# اعمال صلاحیت کیفری (تعارض قوانین) در مورد جرائم ارتکابی در فضای سایبر

عاطفه امینی‌نیا[1] حمیدرضا علیزاده[2]

## چکیده

*یکی از مسائل جدیدی که به موازات تحول و پیشرفت تکنولوژی در زمینه فناوری اطلاعات و ارتباطات به وجود آمده است مسأله چگونگی تعیین مرجع قضایی صالح جهت فضای سایبر، ایجاد دنیای مجازی جدید به نام رسیدگی به جرائم ارتکابی در فضای مذکور است. براساس قواعد سنتی مهمترین ضابطه تعیین صلاحیت مراجع قضایی کیفری، مکان وقوع جرم می‌باشد و در فضای جدید سایبر که یک فضایی مجازی و فارغ از مکان می‌باشد، چنین ضابطه‌ای قابل اجرا نبوده و یا مستلزم تعدیل ویژه می‌باشد. در همین راستا برخی سعی کرده‌اند همان قواعد سنتی ناظر بر صلاحیت کیفری مراجع قضایی را با نگرشی جدید در این فضا اجرا کنند و برخی دیگر با طرح تئوری‌های نو درخصوص صلاحیت، از قبیل «فضای سایبر بعنوان یک فضای آزاد بین‌المللی» و یا پیش‌بینی دادگاهی ویژه به نام «دادگاه دیجیتالی یا سایبری» و یا صلاحیت «دادگاه ذی ارتباط منطقی با جرم» را مطرح کرده‌اند. کشور ایران در قانون مجازات جرائم رایانه‌ای در ماده ۸۲ تئوری اول یعنی اجرای قواعد سنتی با نگرشی جدید را اتخاذ کرده است. در این مقاله سعی شده است هر یک از تئوری‌های مطرح شده در این زمینه مورد نقد و بررسی قرار گیرد و در نهایت یک معیار تلفیقی ارائه گردد، با این توضیح که تا جائیکه قواعد سنتی قابل اجرا باشند همان قواعد اجرا می‌شوند و در غیر آن صورت تئوری صلاحیت دادگاه ذی ارتباط منطقی با جرم بعنوان ضابطه نهایی پذیرفته شود.*

**واژگان کلیدی:** صلاحیت کیفری، صلاحیت سایبری، فضای سایبر، دادگاه دیجیتالی، فضای بین‌المللی

---

[1] عضو هیأت علمی دانشگاه آزاد اسلامی واحد ورامین atefeh.amininia@yahoo.com

[2] دانشجوی دکتری حقوق خصوصی، دانشگاه آزاد اسلامی واحد ورامین

**مقدمه**

مسأله صلاحیت مراجع قضایی در رسیدگی به جرائم، یکی از مباحث مهم حقوق جزایی می‌باشد که در کنار سایر قواعد حاکم بر فرایند دادرسی، در آئین دادرسی کیفری مورد بحث قرار می‌گیرد. در حقوق کیفری بطورکلی شایستگی نهادهای قضایی کیفری در رسیدگی به دعاوی در بعد داخلی براساس محل ارتکاب جرم، محل کشف جرم، محل دستگیری متهم و یا محل اقامت او حسب مورد می‌باشد و در بعد بین‌المللی با پیش‌بینی قواعد خاص براساس محل ارتکاب جرم (صلاحیت سرزمینی)، تابعیت متهم (صلاحیت شخصی فعال یا مثبت)، تابعیت مجنی علیه (صلاحیت شخصی غیرفعال یا منفی)، اخلال در نظم و امنیت کشوری (صلاحیت واقعی یا حمایتی) و یا اخلال در نظم و امنیت جهانی و حیات بشریت بطورکلی (صلاحیت جهانی) مشخص می‌شود. بگونه‌ای که در هر دو عرصه بین‌المللی و داخلی به ویژه در مورد اخیر محل وقوع جرم جهت تعیین مرجع قضایی صالح به رسیدگی به دعاوی کیفری از اهمیت ویژه‌ای برخوردار است و حتی درخصوص صلاحیت سرزمینی که مبتنی بر ضابطه محل وقوع جرم می‌باشد نظریه‌ها و تئوری‌های متفاوتی مطرح شده است بطوریکه برخی آن را خیلی وسیع و حتی ناظر به جرائم واقعه در خارج از سرزمین تحت حاکمیت یک کشور صالح دانسته‌اند. در مقابل برخی آن را خیلی محدود و صرفاً ناظر به جرائم واقع شده در حوزه داخلی و تحت حاکمیت کشوری صالح شناخته‌اند. علیرغم وجود اختلافات درخصوص محل وقوع جرم و ضابطه تشخیص آن جهت تعیین مرجع صالح مسأله مهمی که در این زمینه به ویژه در دهه‌های اخیر به وجود آمده است تشخیص محل وقوع جرم در فضای سایبر است. چون ضوابط و معیارهای پیش‌گفته ناظر به جرائم اتفاق افتاده در جهان فیزیکی و ملموس و در قلمرو جغرافیایی مادی و محسوس می‌باشد در حالیکه با گسترش شبکه‌های جهانی اینترنتی، استفاده از شبکه‌های رایانه‌ای به شدت افزایش پیدا کرده است. به موازات



افزایش پیوستن به این شبکه‌ها بحث‌های حقوقی اعم از حقوق خصوصی و حقوق کیفری ظهور پیدا می‌کند چون فضای الکترونیکی و اینترنت با فضای فیزیکی و جغرافیایی ملموس که حقوق سنتی ناظر به آن است متفاوت است بطوریکه این فضا کاملاً غیرملموس و مجازی است و مرز جغرافیایی نمی‌شناسد که این تفاوت مسائلی از قبیل محل انعقاد عقد و محل اجرای آن و تشخیص قواعد حاکم بر روابط طرفین عقد در حقوق خصوصی و مسائلی از قبیل ادلهٔ اثبات دعاوی درخصوص جرائم اینترنتی، صلاحیت دادگاه‌های مختلف در رابطه با آن جرائم در حقوق کیفری را برانگیخته است.

در این مقاله منحصراً به مسأله مهم صلاحیت کیفری مراجع قضایی در محیط سایبر پرداخته می‌شود و به این سوال پاسخ داده می‌شود که در محیط سایبر چه معیارهایی می‌توانند تعیین کننده صلاحیت باشند؟ این

سوال از آنجا شدت پیدا می‌کند که در محیط سایبر قواعد سنتی با چالش‌هایی از قبیل نامعین بودن حیطه-های 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 که باتوجه به اینکه در راستای پاسخگویی به این سوال نویسندگان و حقوقدانان رویکردهای مختلفی را مطرح کرده‌اند برخی رویکردها در واقع مبتنی بر ضوابط سنتی تعیین صلاحیت، مانند اصل سرزمینی، شخصی، حمایتی و یا جهانی می‌باشند. به همین خاطر ما در مبحث اول به این رویکردها می‌پردازیم و سایر مباحث را به رویکرهای انفرادی دیگر از قبیل رویکرد فضای سایبری بعنوان یک فضای آزاد بین‌المللی و رویکرد دادگاه سایبری (دیجیتالی) و رویکرد ارتباط حداقلی یا ارتباط منطقی دادگاه مدعی صلاحیت و جرم ارتکابی من حیث‌المجموع اختصاص می‌دهیم.

## چارچوب نظری: تعاریف و مفاهیم

### ۱- سیستم رایانه‌ای

سیستم رایانه‌ای، هر دستگاه یا مجموعه‌ای از دستگاه‌های بهم متصل است که یک یا چند تا از آنها مطابق یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد؛ به عبارت دیگر سیستم رایانه‌ای، دستگاهی است که از نرم‌افزار و سخت‌افزاری که برای پردازش خودکار داده‌های دیجیتال طراحی شده تشکیل یافته و ممکن است شامل ورودی، خروجی و امکانات ذخیره‌ساز اطلاعات شود. سیستم رایانه‌ای می‌تواند به صورت مستقل یا متصل به شبکه‌ای از سایر دستگاه‌های مشابه عمل کند. منظور از خودکار این است که انسان دخالت مستقیم ندارد. منظور از پردازش داده‌ها این است که داده‌های سیستم رایانه‌ای با اجرای یک برنامه رایانه‌ای عمل کنند. یک برنامه رایانه‌ای مجموعه‌ای از دستورالعمل‌هاست که رایانه می‌تواند آنها را برای نتیجه موردنظر اجرا کند. رایانه می‌تواند برنامه‌های مختلفی اجرا کند. معمولاً سیستم رایانه‌ای از دستگاه‌های مختلفی تشکیل شده است که به پردازشگر یا واحد پردازش مرکزی و وسایل جانبی تفکیک می‌شوند. یک وسیله جانبی دستگاهی است که کارکردهای خاصی را در برهم‌کنش با واحد پردازشگر انجام می‌دهد، نظیر چاپگر، نمایشگر، خواننده یا نگارشگر لوح فشرده یا سایر وسایل ذخیره‌ساز (زندی،۱۳۸۹: ۱۴۲).



### ۲- داده رایانه‌ای

هرگونه نماد حقایق، اطلاعات یا مفاهیم به شکلی مناسب برای پردازش در یک سیستم رایانه‌ای است که شامل برنامه‌ای می‌شود که برای کارکرد یک سیستم رایانه‌ای مناسب است (همان، ۱۴۴).

## تعریف و تبیین حقوق سایبری و ارزیابی ویژگی‌های آن

### ۱- تعریف و تبیین حقوق سایبری

فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود به نظر می‌رسد بکارگیری این اصطلاح در این زمینه و برای ارجاع به امور فنی به آن رنگ و بویی صرفا فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشان می‌دهد که این واقعیت، وجوه و جنبه‌های متنوعی از جمله خصلت-های روانشناختی قابل توجه نیز دارد (Spinello,2012: 12).

واژه سایبر از لغت یونانی[1]به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر[2]در کتابی با عنوان "سایبرنتیک و کنترل ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (و کامپیوترها) است. ریشه یونانی واژه "سایبر" به معنای توانمند در هدایت و کنترل است. نظر غالب آن است که واژه "سایبرنتیکس" در کتاب سایبرنتیکس یا کنترل ارتباط در حیوانات و ماشین وضع شده است. نوربرت وینر مولف این کتاب، این واژه را از منظر کنترل سیستم‌های پیچیده در دنیای حیوانات و شبکه‌های مکانیکی بکار برده است. سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه‌های ترکیبی بسیاری از کلمه سایبر بوجود آمده است.



همچنین این کلمه در علم پزشکی برای اشاره به تلفیق انسان‌ها و حیوانات به وسیله دستگاه‌ها بکار رفته است. در هر حال، واژه سایبر از زمانی که ابداع شده معانی مختلفی به خود گرفته است. این واژه به صورت قابل توجهی در تجارت، حقوق و سیاست بکار رفته است. و اکنون کاربرد گسترده‌ای دارد و می‌تواند برای اشاره به دنیای مجازی[3] که به وسیله اینترنت و دیگر وسایل ارتباطی الکترونیکی به وجود آمده، مورد استفاده قرار گیرد. از طرف دیگر، فضای سایبر بدون اجزای فیزیکی که از آن ساخته شده، وجود ندارد. وجود کلمه فضا در این ترکیب حاکی از آن است که "فضای سایبر" باید بعد داشته باشد؛ یعنی باید فضا اشغال کند. علاوه بر این، فضای سایبر را بعضی عرصه‌ای جدید مانند زمین، فضای دریا و فضای کیهانی می‌دانند. در هرحال، اینها طبیعی هستند، اما سایبر مصنوعی و ساخته دست بشر است (Friedman,2014: 53). واژه فضای سایبر را نخستین بار ویلیام گیبسون نویسنده داستان علمی تخیلی در کتاب نورومنسر[4]در سال ۱۹۸۴

[1] Kybernetes
[2] Norbert Wiener
[3] Virtual
[4] Neuromancer

بکار برده است. وی در کتاب علمی و تخیلی خود چنین تعریفی برای فضای سایبر ارائه کرده است (توهمی که در مورد آن اتفاق‌نظر وجود دارد) (Gibson,2011: 14).

تعریف رسمی وزارت دفاع از فضای سایبر به این معنا است که فضای سایبری شبکه‌ای متصل به هم از زیرساخت‌های فناوری اطلاعات است که اینترنت شبکه‌های مخابراتی سیستم‌های کامپیوتری پردازشگرها و کنترل‌گرها داخل صنایع مهم را شامل می‌شود (Libicki,2009: 179). با این حال تعریف ارائه شده از سوی وزارت دفاع به تمامی جنبه‌های فضای سایبری اشاره ندارد و برای تکمیل این تعریف ناگریز از بکار بردن دو کلمه دیگر یکی قدرت سایبری و دیگر استراتژی سایبری می‌باشیم.

قدرت سایبری به معنای توانایی استفاده از فضای سایبری برای سودآوری و تأثیرگذاری حوادث رخ داده در محیط‌های عملیاتی و ابزار های قدرت که ابزارهای قدرت شامل اهرم‌های سیاسی دیپلماتیک اطلاعات نظامی و اقتصادی می‌باشد. استراتژی سایبری که با دیگر حوزه‌های عملیاتی هماهنگ و یکی شده باشد و به منظور دستیابی به اهداف از طریق ارکان مختلف قدرت سایبری بکار گرفته شود در تعریف فضای سایبری برخی دیگر از نویسندگان عنوان کرده‌اند که فضای سایبری محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع فراتر از مرزهای جغرافیایی روی می‌دهد قید واقعی بودن به این معنا نیست که تصور شود مجازی بودن این فضا به معنای غیرواقعی بودن آن می‌باشد چراکه در این فضا همان ویژگی‌های تعاملات انسانی در دنیای خارج همچون مسئولیت وجود دارد (Hu,2013: 101). اینترنت بزرگترین مولفه فضای سایبری است بیشتر سامانه‌هایی که به فضای سایبری وابسته‌اند و از آن استفاده می‌کنند از اینترنت بعنوان یک ضعف امنیتی یاد می‌کنند که می‌توان در جهت انجام حملات از آن استفاده نمود بیشتر این سامانه‌ها بگونه‌ای طراحی شده‌اند که بتوانند استفاده ارزان و وسیعی از دسترسی به شبکه داشته باشند و این موضوع توانایی سوء استفاده مهاجمین به منظور استشمار و آسیب‌پذیر نمودن شبکه‌ها و سرویس‌ها را افزایش داده است. در واقع فضای سایبری را مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیایی فیزیکی را تشکیل می‌دهد (Lessig,1999: 25).

یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد (Betz and Stevens,2011: 92).

این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهت‌های فضای سایبر با حالت‌های ناهشیاری، بخصوص حالت‌های ذهنی که در رویاها ظاهر می‌شوند، بپردازند. آنان با الهام از گفته‌های یکی از

رهبران بزرگ "ذن" به نام چانگ تزو[1]برای تحقیقات خود در زمینه کشف شباهت‌هایی بین فضای سایبر و رویا بهره جسته‌اند (Carr,2011: 195). گفته می‌شود که: "چانگ تزو شبی در خواب می‌بیند که یک پروانه شده است. وقتی بیدار می‌شود با خود می‌اندیشد: آیا من مردی هستم که خواب می‌بیند پروانه شده است، یا اینکه پروانه‌ای هستم که اکنون خواب می‌بیند یک مرد شده است (Ibid, 187).

روند کاری یک کاربر کامپیوتر در فضای سایبر دقیقا نوعی یکی شدن یا محو شدن در درون واقعیتی متفاوت یعنی واقعیتی مجازی که ورای قوانین و واقعیت‌های واقعی است. مانند یک رهبر ذن در هنگام مدیتیشن که با محیط اطراف خود به وحدت می‌رسد، کاربر کامپیوتر هم در هنگام کار در فضای مجازی با آن یکی می‌شود. شما تقریبا بی‌حرکت و آرام می‌نشینید، چشمانتان روی پرده‌ای درخشان خیره می‌شود، اتاق کاملا تاریک است، تنها منبع نور در درون شما است و در حالیکه همه توجه و ذهنتان بر کلمات و تصاویر این پرده درخشان متمرکز است، انگشتانتان کلیدهای کیبورد را می‌نوازد. در این لحظه دوست دارید با ذهنیات و تصورات خود یگانه شوید. مرز بین دنیای درون و بیرون تقریبا ناپدید می‌شود و دیگر گذر زمان معنایی ندارد (Ibid, 97).

البته این سناریوی هر روز کاربران کامپیوتر نیست. زیرا اغلب اوقات ما صرفا به جهت انجام کاری مشخص و بدون آنکه به درون جهان مجازی فرو رویم به صفحه کلید ضربه می‌زنیم اما اگر از استفاده‌های دم‌دستی کامپیوتر صرف‌نظر کنیم و از کاربران حرفه‌ای و پروپاقرص کامپیوتر پرس‌وجو کنیم درخواهیم یافت که بسیاری از آنها به راحتی لحظاتی را به یاد می‌آورند که گویی هیچ حائل و فاصله‌ای بین خود و کامپیوترشان احساس نمی‌کردند.



در واقع می‌توان گفت که فضای سایبر گستره‌ای از ذهن است که می‌تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد فضای سایبر را نمی‌توان تنها یک **شاهراه بزرگ طلاعاتی** ساده دانست. زیرا تجربه ذهنی ما در فضای مجازی با تجربه ذهنی ما زمانی که بی‌هیچ هدف و ارزشی خیال‌بافی می‌کنیم، کاملا متفاوت است. در واقع همانگونه که علم روانشناسی خواب شبانه را برای حفظ سلامتی، توسعه عاطفی و رشد شخصیت یک فرد ضروری می‌داند، این فضای مجازی هم بیش از هر چیز دیگری در خدمت روان انسان است. زیرا مرزهای بین واقعیت‌های آگاهانه و ناآگاهانه را به هم نزدیک ساخته و می‌تواند درباره معنای واقعیت چیزهایی به ما بگوید (Palloff & Pratt,2002: 75).

محیط[2] یک محیط چت گرافیکی است که ما برای این تحقیق آن را انتخاب کرده‌ایم. کاربران در این محیط می‌توانند برای برقراری ارتباط با دیگران از بین صورتک‌های گرافیکی موجود در آن محیط، یک یا چند

[1] Chaung Tzu
[2] Palace

صورتک را برای بازنمایی شخص خود انتخاب کنند. این صورتک‌ها هر یک موقعیت یا حالت روانی خاصی را بیان می‌کند. بعضی از این حالت‌های رویاگونه در محیط را می‌توان در دیگر فضاهای مجازی هم پیدا کرد (Powner,2013: 8).

فضای سایبری[1] محیط مجازی و غیرملموسی است، که در آن تمامی شاهراه‌های اطلاعاتی مثل اینترنت به هم متصل هستند و تمام اطلاعات راجع به افراد، فرهنگ‌ها ملت‌ها و کشورها و بطورکلی هر آنچه که در کره خاکی به صورت فیزیکی و مملوس وجود دارد (نوشته، تصویر، صوت، اسناد) در این فضا به شکل دیجیتالی موجود بوده و قابل استفاده و دسترس کاربران می‌باشد. جوزف نای[2] پدر قدرت نرم در مورد فضای سایبری می‌گوید: قدرت براساس منابع اطلاعاتی چیز جدیدی نیست ولی قدرت در فضای سایبری حرف جدیدی دارد. فضای سایبر بعنوان زیرساخت جهانی اطلاعات و ارتباطات تمامی حوزه‌ها و عرصه‌های کار و زندگی اعم از عرصه‌های سیاسی، اقتصادی، مذهبی، اجتماعی و نظامی را در خود جای داده است این فضا دارای ویژگی‌ها و قواعد مخصوص به خود می‌باشد بنابراین می‌توان مدعی شد ما با جامعه‌ای متفاوت به نام جامعه مجازی روبرو هستیم بحث در مورد ارائه تعریف مناسب برای اصطلاحات کلیدی فضای سایبری همچنان ادامه دارد (Ray,2002: 12).

فضای مجازی را نمی‌توان تنها یک شاهراه بزرگ اطلاعاتی دانست فضای سایبر در واقع محیطی است که مجموعه‌ای از ارتباطات در آنجا انجام می‌شود گرچه ممکن است این ارتباطات در همه حال آنلاین نباشد ولی واقعی است از این‌رو تأثیر بالایی در این روابط رخ می‌دهد. این فضا شامل همه شبکه‌های رایانه‌ای موجود در دنیا و هر چیزی است که به این شبکه‌ها متصل است یا آنها را کنترل می‌کند. این فضا فقط اینترنت نیست بلکه در برگیرنده اینترنت به علاوه بسیاری از شبکه‌های خصوصی بسیار مشابه به اینترنت بخش‌های دیگر فضای سایبر شبکه تراکنشی هستند که کارهایی همچون ارسال اطلاعات درباره جریان پول، مبادلات بازار سهام و اعتبارات و تراکنش‌های این بازار را ارسال می‌کنند (Roscini,2014: 237).

فضای سایبری همانند قلمرو خشکی دریا و هوا بعنوان قلمرو استراتژیکی مستقلی در نظر گرفته می‌شود که وجه تمایز آن با سایر قلمروها این است که قلمرو سایبری ساخته دست بشر می‌باشد.

به هر حال مسئله تعریف فضای سایبری مسئله ساده و سطحی نمی‌باشد هر آنچه در شکل‌گیری فضای سایبری سهیم می‌باشد پیامدهای مهمی برای اعمال قدرت دارد زیرا گستره و دامنه فعالیت‌های سایبری توسط نیروهای سایبری مشخص می‌شود بنابراین از میان همه دیدگاه‌ها و برداشت‌های ارائه شده می‌توان گفت دو برداشت اصلی از فضای سایبری موجود است: برداشت اول بر این اساس فضای سایبری نماد یا فضای



[1] Cyber Space
[2] Jozef Nay

موجود میان قطعات سخت‌افزاری شبکه‌های رایانه‌ای است و فضای جغرافیایی نیست تجربه بودن در فضای سایبری طوری است که بسیاری از مشخصه‌های فضای فیزیکی را دارا می‌باشد ولی پس از مقایسه و ارتباط با دنیای فیزیک می‌توان درک نمود که این محیط‌های مجازی از نظر واقعیت داشتن از جهان فیزیکی چیزی کم ندارند و می‌توان آن را جزئی از جهان واقعی قلمداد نمود (Rid,2013: 96). بنابراین فضای سایبری فضایی است که در سیم‌ها و هوا وجود دارد البته از برخی جهات هم فضای سایبری وجود دارد البته در ذهن کاربران در مقابل این دیدگاه برداشت و الگویی دیگری وجود دارد که براساس آن متخصصان فضای سایبری را فضای دارای زیرساخت معرفی کرده. که دارای انواع مختلف می‌باشد این الگو از الگوی پیشین ساده‌تر است که بر این اساس زیرساخت مورد نیاز برای محیط اجتماعی را در بر می‌گیرد این الگو در ساده‌ترین شکل خود شامل لایه مجازی از اطلاعات است که روی لایه فیزیکی سخت‌افزاری قرار می‌گیرد (Ibid, 97). فضای سایبری اغلب از طریق واژه‌ها و اصطلاحات شبکه‌ای توصیف می‌شود با این حال می‌توان آن را جریان جهانی در نظر گرفت واژه‌های فراگیر که جریان‌های جهانی می‌توانند از طریق شبکه‌ها عمل کنند جریان‌های جهانی تا حدودی شبکه ماشین‌ها، فناوری‌ها، سازمان‌ها، متون و بازگیرانی به وجود می‌آورند که هریک نقش گره‌های متصل به همدیگر را ایفا کرده و از طریق آنها سرمایه، اندیشه، انرژی اجتماعی به بخش‌های دیگر منتقل می‌شود (Perry, 1996).



این جریان‌ها توجهی به مرزهای جغرافیایی و اجتماعی از پیش تعیین شده نداشته پیدایش فضای سایبری تاثیر بنیادین بر چگونگی تعامل بازیگران با یکدیگر داشته در فضای سایبری دو بازیگر می‌توانند با اختلاف چند هزارم ثانیه به یکدیگر ارتباط برقرار کنند این همان چیزی است که ارتش ایالت متحده از آن بعنوان سرعت نت یاد می‌کند و تقریباً برای هر مقصود و هدفی بکار می‌رود. کاهش زمان و فضای مورد نیاز برای قراری ارتباط میان بازیگران باعث افزایش تعداد بازیگران فضای سایبری شده همین پویایی فضای سایبری است که بیش از هر چیزی دیگری توجه بازیگران و کاربران را برای استفاده از آن جلب نموده است. از آغاز دهه ۱۹۸۰ مفهوم فضای سایبری دستخوش تغییرات فراوانی شده است بطوریکه در حوزه نظامی آن را قلمرو جدیدی از عرصه نبود تعریف کرده‌اند در حالیکه در حوزه گسترده‌تر اجتماعی از آن بعنوان زیربنای اطلاعاتی یاد می‌شود که در سایه آن تمامی اکوسیستم‌های اقتصادی و صنعتی رشد می‌کند (Graham,2014: 188).

## ۲- ویژگی‌های فضای سایبر

جهانی و فرامرزی بودن: ویژگی منحصر به فردی که فضای سایبری را از دیگر رسانه‌ها جدا می‌کند برد جهانی این فضا است در واقع هر آنچه که در فضای سایبر منتشر می‌شود در کل جهان قابل درک است این جهانی

بودن با ارسال گسترده امواج ماهواره از یک نقطه خاص به سراسر جهان متفاوت است زیرا تولید و انتشار اطلاعات در فضای سایبری با هزینه و امکانات بسیار کم در مقایسه با سایر رسانه‌ها صورت می‌گیرد.

امکان ارتباط دوطرفه: امکان ارتباط دوطرفه سهل و آسان است به عبارت دیگر در این محیط امکان‌های خاصی برقراری رابطه سریع و آسان میان کاربران را تسهیل می‌کند این ویژگی نیز در انواع دیگر رسانه‌ها به محدودیت روبرو است.

جذابیت و تنوع: در فضای سایبری علاوه بر اینکه امکان بهره‌برداری از همه جذابیت خاص رسانه وجود دارد (مثل فیلم، عکس) مشتری‌مداری محض نیز تاثیر به سزایی دارد.

تاثیرگذاری بر مخاطب خاص: تاثیرگذاری بسیار بالای اینترنت[1] و فضای مجازی باعث ایجاد و پیدایش مرجعیت سیاسی و فکری برای کابران می‌شود. امکان عبور و عدم تقید به بخش مهمی از قوانین و محدودیت-های رایج در سایر رسانه‌ها:

ساختار فضای سایبری شرایط را برای تولید کنندگان محتوا به صورتی رقم می‌زند که بدون داشتن دغدغه پاسخگویی با عبور و عدم تقید به بخش مهمی از قوانین و محدودیت‌های رایج در سایر رسانه‌ها تمامی افکار و عقاید خود را در این فضا منتشر کند (Ibid, 190).



و دیگری گمنام بودن فضای سایبری است که هویت و مکان بازیگران خود را پنهان می‌کند این امر به موجب معماری فیزیکی و نرم‌افزارهای خاص این فضا امکان استفاده از اسامی جعلی و پروکسی‌هایی را فراهم می‌کند که نفوذ به آنها کار دشواری است فضای سایبری سرعت ارتباطات را افزایش داده است و دسترسی به آن در اقصی نقاط دنیا رو به افزایش است و این افزایش و سهولت دسترسی به فضای سایبری حتی فقیرترین مناطق جهان را نیز شامل می‌شود (Richard and Others,2010: 98). کم رنگ شدن نقش جغرافیا فضای سایبری سرعت انتقال اطلاعات به سراسر جهان را در مدت کوتاه فراهم می کند. . و دیگر پایین بودن احتمال تنبیه یا بازخواست اقدامهای مجرمانه در فضای سایبر در نتیجه افراد و سازمانها این فضا را درمقایسه با گزینه های دیگر مطمئن ترو دارای خطرات کمتری بینند.

[1] فناوری اطلاعات شامل چهار عنصر اساسی است: ۱- اینترنت؛ ۲- سازه‌های مخابراتی سنتی؛ ۳- وسایل بکار رفته در رایانه و ۴- وسایل اختصاصی رایانه‌ای. روش‌هایی که فناوری اطلاعات را از کار می‌اندازند سه دسته‌اند: الف) جلوگیری از دسترسی به اینترنت؛ ب) اختلال در اینترنت (در این حالت نتایج و اطلاعاتی که بطور معمول انتظار می‌رود بدست نمی‌آید؛ ج) بدنام کردن شبکه اینترنتی (در این حالت به افراد اطلاعات محرمانه‌ای با اهداف مغرضانه داده می‌شود).

## صلاحیت‌های قوانین

### ۱- صلاحیت برون مرزی در قانون مجازات اسلامی

در موارد ذیل، چنانچه حتی جرم در خارج از قلمرو حاکمیت زمینی، هوایی و دریایی جمهوری اسلامی ایران اتفاق بیافتد، مراجع کیفری ایران صلاحیت رسیدگی دارند:

الف) در مورد ایرانیانی که در خارج از کشور مرتکب جرم می‌شوند، اعم از اینکه بزه ارتکابی از بزه‌های مندرج در ماده ۵ قانون مجازات اسلامی یا هر جرم دیگری باشد (ماده ۷ قانون مذکور)، صلاحیت رسیدگی به مراجع داخلی واگذار شده است. قانونگذار با استعمال عبارت «هر ایرانی که در خارج ایران مرتکب جرمی شود ...» در ماده ۷ قانون مجازات اسلامی، تفاوتی بین کارمندان دولت و سایرین و نیز نوع جرم ارتکابی قائل نشده است. در مواردی که قسمتی از جرم در ایران ارتکاب یابد ولی نتیجه آن در خارج حاصل شود و برعکس نیز، به طریق اولی، صلاحیت رسیدگی با دادگاه‌های داخلی است (ماده ۴ ق. م. ا).

ب) در مورد جرائم بین‌المللی از قبیل قاچاق مواد مخدر، تروریسم، بچه‌دزدی، معامله فحشا و هواپیماربایی که طبق قانون خاص یا عهود بین‌المللی مرتکب در هر کشوری یافت شود، در همان کشور محاکمه می‌گردد، چنانچه متهم در ایران دستگیر شود دادگاه‌های ایرانی صلاحیت رسیدگی داشته و متهم طبق قانون مجازات اسلامی به کیفر خواهد رسید (ماده ۸ ق. م. ا) (دزیانی(الف)،۱۳۷۷: ۴۱).



### ۲- صلاحیت درون‌مرزی مراجع کیفری

همه دادگاه‌ها و مراجع تحقیق موجود در کشور، صالح به رسیدگی به همه جرائمی که در سطح کشور یا در حوزه قضایی آنها اتفاق می‌افتد، نیستند. به عبارت دیگر رسیدگی به جرائم، باید بین مراجع رسیدگی تقسیم شود و هریک از آنها شایستگی و توانمندی رسیدگی به تعدادی از جرائم یا جرائم با ویژگی‌های خاص، بویژه باتوجه به نوع اتهام، را دارند. بدین ترتیب، پس از وقوع و کشف جرم، این پرسش اساسی و مهم مطرح می‌شود که تعقیب متهم، انجام دادن تحقیقات مقدماتی و سرانجام محاکمه و رسیدگی توسط کدام یک از مراجع کیفری موجود در کشور باید انجام شود. پاسخ به این پرسش را باید در قواعد حاکم بر صلاحیت مراجع کیفری داخلی، جستجو کرد (همان، ۴۲).

### ۳- صلاحیت محلی در قانون آئین دادرسی کیفری

قانون آئین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در مبحث سوم از فصل دوم (ماده ۵۱) پس از تذکر این مطلب که دادگاه‌ها فقط در حوزه قضایی محل مأموریت خود ایفای وظیفه می‌کنند و به عبارت دیگر با تحدید اختیار رسیدگی دادگاه‌ها به حوزه قضایی محل مأموریت، جهات قانونی برای شروع به تحقیق

و رسیدگی را به شرح زیر بیان داشته است: الف) جرم در حوزه قضایی آن دادگاه واقع شده باشد. ب) جرم در حوزه قضایی دیگری واقع شده ولی در حوزه قضایی آن دادگاه کشف یا متهم در آن حوزه دستگیر شده باشد. ج) جرم در حوزه دادگاه دیگری واقع ولی متهم یا مظنون به ارتکاب جرم در حوزه آن دادگاه مقیم باشد.

بدین ترتیب، مقنن ایرانی در قانون آئین دادرسی کیفری جدید (همانند قانون آئین دادرسی کیفری ۱۲۹۰ شمسی) ضوابط چهارگانه محل وقوع، محل کشف، اقامتگاه و محل دستگیری را در تعیین صلاحیت محلی مراجع کیفری عمومی و انقلاب مدنظر داشته (زندی،پیشین: ۴۷). النهایه حق تقدم برای محل وقوع جرم قائل شده است و در ماده ۵۴ مقرر می‌دارد: «متهم در دادگاهی محاکمه می‌شود که جرم در حوزه آن واقع شده است ...». بدین ترتیب در مواردی که جرمی خارج از حوزه قضایی دادگاه واقع شده لیکن در حوزه آن کشف یا مرتکب در حوزه آن دستگیر شود و نیز در مواردی که دادگاه صلاحیت محلی برای رسیدگی نداشته باشد دادگاه موظف است تحقیقات مقتضی و ضروری را به عمل آورده و پرونده را همراه با متهم (در صورت دستگیری) به دادگاه محل وقوع جرم ارسال دارد.

توجه قانونگذار و تأکید رویه قضایی بر صلاحیت مرجع کیفری محل وقوع جرم سبب می‌شود که دادگاه حوزه اقامت متهم را نیز مکلف به ارسال تحقیقات انجام شده نزد دادگاه محل وقوع جرم بدانیم. بدیهی است در ۳۱
مواردی که محل وقوع جرم مشخص نباشد دادسرای محل کشف مکلف است به تحقیقاتی که شروع کرده تداوم بخشد تا وقتی که تحقیقات ختم یا محل وقوع جرم معلوم شود. چنانچه محل وقوع جرم مشخص نگردد تعقیب را ادامه داده و سپس دادگاه اقدام به صدور رأی می‌کند (همان، ۶۵).

با این همه باید گفت که پس از محل وقوع جرم، محل دستگیری متهم در حقوق ایران و در مرحله دوم در تعیین صلاحیت موثر است. برای مثال، چنانچه جرائم ارتکابی از حیث مجازات از یک درجه باشد طبق ماده ۵۴ قانون آئین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری، دادگاهی که مرتکب در حوزه آن دستگیر شده صالح به رسیدگی خواهد بود. توضیح اینکه متهم ممکن است مرتکب چند جرم در حوزه‌های قضایی مختلف شود در این صورت بصراحت صدر ماده ۵۴ قانون مذکور، در دادگاه‌هایی که مهمترین جرم در حوزه آن واقع شده است محاکمه خواهد شد. لیکن چنانچه جرائم ارتکابی از حیث مجازات در یک درجه باشد، دادگاه محل دستگیری صلاحیت رسیدگی خواهد داشت. در این صورت چنانچه اقدامات تحقیقی به وسیله سایر دادگاه‌ها (محل وقوع جرائم دیگر)، بعمل آمده باشد، پرونده‌های متشکله به دادگاه محل دستگیری متهم ارسال خواهد شد. همچنین، در موردی که یکی از اتباع ایران در خارج از قلمرو حاکمیت جمهوری اسلامی

ایران مرتکب جرمی شود، در صورت دستگیری در داخل کشور، در دادگاهی که در حوزه آن دستگیری به عمل آمده است باید مورد محاکمه قرار گیرد (دزیانی(الف)،پیشین: ۴۴).

در پایان یادآور می‌شویم در مواردی که جرائم منتسب به متهم در حوزه‌های قضای مختلف ارتکاب یافته ولی متهم دستگیر نشده باشد، دادگاهی که ابتداً شروع به تعقیب نموده، صلاحیت رسیدگی به کلیه جرائم ارتکابی از ناحیه متهم را خواهد داشت. برغم اهمیتی که صلاحیت محلی در رسیدگی به امور کیفری داراست، قانونگذار، خود در مواردی از قواعد عمومی ناظر به تعیین صلاحیت عدول نموده و صلاحیت موازی، برای مراجع متعدد رسیدگی در نظر می‌گیرد (مستثنیات) و یا تشخیص ضرورت عدم رعایت مقررات ناظر به صلاحیت محلی را، طی شرایطی، به مقامات قضایی واگذار می‌نماید. (احاله).

## چالش‌های قواعد دادرسی در فضای سایبر

گسترش شبکه‌های جهانی رایانه‌ای چندیست که مرزهای جغرافیایی را با خلل روبرو کرده است. استفاده از شبکه‌های جهانی اینترنتی به شدت رو به افزایش است. همین که پیوستن به شبکه‌های اینترنتی افزایش می‌یابد، یعنی جائیکه بسیاری از از افراد با هم تبادل دارند، مباحث حقوقی، اهم از کیفری و خصوصی به شکل تازه‌ای مطرح می‌گردد.



### ۱- نامعین بودن حیطه‌های جغرافیایی

قوانین و مقررات حاکم بر بستر عبور و مرور در فضای مبادلات اینترنتی بی‌شک، از مقررات موجود برای مبادلات تجاری در دنیای واقعی، بسیار متفاوت خواهند بود. بخش عمده‌ای از این تفاوت ناشی از خصوصیاتی است که در اینترنت، زمینه حضور راه دور را فراهم می‌آورند و شبکه را به لحاظ فناوری از بعد مکانی و فیزیکی متمایز می‌کنند. موقعیت شبکه آنچنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. اطلاع از این موقعیت مکانی برای عملکرد شبکه و ایجاد کنندگان آن اهمیتی ندارد، لذا در طراحی یک شبکه امکان تشخیص مکان جغرافیایی در نظر گرفته نشده (همان، ۴۵). در فضا و مکان واقعی، یک شرکت یا طرف تجاری معمولاً می‌تواند مکانی واحد یا شخصی را که با او در تبادل است شناسایی نماید. چرا که این کار به شناسایی طرفین و اعتبار و مشروعیت مبادلات کمک می‌کند. ولی انجام این کار در محیط مجازی رایانه‌ای بسیار دشوار است. زیرا در اینجا طرفین یک مبادله ممکن است در دو اتاق هم‌جوار یا در دو سوی جهان باشند و شبکه هم راهی برای تشخیص این تفاوت ارائه نمی‌دهد. ماشین‌های اینترنتی «آدرس» دارند ولی این آدرس جایگاه آنها را در شبکه مشخص می‌کند نه در مکان و موقعیت ارضی. البته بعضی آدرس‌های اینترنتی مشخص‌کننده‌های جغرافیایی، یا مشخص‌کننده‌هایی

که از نظر جغرافیایی قابل تعیین باشند را در خود دارند. برای مثال، یک آدرس اینترنتی که پسوند (UK) را داشته باشد در بریتانیای کبیر (United Kingdom) قرار دارد. ولی متأسفانه اکثر آدرس‌های اینترنتی فاقد چنین تعیین‌کننده‌های جغرافیایی هستند. مهمتر از آن، تمام آدرس‌های اینترنتی به راحتی قابل انتقال هستند، زیرا برخلاف آدرس‌های فیزیکی در فضای واقعی زندگی آدرس‌هایی قراردادی در شبکه هستند. به عبارت دیگر، هیچگونه هماهنگی و همسویی بین فضا و مکان واقعی از یک‌سو و فضای مجازی رایانه‌ای وجود ندارد (دزیانی(ب)،۱۳۸۴: ۱۱۲).

## ۲- صلاحیت قضایی در قبال مجرمین

مسائل مربوط به صلاحیت قضایی در قبال جرائم، تقریباً همیشه با در نظر گرفتن محل ارتکاب آنها بیان می‌شوند. این بدان دلیل است که صلاحیت قضایی جنایی همواره برمبنای حضور واقعی و فیزیکی مجرم در درون حوزه استحفاظی و در مقابل میز محاکمه تعیین می‌شود. براساس قواعد صلاحیت قضایی اگر عنصر مادی یک جرم درون حوزه قضایی شروع یا کامل شده باشد، آن حوزه قضایی صالح بر رسیدگی خواهد بود. در مورد جرائم چندصلاحیتی، مانند آدم‌ربایی، تنها کافی است که یک عنصر مادی از جرم، درون یک حوزه قضایی در حال انجام باشد تا آن حوزه صالح بر رسیدگی شناخته شود (زندی،پیشین: ۶۸). تعامل و ادغام این قوانین ممکن است کاربران اینترنتی را با احتمال مجرم بودن در هر حوزه ذیصلاحی که با اینترنت در ارتباط است روبرو کند. همچنین ماهیت اینترنت امکان ارتباط متقابل بین چندین حوزه قضایی را فراهم آورده و عناصر یک جرم ممکن است نه تنها در مکان و حوزه‌ای با حضور فیزیکی مجرم شروع شده، و یا به نتیجه رسیده باشند، بلکه این امکان نیز هست که در تمام حوزه‌های دیگری که در اثر عملکرد کاربر به صورت الکترونیکی درگیر شده‌اند نیز بحث وقوع جرم مطرح باشد (همان، ۶۹).



اما مسئله مهم اینجاست که باتوجه به ماهیت جرائم اینترنتی تعیین محل وقوع جرم و یا محل حصول نتیجه همیشه و به آسانی مقدور نیست و به فرض شناسایی محل ارتکاب جرم و یا محل حصول نتیجه جرم (در صورت تعدد محل‌های ارتکاب)، کدام حوزه صالح به رسیدگی خواهد بود و اگر چندین کشور درگیر چنین جرائمی شده باشند، اینکه کدام کشور و مهمتر اینکه داخل هر کشور، کدام‌یک از حوزه‌های قضایی داخلی، صالح به رسیدگی خواهند بود، موضوع بحث‌است (دزیانی(ب)،پیشین: ۱۱۳).

اینک مطالعه‌ای تطبیقی درخصوص روش‌های اتخاذ شده توسط برخی از کشورهای دنیا در قبال مسئله صلاحیت قضایی در رسیدگی به جرائم سایبر خواهیم داشت:

**الف) ایالات متحده:** کشور ایالات متحده امریکا باتوجه به اینکه متأثر از قواعد و قوانین کامن‌لا است، بیش از هر منبع و مأخذ حقوق نوشته، به عرف و رویه‌های قضایی استناد نموده و خصوصاً در استناد به قواعد

عرفی، بیش از هر چیز مسئله انصاف و منطق را مدنظر قرار خواهد داد. در دادگاه‌های جنایی استنباط از عرف، عدل و انصاف و به معنای کلی، احراز نظر وجدان عمومی، بعهده هیأت منصفه نهاده شده. درخصوص جرائم سایبر نیز، دادگاه‌ها به عرف و منطق متوسل شده و در احراز و یا عدم احراز صلاحیت دادگاه، به ارتباط منطقی و عرفی میان کاربران اینترنتی و مجرمین اینترنتی توجه می‌نمایند. چرا که بدرستی دریافته‌اند چنانچه بخواهند با قواعد دادرسی کیفری سنتی به جرائم سایبر نیز رسیدگی کنند، می‌بایست به دنبال محل وقوع جرم، محل حصول نتیجه مجرمانه و محل دستگیری متهم و ... گشت و باتوجه به توضیحات قبلی درخصوص معین نبودن هیچیک از این مکان‌ها در فضای مجازی، درگیر دور باطل خواهند شد. بنابراین از عرف، منطق و وجدان عمومی استمداد جسته و بحث ارتباط منطقی را مطرح نموده‌اند. در بحث ارتباط منطقی، دادگاه بررسی می‌کند که آیا متهم در جرائم سایبر، تا چه میزان موفق به برقراری ارتباط اینترنتی با بزه‌دیده گردیده و آیا این میزان برقراری ارتباط کافیست تا دادگاه محل اقامت یا شکایت بزهدیده صالح بر رسیدگی به اتهام مزبور باشد یا خیر! تشخیص این امر که ارتباط پدید آمده در چه حد از اهمیت است و این حد ارتباط برای احراز صلاحیت دادگاه محل اقامت بزه‌دیدگان کافیست یا خیر، بعهده خود دادگاه است و ملاک و معیار این تشخیص، عرف، منطق و رجوع به رویه قضایی خواهد بود و این امریست که فقط در سیستم حقوقی کامن‌لا و در کشورهایی از جمله ایالات متحده قابل اجراست چرا که در کشورهای دارای سیستم حقوق نوشته، احراز صلاحیت دادگاه نه براساس رجوع به عرف و منطق حقوقی بلکه باتوجه به نصوص صریح قانونی از پیش نوشته، صورت می‌پذیرد (Betz, David and Stevens,Ibid: 42).



**ب) کشورهای اروپایی (حقوق نوشته):** اغلب کشورهای اروپایی از جمله، فرانسه، بلژیک، آلمان و ... دارای رژیم حقوقی نوشته هستند. قبل از وارد شدن به بحث صلاحیت قضایی در کشورهای دارای حقوق نوشته یادآور می‌شویم قریب به اتفاق کشورهای پیشرفته (حدود ۴۰ کشور)، با عضویت در کنوانسیون بین‌المللی جرائم محیط سایبر، تحت عنوان کنوانسیون بوداپست ـ۲۰۰۱، سیستم واحدی را که کنوانسیون درخصوص کلیات، تعاریف، جرائم، مجازات‌ها و دادرسی کیفری جرائم محیط سایبر پیشنهاد نموده، بطور متحد پذیرفته‌اند.

**ج) کنوانسیون جرائم محیط سایبر ـ بوداپست ۲۰۰۱:** بخش دوم از فصل دوم کنوانسیون، تحت عنوان صلاحیت، به تبیین اصول کلی صلاحیت کشورهای عضو در رسیدگی به جرائم محیط مجازی پرداخته. در این بخش تنها یک ماده (ماده ۲۲) دارای ۵ بند، به این مهم اختصاص یافته. هرچند نقد ماده ۲۲ کنوانسیون، در حوصله این مقال نمی‌گنجد، اما به ناچار و به نحو گذرا به بررسی این ماده می‌پردازیم:

بند ۱: «هریک از اعضاء باید بگونه‌ای اقدام به وضع قوانین و مقررات بنماید که در صورت لزوم در زمانی که جرم در موارد ذیل به وقوع می‌پیوندد، صلاحیت رسیدگی به هریک از جرائم مندرج در مواد ۲ تا ۱۱ کنوانسیون را بوجود آورد:

الف) جرم در قلمروش بوقوع پیوسته باشد. یا؛ ب) جرم در کشتی بوقوع پیوسته که پرچم آن کشور بر فراز آن برافراشته باشد. یا؛ ج) جرم در هواپیمایی بوقوع پیوسته که مطابق مقررات آن عضو به ثبت رسیده. یا؛ د) در جائیکه جرم موردنظر مطابق قوانین جزایی قابل مجازات شناخته شده و توسط تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرائم واقع در حوزه صلاحیت جهانی حقوق جزا باشد.» صدر بند ۱ ماده ۲۲ بگونه‌ای نگارش یافته که این امید را زنده می‌کند: که کشورهای عضو مجاز شناخته شده‌اند تا قوانین خاص و جدیدی در راستای پیشگیری و مبارزه با جرائم محیط سایبر و منطبق با ماهیت مجازی شبکه، وضع نمایند. اما بلافاصله با برشمردن شقوق چهارگانه، این گمان را از ذهن بیرون می‌برد و وضع به حالت دادرسی‌های سنتی برمی‌گردد. شقوق چهارگانه بند ۱ ماده ۲۲ دقیقاً همان مواردی را دربرمی‌گیرد که در دادرسی‌های کیفری سنتی خوانده‌ایم. حال آنکه ورود آنها در قوانین محیط سایبر نه تنها هیچگونه انطباقی با اوضاع و احوال و شرایط ارتکاب جرائم سایبر ندارد بلکه با آن منافات نیز دارد.

درخصوص جرائم ارتکابی توسط تبعه و یا جرائم حوزه صلاحیت جهانی، در قوانین دادرسی سنتی هیچ‌یک از ۳۵
کشورها ابهامی در صالح بودن کشور صاحب قلمرو نیست و اصلاً نیازی به دوباره نویسی این موارد در بند ۱ نبوده. بحث اصلی، حل این مسئله است که در جرائم سایبر، اصلاً محل وقوع جرم کجاست؟! و مجرم کیست؟! زمانیکه این سوالات پاسخ داده نشده چگونه می‌توان به تبیین صلاحیت سرزمینی و یا شخصی برای کشورها پرداخت؟ آیا ابتدا نباید دانست جرم در حوزه کدام کشور و توسط چه شخصی ارتکاب یافته و بعد، حوزه ارتکابی را صالح بر رسیدگی دانست؟ بند ۲ ماده ۲۲ نیز، چون ناظر به شقوق ب تا د بند ۱ است، تبعاً با سوالات فوق روبروست (Ibid, 47).

بند ۲: «هریک از اعضاء می‌توانند حق عدم اجرا یا اجرای موضوعات یا شرایط بخصوصی را در محدوده مقررات صلاحیتی مندرج در شقوق ب تا د این ماده یا قسمتی از آن برای خود محفوظ دارند.» به صراحت قسمت دوم بند ۳ ماده ۲، این قواعد صلاحیتی را در جایی مجری دانسته که متهم در حوزه کشور عضو قرار دارد و کشور عضو آن متهم را با استناد به اصل عدم استرداد تبعه، به کشور تقاضا کننده استرداد، مسترد نمی‌دارد. پس کشور عضوی که متهم در آن قرار دارد را ملزم به احراز صلاحیت کیفری خود و محاکمه و مجازات مرتکب نموده.

بند ۳: «هریک از اعضاء باید بگونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم امکان وضع صلاحیت درباره جرائم مندرج در پاراگراف ۱ ماده ۲۴ این کنوانسیون وجود داشته باشد. این موارد در جایی است که متهم در قلمرو آن عضو قرار دارد و آن عضو نیز متهم موردنظر را صرفاً به خاطر تابعیت و پس از دریافت درخواست استرداد از طرف دیگر دولت عضو، مسترد نمی‌کند». در بند ۴ ماده ۲۲، کنوانسیون را معارض قوانین صلاحیت داخلی کشورها ندانسته و به نوعی خواسته تا کشورها را ترغیب به وضع قواعد صلاحیتی در این باب نماید.

بند ۴: «این کنوانسیون مانع اجرای هرگونه صلاحیت کیفری که مطابق قانون داخلی به مرحله اجرا درمی‌آید نمی‌شود.»

همانطور که ملاحظه می‌شود باز هم کنوانسیون راه‌حل عملی و منطقی در راستای حل معضلات صلاحیت ارائه نمی‌کند. از سوی دیگر بدیهی است که کشورهای عضو در هر کنوانسیون، اختیارات داخلی قانونگذاری خود در مسائل مختلف حقوقی، خصوصاً حوزه قانونگذاری حقوق کیفری را ساقط و یا محدود نمی‌کنند و تصریح بند ۴ به این اختیار دولت‌ها، امری راهگشا نخواهد بود. در بند ۵ ماده ۲۲ بحث تعارض صلاحیت دولت‌ها در جائیکه چند کشور صالح به رسیدگی هستند مطرح گردیده اما تنها راه‌حلی که ارائه شده به شور نشستن کشورهای صالح و انتخاب یک کشور و تفویض اختیار تعقیب و رسیدگی قضایی به کشور منتخب بوده است. چنانچه گذشت، حتی بند ۵ نیز راه‌حلی در جهت حل تعارض صلاحیت‌ها ارائه نداده و تنها شور و انتخاب نماینده را برای رسیدگی کیفری پیشنهاد نموده است (زندی،پیشین: ۷۴).



## مسائل لاینحل

اول: تعیین محل ارتکاب جرم سایبر؛

دوم: شناسایی تابعیت شخص مرتکب؛

سوم: حل تعارض صلاحیت‌ها.

**مسئله اول: تعیین محل ارتکاب جرم سایبر:** جرم سایبر به لحاظ ماهیت مجازی و غیرواقعی خود، حقیقتاً نمود عینی و ملموسی، شبیه آنچه در جرائم سنتی مثل ضرب و جرح و یا سرقت و ... مشاهده می‌کنیم از خود به نمایش نمی‌گذارد. بلکه جرم سایبر در واقع در بستر مبادلات الکترونیکی و بر روی داده‌ها و اطلاعات و بعضاً (بندرت) بر روی سیستم‌های فیزیکی و سخت‌افزاری ارتکاب می‌یابد. در جائیکه جرم سایبر بر روی داده‌ها ارتکاب یافته، تعیین محل ارتکاب جرم کاری بس دشوار و در برخی موارد حتی غیرممکن بنظر می‌رسد. محل وقوع جرم سایبری بطور دقیق یعنی محل و مکانی که این داده‌ها دستخوش حملات مجرمانه قرار گرفته و دگرگون شده‌اند. چگونه می‌توان یک رخداد غیرفیزیکی و مجازی را در دنیای فیزیکی و در بعد

مکانی جستجو کرد؟ حتی اگر جرم سایبری بر روی قطعات فیزیکی و سخت‌افزاری ارتکاب یافته و باعث بروز اختلالات و یا از کارافتادگی آنها گردد، باز هم بطور قطع نمی‌توان نظر داد که محل وقوع جرم سایبری همان محل وجود قطعات سخت‌افزاری آسیب دیده خواهد بود. چراکه در قریب به اتفاق اینگونه جرائم، عمل مجرمانه در مکانی دیگر انجام گرفته و تنها نتیجه مجرمانه بر روی قطعات سخت‌افزاری پدیدار گشته. در هر صورت، تعیین محل ارتکاب فعل مجرمانه (سایبری) در فضای مجازی مبادلات داده‌ها، به راحتی امکانپذیر نبوده و نیست. ملاحظه می‌شود که جرائم محیط سایبر برخلاف جرائم سنتی که در مکان‌های مشخص و یا محصوری اعم از یک اتاق، یک ساختمان و یا یک منطقه رخ می‌دهند، ممکن است در چند گوشه کره زمین ارتکاب یابند همچنین با این تفاوت که نه تنها از نقطه‌نظر فنی و تکنیکی بلکه از نقطه‌نظر حقوق کیفری نیز نمی‌توان بطورحتم مکان واحدی را بعنوان محل ارتکاب جرم برگزید. با این اوصاف تدابیر قوانین دادرسی سنتی که با پارامترهایی همچون محل ارتکاب جرم (صلاحیت سرزمینی) تبیین شده‌اند، کارایی خود را از دست خواهند داد. زیرا اصلاً در وهله نخست شروع به تعقیب و رسیدگی به این جرائم خاص نمی‌دانیم جرم در کدام حوزه واقع شده تا بنابه اصل صلاحیت سرزمینی اولاً کشور صالح و سپس باتوجه به قواعد پیش‌بینی شده در قوانین دادرسی، حوزه قضایی صالح را شناسایی نمائیم (همان، ۶۹).

**مسئله دوم: شناسایی تابعیت شخص مرتکب:** هنگامیکه بحث از تابعیت شخص مرتکب به میان می‌آید بلافاصله مفهوم صلاحیت شخصی در آئین دادرسی کیفری به ذهن متبادر می‌شود. اینکه مرتکب دارای چه تابعیتی است در بسیاری موارد کشور متبوع وی را صالح به رسیدگی به اتهامات وی می‌نماید چنانکه در ماده ۷ قانون مجازات اسلامی نیز رسیدگی به کلیه جرائم ارتکابی توسط ایرانیان در هر کجای جهان را در صلاحیت دادگاه‌های کیفری داخلی دانسته. اما در جرائم سایبری، حتی تابعیت مرتکب نیز ناشناخته است. چراکه در فضای مجازی کاربران با شناسه‌های قراردادی همچون IP ها (قراردادهای اینترنتی) که تماماً مجازی و غیرقابل مشاهده و لمس هستند، شناسایی می‌شوند و حتی در صورت شناسایی کاربر مرتکب جرم، در واقع ما هویت مجازی و قراردادی وی را شناسایی کرده‌ایم نه هویت واقعی او را همچنان که در ادارات تشخیص هویت پلیس کشورها صورت می‌پذیرد (همان، ۳۲). ۳۷

**مسئله سوم: حل تعارض صلاحیت‌ها:** بدون پاسخ به پرسش‌های اول و دوم (که بعداً به آنها اشاره خواهیم کرد) فرضی را در نظر می‌گیریم که صلاحیت قضایی بیش از یک کشور و یا در سیستم داخلی، بیش از یک حوزه قضایی در رسیدگی به یک جرم و یا اتهام مرتکب احراز گردیده. ظاهراً این تعارض پدید آمده شبیه به تعارضات سنتی و تابع قواعد حل تعارضات سنتی خواهد بود. اما می‌دانیم در تعارض صلاحیت‌ها در حالت سنتی، ابعاد دامنه جرم یا جرائم، مشخص و محدود است و با توسل به راهکارهای ارائه شده از جمله استرداد

و ... تا حد قابل توجهی می‌توان به این تعارضات خاتمه داد. اما نظر به دامنه شمول جرائم موضوع این بحث و فراگیر بودن و امکان ورود خسارات و زیان‌های غیرقابل تصور (همانند خواباندن شبکه سراسری برق‌رسانی یک کشور یا چند کشور همجوار) دیگر به سادگی قبل نمی‌توان تعارض پیش آمده در صلاحیت دولت‌ها را حل نمود. چرا که هر دولت آنچنان از این جرایم صدمه دیده که براحتی حاضر نیست از صلاحیت خود صرف نظر نموده و اختیار رسیدگی را به دولت‌های دیگر محول نماید (دزیانی(الف)،پیشین: ۹).

**حل مسئله:** در یک رویکرد کلی درخصوص جرائم سایبری می‌بایستی فضای ذهنی قانونگذار را از محیط واقعی و فیزیکی خارج نموده و در محیط کاملاً مجازی و غیرواقعی قرار داد. از سوی دیگر ماهیت غیرواقعی جرائم سایبری باعث گردیده تا مزرهای جغرافیایی و مفهوم سرزمین‌های مجزا، رنگ‌باخته و اصطلاحاً عبارت «صلاحیت غیر مبتنی بر مرز» یا «صلاحیت فرامرزی» جایگزین صلاحیت‌های مبتنی بر حیطه‌بندی‌های جغرافیایی سیاسی و طبیعی گردد. چرا که ماهیت جرائم سایبر اصولاً ماهیتی فرامرزی بوده و می‌بایست بدون در نظر گرفتن مکان و موقعیت فیزیکی مرتکب، محل ارتکاب و ... مورد بررسی قرار گیرند (همان، ۱۳).

**نتیجه:** راه‌حل پیشنهادی در تعیین دادگاه صالح، تنها عبور از قواعد سنتی و در نظر گرفتن موقعیت بزه‌دیده است. یعنی چنانچه بزه‌دیده جرائم سایبر به دادگاه کیفری محل اقامت خود، تقدیم شکوائیه نماید دادگاه، تنها برمبنای اینکه بزه‌دیده در حوزه آن دادگاه ساکن است می‌باید خود را صالح بر رسیدگی دانسته و با قبول شکایت، اقدام به تعقیب و رسیدگی قضایی نماید. زیرا تنها محلی که می‌توان تحقیقات مقدماتی را از آنجا آغاز نمود و امکان جمع‌آوری آثار جرم درآن وجود دارد, محلی است که متهم در آن اقامت داشته وحداقل، نمایشی از وقوع جرم سایبر بر روی داده‌ها و یا سیستم‌های او قابل رؤیت می‌باشد. مشکلی که در پی این قضیه پیش خواهد آمد، تعدد بزه‌دیدگان و در نتیجه تعدد مراجع قضایی صالح به رسیدگی خواهد بود. در سطح جهانی اولاً بنابه پیشنهاد بند ۵ ماده ۲۲ کنوانسیون بوداپست درخصوص کشورهای عضو، مشورت و اتخاذ تصمیم درخصوص صالح دانستن یکی از اعضاء، به رسیدگی به تمامی اتهامات وارده و شکایات واصله خواهد بود و چه در مورد کشورهای عضو کنوانسیون مزبور، و چه درخصوص کشورهای غیرعضو، بهترین و کارآمدترین راه‌حل، تقویت همکاری‌های بین‌المللی و یا همان معاضدت قضایی بین‌المللی است که البته کنوانسیون نیز نظر به اینکه در قسمت صلاحیت نهایتاً راه‌حل روشنی ارائه ننموده، بلافاصله پس از مبحث مربوط به صلاحیت، ذیل فصل سوم تحت عنوان همکاری‌های بین‌المللی، از ماده ۲۳ تا ۳۵ طی ۱۳ ماده اصول همکاری‌های قضایی و پلیسی بین‌المللی را تبیین نموده و حتی در ماده ۳۵، یک نقطه تماس بین‌المللی را که بطور ۲۴ ساعته و بصورت On Line آماده دریافت، پیگیری و ارائه گزارشات مربوط به همکاری کشورها در مبارزه با جرائم سایبری است، برای هریک از اعضاء پیش‌بینی نموده تا از این طریق با سریع‌ترین وسایل ارتباطی که به آنها نیز تحت بند ۳ ماده ۲۵ قابلیت استناد بخشیده، بتوانند به پیگیری و تعقیب و رسیدگی

این جرائم اهتمام ورزند. حتی در رسیدگی‌های قضایی با یادآوری اصول مربوط به استرداد مجرمین (ماده ۲۴) سعی در تقویت معاضدت قضایی دولت‌ها نموده. و اما درخصوص تعارض صلاحیت در حوزه‌های قضایی داخلی، می‌توان با تأسیس یک هیأت و یا شعبه مرکزی، درخصوص رسیدگی به جرائم سایبر در کشور، که باتوجه به قابلیت‌های تخصصی و امکانات مالی و تجهیزاتی علی‌القاعده در تهران برپا خواهد شد، به تمامی مراجع قضایی سراسر کشور تکلیف نمود، تا در صورت دریافت هرگونه گزارش از مقامات ذیصلاح و یا وصول شکوائیه و یا مشاهده هرگونه جرمی از جرائم محیط سایبر، بلافاصله شعبه مرکزی را در جریان امر قرار داده و منتظر تعیین تکلیف از سوی شعبه مرکزی بمانند.

با این روش چنانچه بزه‌دیدگان متعددی در سراسر کشور اقدام به تقدیم شکوائیه نموده و خواستار پیگیری قضیه شده باشند، تمامی این شکایات و اعلامات در شعبه مرکزی منعکس شده و این شعبه، با در نظر گرفتن معیارهای اصولی همچون تراکم بزه‌دیده در نقطه یا نقاط خاص، وجود و اعلام احتمالی کشف ادله جرم در یک یا چند حوزه خاص و یا دستیابی احتمالی هریک از حوزه‌ها به اطلاعات مرتکب یا مرتکبین، با ارجاع پرونده به حوزه‌ای که بیشترین پارامترها را در اختیار دارد و همچنین تکلیف دیگر مراجع گزارش دهنده، به اینکه تمامی پرونده‌های متشکله و تحقیقات احتمالی انجام گرفته را نزد شعبه مرجوع‌الیه ارسال نمایند، گامی موثر در جهت تعیین مرجع صالح واحد و جلوگیری از تراکم پرونده در حوزه‌های مختلف و اصدار آراء متهافت و متعارض برداشته خواهد شد. ۳۹

## نتیجه‌گیری

در تعیین محل ارتکاب جرم اغلب به دکترین استناد می‌شود. وقوع جرم در داخل حوزه قضایی یک کشور در صورتی محرز می‌شود که یکی از عوامل تشکیل دهنده جرم با نتیجه نهایی آن در داخل مرزهای آن کشور واقع شده باشد. در کشورهای مبتنی بر کامن‌لا ضمن تاکید بر عمل فیزیکی از نتیجه آثار و نتایج نیز استفاده می‌شود طبق این نظریه اگر جرمی در سرزمینی واقع شود فرض می‌شود که آثار و نتایج جرم در آن سرزمین ظاهر شود یا در واقع ظاهر شده است بنابراین در مواردی که عوامل یا آثار مختلف یک جرم ممکن است در بیش از یک کشور واقع شود ممکن است دو دکترین صلاحیت سرزمینی بر ادعاهای صلاحیتی شروع و متقارن منتهی شود. کشورها به نظر باید در اجرای اصول صلاحیتی راه اعتدال در پیش بگیرند تا از تضادهای صلاحیتی مهم جلوگیری شود اصل شخصی بودن منفعل که گرچه حافظ منافع اقتصادی اتباع کشورها است شدیدا محل بحث می‌باشد در حالیکه اصل جهانی بودن کاملا براساس مقررات صریح معاهدات محدود است اما اصل حمایتی ممکن است در مورد انواع خاصی از جرائم رایانه‌ای بی‌مناسب نباشد زیرا یک کشور مطابق

با این اصل می‌تواند بعنوان دفاع از منافع اساسی آن کشور، صلاحیت لازم برای رسیدگی به جرائم واقع شده در خارج از سرزمین خود را به دست آورد.

باتوجه به صلاحیت‌های سرزمینی و فراسرزمینی کشورها، حل مسئله تعارض صلاحیت‌ها اغلب به توافق بین کشورها نیاز دارد. بنابراین ممکن است که اجرای موثر قوانین مورد توافق مسائل استرداد مجرمان نیز می‌باشد. زیرا محل اقامت فیزیکی فرد متهم ممکن است الزاما مرجع مناسبی برای رسیدگی به جرم نباشد. این مطلب قابل تسری به جرایم رایانه‌ای/سایبری می‌باشد اما باید به شرایط مندرج در قانون معاهده استرداد مجرمان توجه کرد. در مسئله صلاحیت در دعاوی فرامرزی، امکان مطرح شدن صلاحیت‌های متناقض وجود دارد که در نهایت به انجام تعقیب‌های متعدد و ایجاد اصطکاک بین دولت‌ها منجر می‌شود. روش انتقال جریان دادرسی، به نسبت موثرتری برای حل این مسئله به شکلی هماهنگ فراهم می‌آورد. با انعقاد موافقت‌نامه‌هایی که براساس آن کشوری از حقوق مربوط به صلاحیت خود بنحو کشوری دیگر صرف‌نظر می‌کند حل و فصل مشکلات تعارض قوانین امکانپذیر می‌شود.

دلایل این عمل غیر از اجتناب از تعارض صلاحیت‌ها، عبارت از اجرای موثر عدالت کیفری، حفظ منافع بزه‌دیده و پذیرش مجدد مجرم در جامعه است. بدیهی است نظر به سرعت خیره کننده مبادلات در محیط سایبر، و به تبع آن، سرعت ارتکاب جرائم سایبر و امکان فرار بسیار سریع مرتکب، از صحنه جرم (مجازی)، و امکان اختفاء و یا حتی امهاء آثار و دلایل جرم، اینگونه اطلاع‌رسانی و ارجاع واحد، بایستی با حداقل تلف زمانی صورت پذیرد که این سرعت عمل امری بایسته و تفکیک‌ناپذیر، در پیشگیری و مبارزه با جرائم سایبر خواهد بود. در کشور ایران، قانون جرائم رایانه‌ای مصوب خرداد ۱۳۲۲ مطالبی را در مواد ۲۸-۲۹-۳۰-۳۱ به مسئله صلاحیت اختصاص داده است. در بندهای الف و ب ماده ۸۲ 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 دامنه مرتبه بالای کد کشوری ایران، قاعده صلاحیت سرزمینی را بگونه‌ای دیگر نسبت به جرائم ارتکابی در فضای سایبر اعمال کرده است. در بند (ج) صلاحیت شخصی سنتی و در بند (د) صلاحیت جهانی را برای رسیدگی به جرائم سایبری پیش‌بینی کرده است. درخصوص تعارض صلاحیت در حوزه‌های قضایی داخلی اگرچه ماده ۳۱ قانون فوق‌الذکر مقرر کرده است که حل اختلاف درخصوص صلاحیت مطابق مقررات قانون آئین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهد بود. ولی برای سهولت رسیدگی می‌توان با تصویب قانونی و تأسیس یک هیأت یا شعبه مرکزی در پایتخت، درخصوص رسیدگی به جرائم سایبری در نقاط مختلف کشور، به همه مراجع قضایی داخلی تکلیف کرد تا در صورت دریافت هرگونه گزارش از مقام صلاحیت‌دار یا دریافت شکوائیه و یا مشاهده هر نوع جرم از جرائم سایبری بلافاصله شعبه مرکزی را در جریان امر قرار داده و منتظر تعیین تکلیف از آن باشند.

## فهرست منابع

**فارسی:**

۱- زندی، محمدرضا (۱۳۸۹)، **تحقیقات مقدماتی در جرائم سایبری**، چ۱، تهران: انتشارات جنگل.

۲- دزیانی(الف)،محمدحسن (۱۳۷۷)، «صلاحیت رسیدگی به جرائم سایبر»، **خبرنامه انفورماتیک**، ش۱۸.

۳- دزیانی(ب)، محمدحسن (۱۳۸۴)، **نگاهی به جرائم سایبری**، تهران: انتشارات معاون برنامه و بودجه.

**لاتین:**

1- . Betz, David and Stevens, Tim (2011). Cyberspace and the State: Toward a Strategy for Cyber-power, Routledge.

2- Carr, Jick (2011). Inside Cyber Warfare: Mapping the Cyber Underworld, O'Reilly Media; Second Edition.

3- Friedman, Singer and Others (2014). Cybersecurity: What Everyone Needs to Know, Oxford University Press.

4- Gibson, William (2011). Neuromancer, HarperCollins Publishers.

5- Graham, Midd (2014). Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities, The Geographical Journal, vol. 179, no. 2.

6- Hu, Fei (2013), Cyber-Physical Systems: Integrated Computing and Engineering Design, CRC Press.

7- Lessig, Lawrence (1999). Code and Other Laws of Cyberspace, Basic Books.

8- Libicki, Mouda (2009). Cyberdeterrence and Cyberwar, Rand Corporation.

9- Palloff, Rena and Pratt, Koud (2002). Lessons from the Cyberspace Classroom: The Realities of Online Teaching.

10- Perry, Barlow (1996). A Declaration of the Independence of Cyberspace.

11- Powner, David (2013). National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture.

12- Ray, Alis (2002). International Cyber-Jurisdiction. A comparative analysis.

13- Richard, Rbert and Others (2010). Cyber War: The Next Threat to National Security and What to do about it, New York.

14- Rid, Tiee (2013). Cyber War Will Not Take Place, Oxford University Press.

15- Roscini, Morall (2012). Cyber Operations and the Use of Force in International Law, Oxford University.

16- Spinello, Richard (2012). Tavani, Herman Readings in Cyberethics, Jones and Bartlett Publishers.