صلاحیت کیفری در فضای سایبری

اسماعیل عبدالهی[1]، سکینه مرادی[2]

تاریخ دریافت: ۱۳۹۴/۱۰/۱۳
تاریخ پذیرش: ۱۳۹۴/۱۱/۱۹

چکیده

یکی از مسائل جدید که به موازات تحول فنّاوری در زمینه اطلاعات و رایانه به وجود آمده است، دنیای مجازی جدید به نام فضای سایبر است. از مهم‌ترین مسائلی که باید در این حوزه مورد توجه قرارداد، تعیین تکلیف راجع به چگونگی تعیین مرجع قضایی صالح جهت رسیدگی به جرائم ارتکابی در فضای مذکور یعنی صلاحیت کیفری مراجع قضایی است. علی‌رغم وجود اختلافات در خصوص محل وقوع جرم و ضابطه تشخیص آن جهت تعیین دادگاه یا دادسرای صالح مسئله مهمی که در این زمینه به ویژه در دهه‌های اخیر به وجود آمده است، تشخیص محل وقوع جرم در فضای سایبر است. چون فضای الکترونیکی و اینترنت با فضای فیزیکی و جغرافیایی ملموس که حقوق سنتی ناظر به آن است متفاوت است به طوری که این فضا کاملاً غیر ملموس و مجازی است و مرز جغرافیایی نمی-شناسد. این تفاوت صلاحیت مراجع قضایی مختلف در رابطه با آن جرائم در حقوق کیفری را برانگیخته است.این پژوهش با استفاده از روش توصیفی – تحلیلی به انجام می‌رسد، ابتدا عناصر متشکله جرم سایبری مورد بررسی قرار می‌گیرد، آنگاه با توجه به ماهیت جرم مذکور و شرایط ارتکاب جرم (بالاخص مکان ارتکاب جرم) به تحلیل صلاحیت در خصوص رسیدگی به جرائم ارتکاب یافته می‌شود.در این تحقیق، روش گردآوری اطلاعات به صورت کتابخانه‌ای است. بدین نحو که اسناد شامل قوانین موضوعه، مقررات جزایی و رویه‌های موجود جمع‌آوری گردیده و مورد بررسی قرار می‌گیرد. آثار صاحب‌نظران شامل کتب و مقالات علمی در تحلیل قوانین مذکور، مورد توجه نگارنده است.

یافته‌های پژوهش نشان می‌دهد. که در حقوق ایران به جز موارد مصرح در قانون جرائم رایانه‌ای که به ترسیم قلمرو حاکمیتی ایران در جرائم سایبر پرداخته به نظر می‌رسد در سایر موارد بتوان از عمومات قانون آیین دادرسی کیفری مانند صلاحیت ذاتی، محلی، شخصی و احاله در مورد جرائم سایبر و نیز در تعارض صلاحیت‌ها اعم از مثبت و منفی در حوزه داخلی بهره برد.

واژه‌های کلیدی: صلاحیت کیفری، اینترنت، فضای سایبری، قلمرو سرزمینی

---

[1]- استادیار حقوق جزا و جرم‌شناسی دانشگاه آزاد اسلامی واحد بوشهر(نویسنده مسئول) :Email: dr.Abdollahi2009@yahoo.com
[2]- کارشناس ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی بوشهر

مقدمه

در عصر حاضر حوزه‌های مختلف از جمله حوزه پزشکی، هسته‌ای و ...با تحول مواجه شده‌اند. آنچه که به عنوان عنصر مشترک همه این حوزه‌ها می‌توان نام برد موضوع اطلاعات است. ایجاد فضای مجازی «سایبر» در مقابل فضای فیزیکی و حذف فاصله‌ها و سرعت ارتباط و دسترسی آسان و امکان استفاده راحت از امکانات مذکور در زمینه‌های تجارت، اقتصاد، دادرسی، اطلاع‌رسانی و ... افق تازه‌ای را در مقابل جهانیان گشود. البته بزه‌کاران نیز به سبب عدم شناسایی، فرامرزی بودن، و به لحاظ صرف هزینه و سود، در استفاده از این فضا جهت اهداف مجرمانه غافل نشده‌اند. طبیعی است همه عرصه‌ها به ویژه عرصه حقوق با چالش‌ها و مشکلات اجتناب‌ناپذیر این فضا و فنّاوری خود را آماده نمایند. از چالش‌برانگیزترین مباحث و معضلات موجود در مقررات شکلی بحث صلاحیت است. صلاحیت یکی از مفاهیم حقوقی است و به معنی اختیار و وظیفه هیأت حاکمه (به نمایندگی قوه قضاییه) در اداره محاکم می‌باشد و صلاحیت کیفری به معنی اختیار و شایستگی هیأت حاکمه در رسیدگی به دعاوی کیفری است. در کشور ما قانون مجازات جرائم رایانه‌ای که در خردادماه ۱۳۸۸ به تصویب رسید، در بخش دوم تحت عنوان آیین دادرسی به این مسئله پرداخته و در این زمینه قواعد جدیدی را پیش‌بینی کرده است. با توجه به اینکه در محیط سایبر قواعد سنتی صلاحیت با چالش‌هایی از قبیل نامعین بودن مرزهای جغرافیایی و به تبع آن مشکل تعیین محل ارتکاب جرم مشکل تعیین تابعیت مرتکب و در نتیجه عدم وجود ضابطه‌ای واحد جهت تعیین مرجع قضایی صالح روبرو می‌شوند لذا در این تحقیق سعی بر آن است با بررسی قانون جرائم رایانه‌ای و تجزیه و تحلیل نظریات مطرح‌شده نحوه اعمال صلاحیت در فضای سایبری را مورد بررسی قرارداد.

بیان مسئله

صلاحیت کیفری را می‌توان به توانایی و شایستگی قانونی و نیز تکلیف مرجع قضایی به رسیدگی به یک دعوای کیفری تعبیر کرد (دولتشاهی،۱۳۸۴؛ ۱۴۱). نخستین مسئله‌ای که مراجع تحقیق باید به آن بپردازند، بررسی صلاحیت خود در جهت شروع به تحقیقات است و در صورتی که خود را صالح به رسیدگی ندانند، موظف به اصدار قرار عدم صلاحیت هستند(آشوری، ۴۸؛۱۳۸۸). صدور قرار عدم صلاحیت، یک نوع تصمیم‌گیری قضایی است و باید جدا از ماهیت دعوی اعلام گردد.

در امور کیفری، کلیه قواعد راجع به صلاحیت، آمره هستند و برخلاف امور حقوقی که در پاره‌ای از موارد اصحاب دعوی می‌توانند با توافق یکدیگر از صلاحیت مرجع خاص عدول کنند، در امور کیفری عدم رعایت قواعد و مقررات در رابطه باصلاحیت، حتی با توافق طرفین دعوای کیفری، امکان‌پذیر

نمی‌باشد؛ لذا نادیده گرفتن این قواعد به جز در موارد استثنایی مصرح در قانون، نقض قرار یا حکم صادره از سوی مراجع تالی توسط دادگاه‌های عالی را در بردارد(الهی منش، ۱۳۹۱؛ص۱۵۰).

آنچه که به عنوان جنبه‌ی مجهول و مبهم در خصوص صلاحیت در جرائم سایبری مورد توجه قرار می‌گیرد، امکان گمنامی کنشگران سایبری، نامعین بودن مرزهای جغرافیایی این فضا و دشواری تعیین محل ارتکاب جرائم رایانه‌ای در این بستر، مبحث صلاحیت رسیدگی کیفری را با دشواری‌هایی مواجه ساخته که در واقع اولین اثر جرائم رایانه‌ای بر مبحث «صلاحیت» است. این جنبه‌ی مجهول و مبهم در مبحث صلاحیت مربوط به جرائم سایبری در قانون جرائم رایانه‌ای مورد توجه قرارگرفته است.

ماده ۲۸ قانون جرائم رایانه‌ای (م ۷۵۶ ق.م.ا) در مقایسه با ماده ۴ قانون مجازات اسلامی، صلاحیت سرزمینی نظام حقوق کیفری ایران را گسترده‌تر نموده است؛ بدین صورت که در شرایطی که تنها بخشی از رفتار مجرمانه یا نتیجه حاصل از آن در قلمرو حاکمیتی کشور ارتکاب یابد، جرم مورد نظر، ارتکاب یافته در ایران تلقی می‌شود.

ماده ۲۸ قانون جرائم رایانه‌ای در خصوص قلمرو حاکمیتی ایران در فضای سایبر، به بحث صلاحیت پرداخته و چنین مقرر می‌دارد: «علاوه بر موارد پیش‌بینی‌شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود.

الف)داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کاررفته است به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق تارنما (وب‌سایت‌های) دارای دامنه بالاتری کد کشوری ایران در سطح گسترده ارتکاب یافته شده‌باشد.

ج) جرم توسط هر ایرانی یا غیر ایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایت‌های) مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا موسسه‌ای که خدمات عمومی ارایه می‌دهد یا علیه تارنماهای(وب‌سایت-های) دارای دامنه‌ی مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال اعم از آنکه مرتکب یا بزه دیده ایرانی یا غیر ایرانی باشد.»

پیشینه تحقیق

۱- آلبوعلی، امیر، ۱۳۹۲، صلاحیت کیفری در فضای سایبر: در این کتاب به مسئله صلاحیت کیفری مراجع قضایی در محیط سایبر پرداخته شده است. بخش اول کتاب به بیان مفاهیم فضای سایبر و صلاحیت و بخش دوم به بحث صلاحیت در فضای سایبر و چالش‌ها و رویکردهای حاکم بر آن را مورد بررسی قرار داده است و به این نتیجه دست‌یافته که بر اساس قوانین کنونی ایران اصل بر این است که مرجع صالح رسیدگی به جرائم سایبری محل وقوع جرم و در صورت عدم امکان تعیین محل وقوع جرم، محل کشف یا گزارش ملاک می‌باشد.

۲- باستانی، برومند، ۱۳۹۰، جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، بخش اول کتاب به تعاریف و گونه‌های جرائم رایانه‌ای و بخش دوم به بررسی حقوق جزای ماهوی و شکلی جرائم رایانه‌ای پرداخته است و در نهایت به لزوم تعاون و همکاری بین‌المللی در رسیدن به راه‌حلی جهت رسیدگی به جرائم رایانه‌ای تأکید کرده است.

۳- جلالی فراهانی، امیرحسین، ۱۳۸۹، آیین دادرسی جرائم سایبری، در این کتاب آیین دادرسی کیفری جرائم سایبری مورد بررسی قرارگرفته و فصل اول کتاب به مفاهیم صلاحیت کیفری و فصل دوم با توجه به مقررات کنوانسیون جرائم سایبر به صلاحیت کیفری در جرائم سایبر پرداخته و در نهایت به این نتیجه رسیده که به دلیل پیچیدگی موضوع صاحب‌نظران به راه حل حقوقی مشترک دست نیافته و کنوانسیون جرائم سایبر نیز در این خصوص ساکت است.

بخش اول: مفاهیم و چارچوب نظری تحقیق

الف) مفهوم فضای سایبر

فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. فضای سایبر گرچه اصطلاحی نسبتاً جدید است اما مفهوم آن جدید نیست و پیدایش این مفهموم هم زمان با اختراع تلفن توسط الکساندر گراهام بل در سال ۱۸۷۶ بوده است(دی انجلیز، ۱۳۸۳ ؛۷). واژه فضای سایبر اولین‌بار توسط ویلیام گیبسون در کتاب تئورامانسر، که در آن فضای مذکور را به عنوان موطن داده‌ها و اطلاعات موجود در یک آینده دور تاریک توصیف می‌کند، به‌کاربرده شده پس از آن واژه مذکور در فرهنگ‌های مختلف دنیا مورد استفاده قرار گرفت(همشهری آنلاین، ۱۳۹۰؛ ۱).

برای فضای سایبر تعاریف متعددی شده که به برخی از آن‌ها اشاره می‌شود:

- فضای سایبر یک ناحیه‌ای واقعی است. فعالیت‌هایی که در این فضا اتفاق می‌افتد شامل تبادل اطلاعات و راه‌هایی برای تجمیع اطلاعات مثل گردهمایی خبری می‌باشد(مصطفوی، ۱۳۸۷؛۴).
- فضای سایبر توهم و تصور باطل و توافقی است که انسان‌ها خلق کرده‌اند(همان).
- محیطی غیر ملموس و غیر فیزیکی که با اتصال شبکه‌های ارتباطی یا مخابراتی به وجود آمده و محتوای آن به صورت غیر ملموس و مجازی است که داده گفته می‌شود و مشتمل بر صوت و تصویر و نوشته و سند و از این قبیل موارد است و ظرفیت انجام فعالیت‌های مختلف را دارد(آلبوعلی، ۱۳۹۲؛ ۳۵).

ب) مفهوم جرم سایبری

تا کنون تعاریف گوناگونی از جرم رایانه‌ای از سوی سازمان‌های بین‌المللی قانون گذران و مراجع رسمی و غیررسمی برخی کشورها ارائه شده است که وجود تفاوت و گاه تعاریف در آن‌ها بیانگر ابهامات موجود در ماهیت و تعریف این جرائم می‌باشد هنوز یک تعریف کلی برای جرائم رایانه‌ای به دست نیامده و به جای آن تعاریفی کاربردی ارائه شده است(قراچوزلو، ۱۳۹۰، ۵۸).

شورای اروپا در تعریف جرم رایانه‌ای بیان می‌دارد: "سوءاستفاده از رایانه به عنوان هر رفتار غیر-قانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش اتوماتیک و انتقال داده‌ها".

«عمل غیرقانونی جهت از بین بردن، تغییر، حذف، و یا دسترسی به اطلاعات ذخیره شده در حافظه کامپیوتر یا فضای انتقال آن‌ها»

با توجه به تعریف و گستره فضای سایبر و با در نظر گرفتن اصل قانونی بودن جرم از طرف دیگر می‌توان چنین تعریفی را از جرم سایبری ارائه داد که به صواب نزدیک‌تر است.

«هر فعل یا ترک فعلی که در فضای سایبر اتفاق افتاده و قانون آن را جرم شناخته و برای آن مجازات مشخص کرده باشد.» با این تعریف، جرائم علیه سخت‌افزار کامپیوتر نظیر سرقت یا تخریب مانیتور از شمول جرائم سایبری خارج می‌گردد.

ج) تقسیم‌بندی جرائم در فضای سایبری

۱) جرائم کلاسیک با توصیف سایبری

جرائمی در این دسته قرار می‌گیرند که جرائم سنتی تلقی می‌شوند، اما در حال حاضر به علت پیشرفت فناوری با وسایل نوینی انجام می‌شوند. برخی از این جرائم عبارتند از: کلاهبـــرداری سایبری، جعل سایبری.

۲) جرائم صرف (محض) سایبری:

این دسته از جرائم صرفاً بعد فنی دارند اگرچه بعضی از آن‌ها قبلاً در جرائم کلاسیک قابل ملاحظه هستند. این جرائم صرفاً در عالم سایبر به وقوع می‌پیوندند و امکان ارتکاب آن‌ها در دنیای فیزیکی قابل تصور نیست. این جرائم را جرائم رایانه‌ای محض نامیده‌اند به خاطر اینکه خاص دنیای سایبر هستند اما آثار آن‌ها در دنیای واقعی ظاهر می‌شوند(مصطفوی، ۱۳۸۷؛ ۲۱). از قبیل نشر ویروس و تخریب داده‌ها.تغییر، ایجاد، محو یا متوقف کردن داده‌های رایانه‌ای مخابراتی به قصد تقلب که به طور عمده شامل دستیابی غیرمجاز، استفاده غیرمجاز و.... است.

۳) جرائم علیه محرمانه بودن داده‌ها و سیستم رایانه‌ای و مخابراتی:

هر نمادی از موضوع‌ها مفاهیم یا دستورالعمل‌ها از جمله متن صوت یا تصویر را که برای برقراری ارتباط میان سیستم‌های رایانه‌ای یا پـــردازش توسط شخـــص یا سیـــستم رایانه ایجاد می‌گردد داده‌ی محتوا می‌گویند. از جمله جرائمی که در این دسته جای می‌گیرند می‌توان به شنود غیرمجاز داده‌های مخابراتی در یک ارتباط خصوصی یا داده‌های سری که واجد ارزش برای امنیت داخلی و خارجی کشور می‌باشند اشاره کرد.

د) تعریف اینترنت و ارتباط آن با جرائم سایبری

شبکه بین‌المللی یا اینترنت، نام مجموعه‌ای از منابع اطلاعاتی جهان است که در سطح دنیا گسترده است. گستردگی این مجموعه به حدی است که می‌توان گفت هیچ انسانی نمی‌تواند به تنهایی تمامی اینترنت یا حتی بخشی از آن را بشناسد. جرائم اینترنتی را می‌توان مکمل جرائم رایانه‌ای دانست به خصوص اینکه جرائم نسل سوم رایانه‌ای که به جرائم سایبری معروف است غالباً از طریق این شبکه‌ی جهانی به وقوع می‌پیوندد (باستانی، ۱۳۹۰، ۳۵). با عنایت به مفهموم عامی که از جرم رایانه‌ای ارائه شد، می‌توان جرم اینترنتی را نـوع خاص از جرائم رایانه‌ای دانست به عبارت دیگر رابطه بین جرائم رایانه‌ای و جرائم اینترنتی عموم و خصوص مطلق است یعنی هر جرم اینترنتی رایانه‌ای تلقی می‌شود ولی هر جرم رایانه‌ای اصولاً اینترنتی نیست (اسماعیلی فلاح، ۱۳۹۰، ۱۵).

هـ) مبانی نظری

قواعد سنتی تعیین دادگاه صالح در مورد جرائم ارتکابی در فضای سایبر به خاطر ماهیت و ویژگی-های خاص آن فضا، که آن را از فضای سنتی یعنی فضای جغرافیایی متمایز می‌کند به گونه‌ای است که طرح قواعد جدید مطابق با فضای مذکور از موارد غیرقابل انکار حقوق کیفری شکلی در این زمینه می‌باشد. در این خصوص تئوری‌ها و پیشنهادهای مختلفی مطرح‌شده است که هر کدام علی‌رغم رفع

برخی گوشه‌های ابهام ، از انتقاد و نقص مصون نیست. در این مبحث به طور ویژه به این تئوری‌ها پرداخته و هر کدام مورد نقد و تحلیل قرار می‌گیرد. می‌باشد. مهم‌ترین این نظریات عبارتند از:

۱) نظریه محل قرارگیری وسیله موثر در ارتکاب با جرم (کامپیوتر یا ماهواره) [۳]

در این نظریه جایی که کامپیوتر تأثیرگذار در وقوع جرائم رایانه‌ای یا سایبری قرار دارد و یا جایی که ماهواره وسیله ارتکاب جرم ثبت شده است، محل ارتکاب جرم محسوب شده و نظام قضایی همان محل جهت تعقیب جرم صالح خواهد بود. اما مشکلی که در خصوص ماهواره‌ها ابراز داشته‌اند این است که هیچ‌گاه نمی‌توان به آن‌ها در قالب صلاحیت سرزمینی استناد کرد.

منظور این است که چون هر داده و اطلاعاتی که به عنوان وسیله جهت ارتکاب جرم مورد استفاده قرار می‌گیرد حتماً در بستر فضای سایبر تاثیر خود را می‌گذارد و فضای سایبر بستری جز سرورهای محدود و معدود ندارد بنابراین باید دید که جرم از فضای کدام سرور عبور کرده است. که در این صورت محل استقرار همان سرور صالح به رسیدگی خواهد بود. این نظریه علی‌رغم انطباق بیشتر با واقعیت قابلیت اجرایی خیلی کمی دارد. این نظریه از آن جهت با واقعیت منطبق است که بر روی خاک واقعی فضای سایبر دست گذاشته و از آنجا که این سرورها در روی یک قلمرو زمینی معین قرار دارند در واقع قاعده صلاحیت سرزمینی سنتی را که مادر قواعد صلاحیتی محسوب می‌شود، اجرا کرده است چون در واقع جرائم سایبری در جزیی از خاک همان محل ارتکاب یافته است.

در خصوص قابلیت اجرایی چنین نظریه‌ای باید گفت که جهت اجرای این نظریه باید کلیه‌ی بزه دیدگان جرائم سایبری از سراسر جهان مجبور شوند به سه یا چهار کشور دارنده سرور جهت شکایت مراجعه کنند و نزد محاکم آن‌ها اقامه دعوی کنند و آن مراجع مجبور شوند به صدها هزار پرونده سایبری رسیدگی کنند.[۴]

۲) محل حضور بار گذار[۵] و پیاده ساز[۶] شبکه‌ای به عنوان محل ارتکاب جریم سایبری

به طور کلی، کنشگران اصلی فضای سایبر از دو حالت اصلی خارج نیستند: یا داده‌ها را در آن می‌گنجانند که در این صورت به آن‌ها بار گذار می‌گویند و یا اینکه داده‌ها را از این فضا دریافت

---

[3] - **Location of computers**

[2]- **Li.Xingan.(2004)."Theories And Practices of Internaional jurisdiction of cybercrime". Lex publication.p31.**

[۵] -انتقال یک کپی از یک برنامه ، انتقال داده از یک سیستم استفاده کننده به یک سیستم کامپیوتری راه دور **Location of downloading and uploading**

[۶]- فرآیند انتقال اطلاعات از یک سیستم کامپیوتر مرکزی بزرگ به سیستم کامپیوتر کوچک و دور (**Uploader & downloader**)

می‌کنند که به آن‌ها پیاده ساز گفته می‌شود. در اینجا بار گذار اطلاعات مورد نظر خود را در فضای تخصیص‌یافته از سوی خدمات میزبانی قرار می‌دهد تا متعاقباً پیاده ساز به آن‌ها دسترسی یابد. هیچ نیازی نیست که آن‌ها از هویت یکدیگر آگاهی داشته باشند. بنابراین نباید آن‌ها را با فرستنده[۷] و گیرنده[۸] که معمولاً هویتشان در ارتباطات الکترونیکی معلوم است اشتباه گرفت ، زیرا در اینجا آن هدف خاص از مبادله اطلاعات که در ارتباطات طرفینی وجود دارد مشاهده نمی‌شود(زندی، ۱۳۹۳؛ ۷۱).

با این حال نباید ضابطه بار گذار و پیاده ساز را بر روی بزهکار و بزه دیده پیاده کرد همان قدر که احتمال دارد بار گذار مرتکب جرم باشد، بزه دیده بودن آن دور از انتظار نیست. برای مثال در جایی که بار گذار محتوای مجرمانه‌ای را نظیر تصاویر وقیح، هتک حرمت یا توهین یا حتی ویروس خطرناک بر روی شبکه قرار می‌دهد، وی مرتکب جرم است. اما هنگامی که داده‌های مشروعی که بارگـــذاری کرده، به طور غیرمجاز توسط یک پیاده ساز مورد سوءاستفاده قرار می‌گیرد، بزه دیده است. بنابراین نسبت به اینکه کدامیک از اعمال بارگذاری یا پیاده‌سازی مجرمانه است محل عامل همان عمل در لحظه‌ی انجام ملاک صلاحیت محسوب می‌گردد.

نکته‌ی دیگر که در این خصوص قابل طرح است این است که کشور محل بارگذاری یا پیاده‌سازی مجرمانه ممکن است آن عمل را جرم انگاری نکرده باشد درحالی‌که در کشورهای متبوع بزه دیده چنین عملی جرم باشد که در این صورت بزه دیده نمی‌تواند با استناد به قانون کشور خود و در همان کشور اقامه دعوی کیفری نماید.

۳) نظریه دادگاه سایبری دیجیتالی[۹]

در این تئوری مساله‌ی تعارض صلاحیت‌های مختلف منتفی می‌شود. چون دادگاه سایبری به تمام جرائم ارتکابی در فضای مذکور رسیدگی می‌کند و سیستم قضایی واحدی بر فرآیند دادرسی آن حکومت می‌کند. البته این دادگاه می‌تواند شعب مختلفی داشته باشد ولی تمام شعب به یک نهاد دادگاه بین‌المللی وابسته هستند و رسیدگی در هر کدام از این شعب بر اساس هیات مرکزی دادگاه صورت می‌گیرد و این به معنی عدم امکان ایجاد تعارض صلاحیتی در چنین دادگاهی است.

---

[3]- sender
[4]- receiver
[5]- Digital court

البته برخی حقوقدانان[۱۰] برای رسیدگی به جرائم سایبری در هر کشور پیشنهاد ایجاد یک دادگاه دیجیتالی با ماهیت و ساز کاری متفاوت از دادگاه سایبری مذکور در قبل داده‌اند و دادگاه دیجیتالی را بدین گونه تعریف کرده‌اند: " دادگاه دیجیتالی که ویژه جرائم دیجیتالی[۱۱] می‌باشد بر اساس اختصاص محاکم به صورت ویژه از قبیل خانواده، جنایات و امور حقوقی، به امور جرائم دیجیتالی می‌پردازد که این دادگاه مستلزم امکانات بشری و جغرافیایی است"(رضوان هلال،۲۰۰۶؛ ۱۳).

این دادگاه به جرائم رایانه‌ای خواه جرم به وسیله رایانه خواه علیه آن ارتکاب شود، همچنین به جرائم شبکه‌ای و اینترنتی از جمله شبکه‌ی جهانی اینترنت و جرائم تلفن‌های سیار یا موبایل رسیدگی کند.

حدود قلمرو اجرایی چنین دادگاهی بدین ترتیب است که در هر دولتی به صورت دادگاه داخلی در پایتخت آن دولت شروع به کار کند و به رسیدگی به جرائم فرامرزی و غیر محدود که قوانین حاکم بر آن از یک دولتی نسبت به دولتی دیگر متفاوت است مبادرت می‌کند اگر چه اساس آن قوانین مختلف یکی باشد.

تئوری دادگاه سایبری یا دیجیتالی به هر دو شکل آن چه یک دادگاه فراملی و بین‌المللی با کادر مشترک و چه به صورت دادگاه داخلی در هر کشور با نقص و مشکل مواجه است. بدین توضیح که شکل اول، یک تئوری آرمان‌گرایانه و بلند پروازانه است و از اندیشه و تئوری، تا محقق ساختن و عمل نمودن آن فاصله نسبتاً دوری وجود دارد. همان طور که در قلمرو جغرافیایی و ملموس جرائم ارتکابی در آن با آن همه سابقه و قدمتی که دارد کشورهای جهان بعد از تلاش‌های وسیع و پیوسته در دهه اخیر توانستند یک دادگاه کیفری با ماهیت بین‌المللی ایجاد کنند آن هم:

اولاً نسبت به تعداد خیلی محدودی از جرائم که عبارتند از: جرائم نسل‌کشی، جرائم علیه بشریت، جنایات جنگی، جنایات تجاوز قدرت اجرایی و تعقیب دارد.

ثانیاً تاکنون از جانب بسیاری از کشورها، به عنوان مثال ایالات‌متحده امریکا، مورد امضا و قبول قرار نگرفته است.

ثالثاً طبق اساسنامه آن، راه‌های نفوذ و سنگ‌اندازی بر روند تعقیب و رسیدگی به کرات مشـــاهده می‌شود. کما اینکه مسایل مجازات کردن مجرمین و شیوه استرداد آن‌ها و سایر عملیات فیزیکی در چنین دادگاهی دچار بحران می‌شود اگر چه در خصوص مجازات هم راه‌هایی از قبیل تغییر ماهیت

---

[۱۰]- محمد رضوان کارشناس تحقیقاتی در وزارت دادگستری مصر

[1]- Digital crime

مجازات و سایبری کردن آن مانند محرومیت از یک سری خدمات شبکه‌ای و یا مجازات مالی برای دارندگان حساب مالی وجود دارد.

شکل دوم دادگاه دیجیتالی از آن جا که در راستای هرچه تخصصی کردن شعبه‌های دادگاهی و در عرض دادگاه‌های خانواده، جرائم اقتصادی جرائم امنیتی و غیره آمده است ابداع جدیدی محسوب نمی‌شود و نمی‌تواند پاسخ‌گوی چالش‌های آیین دادرسی کیفری در فضای سایبر باشد.

۴) نظریه ارتباط حداقلی[۱۲] یا ارتباط منطقی[۱۳]

به لحاظ اینکه اجرای تئوری‌های پیش گفته، به دلیل وجود مشکلات تعیین محل ارتکاب جرم و تابعیت مرتکب و تعدد دخالت کنندگان در یک جرم سایبری اعم از مرتکبان و بزه‌دیدگان، با بحران و چالش مواجه بود. برای خروج از این بحران و پاسخ‌گویی به مشکل تعیین حوزه قضایی صالح، برخی از نویسندگان ضابطه ارتباط حداقلی را مطرح کرده‌اند که در آن بالحاظ رفتارهای مرتکب بررسی می‌شود که کدام حوزه‌ی قضایی حداقل ارتباط لازم جهت رسیدگی به اختلاف را دارد(زندی، ۱۳۹۳؛ ۶۱). در این صورت، یک رفتار منفرد و یا یک معامله چنین رابطه‌ای را مشخص می‌سازد[۱۴] با این وجود عمل هرچه باشد باید در دولت مدعی صلاحیت انجام شده باشد. بنابراین در جایی که نه عمل در دولت مدعی صلاحیت انجام شده باشد و نه اثر آن در آنجا اتفاق افتاده باشد ارتباط حداقلی حاصل نشده است.

در این تئوری دادگاه‌ها و مراجع قضایی به عرف و منطق متوسل شده و در جهت احراز صلاحیت خود به ارتباط منطقی و عرفی میان کاربران و مجرمان اینترنتی و حوزه‌ی مربوطه توجه می‌کنند. در بحث «ارتباط منطقی» مرجع قضایی این مسئله را بررسی می‌کند که متهم جرائم واقعه در فضای سایبر تا چه اندازه موفق به برقراری ارتباط اینترنتی با بزه دیده‌شده و آیا این میزان برقراری ارتباط کافی است تا دادگاه یا مرجع قضایی محل اقامت یا شکایت بزه دیده صالح به رسیدگی به اتهام مزبور باشد یا خیر؟

تشخیص این امر که ارتباط پدید آمده در چه حد از اهمیت است و این اندازه ارتباط برای احراز صلاحیت دادگاه محل اقامت بزه دیدگان کافی است یا خیر؟ بر عهده‌ی خود دادگاه است و ملاک و معیار این تشخیص عرف، منطق و رویه‌ی قضایی خواهد بود(دولت شاهی، پیشین، ص ۱۴۹).

---

[2]- Minimum contacts
[3]- Reasonable contact
[1]- kopsell. david.r(2000). an emerging ontology of jurisdiction in cyberspace, p100.

بخش دوم: مصادیق صلاحیت در فضای سایبر

در بررسی صلاحیت کیفری دادگاه‌ها در خصوص جرائم سایبری چه در حیطه داخلی و چه در حیطه فراملی مکان و مرز جغرافیایی نقش اساسی در تعیین دادگاه صالح دارد. درحالی‌که در فضای سایبر این فضا فارغ از مکان است پس مرز جغرافیایی نمی‌شناسد لذا در این بخش با توجه به ماده ۲۸ قانون جرائم رایانه‌ای به بررسی مصادیق صلاحیت در فضای سایبر در حیطه داخلی و فراملی پرداخته می‌شود. اعمال صلاحیت دولت‌ها در جایی که عملی اقتدار و امنیت آن‌ها را به خطر اندازد ، اگرچه هم توسط اتباع خارجی و در خارج از حوزه اقتدار آن‌ها باشد، صلاحیت برون‌مرزی نامیده می‌شود که مواردی از قبیل صلاحیت حمایتی، شخصی، و جهانی را در برمی‌گیرد که بند «ج» و «د» ماده ۲۸ قانون جرائم رایانه‌ای به این امر تأکید دارد.

۱) صلاحیت حمایتی و فضای سایبر[۱۵]

این ضابطه که مبتنی بر اصل صلاحیت حمایتی یا واقعی می‌باشد به کشوری که امنیت و یا منافع حیاتی آن تهدید شده اجازه می‌دهد که مرتکب آن جرم را تعقیب و مجازات کند اگر چه مجرم تبعه آن کشور نباشد و یا اینکه جرم در خارج از قلمرو حاکمیتی آن دولت ارتکاب یافته باشد(پور باقرانی، پیشین، ص ۶۲).

در کشور ما در قانون مجازات جرائم رایانه‌ای در بند «ج» ماده ۲۸ صلاحیت حمایتی را پذیرفته و مصادیق آن را نیز مشخص کرده است. بند «ج» این ماده مقرر می‌دارد که:«جرم توسط هر ایرانی یا غیر ایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایت های) مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا موسسه‌ای که خدمات عمومی ارایه می‌دهد یا علیه تارنماهای(وب‌سایت‌های) دارای دامنه‌ی مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد». در این بند قانون رویکرد حمایتی گسترده‌ای را اتخاذ کرده که قید «ایرانی» زائد به نظر می‌رسد. زیرا استناد به صلاحیت تابعیتی، در هر حال نسبت به صلاحیت حمایتی در اولویت قرار دارد.

و قید «ارتکاب جرم در خارج از ایران» از آن جهت بوده که اگر در داخل قلمرو حاکمیتی ایران ارتکاب یابد، باید به صلاحیت سرزمینی استناد کرد که اولی از انواع صلاحیت‌های کیفری به شمار می‌آید. لذا موارد مشمول این ماده را می‌توان دو گزینه دانست:

الف. سامانه‌های رایانه‌ای و مخابراتی

---

[2]- **Protective principle**

ب. وب‌سایت‌ها

این موارد باید مورد استفاده یا تحت کنترل مراجع مذکور در این بند باشد لذا ضرورتی ندارد مالکیت آن را در اختیار داشته باشند. یا اینکه محل استقرار سامانه‌ها یا ذخیره داده‌های وب‌سایت‌های مذکور در آن واقع باشد(الهی منش و سدره نشین، ۱۳۹۱؛ ۱۵۲).

۲) صلاحیت تابعیتی

مهم‌ترین اصل حاکم بر صلاحیت کیفری فرا سرزمینی که به واقع می‌تواند در مقام رقابت باصلاحیت سرزمینی ظاهر شود، تابعیت مرتکبین یا قربانیان جرائم است(مصدق،۱۳۹۲: ۲۸). امروزه بعضی کشورها به دلایلی قواعد صلاحیت تابعیتی را گسترش داده و علاوه بر مرتکبین جرائم ، نسبت به اتباع بزه دیده‌ی[۱۶] خود نیز اعمال می‌کنند. در این راستا گروهی صلاحیت تابعیتی نسبت به مجرمین را صلاحیت فعال[۱۷] و صلاحیت تابعیتی نسبت به بزه دیدگان را صلاحیت تابعیتی منفعل[۱۸] نامیده-اند(محمد زاده،۱۳۸۸: ۱۲).

الف : صلاحیت شخصی فعال یا صلاحیت مبتنی بر تابعیت مرتکب جرم

صلاحیت مبتنی بر تابعیت مجرم دومین فاکتور برای تعیین دادگاه صالح پس از صلاحیت مبتنی بر محل وقوع جرم یا صلاحیت سرزمینی[۱۹] محسوب می‌شود. این ضابطه همان طور که در جرائم سنتی قابل‌اجراست نسبت به جرائم سایبری نیز قابلیت اجرایی دارد ولی مشکلی که در جهت اجرای این ضابطه در جرائم سایبری وجود دارد این است که در فضای سایبر هویت مرتکب به سختی قابل کشف می‌باشد(جلالی فراهانی،۱۳۸۳: ۲۵).

ب : صلاحیت شخصی منفعل یا صلاحیت مبتنی بر تابعیت مجنی علیه

این نوع صلاحیت در قلمرو جغرافیایی به دو دلیل زیاد مورد توجه قرار نگرفته است. اولاً اعمال صلاحیت نسبت به بزه دیده به معنی عدم کفایت قوانین دیگر کشورها در محاکمه مجرمین جرائم است. ثانیاً مخاطب اصلی فرایند کیفری مجرم است نه بزه دیده و چنان چه یک کشور چنین حقی برای خود قائل شود باید امکانات و نیروی کافی جهت برگزاری یک رسیدگی عادلانه و مناسب را تدارک دیده باشد. این موضوع به ویژه در جایی اهمیت می‌یابد که مجرم و محل ارتکاب جرم همگی در خارج از کشور قرار دارند که در این صورت جمع‌آوری ادله و تحقیقات و یا استرداد متهم مشکل

16- **Nationality of the victin**
17- **Active Wationality**
18- **Passive nationality jurisdiction**
19- **Therritoniality principle**

خواهد بود. به همین دلیل عده‌ای معتقدند اعمال این نوع صلاحیت تنها در مورد جرائم شدید[20] توجیه‌پذیر است.[21] ولی در زمینه جرائم سایبری، به خاطر نبود برخی مشکلات مذکور و همچنین ماهیت ویژه فضای سایبر، کشورها نسبت به صلاحیت در فضای مزبور رغبت بیشتری از خود نشان داده‌اند. کما اینکه کشور هلند در جرم سایبری یعنی ساپوتاژ رایانه‌ای[22] و تخریب داده‌ها [23]در جایی که تبعه‌ی خود وی، بزه دیده واقع‌شده خود را صالح به رسیدگی شناخته است(آلبوعلی، پیشین،ص ۱۱۲). در بند«د» ماده ۲۸ قانون جرائم رایانه‌ای قانون گذار با به کار بردن اصطلاح «بزه دیده» در این بند، اصل صلاحیت شخصی قوانین کیفری را بر پایه‌ی بزه دیده شناسی متحول ساخته است. بر این اساس افزون بر صلاحیت شخصی(کنش‌گرانه) که در ماده ۷ قانون مجازات اسلامی پیش‌بینی‌شده است به جرم‌هایی که به موجب قانون جرائم رایانه‌ای علیه بزه دیده ایرانی ارتکاب می‌یابد، نیز در دادگاه‌های ایران قابل رسیدگی است.(اصل صلاحیت شخصی کنش‌گرانه یا بزه‌دیده‌مدار) (رایجیان اصلی، ۱۵؛۱۳۸۸).

۳)صلاحیت جهانی و فضای سایبر

برخی جرائم متضمن رفتاری مغایر با نظم جهانی و نوع بشر هستند به گونه‌ای که صرف‌نظر از شخص یا دولت خاصی که جرم علیه او واقع‌شده علیه تمام ملت‌ها محسوب شده و از مرتکب آن به «دشمن نوع بشر»[24]یاد می‌شود. اقتدار یک دولت بر عهده‌دار شدن تعقیب مرتکب چنین جرائمی را «صلاحیت جهانی»[25] می‌گویند. این قاعده معمولاً مغایر حقوق بین‌الملل است مگر برای جرائم علیه حقوق بین‌الملل نظیر دزدی دریایی[26] بنابراین هر جرمی را نمی‌توان تحت شمول این قواعد قرارداد. بلکه می‌بایست یک توافق بین‌المللی در خصوص ضرورت مبارزه همگانی با آن وجود داشته باشد (حسینی نژاد، ۱۳۷۳: ۵۹).

بنابراین ارتکاب جرم مشمول صلاحیت جهانی در فضای سایبر نه تنها بر قابلیت اجرایی قاعده مذکور تاثیر منفی نگذاشته است بلکه به لحاظ ویژگی‌های خاص چنین جرمی از جمله سهولت در ارتکاب، فراملی بودن، گسترده بودن و صبغه جهانی داشتن آن، حفظ نظم و انسجام جهانی اقتضا می‌کند که تعقیب آن در سریع‌ترین و راحت‌ترین شکل تدابیر کیفری صورت بگیرد. اجرای این

20- **Serious offences**
21- **Lixingan, Ibid.p17**
22- **Computer sabotage**
23- **Data damage**
24- **Hostis human gentium**
25- **Universality nexus**
26- **Piracy**

صلاحیت به طور کلـی و به ویژه در خصوص جرائم سایبری در صورتی امکان‌پذیر است که تمامی کشورها بتوانند با استفاده از صلاحیت جهانی به آن رسیدگی کنند یا مرتکب آن را تعقیب نمایند. با این حال تاکنون در فضای سایبر نسبت به برخی جرائم نظیر هرزه نگاری کودکان این اجماع و توافق به طور نسبی محقق شده ولی هنوز قدرت اجرایی پیدا نکرده است. قانون مجازات جرائم رایانه‌ای ایران در ماده «۲۸» مقرر داشته: « علاوه بر مواد پیش‌بینی‌شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بو«... د)جرائم رایانه‌ای متضمن سو استفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکه مرتکب یا بزه دیده ایرانی یا غیرایرانی باشد».

۴- صلاحیت سرزمینی و فضای سایبر

این ضابطه مهم‌ترین و رایج‌ترین اصل در اعمال صلاحیت کیفری در قواعد سنتی است. این اصل بر پایه احترام متقابل به حاکمیت برابر کشورها و همچنین پیوند آن با اصل عدم مداخله آن‌ها در امور داخلی یکدیگر بنا شده است. به همین دلیل معمولاً استناد به دیگر اصول صلاحیت کیفری در اولویت بعدی قرار می‌گیرند (حامد، ۱۳۸۴: ۳۶). برای درک مفهوم قلمرو سرزمینی در فضای سایبر ابتدا لازم است بستر تشکیل‌دهنده و ابزار دسترسی به آن تشریح گردد.

الف) بستر ارتباطات و مبادلات الکترونیکی

منظور از بستر ارتباطات و مبادلات الکترونیکی مجموعه‌ای عظیم از صفر و یک‌هایی است که داده‌های الکترونیکی را تشکیل می‌دهد و آن‌ها نیز در قالب‌های مختلف مفاهیم را به شکل الکترونیکی منعـــکس می‌کنند. در واقع فضای سایبر همین بستر است که داده‌های الکترونیکی در آن ذخیره به انحای گوناگون پردازش و در نهایت به شیوه مورد نظر منعکس می‌شوند(جلالی فراهانی، ۱۳۸۹؛ ۱۰۰).

به این ترتیب شاید بتوان چنین نتیجه‌گیری کرد که هر جا مراکز تولیدکننده بسترهای الکترونیکی قرار داشته باشند، که اصطلاحاً به آن‌ها مراکز داده اینترنتی[۲۷] یا سرور[۲۸] گفته می‌شود و از لحاظ فنی به ارایه خدمات میزبانی و ملزومات تبعی آن می‌پردازند جزء قلمرو حاکمیت آن کشور به شمار می‌روند(زندی ، ۱۳۹۳؛۶۴).

ب) ابزار دسترسی به بستر ارتباطات و مبادلات الکترونیکی

[27]- **Internet data center**
[28] **-server**

شیوه دسترسی به بستر فضای سایبر، ابزارهای هویت فضای مجازی شبکه‌ای با عنوان نام دامنه[۲۹] است که از سوی عوامل مربوط ارائه می‌شود. این نام‌ها در واقع مجموعه دوازده رقمی از شمارگان هستند که به صورت سه‌تایی تقسیم‌شده‌اند و برای راحتی کاربران به صورت نام به نمایش در می‌آیند نظیر شماره ۱۹۳،۰۰۰،۰،۱۹۹ .

بخشی از دامنه که به دامنه مرتبه بالا معروف است خود دارای دو بخش است: ۱- دامنه مرتبه‌ی بالای عمومی[۳۰] ۲- دامنه مرتبه بالای کد کشوری[۳۱]

اگر چه تمام این دامنه‌ها از جانب یک شرکت آمریکایی به نام آیسان[۳۲] صادر می‌شود اما بر اساس رویه‌ی معمول کدهای کشوری فقط به دولت‌ها واگذار می‌شوند تا آن‌ها نسبت به تخصیص آن سیاست‌گذاری و اقدامات لازم انجام دهند. لذا عملاً این کدها به مصداق بارزی از اعمال حاکمیت کشورها در فضای سایبر تبدیل شده است. بنابراین حاکمیت دولت‌ها در حوزه‌های مربوط به آن نمود پیدا می‌کند و شاید صالح دانستن همان دولت نسبت به جرائم ارتکابی بر روی دامنه‌های مربوط به آن راهکار منطقی و قابل‌اجرا باشد(کاشیان و همکاران، ۱۳۷۷ ؛ ۲۸۳). ماده «۲۸» قانون جرائم رایانه‌ای قلمرو حاکمیتی ایران در فضای سایبر را تصریح نموده و بند «الف» و «ب» این ماده ناظر بر اصل صلاحیت سرزمینی بوده و حتی در مقایسه با ماده «۴» قانون مجازات اسلامی صلاحیت سرزمینی حقوق کیفری ایران را گسترده‌تر نموده است، بدین صورت که در شرایطی که تنها بخشی از رفتار مجرمانه یا نتیجه حاصل از آن در قلمرو حاکمیتی کشور ارتکاب یابد، جرم مورد نظر ارتکاب یافته در ایران تلقی می‌شود.

بند «الف» با مبنا قرار دادن قلمرو حاکمیتی ایران، مستند به قانون مجازات اسلامی محل استقرار سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده را مورد توجه قرار داده است. بنابراین هر سامانه رایانه‌ای یا مخابراتی اعم از رایانه‌های کیفی یا حتی گوشی‌های تلفن همراه یا هر وسیله دیگری که در تعریف فنی سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده بگنجد(مانند لوح‌های فشرده) و در قلمرو حاکمیتی ایران قرار داشته باشند، مشمول این بند می‌شود. البته به شرطی که لااقل حاوی حداقل یکی از دو نوع داده زیر باشند:

29- **Domain name**
30- **Generic top level domain name**
31- **Contr code top level domain name**
32- **ICANN**

الف. داده‌های مجرمانه که در واقع همان محتوای مجرمانه است و نتیجه و محصول جرائم رایانه‌ای به شمار می‌آیند؛ مانند محتویات مبتذل و مستهجن؛

ب. داده‌هایی که برای ارتکاب جرم به‌کاررفته‌اند؛ مانند داده‌های سری یا گذر واژه‌های سرقت شده که برای ارتکاب جرم به‌کاررفته‌اند.

بند «ب» با توجه به نام دامنه ملی و انحصاری بودن آن برای حاکمیت ملی کشورها، قلمرو حاکمیتی سایبری ایران را ترسیم می‌کند که عبارت از دامنه‌های «آی‌آر»[۳۳] و «ایران»[۳۴] لذا هر وب‌سایتی که دارای یکی از این دو پسوند باشد؛ حتی اگر محتوای آن‌ها به زبان فارسی نباشد و یا دارندگان و گردانندگان آن‌ها ایرانی نباشند نیز مشمول این قانون خواهند بود.

نتیجه‌گیری و پیشنهادها

در کشور ما از لحاظ رویه‌ی عملی، تا قبل از تصویب قانون مجازات جرائم رایانه‌ای قضات سعی در اجرای قواعد سنتی صلاحیت با اتخاذ معیاری جدید و موافق با فضای جدید سایبر داشتند که در این خصوص رویه‌ی واحدی هم اتخاذ نشده بود. با تصویب قانون جرائم رایانه‌ای، این قانون مطالبی را در مواد۲۸، ۲۹، ۳۰،۳۱به مساله‌ی صلاحیت اختصاص داده است. در بندهای الف و ب ماده‌ی ۲۸ با تسری قلمرو حاکمیت کشور به سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی و کشور و تارنماهای دارای دامنه‌ی مرتبه‌ی بالای کد کشور ایران، قاعده‌ی صلاحیت سرزمینی را به گونه‌ای دیگر نسبت به جرائم ارتکابی در فضای سایبر اعمال کرده است. در بند «ج» صلاحیت شخصی سنتی و در بند «د»، با قبول جرم هرزه نگاری اطفال به عنوان جرم موضوع صلاحیت جهانی، قاعده‌ی صلاحیت جهانی را برای رسیدگی به جرائم سایبری پیش‌بینی کرده است». قانون تجارت الکترونیکی مصوب ۱۳۸۲ هم که در مورد محل انجام یک عمل تجاری در تجارت الکترونیکی در ماده‌ی ۲۹ قواعدی را بیان کرده است در فصل چهارم به بحث صلاحیت جزایی اشاره‌کرده و مقررات حاکم بر صلاحیت جزایی در خصوص جرائم تجارت الکترونیکی را به قانون احاله کرده است، که در همین راستا با تصویب و تأیید قانون جرائم رایانه‌ای فوق‌الذکر قواعدی راجع به شیوه‌ی اعمال صلاحیت در بخش دوم همین قانون پیش‌بینی‌شده است. البته باید این نکته را در نظر داشت که در رسیدگی به جرائم رایانه‌ای مانند جرائم سنتی قواعد صلاحیت ذاتی و شخصی نیز رعایت می‌شود به عنوان مثال در فرضی که متهم مرتکب سرقت رایانه‌ای و جاسوسی رایانه‌ای می‌گردد اتهام

---

[33]- **ir**

[34]- **iran**

وی از حیث جاسوسی رایانه‌ای در دادگاه انقلاب رسیدگی می‌گردد و از حیث صلاحیت شخصی نیز برخی جرائم هستند که محل وقوع آن‌ها نقش در تعیین صلاحیت محلی دادگاه ندارد مانند جرائمی که شخصیت مرتکب تعیین‌کننده صلاحیت است مانند جرائم استانداران، روحانیون، قضات و ... یا مواردی که سن مرتکب تعیین‌کننده صلاحیت باشد مانند جرائم اطفال یا مواردی که به اعتبار شغل متهم باشد مانند جرائم مربوط به افراد نظامی که به مناسبت شغل در حین انجام وظیفه مرتکب می‌شود که در این حالت با پیروی از قاعده صلاحیت شخصی در مراجع صالح یعنی دادگاه پایتخت یا مرکز استان یا اطفال یا دادگاه نظامی حسب مورد رسیدگی می‌شود.

در خصوص تعارض صلاحیت در حوزه‌های قضایی داخلی اختلاف در صلاحیت و چگونگی آن در فصل دوم از باب اول مواد ۲۶ الی ماده ۳۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی سال ۷۹ آمده است. در طرح دادرسی الکترونیکی که در کمسیون قضایی مجلس مطرح می‌باشد در بخش سوم تحت عنوان آیین دادرسی جرائم رایانه‌ای از ماده ۱۰۲ تا ماده ۱۰۵ عیناً موارد فوق‌الذکر آمده است با این تفاوت که با توجه به تغییر تشکیلات قضایی قوه‌ی قضاییه در ماده ۱۰۴ موظف شده به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های کیفری یک، کیفری دو، اطفال و نوجوانان، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد. همچنین شعبه پایتخت میتواند در برخی نقاط کشور شعبات فرعی داشته باشد همان طور که ماده ۳۰ قانون جرائم رایانه‌ای در زمینه مقرر می‌دارد: «قوه قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد». دادگاه فوق می‌تواند به صلاحدید خود و بر اساس قواعد پیش‌بینی‌شده در ماده‌ی ۲۹ قانون جرائم رایانه‌ای یا دیگر قواعد، نظیر ارتباط منطقی با یک حوزه، پرونده‌ها را به آن‌ها ارجاع یا احاله کند.

بر اساس ماده اخیر«چنانچه جرم رایانه‌ای 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 می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد». لذا دیده می‌شود که قانون مجازات جرائم رایانه‌ای ایران با در نظر گرفتن چالش‌های فضای سایبر و مشکل بودن تعیین محل ارتکاب جرم سایبری، محل گزارش جرم و یا محل کشف جرم را، در جایی که محل وقوع قابل تعیین نباشد، جایگزین ضابطه‌ی محل وقوع جرم نموده و همان مراجع را صالح به رسیدگی دانسته است. در هر حال بر اساس قوانین کنونی ایران اصل بر این است که مرجع صالح رسیدگی به جرائم سایبری مرجع محل وقوع جرم است ولی در

صورت عدم امکان تعیین محل وقوع جرم (که غالباً چنین امکانی وجود ندارد) محل گزارش یا کشف ملاک خواهد بود. در میان محل گزارش و محل کشف اگرچه غالباً این دو محل یکی هستند ولی در صورت متفاوت بودن آن‌ها حسب ماده ۲۹ مزبور اولویت با محل کشف است و محل گزارش ناظر به زمانی است که جرم کشف نشده باشد. و در مواردی که اجزاء مختلف عنصر مادی جرم در چند حوزه قضایی مختلف اتفاق می‌افتد یا مواردی که یک شخص مرتکب چندین جرم متفاوت سایبری در حوزه قضایی مختلف می‌شود در این صورت ممکن است چندین حوزه قضایی خود را صالح به رسیدگی بداند که در این حالت تبصره ماده ۵۲ قانون جرائم رایانه‌ای مقرر می‌دارد: «در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه‌ای مقررات خاص از جهت آیین دادرسی پیش‌بینی نشده است، طبق مقررات قانون آیین دادرسی اقدام خواهدشد.»

حال با در نظر گرفتن مقررات شکلی قانون جرائم رایانه‌ای و مقررات مربوط به صلاحیت مندرج در قانون آیین دادرسی کیفری مصوب ۹۲ فروض مختلفی جهت تعیین دادگاه صالح از حیث صلاحیت محلی متصور می‌باشد که، به شرح آن می‌پردازیم :

۱. مطابق اصول کلی آیین دادرسی کیفری و نیز قانون جرائم رایانه‌ای در جایی که محل وقوع جرم معلوم باشد دادگاه محل وقوع جرم صالح به رسیدگی می‌باشد.

۲. یک یا چند جرم سایبری (مشابه از حیث مجازات است) در یک حوزه قضایی کشف یا گزارش شود که محل وقوع آن معلوم نباشد: مطابق ماده ۲۹ قانون جرائم رایانه‌ای 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 می‌کند و دادگاه مربوطه نیز رأی مقتضی صـــادر می‌کند .

۳. یک جرم سایبری واقع‌شده؛ ولی اجزاء مختلف عنصر مادی آن در دو حوزه واقع‌شده‌اند. و محل وقوع جرم معلوم نباشد به دلیل بروز اختلاف میان مراجع قضایی رأی وحدت رویه شماره ۷۲۹ مورخ ۹۱/۱۲/۱ در خصوص جرم کلاهبرداری مرتبط با رایانه مقرر می‌دارد.

«هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضایی مختلف صورت گرفته باشـد، دادگاهی که بانک افتتاح کننده حساب زیان دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزه آن قرار دارد، صالح به رسیدگی است».

۴. در صورت وقوع چند جرم مختلف از حیث مجازات در حوزه‌های قضایی متفاوت (اعم از سایبری و غیر سایبری) در صورتی که محل وقوع جرائم معلوم باشد، دادگاه محل وقوع مهم‌ترین جرم صالح به رسیدگی می‌باشد.

۵. در صورت وقوع چند جرم مشابه از حیث مجازات (اعم از سایبری و غیر سایبری) که محل وقوع جرائم مشخص نباشد و متهم نیز دستگیر نشده باشد دادگاهی که ابتدا شروع به رسیدگی کرده صالح می‌باشد.

۶. در صورت وقوع چند جرم مشابه از حیث مجازات در حوزه‌های قضایی مختلف که محل وقوع جرائم نیز معلوم نباشد دادگاه محل دستگیری متهم صالح به رسیدگی می‌باشد.

۷. در صورت وقوع چند جرم مشابه از حیث مجازات در حوزه‌های قضایی مختلف که متهم نیز دستگیرشده ولی محل دستگیر شدن محل وقوع جرم نباشد دادگاه محل وقوع جرم که ابتدا شروع به رسیدگی نموده است صالح به رسیدگی می‌باشد

پیشنهادها

۱. در رابطه با تعارض صلاحیت در حوزه‌های قضایی داخلی پیشنهاد می‌شود که با تشکیل یک هیات تخصصی و ایجاد یک سامانه‌ی رایانه‌ای یک پارچه میان حوزه‌های قضایی کل کشور تا در صورت دریافت هرگونه گزارش از مقامات ذیصلاح یا وصول شکوائیه، بلافاصله مراتب در سامانه‌ی مذکور ثبت و به اطلاع هیات رسانیده شود. و حوزه‌های قضایی بر اساس ماده ۲۹ قانون جرائم رایانه‌ای نسبت به جمع‌آوری ادله جرم و جلوگیری از فرار یا مخفی شدن متهم اقدامات لازم را بعمل‌آورده و مراتب را به نحو فوق‌الذکر منعکس نموده تا هیات تخصصی، با در نظر گرفتن معیارهای اصولی همچون تراکم بزه دیده در یک نقطه یا نقاط خاص، و اعلام احتمالی کشف ادله جرم در یک یا چند حوزه خاص و یا دستیابی احتمالی هر یک از حوزه‌ها به اطلاعات مرتکب یا مرتکبین، با ارجاع پرونده به حوزه‌ای که بیشترین پارامترها را در اختیار دارد و همچنین مکلف نمودن تمام مراجع قضایی دیگر به ارسال پرونده‌ها به مرجع تعیین‌شده اقدام نماید تا بدین صورت مرجع قضایی صالح تعیین و از تراکم پرونده‌ها، اطاله در روند تحقیقات و صدور آراء متهافت و متعارض جلوگیری گردد.

۲. همکاری و تعاون با مجامع بین‌المللی در زمینه حقوق شکلی

۳. همکاری با مجامع علمی و دانشگاهی دنیا و تبادل افکار و تجربیات آنان در راستای بومی‌سازی مسائل مربوط و ایجاد بستر حقوقی مناسب برای درک مفاهیم و مبانی جرائم سایبری در حقوق داخلی

منابع

۱- آشوری ، محمد (۱۳۸۸). **آیین دادرسی کیفری**، چاپ سوم، تهران: انتشارات سمت.

۲- آلبوعلی، امیر (۱۳۹۲). **صلاحیت محاکم در جرائم سایبری**، چاپ اول، انتشارات جنگل.

۳- باستانی، برومند(۱۳۹۰). **جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزه کاری** ، چاپ سوم، انتشارات بهنامی.

۴- جلالی فراهانی، امیرحسین (۱۳۸۴). **پولشویی الکترونیکی، فصلنامه تخصصی فقه و حقوق اسلامی**، سال اول، شماره چهارم.

۵- جلالی فراهانی، امیر حسین(۱۳۸۹). **در آمدی بر آیین دادرسی کیفری جرائم سایبری** ، چاپ اول ، انتشارات خرسندی.

۶- حسینی نژاد، حسین قلی(۱۳۷۳). **حقوق کیفری بین الملل**، نشر میزان.

۷- دی انجلیز، جینا(۱۳۸۳). **جرائم سایبر**، ترجمه سعید حافظی و عبدالصمد خرم‌آبادی، چاپ اول، دبیرخانه شورای عالی اطلاع‌رسانی.

۸- رایجیان اصلی، مهرداد(۱۳۸۸). **قانون جرائم رایانه‌ای**، نوآوری‌ها و کاستی‌ها، مجله پژوهش‌های حقوقی، تهران: مؤسسه مطالعات و پژوهش‌های حقوقی ، شماره ۱۵، سال هشتم.

۹- زندی، محمدرضا(۱۳۹۳).**تحقیقات مقدماتی در جرائم سایبری**،چاپ اول، انتشارات جنگل.

۱۰- کاشیان، علیرضا و دیگران، ۱۳۷۷ ، **راهبری اینترنت** ، دبیرخانه شورای عالی اطلاع‌رسانی ، تهران.

۱۱- مصطفوی، امیر،۱۳۸۷، **ادله اثبات دعاوی کیفری در فضای سایبر**، پایان‌نامه کارناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه شیراز .

۱۲- الهی منش، محمدرضا و سدره نشین، ابوالفضل، ۱۳۹۱، **محشای قانون جرائم رایانه‌ای**، چاپ دوم، انتشارات مجد.

۱۳- اسماعیلی فلاح، مرضیه، (۱۳۹۰)، **دادگاه صالح در رسیدگی به جرائم سایبر**، ماهنامه مدرسه حقوق، شال پنجم، شماره ۵۸.

۱۴- جلالی فراهانی، امیرحسین،(۱۳۸۳)، **ترجمه کنوانسیون جرائم محیط سایبر بوداپست**،۲۰۰۱، مرکز مطبوعات و انتشارات قوه قضاییه.

۱۵- جلالی فراهانی، امیرحسین ،(۱۳۸۷)،**صلاحیت کیفری در پرتو قوانین داخلی** ، مجموعه مقاله‌های حقوق فناوری اطلاعات و ارتباطات.

۱۶- حامد، سهیلا،۱۳۸۴، **صلاحیت جهانی**، انتشارات جهاد دانشگاهی.

۱۷- دولتشاهی،شاپور،۱۳۸۴،**صلاحیت قضایی در محیط مجازی**،مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات.

۱۸- قراچوزلو، رزا، ۱۳۹۰، **پیشگیری از جرم سایبری**، ماهنامه مدرسه حقوق، سال پنجم، شماره ۵۸.

۱۹- کاشیان، علیرضا و دیگران، ۱۳۷۷ ، **راهبری اینترنت** ، دبیرخانه شورای عالی اطلاع‌رسانی، تهران.

۲۰- محمد زاده، شهرام،۱۳۸۸، **صلاحیت مبتنی بر تابعیت در حقوق کیفری ایران**، منتشر در پیام آموزش، شماره ۲۸.

۲۱- همشهری آنلاین: WWW.hamshahrionline.ir/news-126496.asdx