فصلنامه علمی حقوق و مطالعات نوین، دوره ۳، شماره ۴، پیاپی ۹، زمستان ۱۴۰۱ www.jhvmn.ir
شماره مجوز انتشار: ۸۷۰۱۹ ISSN: 2783-1329

بررسی تطبیقی جایگاه صلاحیت سرزمینی در رسیدگی به جرایم سایبری با تکیه بر نظام کیفری ایران

حسن حیدری[۱] / دکتر علیرضا میلانی[۲]

* نوع مقاله: پژوهشی / تاریخ دریافت: ۱۴۰۱/۰۵/۱۱ / تاریخ پذیرش: ۱۴۰۱/۰۶/۱۳

چکیده

بکارگیری و بهره مندی از تکنولوژی و فن آوری اطلاعات و ارتباطات، علیرغم آثار مثبت و تسهیل ارتباطات و مراودات جهانی، سبب چالش در تعیین قواعد حاکم بر صلاحیت دادگاه های کیفری در مورد جرائم ارتکابی در فضای مجازی شده است. زیرا قواعد مربوط به تشخیص و تعیین دادگاه کیفری صالح به رسیدگی به جرائم ارتکابی در فضای واقعی عمدتاً مبتنی بر مکان و مرز می باشند، حال آنکه در فضای مجازی مرز و حصری وجود ندارد. بنابراین تحقیق حاضر به این سؤال پاسخ می دهد که آیا قواعد سنتی مربوط به صلاحیت در فضای مجازی قابل اعمال می باشد؟ و اعمال این صلاحیت در فضای مجازی چه چالش هایی را در بردارد؟ بیشترین چالش در تعیین دادگاه صالح کیفری در مورد جرائم ارتکابی در فضای سایبر مربوط به صلاحیت سرزمینی است چرا که عدم وابستگی به مکانی خاص از ویژگی های فضای مجازی است. با ظهور جرایم سایبری، قواعد مربوط به صلاحیت دستخوش تغییر و تحول شده و در نتیجه دیگر نمی توان با تکیه بر قواعد سنتی در خصوص این جرایم اقدام نمود و لیکن قواعد قبلی به کلی منسوخ نشده و با اندکی تغییرات در آنها می توان انواع صلاحیت ها در جرایم سایبری را باز تعریف نمود. هر چند جهت رفع مشکلات مرتبط با صلاحیت دادگاه ها در جرائم سایبری، عوامل ارتباطی جدید و خاصی برای فضای سایبر ارائه شده لیکن علیرغم آن، اعمال صلاحیت سرزمینی در فضای سایبر نسبت به سایر صلاحیت های شناخته شده با بیشترین چالش رو برو بوده و مسلماً در آینده یکی از مواردی که در تدوین قوانین و مقررات شکلی مورد توجه قرار خواهد گرفت این موضوع خواهد بود و قانونگذار می بایست نسبت به پیش بینی آن در قوانین جدید اقدام نماید.

واژگان کلیدی: صلاحیت سرزمینی، جرایم سایبری، فضای مجازی، رسیدگی کیفری.

[۱] دانشجوی دکتری تخصصی حقوق جزا و جرم شناسی، دانشکده حقوق، دانشگاه آزاد اسلامی واحد شهر قدس. (نویسنده مسئول)
hasanhaydari@yahoo.com
[۲] استادیار و عضو هیأت علمی، دانشکده حقوق، دانشگاه آزاد اسلامی واحد اسلامشهر.
alirezamillani@yahoo.com

مقدمه

پیشرفت بشر در زمینه‌های مختلف همواره مشکلاتی را نیز در بر داشته است یکی از این پیشرفت ها مربوط به توسعه فناوری اطلاعات و ارتباطات است که از آن جمله می‌توان به ظهور پدیده‌ای به نام اینترنت اشاره کرد، فضای مجازی سبب ارتباط بیشتر اشخاص در سراسر گیتی شده به نحوی که مرزها را در نوردیده و با سرعت زیاد خود باعث تسهیل ارتباطات و انتقال اطلاعات می‌شود. (خرم آبادی، ۱۳۹۱: ۴۸) رایانه ها ابزار دسترسی به اینترنت در فضای مجازی محسوب شده و با فشردن یک کلید، حجم زیادی از اطلاعات در یک لحظه از یک نقطه به نقطه دیگر قابل ارسال خواهد بود، نقاطی که ممکن است در دو سوی کره خاکی قرار داشته باشد. لازم به ذکر است که فضای سایبر منحصر به اینترنت نبوده و شامل ماهواره های واقع در مدار زمین و ایستگاه‌های زمینی آن‌ها نیز می‌شود لیکن از نظر کاربرد، مهمترین بخش فضای سایبر را اینترنت تشکیل می‌دهد چرا که از نظر تعداد و تنوع کاربران و طیف وسیع ارتباطات و اطلاعات مورد مبادله اینترنت بیشترین سهم در این فضا دارد. (دزیانی، ۱۳۷۳: ۶۳) کاربرد اینترنت و سهولت دسترسی به ارتباطات و اطلاعات در فضای سایبر از یک سو زمینه‌ساز سوءاستفاده برخی افراد سودجو و متخلف شده به نحوی که به روش های مختلف اقدام به ارتکاب جرائمی نظیر کلاهبرداری و هرزه نگاری و ... می نمایند و از سوی دیگر فضای سایبر دارای ویژگی ها و مختصات خاص خود می‌باشد که از آن جمله می‌توان به گستردگی و جهانی بودن، سرعت انتقال اطلاعات، امکان گمنامی و عدم حاکمیت عوامل کنترل اجتماعی فراوانی جرم و بزه دیدگان و ... اشاره کرد. اما مهمترین ویژگی این فضا اختصاص نداشتن و محدود نبودن آن به مرزهای جغرافیایی کشورهاست که به آن اصطلاحاً ویژگی «فرا مکانی» می گویند. این ویژگی سبب می شود تعیین دادگاه صالح جهت رسیدگی به جرایم ارتکابی در این فضا با مشکلات اساسی مواجه گردد. (دولتشاهی، ۱۳۸۳: ۵۵) در فضای واقعی جهت اعمال صلاحیت سرزمینی عواملی نظیر محل وقوع جرم، محل کشف جرم، محل اقامت و دستگیری متهم ملاک عمل است لیکن با توجه به ویژگی‌های فضای سایبر که مهمترین آن اختصاص نداشتن به مکانی خاص «فرا مکانی بودن» می‌باشد اعمال صلاحیت سرزمینی در این فضا سبب بروز تعارض مثبت بین محاکم کشورهای مختلف می‌گردد. لذا تعیین قلمرو این اصل بیشترین چالش را در رسیدگی به جرایم فضای سایبر ایجاد کرده و در رویه های مختلف کشورهای جهان می توان به محل استقرار رایانه، محل حضور بارگذار یا پیاده ساز، محل وقوع عمل، محل اثر و یا سایر امور دیگر بعنوان عوامل ارتباط دهنده صلاحیت دادگاه با عمل مجرمانه واقع شده در

فضای سایبر اشاره داشت که در این مقاله به تحلیل هر یک و امکان اعمال یا عدم امکان کاربرد آنها در فضای سایبر خواهیم پرداخت.

۱- مفهوم شناسی صلاحیت سرزمینی و فضای سایبر

صلاحیت سرزمینی یا درون مرزی به معنی اعمال صلاحیت بر اموال، اشخاص و امور واقعه در یک سرزمین یا کشور و قلمرو آن است. (آخوندی، ۱۳۹۰: ۳۴۲) قلمرو یک کشور محدود به خاک یک کشور نمی شود بلکه شامل دریای سرزمینی و قلمرو هوایی نیز می گردد. علاوه بر آن از آنجا که گاهی برخی عناصر یک جرم در خارج از قلمرو سرزمینی کشور شکل می گیرد. لذا برخی اساتید معتقد به گسترش مفهوم صلاحیت سرزمینی تحت عنوان «صلاحیت ذهنی سرزمینی»[1] می باشند. صلاحیت ذهنی سرزمینی به معنی تعقیب و مجازات جرائمی است که در قلمرو سرزمینی یک کشور شروع ولی در قلمرو سرزمین کشوری دیگر تکمیل شده یا به نتیجه رسیده باشد. (آشوری، ۱۳۸۹: ۳۳۲)

برخلاف اصل «صلاحیت ذهنی سرزمینی»، اصل «صلاحیت عینی سرزمینی»[2] حاکی از اعمال صلاحیت کشور در مورد جرائمی است که در کشور دیگر شروع شده ولی در سرزمین آنها کامل شده یا به نتیجه رسیده است و یا ارتکاب آن جرائم برای نظم اجتماعی و اقتصادی کشور آنها زیان آور بوده باشد. لذا مهمترین اصل در اعمال صلاحیت کیفری اتکاء به قلمرو حاکمیتی است که مصداق بارز آن قلمرو سرزمینی است.(جلالی فراهانی، ۱۳۸۹: ۸۷)

برای یک کشور، مؤثرترین و راحت ترین وضعیت مقابله با جرائم برخورد و مجازات آنها از طریق ملاک قرار دادن محل وقوع جرائم در قلمرو سرزمینی هر کشور می باشد، اصولاً جرایم ماهیتی محلی دارند لذا مهمترین شیوه مجازات و مقابله با آن اجرای صلاحیت محلی می باشد. البته در کنار این امر سهولت جمع آوری دلایل و قرائن و امارات محکمه پسند در کنار تأمین اهداف ارعاب انگیزی و عبرت آموزی مجازات را نباید فراموش کرد. اعمال هر گونه محدودیت نسبت به استقلال و آزادی عمل دولت ها فرضی محال و غیر ممکن است. (زندی، ۱۳۸۸: ۶۰ و ۶۶) اصل کلی این است که یک کشور تحت هیچ شرایطی مجاز به اعمال قدرت خود در قلمرو کشوری دیگر نمی باشد. از این رو صلاحیت امری سرزمینی است و اعمال آن توسط یک کشور در خارج از مرزها و قلمرو خود، جز از طریق عرف یا معاهدات بین المللی میسر نمی باشد. اما آنچه که در این مورد

[1] Subjective Territorial principle.
[2] Objective Territorial principle.

اهمیت دارد مقتضیات عصر حاضر در رسیدگی به جرایم است. در این زمینه آنچه در مورد پرونده لوتوس[1] واقع شده بیانگر این مقتضیات است. (Bigos, 2005: 554)

در این پرونده طبق رأی دادگاه دائمی دادگستری بین المللی حقوق بین المللی محدودیتی برای صلاحیتی که یک کشور ممکن است به خود اختصاص دهد قائل نشده است مگر آنکه با قاطع ترین ادله بتوان ثابت کرد که این محدودیت به عنوان یک اصل در حقوق بین الملل به رسمیت شناخته شده است در واقع دولت منکر وجود صلاحیت است که باید ثابت کند که اعمال صلاحیت غیر موجه و خلاف حقوق بین الملل است. از این رأی شاید بتوان در توسعه صلاحیت سرزمینی واعمال آن در مورد جرایم ارتکابی در فضای سایبر نیز بهره برد لیکن آنچه در مورد رای صادره شایان توجه است اینکه، ارجاع پرونده به دادگاه دائمی دادگستری بین المللی با توافق دو کشور ترکیه و فرانسه صورت گرفته است. (Brenner , 2004: 332) لذا در استفاده از این رأی برای اعمال صلاحیت سرزمینی خارج از محدوده قلمرو سرزمینی یک کشور این نکته باید در نظر گرفته شود. آنچه در تشخیص و تعیین صلاحیت سرزمینی اهمیت دارد، محل وقوع جرم و محل کشف جرم یا محل دستگیری متهم می باشد. برای تعیین محل ارتکاب جرم در فضای سایبر ابتدا باید قلمرو سرزمینی در این فضا مشخص شود و برای درک مفهوم قلمرو سرزمینی در فضای سایبر لازم است بستر تشکیل دهنده و ابزار دسترسی به آن شناسایی گردد.

۲- آشنایی با مفاهیم فضای مجازی

داده های الکترونیکی مشتمل بر مجموعه ای عظیم از صفر و یک ها «بیت» است. در واقع فضای سایبر همین بستر است که در آن داده های الکترونیکی ذخیره و پردازش و می شوند. بنابراین در

[1] دعوی مربوط به تصادم کشتی باربری ترک بنام «بوز کورت» و کشتی فرانسوی بنام «لوتوس» بود که در آن حادثه در اثر غفلت افسر دیده بانان فرانسوی حادث شد و منجر به غرق کشتی ترک و تلفات جانی شد کشتی فرانسوی به راه خود ادامه داد و در استانبول، دادگاه ترکیه به استناد قانون کیفری خود، افسر فرانسوی را به قتل غیر عمد محکوم کرد. این قانون به دادگاه ترکیه صلاحیت می داد که اتباع بیگانه را که خارج از ترکیه مرتکب جرم علیه ترکیه یا اتباع آن کشور می شوند محاکمه کند. دولت فرانسه مدعی شد که قانون مذکور به دلیل مغایرت با حقوق بین المللی بی اعتبار است، لذا دو دولت موافقت کردند که موضوع برای تعیین تکلیف به دیوان دایمی دادگستری ارجاع شود. دادگاه با رأی نصف بعلاوه یک اعلام کرد که هیچیک از قواعد حقوق بین الملل، دادگاه ترکیه را از احراز صلاحیت در قضیه مطروحه منع نمی کند، زیرا آثار عمل خلاف ناخدای فرانسوی به کشتی ترکیه سرایت کرده است. یکی از قضات دادگاه بنام قاضی مور ضمن قبول اصل صلاحیت عینی، نظر داد که قانون کیفری ترکیه خلاف اصول مسلم حقوق بین الملل است چون تبعه یک کشور هنگام سفر به کشور دیگر حقوق کشورش را برای حفاظت از خود به همراه می برد زیرا در غیر این صورت تبعه یک کشور بیگانه. ممکن است ظرف یکساعت بطور ناخودآگاه تحت عملکرد قوانین کیفری بیگانه قرار گیرد.

هر کشور که مراکز تولید کننده بسترهای الکترونیکی، که به آنها مراکز داده اینترنتی گفته می شود، وجود داشته و از لحاظ فنی به ارائه خدمات میزبانی و ملزومات تبعی آن می پردازند، آن محل جزو قلمرو حاکمیتی آن کشور قرار دارد. هر چند چنین استدلالی مؤثر و قابل دفاع است اما این نکته شایان ذکر است که در حال حاضر بیش از ۸۰٪ مراکز اینترنتی دنیا در آمریکای شمالی و شمال اروپا واقع هستند و بعید است آنها به اعمال چنین صلاحیتی برای رسیدگی به طیف بسیار متنوع و عظیم جرائم ارتکابی در فضای سایبر از سراسر جهان (که به مجرمانه بودن برخی از آنها نیز اعتقاد ندارند) تن دردهند. (فروغی و البوعلی، ۱۳۹۱: ۲۱۱)

۳- ابزار دسترسی به بستر ارتباطات و مبادلات الکترونیکی

منظور از ابزار دسترسی به بستر ارتباطات و مبادلات الکترونیکی تنها خدمات دسترسی مانند (ISP) ها که در لایه های مختلف تأمین، توزیع و عرضه خدمات اینترنتی به فعالیت می پردازند، نیست. بلکه ابزارهای هویت بخش فضای شبکه ای با عنوان، نام دامنه[۱] می باشد که از سوی عوامل مربوط ارائه می شود. آنچه به بحث ما مربوط می شود دامنه مرتبه بالا، نام دارد که بطور کلی به دو دسته تقسیم می شود دامنه مرتبه بالا عمومی[۲] (مانند Com.net) و دامنه مرتبه بالای کد کشوری[۳] (مانند ir). هرچند تمام این دامنه ها توسط یک شرکت آمریکایی بنام (ICANN) صادر می شود، اما طبق روال ایجاد شده کدهای کشوری تنها به دولت ها واگذار می شود تا آنها نسبت به تخصیص آن سیاست گذاری و اقدامات لازم را انجام دهند. در نتیجه این کدها عملاً مصداق بارز اعمال حاکمیت کشورها در فضای سایبر می باشند. برخی اساتید معتقدند این امر باید به نهادهای بین المللی مثل اتحادیه مخابرات بین المللی واگذار شود. (زندی، پیشین: ۹۰) اینک با توجه به شناخت مفهوم قلمرو سرزمینی در فضای سایبر و بسترهای ارتباطی و ابزارهای دسترسی در این فضا جهت بررسی موضوع صلاحیت سرزمینی و ارتباط آن با فضای سایبر و امکان اعمال آن در این فضا و ... لازم است شاخص های تعیین محل ارتکاب جرائم سایبری بررسی تا از این طریق محل ارتکاب و به تبع آن دادگاه صالح بر اساس صلاحیت سرزمینی مشخص و معین شود که به این موضوع تحت عنوان عوامل ارتباطی یعنی عوامل مرتبط با اصل صلاحیت سرزمینی عوامل ارتباط دهنده محل مجرمانه به دادگاه صالح یعنی عوامل ارتباط دهنده عمل مجرمانه با دادگاه صالح

[۱] (Domain Name) : مجموعه ای ۱۲ رقمی از شمارگان که بصورت ۳ تایی تقسیم و برای راحتی کاربران بصورت نام به نمایش در می آید.

[2] Generic top level Domain name.
[3] Country code top level domain name.

(محل وقوع یا کشف جرم ،محل دستگری متهم و ...) در فضای واقعی و امکان یا عدم امکان اعمال آنها در فضای سایبر مورد بررسی و تحلیل قرار می گیرد.

۴- عوامل موثر بر تعیین صلاحیت سرزمینی در جرایم و جایگاه آنها در جرایم سایبری

در فضای واقعی، عوامل ارتباطی اصل سرزمینی حسب مورد محل وقوع جرم، محل کشف جرم، محل اقامت یا دستگیری متهم و ... می باشد. لیکن با توجه به ویژگی های فضای سایبر که عمده آن، اختصاص نداشتن به مکانی خاص «فرامکانی بودن» می باشد. اعمال اصل صلاحیت سرزمینی در این فضا سبب بروز تعارض مثبت بین کشورهای مختلف می گردد.

۴-۱- محل وقوع جرم

غالباً محل وقوع جرم اساس تعیین صلاحیت و اعمال مقررات مربوطه می باشد. کنوانسیون جرائم سایبری در بخش سوم (صلاحیت ها) ماده ۲۲ بند ۱ نیز به این امر اشاره کرده و آورده است: «الف) هریک از اعضاء باید به گونه ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم صلاحیت رسیدگی به جرائم مندرج در ... این کنوانسیون را داشته باشند.[1]

۱- جرم در قلمروش ارتکاب یافته باشد.

بنابراین اتخاذ تصمیم در مورد یک جرم و اعمال صلاحیت منوط به ارتکاب جرم در قلمرو سرزمین یک کشور است اما زمانی که ارتکاب جرم در فضای سایبر باشد قلمرو یک کشور تعبیری ساده نیست. لذا می توان گفت بواسطه رویکرد سنتی موضعین کنوانسیون جرائم سایبری، معضلات مربوط به تعیین محل ارتکاب جرم، شناسایی تابعیت مرتکب وحل تعارض صلاحیت کماکان باقی است. در یک پرونده در خصوص محتوی یک سایت بر خط (on line) که مرکز آن در آمریکا و موضوع آن انتشار و فروش و حراج یادگارهای دوران نازی (که در کشور فرانسه ممنوع ولی در کشور های دیگر ممنوعیتی نداشت) بود، دادگاه فرانسه خود را صالح به رسیدگی دانست. در پرونده ای دیگر انتشار عکس های مستهجن در وب سایت توسط یک تبعه انگلیسی، که در انگلیس جرم ولی در آمریکا جرم نبود سبب رسیدگی دادگاه، انگلیس شد. در پرونده ای دیگر دادگاه آمریکایی رأی داد به اینکه رئیس یک شرکت قمار بازی سازمان یافته که آن را رهبر می کرد مسئول اعمالی (شرط بندی – قمار و ...) شناخته شده که از طریق وی از آمریکا بر روی اینترنت منتشر شد.

[1] Art. 22(1) (a) Convention on Cyber Crime.

(Goodman and Brenner, 2002: 335) لذا ملاحظه می گردد که کشورها با رویه های مختلف بواسطه آنکه اعمال، فروش، انتشار عکس های ممنوعه، تبلیغ قمار و ... در خاک آنها انجام شده خود را صالح به رسیدگی دانسته و وارد رسیدگی شده اند. لیکن کشورها رویکردهای متفاوت و متنوعی در بیان و تعریف جرایم ارتکابی در قلمرو خود دارند. گاه در برخی کشورها یا ایالات مختلف یک کشور، مجرم مورد تعقیب قرار می گیرد چه آنکه انتشار، انتقال، مخابره یا ارسال مطالب خلاف قانون (که عناصر متشکله جرم اند) در مبداء یک کشور یا ایالت صورت گرفته باشد یا اینکه آن مطلب به آن کشور یا ایالت رسیده باشد برای مثال در ایالت کارولینای شمالی، نظیر ایالت آرکانزاس، در خصوص جرائم رایانه ای، فرض بر ارتکاب عمل مجرمانه است چه پیام از آنجا ارسال شده یا به آن محل رسیده باشد. (Ibid, 11) و ((Brenner & Bert, 2004: 11 به عبارت دیگر هر دو محل ارسال و دریافت ملاک تشخیص وقوع عمل مجرمانه می باشد همچنین فرد مسئول و پاسخگو می باشد چه عمل توسط او یا دیگری در داخل یا خارج از کشور یا ایالت یک کشور ارتکاب یافته باشد چنانچه:

۱- تمام یا قسمتی ازعمل مجرمانه در یک کشور یا ایالت صورت گرفته باشد. ۲- عمل مجرمانه انجام شده (شکل گرفته) در خارج یک شروع به جرم در کشور شناخته شود. ۳- عمل مجرمانه انجام شده (شکل گرفته) در خارج توطئه ای علیه کشور محسوب شود. ۴- عمل مجرمانه انجام شده در خارج از کشور نوعی تحریک یا معاونت محسوب شود. همچنین هرگاه قسمتی از یک جرم در یک کشور ارتکاب یافته باشد خواه عناصر این جرم در داخل یا خارج آن کشور ایجاد شده باشد آن کشور صلاحیت رسیدگی خواهد داشت.[1] برای نمونه در ایالات متحده آمریکا در راستای توسعه مقررات مربوط در این خصوص می توان از مقررات سوء استفاده و جرائم کامپیوتری غرب ویرجینیا نام برد که به موجب آن هر شخص که مقررات این قانون را نقض کرده و جهت نیل و دستیابی به کامپیوتر، شبکه کامپیوتری، منابع کامپیوتری، نرم افزار، سخت افزار و ... کامپیوترهایی که در یک ایالت قرار دارند، مرتکب اعمالی نظیر دسترسی، سبب دسترسی، اجازه دسترسی و ... شود، مورد تعقیب و مجازات توسط محاکم آن ایالت قرار خواهد گرفت. در این خصوص در ایالت تاسمانیا بخش مهمی از افعال و اعمال مجرمانه موصوف مرتبط با صلاحیت محاکم ایالت تاسمانیا است.[2] علیرغم موارد مذکور، متأسفانه فقدان قوانین خاص صلاحیت، حتی در اروپا سبب شده تا در برخی موارد تعیین مقررات مربوط به در فضای سایبر مقررات عمومی ناظر بر محل ارتکاب جرم صورت

[1] Utah Code Ann. 76-1-201 (2003) 1.03(1)-(3) (official draft 1962) Ibid, 13.
[2] Art. 257F (2) (a) Tasmanian Criminal Code Act 1924.

گیرد. مثلاً در کشور هلند مقررات کیفری شامل هر متهم و هر جرم واقع در قلمرو سرزمینی آن کشور است یا مقررات کشور آلمان مقرر داشته: ۱) عمل در جایی اتفاق می افتد که مباشر فعلی را انجام دهد یا ترک فعلی نماید که جرم است. ۲) تحقق تحریک یا معاونت جرم تنها در محل وقوع جرم نیست، بلکه محل وقوع خود تحریک یا معاونت یا محل ایجاد سبب ترک فعل یا محلی که تعهدات و الزامات توسط شریک یا معاون و ... ایجاد شده باشد نیز محل وقوع جرم محسوب می شود و قابل رسیدگی و مجازات است. (Ibid, 443) مثلاً چنانچه شخصی در آلمان ایمیلی حاوی ویروس برای کاربری در بنین[۱] ارسال کند و کاربر اخیر آنرا دریافت و منتشر کند طبق قوانین کیفری آلمان به جرم معاونت در انتشار ویروس مسئول شناخته می شود صرف نظر از اینکه انتشار ویروس در بنین جرم باشد یا نباشد. در مورد شروع به جرم در فضای سایبر جالب توجه اینکه ممکن است عمل (شروع به جرم) در جایی خارج از محل مورد نظر صورت گیرد اما در جایی دیگر اثر تخریبی داشته باشد مثلاً شروع به جرمی جهت صدمه به کامپیوترهایی در نیویورک صورت گیرد حال آنکه در سنگاپور سبب صدمه گردد، در این صورت دادگاه سنگاپور صالح به رسیدگی خواهد بود. لذا در این گونه موارد یعنی: «۱) شخصی که ارتکاب جرم را تشویق می کند، مقدماتی را تدارک می بیند، یا پیش بینی می کند ممکن است مسئول شناخته شود. ۲) اثر عمل در جایی که اولین بار ظاهر می شود می تواند ملاک اعمال صلاحیت باشد در مثال فوق محاکم کشور سنگاپور دارای صلاحیت از این نظر خواهند بود.» ایالات متحده آمریکا مقرراتی در باب تلاش غیرمجاز برای تغییر مواد و اسناد کامپیوتری و یا تلاش غیرمجاز برای جلوگیری از کاربرد و استفاده از کامپیوتر وضع نموده است.[۲] لذا ملاحظه می شود که در مورد جرائم سایبری، تعیین دقیق محل وقوع جرم بسیار مشکل است چه آنکه عمل انتقال اطلاعات از طریق کامپیوترها ممکن است چندین کشور را در بر گرفته و پوشش دهد. فرضاً اینکه محتوی بدست آمده در کشوری، از کشوری دیگر شروع شده باشد و یا عمل انتقال اطلاعات از کشور A شروع و در کشور B خاتمه یافته باشد لیکن در این بین کشورهای ... ,C ,D ,F را در بر گیرد. (Ibid , 10) بدین جهت این نظریه مطرح شده که انتشار اطلاعات در وب سایت واقع در محل قرار گرفتن کامپیوتر میزبان (Hosting)، می تواند محل وقوع واقعی اسناد باشد زیرا انتشار اطلاعات عملی مداوم است که مستمراً از لحظه شروع انتقال اطلاعات (از کامپیوتر میزبان) صورت می گیرد. لذا عمل مجرمانه تنها در کشور محل وقوع کامپیوتر میزبان واقع می گردد. (Ibid,16) علی ایحال چنانچه جرم سایبری در محدوده قضایی محاکم کشورهای متعدد واقع شود، همه آنها خود را صالح به رسیدگی

[۱] Benin: شهری در آفریقا.

[2] See, e.g., Or Rev. Stat. 131.215 (2003)

خواهند دانست لیکن فقدان راهنما، الگو یا دستورالعملی خاص در این زمینه برای دولت ها یا کشورها سبب می شود که آنها رویکردهای متفاوتی در برخورد با موضوع صلاحیت در مورد این گونه جرائم داشته باشند. بنابراین بنظر می رسد تعیین محل ارتکاب جرائم سایبری بعنوان مبنایی برای اعمال صلاحیت، از مسائلی است که نیازمند تحقیق و مطالعه ای خاص و گسترده باشد. (فروغی و البوعلی، پیشین: ۲۱۲)

۴-۲- محل قرار گرفتن (موقعیت) رایانه

منظور از رایانه یا سیستم رایانه ای موضوع بحث برابر تعریف ماده ۱ کنوانسیون جرائم سایبری عبارت است از: «هر دستگاه یا مجموعه ای از دستگاه های مرتبط یا متصل به یکدیگر است که یک یا چند تای آنها مطابق یک برنامه، پردازش خودکار داده ها را انجام می دهد.» با توجه به تعریف فوق اولاً؛ کامپیوترهای شخصی و غیر متصل که نقشی در فضای سایبر ندارند از موضوع بحث خارج می باشند. در فضای سایبر تنها کامپیوترهایی مد نظرند که در شبکه، مرتبط «متصل» به یکدیگرمی باشند. ثانیاً؛ همانگونه که قبلاً نیز گفته شد فضای سایبر اختصاص به اینترنت ندارد و موارد دیگری نظیر ماهواره ها و ... را نیز در بر می گیرد، لیکن به جهت اینکه اینترنت واجد تمام ویژگی های خاص فضای سایبر است بیشتر به آن پرداخته می شود. بر اساس قوانین برخی از کشورها، ملاک در تعیین و اعمال صلاحیت محاکم در خصوص جرائم ارتکابی در فضای سایبر محل قرار گرفتن رایانه است لذا چنانچه عمل مجرمانه ای نظیر انتشار یک ویروس یا اعمال متقلبانه نظیر کلاهبرداری و جعل از طریق کامپیوتری که در یک محل قرار گرفته صورت گیرد دادگاه آن محل صالح به رسیدگی می باشد. خواه مرتکب در کشور یا محل قرار گرفتن کامپیوتر ساکن باشد یا نباشد وخواه تبعه آن کشور باشد یا نباشد و خواه اینکه عمل در داخل کشور یا خارج از آن کشور صورت گرفته باشد. (شریفی، ۱۳۷۹: ۳۵۴) در این خصوص مقررات کشور سنگاپور مقرر داشته: «۱- هر شخص که در ارتکاب جرائم مندرج در این قانون معاونت یا شروع به ارتکاب نماید یا مقدمات آن را انجام دهد یا در مسیر ارتکاب آن عمل کند مجرم شناخته و به مجازات مقرر محکوم خواهد شد. ۲- در خصوص جرائمی که مطابق این بخش ارتکاب می یابند محل ارتکاب هیچ تاثیری ندارد.»[1] اما مهمتر از آن در ماده ای دیگر از مقررات یاد شده در خصوص حوزه و قلمرو جرائم آمده: «... ۱- مطابق مقررات این قانون در مورد هر شخص چه تابعیت یا شهروندی سنگاپور را داشته باشد چه نداشته باشد و یا در داخل یا در خارج از این کشور حضور داشته باشد،

[1] Art 10 Singapore Computer misuse Act (25/JAN/2008).

قابل اجرا خواهد بود؛ ۲- در جایی که جرم مطابق این قانون توسط هر شخص در هر محل خارج از این کشور ارتکاب می یابد، فرض بر این است که وی جرم را در داخل سنگاپور مرتکب شده است؛ ۳- ... این قانون نسبت به جرایم زیر نیز قابل اجرا خواهد بود.

الف) متهم در مدت مقتضی در سنگاپور باشد؛ ب) رایانه، برنامه یا داده ها در مدت مقتضی در سنگاپور باشد.»[1]

مقررات کشور مالزی نیز در این خصوص مقرر داشته:

مقررات این قانون نسبت به هر شخص، چه تابعیت یا شهروندی مالزی را داشته یا نداشته باشد و ارتکاب عمل در داخل یا خارج از کشور باشد قابل اجرا خواهد بود. در جایی که جرم مندرج در این قانون توسط هر شخص در هر مکان خارج از کشور مالزی ارتکاب یابد با وی به مثابه ارتکاب جرم در مالزی برخورد خواهد شد. در جهت اهداف ... این قانون در صورتی اجرا خواهد شد که کامپیوتر برنامه یا داده های واقع در مالزی در ارتکاب جرم نقش داشته باشند یا اینکه بتوان در مهلت مقتضی از طریق یک کامپیوتر در مالزی به آنها متصل شد یا آنها را ارسال یا از آنها استفاده کرد.»[2] بنابراین ملاحظه می شود برابر ضوابط برخی کشورها آنچه در تشخیص، تعیین و اعمال صلاحیت در مورد جرایم ارتکابی در فضای سایبر ملاک است، محل استقرار یا موقعیت مکانی سیستم های رایانه ای است.

در ارتباط باسیستم های رایانه ای و محل استقرار آنها استفاده کنندگان، کاربران این سیستم ها می باشند که در تشخیص و تعیین محل ارتکاب جرائم سایبری نقش داشته و در سطور آتی بدان اشاره می نماییم. در خصوص ماهواره هایی که در مدار زمین قرار دارند نیز این بحث مطرح است، بدین صورت که ملاک تعیین و اعطاء صلاحیت محاکم موقعیت ایستگاه زمینی ماهواره و محل استقرار کامپیوترهای مربوطه است البته یکی دیگر از عوامل اعطاء صلاحیت در خصوص ماهواره ها می تواند تابعیت آن یعنی کشوری که ماهواره تحت نام آن کشور به ثبت رسیده باشد.

[1] Art 11 Singapore Computer misuse Act (25/JAN/2008).
[2] Art 9 Singapore computer misuse Act (25/JAN/2008).

۴-۳- محل حضور (بارگذار) یا (پیاده ساز) شبکه رایانه ای به عنوان محل ارتکاب جرایم سایبری

بطور کلی در فضای سایبر دو گروه عمده ایفای نقش می کنند. اشخاصی که داده ها را از طریق کامپیوتر در این فضا قرار می دهند که به آنها بارگذار یا(Up loader) گفته می شود یا اشخاصی که داده ها را از این فضا و از طریق کامپیوتر دریافت می کنند که به آنها پیاده ساز (Down loader) گفته می شود. در اینجا نیازی نیست که هویت همگی این افراد مشخص بوده و یا از یکدیگر مطلع باشند لذا نباید آنها را با فرستنده (Sender) و گیرنده (Receiver) که معمولاًهویتشان در ارتباطات الکترونیکی معلوم است اشتباه گرفت همچنین معیار بارگذار ی و پیاده سازی را نباید و نمی توان بر عناوین «بزهکار و بزه دیده» حمل کرد چه آنکه همان قدر که ممکن است بارگذار مرتکب جرم باشد، احتمال دارد بزه دیده جرم تلقی شود. مثلاً در جایی که بارگذار محتوی مجرمانه ای را نظیر تصاویر مستهجن یا هتک حرمت و یا ویروس یا توهینی را بر روی شبکه قرار می دهد مرتکب جرم است اما هنگامی که داده ها ی مشروعی را بارگذاری کرده ولی این داده ها بطور غیر مجاز توسط یک پیاده ساز مورد سوء استفاده قرار می گیرد، بزه دیده است. لذا در این گونه موارد ملاک تعیین صلاحیت حسب مورد محل شخص بارگذار یا پیاده ساز است، از همین روست که در قوانینی ایالات آرکانزاس و کارولینای شمالی آمده که ارتباطات رایانه ای چه از این ایالت نشأت گرفته یا به آن ختم شود (یعنی خواه بارگذاری و خواه پیاده سازی شده باشد) مراجع قضایی این ایالت صالح به رسیدگی خواهند بود.[1] لذا می توان گفت که اعطاء صلاحیت به دادگاه ها می تواند تحت تأثیر و محل استقرار کامپیوترهایی باشد که مورد استفاده برگذار یا پیاده ساز باشد همچنان که در برخی از ایالات آمریکا اینگونه عمل می شود.[2]

۴-۴- موقعیت مکانی مرتکب جرم

یکی دیگر از مسائلی که در رابطه با اصل سرزمینی و ارتباط آن با جرایم ارتکابی در فضای سایبر جهت تشخیص صلاحیت محاکم کیفری می تواند مورد بحث و توجه قرار گیرد. موقعیت مکانی اشخاص است. برخی اوقات محل استقرار اشخاص مؤثر در تعیین و اعطاء صلاحیت است بعنوان مثال محل استقرار بزه دیده «مجنی علیه» یا قرار داشتن مراکز اصلی یک شرکت یا نمایندگی های آن و ... در داخل قلمرو سرزمینی یک کشور می تواند در تعیین دادگاه صالح مؤثر باشد. (عالی

[1] Ark. Code Ann .5-27 606 (2003).
[2] See Conn. Gen .Stat. Ann 53a-261 (quoted in III (A) supra).

پور، ۱۳۹۰: ۴۳) آنچه اهمیت دارد اینکه، محل استقرار اشخاص که بطور سنتی محل وقوع جرم وبه تبع آن صلاحیت دادگاه را تعیین می کند در فضای سایبر نمی تواند آنچنان تعیین کننده باشد. چرا که نمی توان انتظار داشت در فضای سایبر محل استقرار بزه دیدگان مختلف و متعدد که در مکان های مختلف تحت تأثیر یک جرم سایبری قرار دارند ملاک تعیین و اعطاء صلاحیت باشد برای مثال در مورد ایراد سخنان نفرت انگیز نسبت به یهودیان که بزه دیدگان آن تمام یهودیان بوده و در برخی کشورها جرم تلقی می شود، اگر ملاک تعیین صلاحیت محل استقرار یهودیان باشد در این صورت آیا محاکم هر کشوری که یهودیان در آن ساکن هستند قادر خواهد بود که ادعای صلاحیت نماید؟

مثال دیگر در این خصوص رعایت حقوق کودکان در فضای سایبر و ممنوعیت هرزه نگاری و انتشار تصاویر مستهجن در ارتباط با کودکان است این اقدامات در کشورهایی مانند آمریکا، کانادا و هلند به موجب کنوانسیون های مربوطه جرم تلقی می شود. اما سؤال اینجاست که قربانی این گونه جرایم چه کسانی هستند؟ آیا با این استدلال که تصاویر مستهجن باید قابلیت انتساب به کودکان واقعی را داشته باشد، کودکان واقعی که تصاویر آنها مورد سوء استفاده قرار گرفته قربانیان این جرم اند یا از آنجا که تمام کودکان بالقوه بزه دیدگان این جرم اند، قربانیان این جرم تلقی می شوند؟[1] آیا کشور «الف» که هرزه نگاری کودک در آن جرم است می تواند در مورد هرزه نگاری انجام شده در موقعیت و توسط کشور «ب» ادعای صلاحیت کند؟ پاسخ به این پرسش منوط به اثبات این امر است که آیا هرزه نگاری مذکور در حقیقت تمایلات جنسی در منحرفین ایجاد می کند یا خیر؟[2]

چنانچه کشور «الف» بتواند ثابت کند که تصاویر مذکور که در کشور «ب» ایجاد شده از علت های جرایم ارتکابی علیه شهروندان آن بوده است، می تواند ادعای صلاحیت بر اشخاص ساکن در کشور «ب» که مسئول انتشار این تصاویر مستهجن بوده اند را بنماید، به عبارت دیگر اثبات رابطه سببی «علی– معلولی» بین تولید یا انتشار تصاویر مستهجن از کودکان «هرزه نگاری کودکان» با جرایم ارتکابی علیه کودکان در کشور «الف» می تواند مثبت صلاحیت محاکم این کشور باشد. (خرم آبادی، ۱۳۸۴: ۳۳۲) این در صورتی است که مرتکب جرم در کشور «ب»، تابعیت یا ملیت کشور «الف» را نداشته یا بنا به دلایلی نتواند استرداد وی را تقاضا کند. این امر مد نظر در کنوانسیون

[1] In Ashcroft v. Free Speech Coalition , 535 U.S 234 (2002).

[2] Those who support banning virtual child pornography argue that in incites sexual abuse of children: those who oppose such a ban argue that it provides ,substitute satisfacation ,, and reduces offences. See R.V sharpe, 2001 can sup ct .LEXIS 8(2001).

های مربوط به جرایم سایبر[۱] و نیز اساس و پایه صلاحیت عام در کشور آلمان[۲] است. همچنین کشورها می توانند بر افراد و اشخاص خارجی که مرتکب جرم مذکور در خارج از مرزها و قلمرو سرزمینی کشوری شده اند ولی ساکن و مقیم در آن کشور هستند، حتی اگر درخواست سکونت یا اقامت کرده باشند ادعای صلاحیت نمایند، مانند کشور هلند که در آن تعقیب متهم یا مظنون می تواند صورت گیرد حتی اگر اخذ اقامت پس از ارتکاب جرم باشد.[۳] کشور سنگاپور نیز در این زمینه مقررات مشابهی دارد.[۴]

۴-۵- محل بروز آثار عمل مجرمانه

یکی دیگر از مواردی که می تواند مرتبط با موضوع صلاحیت دادگاه باشد محل واقع شدن اثر فعالیت های غیرمجاز در فضای سایبر است. صلاحیت بطور مرسوم و متعارف دلالت بر کاربرد آن بر مبنای رفتار انجام شده در داخل مرزهای یک کشور دارد اماحکومت هایی که به دنبال اعمال صلاحیت خود بر اعمال ارتکابی در خارج از قلمرو سرزمینی خود هستند تنها در صورتی می توانند صلاحیت خود را بکار برند که عمل انجام شده در خارج از کشور، اثری صدمه آورد در داخل قلمرو سرزمینی آنها ایجاد کرده باشد. مقررات عمومی کیفری ایالت میشیگان در باب صلاحیت مقرر داشته که: ایالت مذکور می تواند شخصی را که جرایمی را در این ایالت ایجاد کرده (مرتکب شده) یا عمل وی واجد اثری در این ایالت است را تحت تعقیب قرار دهد.[۵] همچنین مقررات ناظر بر جرایم رایانه ای دولت مرکزی (فدرال) به دولت آمریکا اجازه داده که بر جرائم کامپیوتری در صورت و جود اثر بین ایالات مختلف یا تجارت یا ارتباطات خارجی ایالات متحده، اعمال صلاحیت کند.[۶]

در ایالت تاسماینا محاکم می توانند نسبت به جرایم سایبری (در صورتی که از ارتکاب این جرائم، صدمه ای اساسی و اثرگذار حادث شده باشد) ادعای صلاحیت نمایند. در این جا ارتباطی اساسی و واقعی با ایالت تاسماینا مد نظر می باشد لذا در این ایالت چنانچه فعل انجام شده کاملاً خارج از

[1] Art, 22(3) convention on cybercrime).Ibid, 19.
[2] (German CC). Ibid, 19.
[3] Art 5 a(2) Wtboek van strafrecht (Dutch CC) (Belgian PTCCP).
[4] Art. 11(3) Singapore Computer Misuse Act.(25/JAN/2008).
[5] State v. Dudley, 354 S.C.514.581 S.E.2d 171 (2003).
[6] U.S Code 1030 (e) (2) (B) (2004). Ibid, 20.

ایالت تاسمانیا واقع شده و یا قسمتی در تاسمانیا واقع شده ولی اثرات صدمه آور اساسی در این ایالت بوجود آورده باشد می توان نسبت به آن ادعای صلاحیت کرد.[1]

۴-۶- سایر عوامل تأثیر گذار بر صلاحیت سرزمینی

یکی از دیگر عوامل ارتباطی بین صلاحیت و جرائم ارتکابی در فضای سایبر محل وقوع سایر امور بجز موارد یاد شده می باشد. این امور که موارد آن را می توان در مقررات ناظر بر جرایم کامپیوتری ایالت ویرجینیای غربی ایالت متحده آمریکا مشاهده کرد که شامل اموری از قبیل دسترسی، مجوز دسترسی، سبب دسترسی، تلاش برای دسترسی به کامپیوتر یا شبکه کامپیوتری، اطلاعات کامپیوتری، منابع کامپیوتری یا نرم افزار و سخت افزار و ... که در ایالت مذکور صورت گرفته یا بصورت گذرا از این ایالت واقع شوند می باشد. مشابه مقررات ایالت ویرجینیای غربی، کشورهای سنگاپور و مالزی نیز رویکرد مشابهی در خصوص جرائم کامپیوتری دارند. مقررات کشور سنگاپور در بندهای مربوط به صلاحیت تحت شرایطی طریق فوق را پذیرفته و مقرر داشته محدوده سرزمینی جرائم رایانه ای مشروط به امور زیر است:

- موضوع جنبه فرعی داشته و ادامه امر اصلی تلقی شود.

- مقررات ناظر به اشخاص داخل یا خارج سنگاپور است چه تابعیت یا ملیت را داشته یا نداشته باشند.

- مقررات مذکور صرفاً ناظر بر جرایم کامپیوتری است خواه متهم یا کامپیوتر یا برنامه و اطلاعات و ... در سنگاپور باشند یا نباشند. مقررات کشور مالزی نیز با اعمال محدودیتی کمتر ولی مشابه با سنگاپور مقرر می دارد:

۱) مقررات جرایم کامپیوتری ناظر بر همه اشخاص است چه تابعیت یا ملیت مالزی را داشته یا نداشته باشند.

۲) مقررات فوق شامل کامپیوترهایی که موارد مذکور در فوق را از طریق کامپیوترهای واقع در مالزی انجام می دهند یا کامپیوترهایی که واسطه انتقال اطلاعات یا ... می باشند، است.[2] در این خصوص موضوعی بحث انگیز در خصوص اعمال صلاحیت که در سال ۲۰۰۰ مطرح شد بیان می

[1] Art, 257F (2) (b) Tasmanian Criminal Code Act 1924.
[2] Art, 9 Malaysia computer Crimes Act, (1997).

شود: در این سال FBI آمریکا دو فرد با نام های راسلی گوراشکف و آلکسی ایوانف را بعنوان هکرهایی که در سیستم های کامپیوتری تجاری آمریکا نفوذ کرده بودند را شناسایی کرد.[1] پلیس آمریکا با تحقیقات و تله گذاری پلیسی نهایتاً موفق به شناسایی و دستگیری گوراشکف و ایوانف شد. در جریان تعقیب گراشکف اقدام به محو مدارک تحصیلی از کامپیوتر روسی کرد در این زمان این سؤال پیش آمد که موضوع ربایش و تصرف داده ها (هک) آیا قوانین آمریکا را نقض کرده و یا برخلاف قوانین روسیه بوده است؟ دادگاه آمریکا اینگونه اظهار نظر کرد که: «آنجا که موضوع مستقیماً متوجه شهروندان امریکا نبوده و نیز اقدامات انجام شده مشمول قانون آمریکا (اصلاحیه چهارم) نمی باشد لذا دادگاه های آمریکا صلاحیت رسیدگی ندارند.» همچنین دادگاه اعلام کرد که اقدامات مذکور مقررات روسیه را نیز نقض نکرده است. برخلاف این نظر عده ای اعتقاد داشتند که اقدامات مذکور تصاحب، تصرف و محو داده های کامپیوتر روسی در حقیقت نقض حاکمیت سرزمینی کشور روسیه محسوب می شود. عده ای دیگر را اعتقاد بر این است که تمام کشورهای متأثر از جرم صالح به رسیدگی می باشند.)خرم آبادی، پیشین: ۳۰۲) در حال حاضر طبق یک نظریه، در مورد چنین اقدامات فرامرزی نظیر آنچه در پرونده گراشکف و ایوانف مطرح شده، زمانی که اطلاعات بطور عمومی قابل دسترسی است، نقض حاکمیت محسوب و اعمال صلاحیت مجاز است مگر اینکه دولت تحت تأثیر به این نفوذ «دسترسی» رضایت دهد. این رویکرد در ماده ۳۲ کنوانسیون جرایم سایبری نیز مد نظر قرار گرفته و دسترسی به داده های عمومی یا دسترسی با رضایت کشورها را مجاز دانسته لیکن آنچه مهم است اینکه موضوع اعمال صلاحیت در این گونه موارد هنوز هم راه حل واحد و قطعی نیافته است. لذا با توجه به اینکه جرایم سایبری گرایش فراملّی و ویژگی و ماهیت نا پایدار دارند. همکاری و معاهدات بین المللی و نیز اقدامات سریع در جهت دستیابی به مدارک جرم اهمیت بسزایی دارند.

۵- آسیب شناسی و بررسی چالش های مرتبط با صلاحیت سرزمینی در جرایم سایبری

در رابطه با جرایم سایبر بیشترین چالش صلاحیتی به اصل صلاحیت سرزمینی بر می گردد چه آنکه به تبعیت از اصل صلاحیت سرزمینی، در صلاحیت محلی (در مفهوم سنتی خود) ملاک اعطا و اعمال صلاحیت به محاکم داخلی حسب مورد محل وقوع جرم محل دستگیری مجرم یا متهم یا محل اقامت مجرم یا متهم است. علی القاعده کشورها تنها قادرند قوانین خود را در قلمرو سرزمینی شان اعمال کنند، لیکن این امر در فضای سایبر با مشکل روبروست، مثلاً در پرونده ای

[1] U.S V. Gorshkove, 2001 WL 1024026 at 1(W.D.W.A.MAY 23, 2001) (2004) op. cit, 21.

در آلمان در ارتباط با تعقیب یک نئونازی استرالیایی که محتوای حاوی انکار هولوکاست را در یک سرور عمومی منتشر کرده بود، تنها زمانی که وارد کشور آلمان شد دستگیر، محاکمه و محکوم شد. (عالی پور، پیشین: ۴۱۱) لذا در مورد در فضای سایبر که با توجه به ویژگی های آن، مکان وجود نداشته، مرز قابل تصور نیست و هر لحظه انتقال اطلاعات در کشورها و نقاط مختلف یک کشور صورت می گیرد و ... سؤال این است که محل وقوع جرم کجاست؟ محل ارسال داده پیام و اطلاعات یا محل دریافت آن یا محل استقرار رایانه یا محل اثر عمل یا امور دیگر که شرح آن گذشت لذا بحث چالش برانگیز این است که کدام دادگاه صالح به رسیدگی به ارتکاب جرایم سایبری است. دادگاه محل ارسال داده پیام، اطلاعات و ... یا دادگاه محل دریافت محل اطلاعات و یا دادگاهی که کامپیوتر حاوی ویروس یا انتقال دهنده ی ویروس در حوزه آن قرار دارد یا برابر یک نظر که به نظریه وب سایت فعال و منفعل معروف است (Active & Passive website) محاکم کیفری یک کشور در صورتی می تواند نسبت به یک وب سایت اعمال صلاحیت کنند که آن وب سایت با آن کشور رابطه فعالی داشته باشد و بطور غیر مستقیم اتباع آن را مخاطب قرار دهد یا نظرات دیگر که هر یک می تواند در این خصوص راهگشا باشد لیکن اعمال هر یک از این نظرات مشکلات و چالش های دیگری نظیر تعارضات صلاحیتی پدید خواهد آورد. چرا که در صورت عدم توافق کشورها بر یک عامل ارتباطی پیشنهاد شده در فضای سایبر ممکن است هر کشور، یکی از این عوامل را ملاک اعمال صلاحیت دانسته (مثلاً کشور «الف» محل وقوع جرم، کشور «ب» محل قرار گرفتن کامپیوتر و ...) فلذا بحث تعارض صلاحیت کماکان باقی خواهد ماند و تنها در صورت توافق کامل کشورها در سطح بین المللی است که می توان با اتخاذ روشی واحد و قرار دادن یک ملاک و معیار مورد توافق بین المللی در تعیین دادگاه صالح در فضای سایبر اقدام نمود. به جهات مشروحه فوق عمده ترین مشکل و چالش صلاحیتی در ارتباط با فضای سایبر به اصل صلاحیت سرزمینی بر می گردد. (خالقی و جودکی، ۱۳۸۹: ۴۰۲)

نتیجه گیری

اهمیت موضوع صلاحیت تا بدان حد است که در حقوق داخلی کشورها سبب تفکیک یا استقلال قوا شده و در بعد بین المللی نیز نشانگر قدرت سیاسی، قضایی، اجرائی و بطور کلی اقتدار یک حکومت است. یکی از اصول صلاحیت و شناخته شده در فضای واقعی صلاحیت سرزمینی است لیکن اعمال این اصل در فضای سایبر در تقابل با ویژگی «لامکانی بودن» یعنی اختصاص نداشتن فضای سایبر به مکان و موقعیت جغرافیایی خاص و بطور کلی یک سرزمین است جهت امکان اعمال این اصل صلاحیتی در فضای سایبر پیشنهاداتی شده تا ملاک هایی برای تعیین صلاحیت دادگاه باشد اما هر یک از آنها واجد معضلات مربوط به خود است. ملاک قرار دادن «محل وقوع جرم» جهت تعیین دادگاه صالح در فضای سایبر با این مشکل روبروست که در این فضا تعیین مکان و محل خاص و محل وقوع جرم مشابه آنچه در فضای واقعی به کار می‌رود عملاً ممکن نیست. یک عمل مجرمانه در فضای سایبر در یک لحظه کشورهای مختلفی را متأثر می کند فلذا محاکم کشورهای متعددی در مورد آن ادعای صلاحیت خواهند کرد. از طرف دیگر ممکن است یک کشور محل وقوع جرم و کشوری دیگر محل شروع به جرم و کشور ثالث محل ارتکاب معاونت جرم را ملاک تعیین صلاحیت بداند، بدین ترتیب مشکل تعارض صلاحیت بین محاکم کشورهای مختلف کماکان باقی خواهد ماند. پیشنهاد دیگر جهت اعمال اصل صلاحیت سرزمینی در فضای سایبر آن است که «محل قرار گرفتن کامپیوتر یا سیستم‌های کامپیوتری» که ابزار مؤثر در اینترنت هستند ملاک تعیین صلاحیت باشد بدین نحو که کشوری که کامپیوتر مورد استفاده در جرم سایبری در آن واقع است صالح به رسیدگی باشد یا اینکه «محل حضور بارگذار (Up loader) و یا پیاده ساز(down loader)» یا «موقعیت مکانی اشخاص بزه دیده ملاک تعیین دادگاه صالح باشد. در خصوص این آخری باید گفت که تعیین موقعیت مکانی اشخاص مشابه آنچه در فضای واقعی ممکن است مورد استفاده قرار گیرد، در فضای سایبر نمی‌تواند تعیین کننده باشد چرا که ممکن است بزه دیدگان مختلف در کشورهای متعدد تحت تأثیر جرم سایبری قرار گیرند. پس به‌طور قطع و یقین نمی توان گفت که دادگاه کدام کشور صالح به رسیدگی است. از دیگر پیشنهادات ارائه شده «محل وقوع یک عمل مجرمانه سایبری» یا «محل وقوع امور دیگر» نظیر دسترسی غیرمجاز تلاش برای دسترسی غیر مجاز و ... است. همانگونه که ملاحظه می‌شود علاوه بر مشکلات خاص هر یک از عوامل پیشنهادی بر فرض قابلیت پذیرش و اعمال آنها، هر کشوری ممکن است یکی از این عوامل را ملاک تعیین صلاحیت محاکم خود بداند به عنوان مثال کشور «الف» محل وقوع جرم کشور «ب» محل قرار گرفتن کامپیوتر، کشور «ج» محل وقوع اثر و ... بدین ترتیب در مشکل

تعارض صلاحیت کماکان باقی خواهد. در نتیجه می‌توان گفت اعمال صلاحیت سرزمینی در فضای سایبر با بیشترین چالش روبرو بوده و به کارگیری عوامل پیشنهادی ارائه شده نیز منوط به توافق تمام کشورها بر سر ملاک قرار دادن یکی از پیشنهادات و اتفاق نظر بین المللی بر تعیین دادگاه صالح به رسیدگی به جرم واقع شده در فضای سایبر می باشد.

منابع

۱- آخوندی، محمود، (۱۳۹۰)، آیین دادرسی کیفری (سازمان وصلاحیت مراجع کیفری)، وزارت فرهنگ و ارشاد اسلامی؛ سازمان چاپ و انتشارات، جلد دوم، چاپ سیزدهم، تهران.

۲- آشوری، محمد، (۱۳۸۹)، آیین دادرسی کیفری (انواع صلاحیت های کیفری و نحوه اعمال آنها در ایران)، انتشارات سمت، جلد دوم، چاپ دوازدهم، تهران.

۳- بای، حسینعلی، و پور قهرمان، بابک، (۱۳۸۸)، بررسی فقهی حقوقی جرایم رایانه ای، انتشارات پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول، تهران.

۴- جلالی فراهانی، امیرحسین، (۱۳۸۹)، درآمدی بر آیین دادرسی کیفری جرایم سایبری، انتشارات خرسندی، چاپ اول، تهران.

۵- خرم آبادی، عبدالصمد، (۱۳۸۴)، جرایم فناوری اطلاعات، پایان نامه مقطع دکتری، دانشکده حقوق و علوم سیاسی دانشگاه تهران.

۶- خالقی، ابوالفتح؛ جودکی، بهزاد، دادگاه ذیصلاح در بزه معاونت در جرم در قلمروی حقوق جزای بین الملل با تکیه بر جرایم سایبری، مجله مطالعات حقوقی، چهاردهم، ۲، ۱۳۸۹. ۳۷-۵۶.

۷- خرم آبادی، احمد، (۱۳۹۱)، حقوق کیفری فناوری اطلاعات، مسؤولیت کیفری ارائه دهندگان خدمات اینترنتی، انتشارات دادیار ، چاپ اول، اصفهان.

۸- دزیانی، محمدحسن، (۱۳۸۰)، صلاحیت رسیدگی به جرایم در فضای سایبر، خبرنامه انفورماتیک، سال دوازدهم، ۷. (۴۳-۴۸)

۹- دزیانی، محمد حسن، (۱۳۷۳)، ابعاد جـزایی کاربـرد کامپیوتر و جرایم کامپیوتری، خبرنامه انفورماتیک، انتشارات شورای عالی انفورماتیک کشور، ۵۱. (۴۴-۶۵)

۱۰- دولتشاهی، شاهپور، (۱۳۸۳)، صلاحیت قضایی در محیط مجازی، مجموعه مقاله های همایش بررسی جنبه های حقوقی فناوری اطلاعات، تهران، دانشگاه شهید بهشتی، دانشکده ادبیات و علوم انسانی، معاونت پژوهشی.

۱۱- زندی، محمدرضا، (۱۳۸۸)، صلاحیت در جرایم سایبری، ماهنامه قضاوت، ۶۰. (۵۴ -۶۷)

ISSN: 2783-1329
شماره مجوز انتشار: ۸۷۰۱۹

۱۲- شریفی، مرسده، (۱۳۷۹)، جرایم رایانه ای درحقوق جزای بین المللی، پایان نامه ارشد دانشگاه آزاد واحد تهران مرکز.

۱۳- عالی پور، حسن، (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، انتشارات خرسندی، چاپ اول، تهران.

۱۴- فروغی، فضل الله؛ البوعل، امیر، (۱۳۹۱)، صلاحیت کیفری مراجع قضایی در فضای سایبر، مجله تحقیقات حقوقی دانشگاه شهید بهشتی، سال دوازدهم، ۴. (۲۱۱-۲۳۲)

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

16- Brenner, Susan W, and Bert Jaap koops, Approaches to Cybercrime Jurisdiction," Journal of High Technology 5 .(۲۰۰۴)

17- 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.

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

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

20- 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.

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

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

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

ISSN: 2783-1329
شماره مجوز انتشار: ۸۷۰۱۹

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

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

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

www.jhvmn.ir
فصلنامه علمی حقوق و مطالعات نوین، دوره ۳، شماره ۴، پیاپی ۹، زمستان ۱۴۰۱
ISSN: 2783-1329
شماره مجوز انتشار: ۸۷۰۱۹

A comparative study of the territorial jurisdiction in dealing with cybercrimes based on Iran's criminal system

Hassan Heydari [1] / Dr. Alireza Milani[2]

Abstract

The use and utilization of information and communication technology, despite the positive effects and facilitation of communication and global interactions, has caused a challenge in determining the rules governing the jurisdiction of criminal courts for crimes committed in cyberspace. And the determination of a competent criminal court to deal with crimes committed in real space are mainly based on place and border, while in cyberspace there are no borders and restrictions. Therefore, the present study answers the question of whether the traditional rules of jurisdiction in cyberspace Is it applicable? And what are the challenges of exercising this competence in cyberspace? The biggest challenge in determining the competent criminal court for crimes committed in cyberspace is related to territorial jurisdiction because the lack of dependence on a specific place is a feature of cyberspace. With the advent of cybercrime, the rules of jurisdiction are changing. As a result, it is no longer possible to proceed based on traditional rules regarding these crimes, but the previous rules are not completely obsolete and with a few changes in them, the types of competencies in cybercrime can be redefined. Although in order to solve the problems related to the jurisdiction of courts in cybercrime, new and specific communication factors have been proposed for cyberspace, but despite that, the application of territorial jurisdiction in cyberspace compared to other known jurisdictions is the most challenging. Certainly, in the future, this will be one of the issues that will be considered in the formulation of formal laws and regulations, and the legislator should take action to provide for it in the new laws.

keywords: Territorial Jurisdiction, Cybercrime, Cyberspace, Criminal Investigation.

[1] Doctoral student in criminal law and criminology, Faculty of Law, Islamic Azad University, Quds branch. (Corresponding Author)
hasanhaydari@yahoo.com
[2] Assistant professor and faculty member, Faculty of Law, Islamic Azad University, Islamshahr branch.
alirezamillani@yahoo.com