومی (۳-۲-۱)*. چاپ بیست و دوم. تهران: میزان، بی‌تا.

مومنی، مهدی. *مبانی حقوق جزای بین‌الملل*. چاپ هشتم. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۱.

نوربها، رضا. *زمینه حقوق جزای عمومی*. چاپ سی و سوم. تهران: کتابخانه گنج دانش، ۱۳۹۱.

یوسفی، مرتضی. «بررسی و تبیین جایگاه فضای سایبر به عنوان عامل ارتکاب جرم». پایان‌نامه کارشناسی ارشد در رشته حقوق جزا و جرم‌شناسی، قم: دانشکده پردیس قم دانشگاه تهران، ۱۳۸۷.

ب) منابع انگلیسی

AZMI, IDA MADIEHA. "Domain Names and Cyberspace: The Application of Old Norms to New *Problems*." *International Journal of Law and Information Technology* 8 (2000): 193-213.

Bigos, Oren. "Jurisdiction over Cross-Border Wrongs on the *Internet*." *International and Comparative Law Quarterly* 54 (2005): 585-620.

Brenner, Susan W., and Bert Jaap Koops. "Approaches to Cybercrime *Jurisdiction*." *Journal of High Technology* 5 (2004).

Goodman, Marc D, and Susan W. Brenner. "The Emerging Consensus on Criminal Conduct in *Cyberspace*." *International Journal of Law and Information Technology* 10 (2002): 139-223.

Kohl, Uta. "Eggs, Jurisdiction and the *Internet*." *International and Comparative Law Quarterly* 51 (2002): 555-582.

Kohl, Uta. *Jurisdiction and the Internet (Regulatory Competence over Online Activity)*. New York: Cambridge University Press, 2007.

Maier, Bernhard. "How Has the Law Attempted to Tackle the Borderless Nature of the *Internet*." *International Journal of Law and Information Technology* 18 (2010): 142-175.

Menthe, Darrel C. "Jurisdiction in Cyberspace: A Theory of International *Spaces*." *Michigan Telecommunications and Technology Law Review* 69 (1998): 69-103.

Stein, Allan R. "The Unexceptional Problem of Jurisdiction in *Cyberspace*." *The International Lawyer* 4 (1998): 1167-1191.

Thierer, Adam, and Clyde Wayne Jr Crews. *Who Rules the Net?*. Washington, D.C: CATO Institute, 2003.

Vidyasagar, Adithya S V. "Jurisdictional Issues in Cyber *Space*." *Acta Iuridica Olomucensis* 5 (2010): 29-47.

Wang, Faye Fangfei. *Internet Jurisdiction and Choice of Law: Legal Practices in EU, US and China*. New York: Cambridge University Press, 2010.

Wilske, Stephan and Teresa Schiller. "International Jurisdiction in Cyberspace: Which States May Regulate the *internet*?." *Federal Communications Law Journal* 50 (1997-1998): 117-178.

The Territorial Jurisdiction of Iranian Courts toward Cybercrimes

Najmeh Ghaffari Elahi Kashani
Ph.D. Student of Criminal Law, Faculty of Law and Political Science,
Tehran University, Tehran, Iran
Email: n8.ghaffari@yahoo.com

The special nature of cyber space and the crimes that committed there, led to the adoption of Computer Crime Act in 1388. Then the legislator repealed the rules of procedure in Computer Crime Act, applied minor changes to them and ultimately attached them to Criminal Procedure Act 1392. But computer crimes procedure in criminal procedure act, includes weak and vague provisions about territorial jurisdiction which is very important in international criminal law. In this section, it is not provided an exact criterion for determination of Iran's sovereignty and location of cybercrimes which are constituent parts of territorial jurisdiction. In this article, by demystification of the obscure phrases about territorial jurisdiction in computer crimes and presentation of solution about defects, we will see Iranian courts when exercise territorial jurisdiction over cybercrimes.

Keywords: Cybercrimes, Territorial Jurisdiction, The Sphere of Sovereignty in Cyber Space, The Location of Cybercrime, Computer Crime Procedure.

ISSN 1682-9220

Journal of LEGAL RESEARCH

VOL. XVII, No. 2 2018-2

S. D. I. L.
The S.D. Institute of Law
Research & Study