فصلنامه علمی
فقه و مبانی حقوق اسلامی
دانشگاه آزاد اسلامی واحد بناب

The Scientific Journal in Jurisprudence and Bases of Islamic law The 16 rd.
Year/NO: 1 Spring 2023

نقش دسترسی آسان و سریع به محکمه در گسترش هنجاری صلاحیت محلی جرائم سایبری

اسماعیل باغبان [۱] بابک پورقهرمانی [۲] فاطمه احدی [۳]

تاریخ دریافت: ۱۴۰۱/۱۰/۰۶
تاریخ پذیرش: ۱۴۰۱/۱۰/۱۶

چکیده

مشخص نبودن قلمرو و مرز در فضای سایبر موجبات مشکلات عدیده‌ای درزمینه‌ی صلاحیت کیفری می‌گردد؛ که مسائلی همچون تعدد محل ارتکاب جرم و درنتیجه تعدد صلاحیت در این فضا و تعیین دقیق محل وقوع جرم، نمونه‌های بارزی از آن می‌باشد. از مهم‌ترین مسائلی که باید در این حوزه موردتوجه قرار داد، تعیین مرجع صالح ازنظر محلی،جهت رسیدگی به جرائم ارتکابی در فضای مذکوراست.سؤال اصلی پژوهش حاضر این است که دسترسی آسان و سریع به محکمه به چه نحوی می‌تواند اعمال صلاحیت محلی را در فضای سایبر ممکن نماید. مقاله حاضر با یاری جستن از روش توصیفی-تحلیلی و استقراء در موازین حقوقی و فقهی ناظر به صلاحیت محاکم،سعی در ارائه‌ی راهکاری برای گسترش صلاحیت محلی در این زمینه دارد. نتایج پژوهش نشان می‌دهد که شیوه‌های نوین رسیدگی به جرائم سایبری ازجمله دادرسی الکترونیکی و لحاظ نمودن شرایط همگون حقوقی با جامعه‌ی بین‌المللی و ایجاد یک سیستم قضایی با صلاحیت جهانی، می‌تواند چالش‌های اعمال صلاحیت محلی در جرائم سایبری را مرتفع و دادرسی را تسهیل و تسریع نماید.

واژگان کلیدی: صلاحیت محلی، جرائم سایبری، احتجاب، عدالت کیفری

[۱]. دانشجوی دکتری تخصصی، رشته حقوق کیفری و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. es.baghban@gmail.com
[۲]. دانشیار گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران(نویسنده مسؤول). b.pourghahramani@yahoo.com
[۳]. استادیار گروه حقوق جزا و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. ahadi-223@yahoo.com

مقدمه

اعمال صلاحیت محلی در فضای سایبری می‌تواند منجر به چالش‌های عدیده‌ای گردد؛در همین راستا پذیرش این اصل در سیستم حقوقی و کیفری کشورهای مختلف با انتقادات فراوانی مواجه گردیده است. لیکن امروزه نیاز جامعه‌ی جهانی، کشورهای مختلف و حتی مخالفان این اصل را به پذیرش این اصل –حداقل در جرائم مهم– وادار ساخته است.

جهت اعمال صلاحیت محلی در جرائم سایبری، لازم است که محل وقوع جرم تعیین شود؛ لیکن با توجه به ویژگی‌های فضای سایبر و عدم اختصاص جرائم به مکانی مشخص، این امر به‌سادگی امکان‌پذیر نخواهد بود؛ لذابرای تعیین مرجع صالح بر روی محل استقرار سامانه‌های رایانه‌ای و یا محل استقرار کنشگران این فضا تکیه می‌کنند؛ که هرکدام از این نظریات معایبی دارد. از طرف دیگر نباید به این بهانه، از تعقیب و شناسایی مرتکبین و محل دقیق ارتکاب جرم صرف‌نظر کرده یا نسبت به آن تعلل ورزید. علاوه بر آن جرائم ارتکابی در فضای سایبر (نظیر فضای واقعی) تنها منحصر به جرائم آنی نیست چراکه ممکن است جرائم ارتکابی در فضای سایبر به شکل مستمر یا مرکب نیز واقع شود، که در این فرض مشکل دوچندان خواهد بود. در خصوص جرائم مستمر که مثال آن در دنیای واقعی آدم‌ربایی است جابجایی قربانی در حوزه‌های قضایی متعدد، محاکم متعددی را درگیرامر صلاحیت می‌نماید، که در فضای مجازی نیز مصادیق زیادی برای تحقق جرائم مستمر متصور است مانند نشر محتوای مغایر باعفت و اخلاق عمومی، نشر اکاذیب و..... در خصوص تشخیص دادگاه صالح به این‌گونه جرائم (جرائم مستمر) در فضای سایبر سه نظر بیان‌شده که «برخی از آن‌ها دادگاه محل شروع ارتکاب فعل (نظر اول) و برخی دادگاه محل انقطاع فعل مستمر (نظر دوم) و برخی دیگر تمامی دادگاه‌هایی که جرم در حوزه آن‌هاواقع‌شده (نظر سوم) را صالح به رسیدگی می‌دانند».(رضوی فرد،موسوی، ۱۳۹۵).

فارغ از بحث آنی یا مستمر بودن جرائم سایبری، موضوع اعمال صلاحیت محلی با چالشی اساسی در این فضا روبرو است؛ لذا به نظر می‌رسد ترسیم روشی کارآمد که بتواند دسترسی به محکمه برای جرائم سایبری را تسهیل و تسریع نماید ضروری خواهد بود. پژوهش حاضر با یاری جستن از روش توصیفی–تحلیلی و استقراء در موازین حقوقی و فقهی در راستای بررسی چالش صلاحیت محلی در جرائم سایبری است و سؤال اصلی مقاله حاضر این است که دسترسی آسان و سریع به محکمه چه تأثیری بر عملیاتی کردن اعمال صلاحیت محلی در فضای سایبر خواهد داشت؛ که در مقام فرضیه‌ی اصلی می‌توان بیان داشت امروزه دسترسی آسان و سریع به دستگاه عدالت کیفری می‌تواند این مشکل را تا حد زیادی رفع و با گسترش مفهوم صلاحیت محلی، اعمال این اصل را در جرائم سایبری ممکن سازد. هدف اصلی نوشته‌ی پیش رو نیز تحلیل و بررسی نقش سهل کردن دسترسی به محاکم کیفری برای رسیدگی به جرائم سایبری و نقش آن در گسترش هنجاری صلاحیت محلی در جرائم سایبری است.

۱.جرم سایبری

۱.۱.مفهوم

جرائم سایبری در اصطلاح به جرائمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد(بیابانی،هادیان فر،۲۲۵:۱۳۸٤). امروزه بسیاری از جرائم سنتی، هم‌زمان با پیشرفت فناوری اطلاعات و ارتباطات به‌شدت متحول شده و به‌صورت جرائم سایبری هم ارتکاب می‌یابند. عنوان جرائم سایبری نیز به جهت گسترش خود، رفته‌رفته جانشین عباراتی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. به جرائم سایبر، جرائم علیه فناوری اطلاعات نیز گفته می‌شود(زندی،۱۳۸۹:٤۰). واژه رایانه به‌گونه‌ای دقیق و جامع نمی‌تواند گستردگی این محیط را نشان دهد زیرا بسیاری از ابزار و وسایل امروزی با داده‌هایی کار می‌کنند که اساساً به آن‌ها رایانه اطلاق نمی‌شود. ازاین‌رو عبارت‌هایی مانند جرم‌های رایانه‌ای یا جرم‌های اینترنتی نیز نمی‌توانند به‌گونه‌ای دقیق جرم‌های ارتکابی مربوط به این حوزه را پوشش دهند. برای نمونه یک سامانه ضبط و پخش الکترونیکی که متصل به اینترنت باشد، رایانه نیست؛ اما به‌طورکلی در زیرمجموعه فضای سایبر قرار می‌گیرد. در جرائم

سایبری، هیچ تأکیدی بر واسطه وجود ندارد. وسایل مختلفی ساخته‌شده‌اند که هرکدام روش جدیدی را در راه‌یابی به این فضا، بدون نیاز مستقیم به رایانه پدید آورده‌اند، مثلاً تلفن همراه یکی از این وسایل است(زندی،۱۳۸۹:٤١).

۱.۲.تاریخچه جرائم سایبری

جرائم سایبری از زمان پیدایش تاکنون، با سه نسل یا گونه مواجه شده است. دهه‌های ٦٠ و ٧٠ و اوایل ٨٠ زمان حاکمیت نسل اول تحت عنوان جرائم رایانه‌ای است. در این زمان در خصوص جرائم، محوریت بحث با رایانه بود. ازاین‌رو تعداد توصیف‌های مجرمانه بسیار کم بود.

به‌تدریج در دهه ۸۰ تا اوایل دهه ۹۰ نسل دوم به میان آمد. بحث محتوا مورداستفاده قرار گرفت یعنی به موضوع جرائم داده و اطلاعات توجه شد. ازاین‌رو نسل دوم تحت عنوان جرائم علیه داده‌ها مطرح شد.

پس از چهار یا پنج سال، حاکمیت نسل سوم که از آن به جرائم سایبری یاد می‌کنیم فرارسید که ویژگی این نسل، تجمیع رایانه با مودم و مخابرات (اعم از ماهواره) با حالات شبیه‌سازی و مجازی‌سازی است. در این نسل تأکید بر رایانه نیست بلکه رایانه خود وسیله ارتکاب جرم است. جرائم نسل سوم در بستر ابر شاهراه‌های الکترونیکی ارتباطی و اطلاعاتی به وقوع می‌پیوندند.

اگر در چهار دهه رواج جرائم رایانه‌ای، ما شاهد جرائم انگشت‌شماری بودیم؛ اما در فضای سایبر پنج دسته اصلی جرم وجود دارد که هرکدام شامل چندین عنوان مادر و عمده می‌شوند و شاید تعداد مصادیق عمد و غیر عمد آن بالغ بر ۲۰۰ عنوان مجرمانه شود(شیرزاد،۱۳۸۸:۲۳).

اولین جرم سایبری در ایران به سال ۱۳۸۱ و ناظر به عمل دانشجویان برای اسکن اسکناس و پرینت رنگی آن بود؛ که یک کارگر چاپخانه و یک دانشجوی رایانه در کرمان اقدام به جعل چک‌های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندانی بین جرم رایانه‌ای و جرم اینترنتی وجود ندارد، عمل آن‌ها به عنوان جرم سایبری محسوب می‌شد. (زندی،۱۳۸۹:۵۰).

۱.۳. ویژگی‌های منحصربه‌فرد جرائم سایبری

جرائم سایبری جزو جرائم ناشی از فناوری‌های مدرن هستند؛ ازاین‌رو دارای ویژگی‌های منحصربه‌فردی‌اند که آن را از جرائم کلاسیک و سنتی جدا می‌کند. در این بخش برخی از این تفاوت‌ها را برمی‌شماریم (زندی:۱۳۸۹:۵۷).

۱.۳.۱. زمان ارتکاب جرم

برخلاف جرائم سنتی که زمان در آن مشهود است، در جرائم سایبری زمان به چند ثانیه یا کسری از ثانیه تبدیل می‌شود.

۱.۳.۲.مکان ارتکاب جرم

مکان نیز در جرائم سایبری به‌واسطه زیرساخت مخابرات و شبکه‌ای شدن رایانه‌ها و گسترش اینترنت، تغییر یافته است. به‌عنوان‌مثال اگر فرد قبلاً برای ارتکاب کلاه‌برداری باید مراحل ارتکاب جرم را تکمیل می‌کرد و در تهران موفق به کلاه‌برداری می‌شد و درنهایت می‌توانست به اصفهان یا شهر دیگری برود و عمل را تکرار کند؛ اما در کلاه‌برداری در فضای سایبر، این تعدد مکانی بیش‌ازحد زیاد می‌شود.

۱.۳.۳.بزه دیده

در حالت سنتی بزه دیده انسان است، به‌عبارت‌دیگر، جرم علیه تمامیت جسمی یا روانی شخص و یا علیه اموال اشخاص حقیقی یا حقوقی صورت می‌گیرد. به‌عنوان‌مثال در جرائم علیه اشخاص، تمامیت جسمانی و روانی فرد یا اموال او، هدف ارتکاب جرم است؛ اما در جرائم سایبری، در بسیاری موارد، بزه دیده، ماشین است که بیشترین مورد تحقق آن در جرائم الکترونیک و جرائم بانکداری الکترونیک است؛ هرچند که ممکن است نتیجه عمل همان اموال شخص باشد؛ ولی نکته تمایز هدف‌گیری این موضوع توسط وسیله‌ای به نام فضای سایبری است.

۱.۳.٤.تعداد قربانیان

تعداد قربانیان در جرائم کلاسیک، تعدادی خاص و محدود هستند درحالی‌که امروز در فضای سایبر، تعداد زیادی قربانی می‌شوند. به‌عنوان‌مثال هنگام انتشار یک ویروس، میلیون‌ها سایت، رایانه و در پی آن میلیون‌ها کاربر، متضرر یا قربانی می‌شوند و یا با راه‌اندازی یک وب‌سایت یا ارسال پیام‌های تبلیغاتی فریب‌کارانه به آدرس‌های الکترونیکی کاربران، میلیون‌ها مخاطب فریب می‌خورند (جلالی فراهانی،۱۳۸٤:۵).

۱.۳.۵.مشکل اعمال صلاحیت

مشکل اعمال صلاحیت قانونی در مقابل جرائم سایبری معضلی اساسی است.استفاده از ادله، داده‌های الکترونیکی یا مدارک الکترونیکی دارای مشکلات متعددی است؛که مهم‌ترین این مشکلات «محل و مکان وقوع جرم» هست. برای غلبه بر این مشکلات پیشنهادهای بسیاری ارائه گردیده است که مهم‌ترین آن‌ها عبارت‌اند از:

۱. امنیت نرم‌افزار شبکه کامپیوتری به‌عنوان یک اقدام پیشگیرانه که می‌تواند در زمینه ایمن‌سازی نرم‌افزار شبکه کامپیوتری، مانند تنظیم دسترسی (کنترل دسترسی)، از طریق مکانیزم احراز هویت با استفاده از رمز عبور انجام شود.

۲. دولت به همراه مقامات مجری قانون باید سریعاً اقدامات متقابل و اجرای قانون را انجام دهند.

۳. تصویب قوانین و مقررات ویژه حاکم بر دنیای سایبری و نهادهای مجری مقررات، یعنی پلیس، دادستان و قضات ویژه که به‌طور خاص به جرائم سایبری رسیدگی می‌کنند و همچنین امکانات یا ابزارهایی برای حمایت از اجرای این مقررات.

٤. اجرای همکاری‌های بین‌المللی و اعمال اصول بین‌المللی که می‌تواند به‌عنوان عرف بین‌المللی برای اجرای قانون به رسمیت شناخته شود، با توجه به اینکه جرائم مدرن از مرزهای ملی عبور کرده‌اند، بنابراین لازم است برای غلبه بر آن‌ها توافقات دوجانبه و رفع مشکلات بین کشورها به‌ویژه جرائم سایبری صورت گیرد.(Rahmatilla, Huala, Jafar, 2021,p.206)

۱.٤.انواع جرائم سایبری

جرائم سایبر را در چهار دسته یا طبقه کلی می‌توان جای داد:

۱. جرائم کلاسیک با وصف 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. ازجمله این جرائم می‌توان به کلاه‌برداری سایبری، جعل سایبری، تخریب سایبری، جاسوسی سایبری و ... اشاره نمود»(راجی،۱۳۸۵:۹٦).

۲. جرائم علیه محرمانه بودن داده‌ها و سامانه‌ها

«هر نمادی از موضوع‌ها، مفاهیم یا دستورالعمل‌ها ازجمله متن، صوت یا تصویر را که برای برقراری ارتباط میان سامانه‌های رایانه‌ای با پردازش توسط شخص یا سیستم رایانه‌ای به کار گرفته‌شده و به‌وسیله سیستم رایانه‌ای ایجاد می‌گردد، داده محتوا گویند. ازجمله 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»(رضوی،۱۳۸٦:۱۲۳).

۳. جرائم علیه صحت و تمامیت داده‌ها و سامانه‌ها

«تغییر، ایجاد، محو یا متوقف کردن رایانه‌ای و مخابراتی به‌قصد تقلب، غیرقابل استفاده کردن، تخریب یا ایجاد اختلال در داده‌ها یا ارسال امواج الکترومغناطیسی، ممانعت از دستیابی اشخاص مجاز به داده‌ها با تغییر رمز ورود و یا رمزنگاری ازجمله جرائمی هستند که در این دسته قرار می‌گیرند»(رضوی،۱۳۸٦:۱۲٤).

٤. جرائم مرتبط با محتوا

«این دسته جرائمی را تحت شمول خود قرار می‌دهد که در آن‌ها، رایانه به‌عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می‌شود و صرفاً فناوری اطلاعات، زمینه ارتکاب آن‌ها را فراهم می‌سازد. برای مثال انتشار محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش جنسی انسان، تبلیغ یا تحریک یا تشویق به انحرافات جنسی یا خودکشی از طریق سیستم رایانه‌ای یا مخابراتی در این دسته قرار می‌گیرند»(رضوی،۱۳۸٦:۱۲٤).

۲.چالش اعمال صلاحیت در فضای سایبر

توسعه فناوری اطلاعات تغییر عمده‌ای در زندگی ما ایجاد کرده است، با فراگیر شدن اینترنت، افراد و سازمان‌ها صرف‌نظر از مکانشان، به یکدیگر نزدیک‌تر شده‌اند. علی‌رغم مزایای آشکار این فضا که ما را قادر ساخته است رشد سریع اقتصاد جهان را شاهد باشیم، شاهد جنبه‌های تاریک اینترنت و پیامدهای منفی تأثیر اینترنت بر انسان نیز هستیم. در فضای موجود، جریان اطلاعات و ارتباطات محدود به مرزهای جغرافیایی و دولتی نیست و این وضعیت مملو از خطر سلب امنیت برای دولت و جامعه است. ظهور انواع جدید جرائم و ارتکاب جرائم سنتی به روش‌های جدید، نتیجه ورود گسترده فناوری اطلاعات به زندگی ماست. نیاز به مقررات قانونی در فضای مجازی واضح است، بااین‌حال، ماهیت فرامرزی، از راه دور و غیر شفاف بودن آن، مشکلات خاصی را ایجاد می‌کند.(Schmitt,2017, p. 215)

مشکل اصلی در این وضعیت پیدا کردن قوانین صلاحیتی مناسب با رهیافتی پاسخگو در فضای مذکور است. درواقع مشکل مقررات فضای سایبری در این واقعیت نهفته است که صلاحیت دولت‌ها مبتنی بر رویکرد سرزمینی است، درحالی‌که احتمالاً باید در مورد مقررات بین‌المللی یا به‌طور دقیق‌تر، در مورد مقررات حقوقی جهانی فضای سایبری باشد. از این گذشته، همه ما علاقه‌مند به قوانین مؤثری هستیم که بتواند روابط حقوقی را تنظیم کند که فراتر از قوانین یک کشور است و به دلیل ویژگی‌های این فضا است که می‌تواند هم‌زمان منافع مختلف چندین کشور را به‌صورت جهانی دربرگیرد.

یکی از ویژگی‌های فضای سایبر که آن را از دنیای واقعی متمایز می‌کند، ناشناس بودن –ناپیدا بودن– است که مشکل شناسایی کاربر و همچنین مشکل محرمانگی از آن ناشی می‌شود؛ که محاکم را با مشکلات اساسی روبرو می‌نماید. به‌عنوان‌مثال، تلاش برای منطقه بندی فضا بر اساس محدودیت سنی به دلیل اینکه در فضای مجازی، جداسازی بر اساس سن، جنسیت یا معیارهای دیگری که جداسازی آن در دنیای واقعی کاملاً آسان است، بسیار دشوار و پرهزینه است، شکست خورده است و بنابراین اعمال هنجارهای حقوقی موجود در این مشکل بی‌تأثیر است. حریم خصوصی در فضای مجازی نیز با توجه به ویژگی‌های آن با حریم خصوصی در دنیای واقعی متفاوت است؛ بااین‌حال، مقررات قانونی مستلزم شفافیت کامل کل اینترنت است، که امروزه ازنظر فنی مشکل‌ساز است. اگر فرض کنید هنگام ورود به اینترنت، شناسایی ویدیویی کاربر رخ دهد، مشکل شناسایی با موفقیت حل می‌شود، اما این روش ازنظر «حریم خصوصی» خطرناک است و بازهم نیاز به شفافیت کامل دارد که اینترنت توانایی فنی این موضوع را ندارد. از سوی دیگر نگرانی‌های قانون‌گذاران در این بخش قابل‌درک است، زیرا مشخص نیست که آیا کنترل دولتی برای شناسایی موجه یا کافی خواهد بود، یا اینکه ما می‌خواهیم به دولت اجازه دهیم چنین اطلاعات محرمانه‌ای را درباره کاربر دریافت کند. موضوع دیگر در مقررات فضای مجازی، رویکرد به مقررات است، زیرا بدون شک اگر یک کشور فضای مجازی را به‌شدت تنظیم کند و کشور دیگر به‌هیچ‌وجه مقرراتی را تنظیم نکند، درنتیجه کلیت مقررات به‌شدت بی‌اثر می‌شود. در این راستا، بحث در مورد تصویب قوانین عمومی برای تنظیم فضای مجازی در سطح بین‌المللی ضروری است.

اصل سرزمینی به‌خودی‌خود مبنای بسیار محدودی برای صلاحیت است. در این صورت، رسیدگی به جنایاتی که عواقبی برای تعداد نامحدودی از کشورهای دیگر دارد، بسیار دشوار خواهد بود. در مورد «پرونده یاهو» در فرانسه، ملاحظه می‌گردد که دادگاه برای مورد پیگرد قرار دادن جرم نتایج آن در فرانسه را مناط اعتبار قرار داده است؛اگرچه هیچ عنصر تشکیل‌دهنده جرم در خاک

فرانسه رخ نداده است. ازنظر حقوقی، بدیهی است که چنین رویکردی در اعمال صلاحیت یک دولت در روابط حقوقی در فضای سایبر ناکافی است.

از سوی دیگر در مسیر اعمال صلاحیت سرزمینی باید این را مدنظر قرارداد که زیرساخت‌های سایبری دولت‌ها به هم مرتبط هستند، بنابراین اعمال صلاحیت قضایی در یک دولت بر زیرساخت‌های سایبری کشور دیگر تأثیر می‌گذارد. البته، این دلیلی برای محدود کردن حاکمیت یک کشور نیست، چراکه مرزهای سایبری جداگانه وجود ندارد، استقلال سیاسی و حاکمیت ارضی دولت توسط قانون محافظت می‌شود و مفهوم سرزمینی حاکمیت در هنگام تنظیم سایر کشورها مصون از تعرض باقی می‌ماند.. اصل موجود حاکمیت ناشی از حقوق بین‌الملل و به‌ویژه از بند ۱ ماده ۲ منشور سازمان ملل متحد، منع مداخله غیرقانونی بین دولت‌ها را پیش‌فرض می‌گیرد. بر اساس اصل حاکمیت سرزمینی، دولت‌ها موظف هستند که اجازه استفاده آگاهانه از قلمرو خود را برای اقداماتی که با حقوق سایر کشورها در تضاد است، ندهند(Corfu Channel case,1949). نمونه‌ای از مداخله غیرقانونی، انتشار اطلاعات نادرست از طریق اینترنت، تحریک ناآرامی سیاسی توسط یک کشور خارجی دیگر به‌منظور مداخله در انتخابات یک کشور دیگر است. به‌عنوان‌مثال، آلمان بر این باور است که «اقدامات سایبری اگر ازنظر مقیاس و تأثیر با اجبار در زمینه‌های غیر سایبری مشابه باشد ممکن است مداخله‌ای ممنوع تحت قوانین بین‌المللی باشد ». علاوه بر این، آلمان این دیدگاه را بیان می‌کند که اگر فعالیت‌های سایبری بخشی از یک درگیری مسلحانه جاری باشد، حقوق بشردوستانه بین‌المللی در مورد فعالیت‌های سایبری در چارچوب یک درگیری مسلحانه اعمال می‌شود(On the Application of International Law in Cyberspace. 2021,p.5). بنابراین، آلمان بر این عقیده است که قوانین بین‌المللی، منشور ملل متحد و حقوق بشردوستانه بین‌المللی، بدون قید و شرط درزمینه‌ی فضای مجازی اعمال می‌شود.نظر مشابهی توسط حقوقدانان روسی وجود دارد که بین صلاحیت قضایی در فضای سایبری و صلاحیت در حقوق بین‌الملل فضایی مشابهی ایجاد کرده‌اند. به نظر آن‌ها، می‌توان تعریف مفهوم قلمرو یک دولت را با گنجاندن فضای دیگری در آن، مثلاً فضای مجازی، گسترش داد(Erentyeva LV ,2019,p.121). در همین حال، به‌منظور اطمینان از ایمنی کار در اینترنت، علی‌رغم بحث‌های داغ برای چندین سال، در فدراسیون روسیه در ماه مه ۲۰۱۹، قانونی به تصویب رسید که در رسانه‌ها «قانون اینترنت مستقل» نامیده شد. این قانون مفاهیم جدیدی مانند «نقطه تبادل ترافیک»[1]، «خطوط ارتباطی فرامرزی»[2]، سامانه نام دامنه ملی در حال ایجاد و تعهدات اپراتورهای مخابراتی برای استفاده از تجهیزات دولتی در نقاط مبادله ترافیک را معرفی کرد. بدون شک تصویب این قانون نشان‌دهنده رویکرد فدراسیون روسیه در رابطه با ایجاد صلاحیت قضایی در فضای مجازی بر اساس مفهوم اعمال اصل سرزمینی است.

(http://publication.pravo.gov.ru /Document/View/0001201905010025)

همچنین اقداماتی از سوی« شورای اروپا» برای مبارزه با جرائم سایبری انجام شده است که نتیجه آن «کنوانسیون بوداپست» در سال ۲۰۰۱ است. این کنوانسیون تعدادی معیار را برای ایجاد صلاحیت در جرائم کیفری تعیین می‌کند، که هنجارهای کنوانسیون بر اساس اصل سرزمینی است و جرائم ارتکابی در قلمرو یک دولت مطابق صلاحیت آن کشور تلقی می‌شود. این کنوانسیون همچنین اصل تابعیت را به رسمیت می‌شناسد. مطابق با فحوای کنوانسیون، کشورها برای مقابله مؤثرتر با جرائم فرامرزی باید وسایل ارتباطی بین‌المللی در مورد چنین موضوعاتی داشته باشند.

با توجه به آنچه بیان گردید باید اذعان داشت که فضای مجازی در حال حاضر بخشی جدایی‌ناپذیر از زندگی ما است و بسیار مهم است که در اسرع وقت از تنظیم کامل حقوقی روابط در کشور اطمینان حاصل شود. این حوزه برای تضمین امنیت بین‌المللی و همچنین حمایت از حقوق و منافع مشروع دولت، جامعه و فرد است. برای تطبیق قانون با چالش‌های جدید، شناخت ویژگی‌های

[1] Traffic exchange point
[2] Cross-border communication lines

فضای مجازی ضروری است. همچنین توسعه یک رویکرد واحد برای تعریف صلاحیت قضایی در فضای سایبری توسط همه دولت‌ها مهم است و باید اذعان نمود که در وضعیت فعلی بهترین معیار برای اعمال صلاحیت در این فضا، صلاحیت سرزمینی است که البته لزوم تسریع دسترسی به محاکم اجتناب‌ناپذیر می‌نماید که در ادامه تحلیل خواهد شد.

۳. اعمال صلاحیت محلی در جرائم سایبری و راهکار دسترسی سریع و آسان به محکمه

به‌موازات تحول فنّاوری درزمینه‌ی اطلاعات، رایانه و به ویژه پیدایش اینترنت، جهان با پدیده‌ی دنیای مجازی به نام فضای سایبر مواجه شده است. از مهم‌ترین مسائلی که باید در این حوزه مورد توجه قرارداد، تعیین تکلیف راجع به چگونگی تعیین مرجع قضایی صالح برای رسیدگی به جرائم ارتکابی در فضای سایبر، یعنی صلاحیت کیفری مراجع قضایی است. علی‌رغم وجود اختلافات در خصوص محل وقوع جرم و ضابطه تشخیص آن جهت تعیین دادگاه یا دادسرای صالح، مسئله‌ی مهمی که در این زمینه به‌ویژه در دهه‌های اخیر به وجود آمده است، دشواری 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 تفاوت دارد؛ به‌طوری‌که این فضا کاملاً غیرملموس و مجازی است و مرز جغرافیایی نمی‌شناسد. این امر مسأله تفاوت صلاحیت مراجع قضایی مختلف در رابطه با آن جرائم در حقوق کیفری را مطرح کرده است (عبدالهی، مرادی،۱۳۹٤:٤۰)

در کشور ما ازلحاظ رویه عملی، تا قبل از تصویب «قانون مجازات جرائم رایانه‌ای مصوب۱۳۸۸» قضات سعی در اجرای قواعد سنتی صلاحیت با اتخاذ معیاری جدید و موافق با فضای سایبر داشتند که در این خصوص رویه واحدی هم اتخاذ نشده بود. با تصویب قانون آئین دادرسی کیفری مصوب ۱۳۹٤، عنوان «دادرسی الکترونیکی»در بخش نهم رسمیت یافته است، که شاید بتوان گفت دادرسی الکترونیکی بیشترین سنخیت را با جرائم سایبری دارد.

دادرسی الکترونیکی در مواجهه با جرائم سایبری مبتنی بر بستر مبادله الکترونیکی است و «بر این قاعده ساده استوار است که پاسخ ارتکاب جرم در فضای سایبر را باید در همان فضای سایبر و با امکانات آن داد»(مؤذن‌زادگان، روستا،۱۳۹٦،ص۱۸۵). به‌طورکلی می‌توان گفت یکی از معیارهای مهم که می‌تواند برای صلاحیت کیفری سایبری مورداستفاده قرار گیرد، معیار تابعیت بزه دیده است، چنانکه در این معیار محل ارتکاب جرم سایبری و یا تابعیت متهم ملاک نیست بلکه کافی است جرمی سایبری علیه یکی از اتباع رخ‌داده باشد تا مراجع قضایی کشور صلاحیت رسیدگی داشته باشد. دراین‌باره ماده ۸ قانون مجازات اسلامی مقرر نموده است که:

« هرگاه شخص غیر ایرانی در خارج از ایران علیه شخصی ایرانی یا علیه کشور ایران مرتکب جرمی شود و در ایران یافت یا به ایران اعاده گردد، طبق قوانین جزایی جمهوری اسلامی ایران به جرم او رسیدگی می‌شود»

بنابراین با تحقق سایر شرایط، فارغ از اینکه تابعیت متهم چیست و درنهایت با توجه به مقررات قانون آئین دادرسی کیفری، مرجع قضایی محل دستگیری یا محل اقامت متهم صالح به رسیدگی خواهد بود.

در پاسخ به این سؤال که آیا صلاحیت محلی یا صلاحیت مبتنی بر تابعیت مجنی‌علیه، می‌تواند در این‌گونه جرائم معضلات را حل کند باید گفت؛ در اغلب موارد دولت متبوع مجنی‌علیه به متهم دسترسی ندارد تا بخواهد وی را در صورت محاکمه، مجازات کند. از طرفی صرف انجام محاکمه‌ای صوری (درصورتی‌که همراه با مجازات نباشد)، نمی‌تواند موجبات تشفی خاطر بزه دیده یا اولیای دم را فراهم آورد و اساساً چنین محاکمه‌ی بی‌اثری، حمایت واقعی از اتباع نیست.

افزون بر این، در موافقت‌نامه‌های راجع به استرداد مجرمان نیز غالباً به استرداد به کشور محل وقوع جرم یا کشور متبوع مجرم توجه شده است نه کشور متبوع مجنی‌علیه؛ برای مثال ماده ۳ قانون راجع به استرداد مجرمان ایران، مصوب ۱۳۳۱، مقرر می‌دارد:

«دولت ایران می‌تواند بنا به درخواست دول خارجی، افراد غیر ایرانی را که در قلمرو ایران اقامت دارند در صورت وجود شرایط زیر به دولت تقاضادهنده تسلیم نماید:

۱- جرم ارتکابی در قلمرو دولت تقاضاکننده، به‌وسیله اتباع آن دولت و با اتباع دولت دیگر واقع‌شده باشد.

۲- جرم ارتکابی در خارج از قلمرو دولت تقاضاکنندهبه‌وسیله‌ی اتباع آن دولت و یا اتباع دولت دیگر واقع‌شده باشد

۳- جرم ارتکابی در خارج از قلمرو دولت تقاضاکنندهبه‌وسیله شخصی غیر از اتباع آن دولت واقع‌شده باشد مشروط بر اینکه جرم ارتکابی مضر به مصالح عمومی کشور تقاضاکننده باشد.»

ملاحظه می‌گردد که سه بند این ماده به ترتیب ، اصل صلاحیت سرزمینی، اصل صلاحیت مبتنی بر تابعیت مرتکب و اصل صلاحیت واقعی را مدنظر قرار داده‌اند و توجهی به اصل صلاحیت مبتنی بر تابعیت مجنی‌علیه ندارند. بنابراین پذیرش صلاحیت محلی نه‌تنها در عمل کاربردی ندارد بلکه باعث مشکلاتی ازجمله تراکم کاری محاکم داخلی می‌گردد، مگر اینکه کشورهایی که این نوع صلاحیت را می‌پذیرند اعمال این صلاحیت را منوط به شرایطی مثل استرداد یا دست‌کم یافت شدن مرتکب در قلمرو کشور خویش کند. برخی از صاحب‌نظران عقیده دارند که «اقدامات و مبادلات در فضای سایبر از یک‌سو مستلزم رعایت اصل صلاحیت سرزمینی در خصوص بزه ارتکابی در قلمرو داخلی یک کشور و از سوی دیگر متضمن آن است که اگر مجرمین به فعالیتی در یک کشور مبادرت می‌نمایند که سبب آثار فراملی در کشور دیگر شده است، کشور اخیر نیز حق اعمال صلاحیت دارد.»

(Semenova,2021, p.1387)

با توجه به مسائل و موضوعات اشاره گردیده به نظر می‌رسد چالش‌های اصل صلاحیت محلی در جرائم سایبر، عبارت از مکان و محل وقوع جرم، زمان وقوع جرم، محل استقرار مرتکب و تعیین هویت او در فضای سایبر، است که جهت بررسی این موارد به‌طور مجزا به آن‌ها می‌پردازیم.

۱-۳.محل و زمان وقوع جرم (عدم احتجاب و دسترسی آسان به محکمه)

مهم‌ترین مانع موجود بر سر راه تعیین صلاحیت دادگاه‌های کیفری و اعمال صلاحیت سرزمینی نسبت به جرائم سایبری، محل وقوع جرم است. موقعیت شبکه رایانه‌ای و محیط سایبری آن‌چنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. ازآنجاکه اطلاع از این موقعیت مکانی برای عملکرد شبکه و اهداف ایجادکنندگان آن اهمیتی ندارد لذا اغلب در طراحی یک شبکه امکان تشخیص مکان جغرافیایی لحاظ نمی‌شود. در جرائم سنتی عواملی که بر تعیین مکان وقوع جرم اثر می‌گذارد بسته به محل شروع جرم، محل استقرار مجرم، محل وقوع نتیجه، محل وجود ادله و محل کشف جرم و ..... تفاوت می‌کند؛درحالی‌که در جرائم سایبری به خاطر مجازی و دیجیتالی بودن محل ارتکاب و همچنین گستردگی شبکه رایانه‌ای و مخابراتی تعدد عوامل مختلف در خصوص مکان به‌صورت یک چالش نمود پیدا می‌کند؛ مانند انتشار ویروس که در آن یک عمل چندین سایت را در اقصی نقاط دنیا آلوده می‌کند و یا فردی که مطالب افتراآمیز را در سراسر شبکه اینترنت منتشر می‌کند، در یک‌لحظه زمانی بسیار کوتاه بیش از چند کشور و به عبارتی چند میلیون سایت را درگیر می‌کند(امینی‌نیا، علیزاده،۱۳۹۷).

اگرچه با به‌کارگیری فنون و شیوه‌های پیشرفته و تلاش‌های مضاعف شاید بتوان محل شروع عملیات یا بارگذاری محتویات را ازنظر فیزیکی مشخص کرد، ولی این تشخیص اولاً نیاز به یک همکاری گروهی و بین‌المللی ازیک طرف و شرکت‌های خدمات‌دهی اطلاعاتی از طرف دیگر است. ثانیاً تشخیص این مکان برای اعمال صلاحیت کافی نیست.

اگرچه سایت‌های اینترنتی آدرس دارند ولی این آدرس جایگاه آن‌ها را در شبکه مشخص می‌کند نه درمکان و موقعیت حقیقی.البته بعضی آدرس‌های اینترنتی مشخص‌کننده جغرافیایی یا مشخص‌کننده‌هایی که ازنظر جغرافیایی قابل‌تعیین باشند را در خود دارند. «برای مثال یک آدرس اینترنتی که پسوند(UK) داشته باشد در انگلستان به ثبت رسیده است. اکثر آدرس‌های اینترنتی فاقد

شاخص‌های جغرافیایی هستندو از سوی دیگر استفاده از فیلترشکن‌ها که می‌تواند آدرس‌ها و «آی.پی» را به کلی تغییر دهد، وضعیت را بغرنج‌تر نیز می‌نماید.

کنوانسیون مربوط به جرائم محیط سایبر بوداپست (۲۰۰۱) ،که به جنبه‌های مختلف جرائم سایبری ازجمله صلاحیت پرداخته است در این زمینه در بخش دوم از فصل دوم بند ۱ ماده ۲۲ تصریح کرده است که:

« هر یک از اعضاء باید به‌گونه‌ای اقدام به وضع قوانین و مقررات کند که در صورت لزوم درزمانی که جرم در موارد زیر ارتکاب می‌یابد صلاحیت رسیدگی به هر یک از جرائم مندرج در موارد ۲ تا ۱۱ کنوانسیون را دارا باشد:

الف) جرم در قلمرو آن ارتکاب یافته باشد یا

ب) جرم در کشتی‌ای ارتکاب یافته باشد که پرچم آن کشور بر فراز آن برافراشته است یا

ج) جرم در هواپیمایی ارتکاب یافته باشد که مطابق مقررات آن عضو به ثبت رسیده است یا

ت)درجایی که جرم موردنظر مطابق قوانین جزائی، قابل مجازات شناخته‌شده و آن را نسبت به تبعه‌اش مرتکب شده و یا جرم ارتکابی ازجمله جرائم واقع در حوزه‌ی صلاحیت کیفری جهانی است».

باکمی دقت در این مقرره فهمیده می‌شود که این بندها درواقع تأکیدی بر قواعد سنتی صلاحیت یعنی صلاحیت سرزمینی و شخصی و جهانی می‌باشند. با این وصف تدوین‌کنندگان کنوانسیون چالش تعیین محل ارتکاب جرم را حل‌شده تلقی کرده و با فرض قابل‌تعیین بودن، آن قواعد را بر آن استوار کرده‌اندرحالی‌که چنین قواعدی بدون ایجاد راهکاری مناسب جهت تعیین محل ارتکاب جرم از فایده چندانی برخوردار نیست.

مسئله زمان وقوع جرم نیز از موارد مهمی است که همیشه موردتوجه است؛ مخصوصاً در کشورهایی که مرور زمان وجود دارد. حتی اگر چنین تأسیسی نیز در قانونی وجود نداشته باشد باز زمان وقوع جرم از حیث قانون حاکم بر آن مورد، مسئله‌ای قابل‌توجه است. منظور آن دسته جرائم سایبری نیست که در زمان مشخصی اتفاق می‌افتد بلکه نوع دیگری از جرائم مدنظر است که در زمان معینی اتفاق نمی‌افتد. برای مثال یک برنامه‌نویس کامپیوتر که در یک بانک مشغول کار است می‌تواند برنامه نوشته‌شده برای کامپیوترهای بانک را به نحوی تنظیم کند که تا مدت مشخصی تمام مسائل به‌خوبی و بدون اشکال پیش بروند ولی پس‌ازاین مدت معین (که با محاسبات برنامه‌نویس تعیین‌شده است و ممکن است چند سال طول بکشد) ناگهان روش کار عوض شود و کامپیوتر از تمام حساب‌های بانکی مبلغ ناچیزی برداشت کرده و به‌حساب برنامه‌ریز واریز نماید و او این مبلغ هنگفت را از حسابش خارج نموده و متواری شود و یا آن را از مکان دیگری دریافت نماید. درباره زمان وقوع چنین جرمی چگونه می‌توان نظر داد؟ آیا هنگامی‌که این برنامه با قصد سوء نوشته می‌شده است زمان ارتکاب جرم است؟ یا زمانی که عمل مرتکب به‌طور کامل محقق می‌شود؟ آیا می‌توان این قضیه را با نظریاتی مثل تحقق عنصر مادی حل کرد؟ مثلاً شخص برنامه‌ریز در زمان دادن برنامه (برفرض محال کشف جرم در این زمان) به این اتهام که سوءنیت داشته محاکمه کرد؟ مشکل تعیین زمان ارتکاب جرم ازآنجا به عنوان یک چالش برای تعیین مرجع صالح محسوب می‌گردد که قوانین ناظر به صلاحیت ممکن است درروند ارتکاب چنین جرائمی دچار تحول شوند و دراین‌بین مشکل تعیین قانون صالح به‌تبع مشکل تعیین زمان ایجاد جرم به وجود آید.

در کشور ایران، قانون جرائم رایانه‌ای مصوب خرداد ۱۳۸۸ مطالبی را در مواد ۲۸ ،۲۹ ،۳۰ و ۳۱ به مسئلهٔ صلاحیت اختصاص داده بود، که در بند های 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 کشور و تارنماهای دارای دامنه‌ی مرتبه‌ی بالای کد کشوری ایران، قاعده‌ی صلاحیت سرزمینی را به‌گونه‌ای دیگر نسبت به جرائم ارتکابی در فضای سایبر اعمال می‌کرد که این مواد با تصریح ماده ٦٩٨ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نسخ صریح گردید و در حال حاضر مستفاد از ماده ٦٦٥ قانون آیین دادرسی کیفری، ملاک

تعیین صلاحیت محلی در جرائم سایبری همچون سایر جرائم سنتی محل ارتکاب جرم است و این در حالی است که با تحلیل و بررسی چالش‌هایی که در خصوص صلاحیت محلی در فضای سایبری به عمل آمد؛ بی‌تردید مبرهن است که به دلیل مشکل تعیین « محل ارتکاب جرم» و در مفهومی عام‌تر فقدان مفهوم «قلمرو و مرز» در این فضا، اعمال صلاحیت‌های فضای حقیقی و به‌طور ویژه « صلاحیت محلی» در این فضا سخت و حتی ممتنع می‌نماید. لذا در ادامه از موضوعی به نام « دسترسی پذیری آسان و سریع» به‌عنوان راهکاری برای اعمال صلاحیت در این فضا سخن خواهیم گفت.

به طور کلی در فقه امامیّه، «تعدّد و تفکیک عرضی و موضوعی» مراحل دادرسی و همچنین «سلسله‌مراتب» آن، پیش‌بینی‌نشده و به عبارتی، مراحل دادرسی یک مرحله‌ای بوده است. البته، این به این معنی نیست که تعقیب و تحقیقی از سوی قاضی صورت نمی‌گیرد، بلکه به این معنی است که قاضی در یک مرحلهٔ واحد و بدون تفکیک مراحل دادرسی، تعقیب و تحقیق و رسیدگی را انجام می‌دهد. همچنین، «ضوابط»حاکم در دادرسی دارای طریقیّت می‌باشند و قاضی مجتهد اسلامی برخلاف قاضی متخصّص اروپایی دارای اختیار بیش‌تری است. به دیگر سخن، قاضی با اختیارات وسیع‌تر خود فرآیند دادرسی را پیش می‌برد و برخلاف قاضی اروپایی که در جهت فرآیند دادرسی حرکت می‌کند، خود به فرآیند دادرسی جهت می‌دهد(آشوری،موحدی،۱۳۹۵،ص۹۸).

در همین راستا دسترس به قاضی نیز سهل و سریع بوده و برای او حاجبی تعیین نمی‌گردد. مرحوم مقدس اردبیلی در مجمع الفائده می فرماید؛ ملازمه است میان ممنوع بودنِ گماشتن حاجب، و این که مردم نیازی به گرفتن اجازه ی ورود به نزد قاضی ندارند. «و من هذه یعلم عدم الاحتیاج للدخول علی القاضی إلی الاستئذان، و کذا من هو مثله جالس لوصول الناس إلیه، فتأمل»(احمدبن‌محمد مقدس‌اردبیلی،۱۳۷۳،ص٤٢) و این موضوع در نهج البلاغه نیز مورد تاکید شدید بوده و در نامه‌ی ۵۳ آمده است که: « أَمَّا بَعْدَ هَذَا فَلَا تُطَوِّلَنَّ احْتِجَابَکَ عَنْ رَعِیَّتِکَ فَإِنَّ احْتِجَابَ الْوُلَاةِ عَنِ الرَّعِیَّةِ شُعْبَةٌ مِنَ الضِّیقِ وَ قِلَّةُ عِلْمٍ بِالْأُمُورِ وَ الِاحْتِجَابُ مِنْهُمْ یَقْطَعُ عَنْهُمْ عِلْمَ مَا احْتَجَبُوا دُونَهُ فَیَصْغُرُ عِنْدَهُمُ الْکَبِیرُ وَ یَعْظُمُ الصَّغِیرُ وَ یَقْبُحُ الْحَسَنُ وَ یَحْسُنُ الْقَبِیحُ وَ یُشَابُ الْحَقُّ بِالْبَاطِلِ».

بحث منع از احتجاب به خوبی می‌تواند دسترسی سریع و اسان به قاضی و محکمه را فراهم آورده و از بی‌کیفرمانی متعهمین در فضای سایبر جلوگیری نماید تا آنجا که در حقوق نوین نیز این موضوع مطرح است.در مسیر سهولت در رسیدگی و دسترسی آسان به محکمه که می‌تواند به صورت «دادرسی الکترونیکی» و حضوری انجام پذیرد و ضرورت اصلی در این روش سرعت و سهولت در دسترسی به عدالت کیفری است و ضرورتا الکترونیکی بودن دادرسی مدنظر نیست هر چند که الکترونیکی بودن می‌تواند در راستای هر دو هدف کارآیی داشته باشد. شاید بتوان ادعا کرد که این شیوه از جهت ویژگی‌ها و بستر تحقق، بیشترین سنخیت را با جرائم سایبری دارد و بر این قاعده ساده استوار است که پاسخ ارتکاب جرم در فضای سایبر را باید در همان فضای سایبر و با امکانات آن داد. این‌چنین رسیدگی به مجرمان سایبری نشان خواهد داد که فقط او نیست که از فضای سایبر برای جرم و سپس مخفی شدن استفاده می‌کند، بلکه این فضا باقابلیت‌های متعدد برای پیگرد آنان، در مقایسه با امکانات سنتی بسیار کارآمدتر است.(موذن‌زادگان و روستا، ۱۸۵:۱۳۹٦). و این‌گونه رسیدگی موجب می‌شود بحث عدم صلاحیت محلی و چالش‌های تعیین دادگاه صالح به رسیدگی منتفی گردد و مجرمان سایبری به‌راحتی تعقیب، محاکمه و مجازات گردند. دادرسی با این روش می‌تواند سبب تقویت بزه دیده جرائم سایبری شود که عامل مهمی برای رویارویی با این جرائم به شمار می‌رود، زیرا برای یک بزه دیده هیچ امری مهم‌تر از دستگیری عامل تجاوز علیه او نیست و این امر با تجهیزات الکترونیکی که بتواند تسریع در رسیدگی را حاصل نموده و فرصت اقدامات بعدی برای متهم در باب عدم شناسایی را از او سلب نماید، میسرتر است.

۲-۳.محل استقرار مرتکب و هویت او

از مشکلات موجود بر سر راه تعیین دادگاه صالح، که خود یکی از عوامل ایجاد چالش پیشین یعنی محل ارتکاب جرم است، دشواری تعیین محل استقرار مرتکب جرم در هنگام ارتکاب جرم و یا پس‌ازآنمی‌باشد. به این دلیل که فضای سایبر فضای غیرملموس

و از طرف دیگر فضایی گسترده و فرامرزی است و همچنین به لحاظ حرفه‌ای و متخصص بودن مرتکبین جرائم در فضای سایبر غالباً اشخاص مرتکب جرائم به‌سادگی طعمه‌های خود را شکار می‌کنند و با استفاده از ترفندها و شیوه‌های تغییر هویت ویژه، سعی در ناشناخته ماندن خود می‌کنند.ازآنجاکه ازجمله اصول تعیین دادگاه صالح، صلاحیت مبتنی بر تابعیت مرتکب و یا صلاحیت دادگاه محل استقرار مرتکب است، جهت تشخیص دادگاه صالح بنا بر یکی از این اصول لازم می‌آید تشخیص داده شود که مرتکب جرم موردنظر چه کسی است و دارای تابعیت کدام دولت می‌باشد و یا اینکه مرتکب جرم در کدام نقطه از جهان قرار دارد؛ درحالی‌که هیچ سامانه‌ای برای شناسایی هویت در فضای سایبر قابل‌تصور نیست و افراد به‌راحتی می‌توانند با هویت غیرواقعی وارد شبکه‌ی اینترنتی یا مخابراتی شوند و هویت خود را کتمان کنند. چون در فضای سایبر کاربران با شناسه‌های قراردادی همچون «آی پی»[1]ها که کاملاً سایبری و مشاهده ناپذیر و لمس نشدنی می‌باشند شناسایی می‌شوند و حتی در صورت شناسایی کاربر مرتکب جرم درواقع ماهیت سایبری و قراردادی وی را شناسایی کرده‌ایم نه هویت واقعی او را. همچنان که در اداره‌های تشخیص هویت پلیس کشورها صورت می‌پذیرد؛ که در همین راستا نیز با توجه به «منع احتجاب» برای قاضی ارائه‌ی راهکار مراجعه به قاضی مستقر در محل می‌تواند به عنوان راهکاری جهت تسریع و سهولت در مقابله با مجرم یا مجرمان سایبری کارآیی داشته باشد.

[1] Internet Protocol Address

نتیجه‌گیری

امروزه به دلیل پدیداری پدیده‌هایی نوین همانند سازمان‌یافتگی جرائم و نیز جهانی‌شدن بزه‌کاری، حجم گسترده‌ای از بزه‌کاری‌های سنتی به فضای سایبر منتقل شده و در کنار جرائم سایبری محض جای گرفته‌اند. از همین رو یافتن قواعدی مناسب و شفاف برای احراز صلاحیت دادگاه‌ها در پرونده‌های رسیدگی به جرائم سایبری اهمیتی ویژه می‌یابد.در همین راستا قواعد حقوقی و قوانین حاضر کشور توانایی تعیین و اعمال صلاحیت محلی در جرائم سایبری را با توجه به چالش تعیین محل وقوع جرم ندارند و در قانون آیین دادرسی کیفری در بخش رسیدگی الکترونیکی برای تعیین قلمرو حاکمیت ایران و محل وقوع جرائم سایبری که دو رکن اصلی برای اعمال صلاحیت سرزمینی محسوب می‌شود، ضابطه دقیقی ارائه نشده است.از سوی دیگر با توجه به چالش‌هایی که در مسیر اعمال صلاحیت محلی در فضای سایبر وجود دارد که مهم‌ترین آن‌ها نیز عبارت‌اند از وجود چالش در تعیین زمان و محل وقوع جرم، شناسایی محل استقرار مرتکب و هویت او و عدم اجماع جهانی در شناسایی مفهوم و مصادیق جرائم سایبری؛ باید طرحی نو در این فضا درانداخته شود که به نظر می‌رسد « دسترسی سریع و آسان به محکمه» یکی از بهترین راهکارها باشد، که درواقع با مجرمان سایبری با توجه به مکان وقوع جرم(فضای سایبر) و موقعیت و اسباب آن برخورد می‌گردد؛ که در این راستا به کیفر رساندن مجرمان سایبری نیازمند همکاری بین‌المللی دولت‌ها به طورجدی و پیش‌بینی کنوانسیون‌های ناحیه‌ای و جهانی و تثبیت قواعدی مقبول می‌باشد. همان‌طور که در بند ۱ ماده‌ی ۸۸ کنوانسیون جرائم سایبری بوداپست مجارستان بر این مسئله، یعنی به شور نشستن کشورهای ذی‌نفع جهت تعیین مناسب‌ترین و شایسته‌ترین عضو صالح به تعقیب و رسیدگی، تأکید شده است.

با توجه به فرضیه‌ی پژوهش حاضر، با گسترش مفهوم صلاحیت محلی و مراجعه سریع و آسان به محکمه، اعمال این اصل را در جرائم سایبری ممکن خواهد بود. باید بیان داشت این شیوه می‌تواند برخی از چالش‌های موجود بر سر راه تعیین دادگاه صالح را از میان بردارد و با اتخاذ شیوه‌ای نوین همچون یاری جستن از ابعادی همچون «کنترل و کارایی» برای تمام جرائم سایبری در محیطی همانند محیط وقوع جرم ، مجرمان را مجازات و حقوق بزه دیدگان را بستاند. و در فقه امامیه نیز می‌توان با توجه به موضوع منع احتجاب برای قاضی، در هریک از محل وقوع جرم یا محل اقامت متهم یا زیاندیده به قاضی و محکمه مراجعه نمود و با توجه به دسترسی آسان و سریع به محکمه از بی‌کیفرمانی احتمالی مجرمین در این فضا جلوگیری نمود.

فهرست منابع

نهج البلاغه

احمدبن‌محمد مقدس‌اردبیلی.(۱۳۷۳)، مجمع الفائده و البرهان فی شرح ارشاد الاذهان (جلد ۱۲)، دفتر انتشارات اسلامی وابسته به جامعه مدرسین حوزه علمیه قم

آشوری، محد، موحدی، جعفر.(۱۳۹۵)،طریقیّت یا موضوعیّت روش دادرسی مطالعهٔ تطبیقی در فقه امامیّه، حقوق اروپایی و حقوق موضوعه، فصلنامه پژوهش حقوق کیفری،دوره ۵، شماره ۱۶، ۹۵-۱۱۵

امینی‌نیا، عاطفه، علیزاده، حمیدرضا.(۱۳۹۷). اعمال صلاحیت کیفری (تعارض قوانین) در مورد جرائم ارتکابی در فضای سایبر،فصل‌نامه پژوهش ملل، شماره۳۰

بیابانی، غلامحسین و هادیان فر، سید رضا. (۱۳۸٤). فرهنگ توصیفی علوم جنایی، انتشارات مرکز تحقیقات کاربردی کشف جرائم و امنیت معاونت آگاهی ناجا

جلالی فراهانی، امیرحسین.(۱۳۸٤). اسپم، جلوه سیاه تبلیغات در سیستم‌های پیام رسان الکترونیکی، مرکز پژوهش‌های مجلس شورای اسلامی، ش ۸٤٥۱

راجی، سید محمد هادی.(۱۳۸۵).نگاهی به قانون تجارت الکترونیک، فصلنامه نشریه حقوقی گواه، ٦-۷، ٦٥-٦۹

رضوی فرد، بهزاد، موسوی، نعمت‌الله.(۱۳۹۵). مسئولیت کیفری در فضای سایبر در حقوق ایران، فصلنامه پژوهش حقوق کیفری، دوره ۵، شماره ۱٦

رضوی،محمد.(۱۳۸٦).جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها، فصلنامه دانش انتظامی ۳۲،۱۲۰-۱٤۰

زندی، محمدرضا.(۱۳۸۹). تحقیقات مقدماتی در جرائم سایبری، انتشارات جنگل

شیرزاد، کامران.(۱۳۸۸). جرائم رایانه‌ای، نشر بهینه فراگیر

عبدالهی، اسماعیل و مرادی، سکینه.(۱۳۹٤).صلاحیت کیفری در فضای سایبری، فصلنامه علمی دانش انتظامی بوشهر، دوره ٦، ۲۰،٤۰-۵۹

موذن‌زادگان،حسنعلی؛ روستا، نرجس.(۱۳۹٦). دادرسی الکترونیکی در رویارویی با جرایم رایانه‌ای: چالش‌ها و بایسته‌ها، مجله حقوقی دادگستری، شماره ۱۰۰

میرزاپور،سلیمان؛ حیدری، ولی.(۱۳۹۲). بررسی کارامدی دادرسی الکترونیک و تحقق آن به عنوان یکی از مولفه‌های شهر الکترونیک،بایسته‌های پژوهش در نظام عدالت کیفری (مقالات برگزیده نخستین همایش ملی پژوهش در نظام عدالت کیفری؛ فرصت‌ها و چالش‌ها)»، تهران، نشر میزان

-Brenner, S (2005), "Cybercrime Scene", translated by DariushBagherian, Supreme Informatics Council

-Erentyeva LV,(2019) Principles for Determining Territorial Jurisdiction of the State in Cyberspace. Lex Russica. (7): 119-129. P.121 (In Russ.)https://doi.org/10.17803/1729-5920.2019.152.7.119-129

-Federal Law of May 1, 2019 N 90-FZ "On Amendments to the Federal Law" On Communications" and the Federal Law "On Information, Information Technologies and Information Protection",(2019), providing for the creation of a national routing system for Internet traffic, tools centralized management, etc. Entered into force on November 1

-International Court of Justice (ICJ), Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania,(1949), Judgment of 9 April. https://www.icj-cij.org/en/case/1/judgments

-On the Application of International Law in Cyberspace,(2021),The Federal Government of Germany. Position Paper – March, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf

-Rahmatilla Aryani Putri, Huala Adolf, Jafar Sidik,(2021), Law Enforcement of Cyber Crime Jurisdiction in Transnasional Law, Advances in Social Science, Education and Humanities Research, volume 658

-Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.).Cambridge: Cambridge University Press. Glossary
-Semenova, N(2021), “Jurisdiction in Cyberspace”, Cyberspace Law eJournal
-The case Yahoo! Inc. against La Ligue Contre Le Racisme et l'Antisemitisme, https://caselaw.findlaw.com/us-9th-circuit/1144098.html
-http://publication.pravo.gov.ru/Document/View/0001201905010025
-https://supreme.justia.com/cases/federal/us/521/844

The Role of Easy and Fast Access to the Court in the Normative Expansion of Local Jurisdiction in Cybercrime

Esmail Baghban[1] Babak Pourgahramani[2] ,Fatemeh Ahadi[3]

Abstract

Uncertainty of territory and borders in cyberspace causes many problems in the field of criminal jurisdiction; Issues such as the multiplicity of places where the crime was committed and, consequently, the multiplicity of jurisdiction in this space and the precise determination of the crime scene are clear examples of this. One of the most important issues to be considered in this area is the determination of a competent local authority to investigate crimes committed in the area. The main question of the present study is how to of easy and fast access to the court can make it possible to exercise this competence in cyberspace.This article, with the help of the descriptive-analytical method and induction in domestic, international and Islamic jurisprudential standards regarding the jurisdiction of courts in Iran, tries to provide a solution to expand local jurisdiction in this field.The results of the research show that the new methods of dealing with cyber crimes, including electronic proceedings and taking into account the same legal conditions with the international community and creating a judicial system with global jurisdiction,can solve the challenges of applying local jurisdiction in cyber crimes and facilitate and speed up the proceedings.

Keywords: Local Jurisdiction, Cybercrime, Ehtejab, Criminal Justice

[1] .Ph.D Student in Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran. s.baghban@gmail.com

[2]. 2 Associate Professor, Department of Criminal Law and Criminology, Maragheh Branch, Islamic Azad University, Maragheh, Iran.(corresponding author) b.pourghahramani@yahoo.com

[3]. assistant professor, Department of Criminal Law and Criminology, Faculty of Law and Humanities, Maragheh Branch, Islamic Azad University, Maragheh, Iran. ahadi-223@yahoo.com