صلاحیت کیفری مراجع قضایی در فضای سایبر

دکتر فضل الله فروغی*
امیر البوعلی**

چکیده

یکی از مسائل جدید که به موازات تحول و پیشرفت تکنولوژی در زمینهٔ فناوری اطلاعات و ارتباطات به‌ویژه با ایجاد دنیایی مجازی جدید به نام «فضای سایبر» به وجود آمده است مسألهٔ چگونگی تعیین مرجع قضایی صالح جهت رسیدگی به جرائم ارتکابی در فضای مذکور است. چون بر اساس قواعد سنتی مهم‌ترین ضابطهٔ 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 در خصوص صلاحیت، از قبیل« فضای سایبر به عنوان 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 ۲۸ 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 جایی که قواعد

---

* استادیار دانشکده حقوق و علوم سیاسی دانشگاه شیراز.
** کارشناس ارشد حقوق جزا و جرم‌شناسی.

سنتی قابل اجرا باشند همان قواعد اجرا می‌شوند و در غیر آن صورت تئوری صلاحیت دادگاه ذی ارتباط منطقی با جرم به عنوان ضابطه نهایی پذیرفته شود.

کلید واژگان

صلاحیت کیفری، صلاحیت سایبری، فضای سایبر، دادگاه دیجیتالی، فضای بین‌المللی.

مقدمه

مسألهٔ صلاحیت مراجع قضایی در رسیدگی به جرائم، یکی از مباحث مهم حقوق جزایی می‌باشد که در کنار سایر قواعد حاکم بر فرایند دادرسی، در آیین دادرسی کیفری مورد بحث قرار می‌گیرد.

در حقوق کیفری به‌طور کلی شایستگی نهادهای قضایی کیفری در رسیدگی به دعاوی در بعد داخلی بر اساس 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 بر اساس محل ارتکاب جرم(صلاحیت سرزمینی)، تابعیت متهم(صلاحیت شخصی فعال یا مثبت)، تابعیت مجنی علیه (صلاحیت شخصی غیر فعال یا منفی)، اخلال در نظم و امنیت کشوری(صلاحیت واقعی یا حمایتی) و یا اخلال در نظم و امنیت جهانی و حیات بشریت به‌طور کلی(صلاحیت جهانی)مشخص می‌شود. به گونه‌ای که در هر دو عرصهٔ بین‌المللی و داخلی- به‌ویژه در مورد اخیر- محل وقوع جرم جهت تعیین مرجع قضایی صالح به رسیدگی به دعاوی کیفری از اهمیت ویژه‌ای برخوردار است و حتی در خصوص صلاحیت سرزمینی که مبتنی بر ضابطهٔ محل وقوع جرم می‌باشد نظریه‌ها و تئوری‌های متفاوتی مطرح شده است به‌طوری که 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 حوزهٔ داخلی و تحت حاکمیت کشوری صالح شناخته‌اند. علی‌رغم وجود اختلافات در خصوص محل وقوع جرم و ضابطهٔ تشخیص آن جهت تعیین مرجع صالح مسألهٔ مهمی که در این زمینه به‌ویژه در دهه‌های اخیر به وجود آمده است تشخیص محل وقوع جرم در فضای سایبر است. چون ضوابط و معیارهای پیش گفته 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 به‌طوری که این فضا کاملاً غیر ملموس 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 در خصوص جرائم اینترنتی، صلاحیت دادگاه‌های مختلف در رابطه با آن جرائم در حقوق کیفری را بر انگیخته است.

در این مقاله منحصراً به مسألهٔ مهم صلاحیت کیفری مراجع قضایی در محیط سایبر پرداخته می‌شود و به این سؤال پاسخ داده می‌شود که در محیط سایبر چه معیارهایی می‌توانند تعیین‌کننده صلاحیت باشند؟ این سؤال از آنجا شدت پیدا می‌کند که در محیط سایبر قواعد سنتی با چالش‌هایی از قبیل نامعین بودن حیطه‌های 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 روبه‌رو می‌شوند که با توجه به اینکه در راستای پاسخ‌گویی به این سؤال نویسندگان و حقوق‌دانان رویکردهای مختلفی را مطرح کرده‌اند برخی رویکردها در واقع مبتنی بر ضوابط سنتی تعیین صلاحیت، مانند اصل سرزمینی و شخصی و 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 به عنوان یک فضای آزاد بین‌المللی و رویکرد دادگاه سایبری (دیجیتالی) و رویکرد ارتباط حداقلی یا ارتباط منطقی دادگاه مدعی صلاحیت و جرم ارتکابی من حیث المجموع اختصاص می‌دهیم.

گفتار اول: رویکردهای مبتنی بر ضوابط سنتی صلاحیت

برخی با تطبیق قواعد و ضوابط سنتی حاکم بر تعیین صلاحیت، همان امور را به عنوان

ضابطهٔ تعیین مرجع قضایی صالح اتخاذ کرده‌اند. ما در این قسمت این ضوابط را با بیان امکان و میزان به‌کارگیری آن‌ها در فضای سایبر بررسی می‌کنیم.

بند اول: ضابطهٔ سیستم قضایی محل وقوع جرم

این ضابطه خود یادگار مهم‌ترین و رایج‌ترین اصل در اِعمال صلاحیت کیفری در قواعد سنتی یعنی صلاحیت سرزمینی است. این اصل بر پایهٔ احترام متقابل به حاکمیت برابر کشورها و همچنین پیوند آن با اصل عدم مداخلهٔ آن‌ها در امور داخلی یکدیگر بنا شده است. به همین دلیل معمولاً استناد به دیگر اصول صلاحیت کیفری در اولویت بعدی قرار می‌گیرند.

برای تعیین محل ارتکاب جرائم در فضای سایبر همانند قواعد سنتی صلاحیت سرزمینی اصولاً قلمرو سرزمینی در این فضا باید مشخص گردد. جهت تشخیص این قلمرو، توضیح و تبیین قلمرو فضای سایبر به اختصار لازم می‌آید.

الف) فضای سایبر و قلمرو آن

فضای سایبر به محیطی غیر ملموس و غیر فیزیکی گفته می‌شود که با اتصال شبکه‌های ارتباطی و سیستم‌های رایانه‌ای یا مخابراتی به وجود آمده و محتوای آن به صورت غیر ملموس و مجازی است که «داده» نامیده می‌شود و مشتمل بر صوت و تصویر و نوشته و سند و از این قبیل موارد است و ظرفیت انجام فعالیت‌های مختلف را دارد. بستر فضای مذکور که به بستر ارتباطات و مبادلات الکترونیکی موسوم است، مجموعه‌ای عظیم از صفر و یک‌هایی است که داده‌های الکترونیکی را تشکیل می‌دهد و آن‌ها نیز در

قالب‌های مختلف، مفاهیم را به شکل الکترونیکی منعکس می‌کنند.[1] محتویات فضای سایبر در همین بستر جا سازی و ذخیره می‌شود و پس از پردازش و تغییرات معین به طریق خاص منعکس می‌شود.

این مجموعه‌های عظیم در کشورهای معدودی، که غالباً از کشورهای پیشرو در زمینهٔ تکنولوژی اطلاعات و اینترنت هستند، مستقر می‌باشند که اصطلاحاً «مراکز داده اینترنتی»[2] یا «سرور»[3] گفته می‌شود. با این توضیح مشخص می‌شود که فضای سایبر دارای یک قلمروی مجازی، غیر ملموس، فراتر از مکان، زمان و به عبارتی فراملی است و بالتبع اعمال واقعه در آن از نظر ارتکاب آسان و از لحاظ کشف بسیار مشکل می‌باشد.

ب) محل ارتکاب جرم در فضای سایبر

در خصوص شناسایی و تعیین محل ارتکاب جرم در فضای سایبر ضوابط و نظریات مختلفی مطرح شده است، لیکن هر کدام در جای خود دارای اشکال و قابل نقد می‌باشد. مهم‌ترین این نظریات عبارتند از:

۱. نظریه محل قرارگیری وسیلهٔ مؤثر در ارتکاب جرم (کامپیوتر یا ماهواره)[4]

در این نظریه جایی که کامپیوتر تأثیرگذار در وقوع جرائم رایانه‌ای (سایبری)، قرار دارد و یا جایی که ماهواره وسیلهٔ ارتکاب جرم ثبت شده است، محل ارتکاب جرم

---

۱. امیر حسین، جلالی فراهانی؛ *صلاحیت کیفری در فضای سایبر*، نشریهٔ فقه و حقوق، سال سوم، شمارهٔ ۱۱، ۱۳۸۵، ص ۱.

2. Internet Data Center.

3. Server.

4. Location of Computers.

محسوب شده و نظام قضایی همان محل جهت تعقیب جرم ارتکابی صالح خواهد بود. برای مثال یکی از رایج‌ترین اقداماتی که هکرها[۵] انجام می‌دهند این است که برای ارتکاب انواع جرائم سایبری نظیر پخش انواع ویروس، نشر هرزه نگاری یا حتی تعقیب ایذایی، یک کامپیوتر بی گناه را حتی در یک کشور دیگر به عنوان پایگاه خود قرار می‌دهند و از طریق آن مرتکب جرائم سایبری می‌شوند.[۶]

در این زمینه قانون برخی ایالت‌ها در آمریکا مانند ایالت کانکتیکا مقرر کرده:«چنانچه کامپیوترهای واقع در این ایالت در تحقق جرم تأثیر قابل توجهی داشته باشند محاکم این ایالت صالح به رسیدگی خواهند بود».[۷]

قانون جرائم رایانه‌ای ایران در مادهٔ ۲۸ این نظریه را نسبت به سیستم‌های واقع در قلمرو حاکمیت کشور ایران پذیرفته است. مادهٔ مذکور مقرر می‌دارد: «علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود: الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته‌اند به هر نحو در سیستم‌های رایانه‌ای و مخابراتی یا حامل‌های دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد. ب) جرم از طریق وب‌سایت‌های دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد».

برخی این نظریه را به گونه‌ای دیگر و تحت عنوان نظریهٔ «صلاحیت بر اساس محل استقرار سرور»[۸] مطرح کرده‌اند و محل مذکور را همیشه عامل مؤثر تلقی کرده و آن را

---

۵. هکر: فردی که علاقه به کار کامپیوتر ندارد اما از طریق سعی و خطا می‌خواهد آن را فراگیرد.

۶. همان، ص۱۲.

7 .Neal kumar katyal, Criminal law in cyberspace, university of Pennsylvania law rteview vol,149.p.1004.

8. The Theory of The Server.

محل ارتکاب جرم قلمداد کرده‌اند. منظور این است که از آنجا که هر داده و اطلاعاتی که به عنوان وسیله جهت ارتکاب جرم مورد استفاده قرار می‌گیرد حتماً در بستر فضای سایبر تأثیر 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 آن بسیار ضعیف است.

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 قاعدهٔ صلاحیت سرزمینی سنتی را، که مادر قواعد صلاحیتی محسوب می‌شود، اجرا کرده است. چون در واقع جرائم سایبری در جزئی از خاک همان محل ارتکاب یافته است.

در خصوص قابلیت اجرایی چنین نظریه‌ای باید گفت که جهت اجرای این نظریه باید کلیهٔ بزه‌دیدگان جرائم سایبری از سراسر جهان مجبور شوند به سه یا چهار کشور دارندهٔ سرور جهت شکایت مراجعه کنند و نزد محاکم آن‌ها اقامه دعوا کنند و آن مراجع مجبور شوند به صدها هزار پرونده سایبری رسیدگی کنند.[۹] در حالی که چنین عملی مشکل و غیر ممکن می‌نماید و شاید به همین دلیل بوده است که تاکنون کشورهای صاحب این سرورها حتی به فکر اجرایی کردن این نظریه نیفتاده‌اند.[۱۰]

9 . Li.xingan.."*Theories And Practices Of International jurisdiction of cybercrime*".lex *publication, 2004,p.31.*

۱۰ . جلالی فراهانی؛ همان، ص ۱۴.

۲. نظریه محل بار گذاری[۱۱] و پیاده سازی[۱۲ و۱۳]

نظریهٔ دیگری که در خصوص تعیین محل ارتکاب جرائم سایبری با امعان نظر به ویژگی‌های خاص فضای سایبر مطرح گردیده است، نظریهٔ صلاحیت بر اساس محل حضور بارگذاران[۱۴] و پیاده سازان[۱۵] محتوای شبکه‌ای است. قائلین به این نظریه معتقدند فعالیت در فضای سایبر از دو حالت خارج نیست یا باید اطلاعات را در آن قرار داد که به این کار بارگذاری می‌گویند یا اینکه اطلاعات را از فضای سایبر پیاده کرد که به آن پیاده سازی می‌گویند.

بنابراین برای تمام اطلاعات و محتویات فضای سایبر می‌توان یک مبدأ و یک مقصد مشخص کرد که در آن مبدأ یعنی بارگذار محتوای مورد نظر خود را در یکی از اجزای بستر فضای سایبر قرار می‌دهد تا پیاده ساز که مقصد آن محتویات بوده است به آن‌ها دسترسی پیدا کند. در خصوص بارگذاری گفته می‌شود که چنانچه بارگذاری متضمن محتویات یا اعمال غیر قانونی و نامشروع باشد چنین بارگذاری غیر قانونی و مجرمانه است و بدیهی است که محل آن محل ارتکاب جرم است .پیاده سازی هم به این صورت آن را محل ارتکاب دانسته‌اند که افراد تا اطلاعات غیر قانونی را پیاده نکنند عملاً جرمی اتفاق نیفتاده است. اگرچه فعل اصلی از سوی مرتکب جرم اولیه (بارگذار)بوده است ولی تا زمانی که کاربران اینترنتی آن را پیاده نکنند، کامل و در واقع محقق نشده است.[۱۶]

---

۱۱. انتقال یک کپی از یک برنامه، انتقال داده از یک سیستم استفاده کننده به یک سیستم کامپیوتری راه دور.

۱۲. فرایند انتقال اطلاعات از یک سیستم کامپیوتر مرکزی بزرگ به سیستم کامپیوتر کوچک و دور.

13. Location of Downloading And Uploading.

14. Uploader.

15. Downloader.

16 . Ibid,p.33.

۳. نظریه محل تحقق اثر یا نتیجهٔ جرم[۱۷]

مفهوم نتیجه در این تئوری با نتیجه در جرائم مقید سنتی متفاوت است بلکه در این تئوری نتیجه عبارت است از آثار زیان‌بار و مضر جرم که به دیگران می‌رسد اعم از اینکه ناشی از یک جرم مقید باشد یا مطلق. چون برخی جرائم مطلق در فضای سایبر اتفاق می‌افتند ولی چنان اثر زیان‌باری در فضای سایبر و عالم خارج بر جای می‌گذارد که محل تحقق اثر خود می‌تواند نقش مهمی در فرایند دادرسی آن جرم داشته باشد اگرچه آن اثر به عنوان نتیجه یک جرم مقید تلقی نمی‌گردد.

صرف نظر از اینکه کدام یک از جرائم سایبری مطلق و کدام مقید است، این واقعیت غیر قابل انکار است که اکثر آن‌ها آثار سوء خود را نه در یک نقطه که در نقاط بسیاری در سراسر جهان به جای می‌گذارند و این نقاط از چند حیث حائز اهمیت هستند. به این توضیح که میان این نقاط یعنی محل وقوع اثر و حوزهٔ قضایی موبوطه رابطهٔ معنی‌دار و منطقی وجود دارد. همچنین همین نقاط غالباً محل پیاده سازی محتویات شبکهٔ سایبری به عنوان یکی از معیارهای محل ارتکاب جرم طبق نظریات دیگر می‌باشد. بنابراین بهتر است همین نقاط به عنوان محل وقوع جرم سایبری مد نظر قرار گیرد و حوزهٔ قضایی همان محل صالح به رسیدگی به جرائم مربوطه باشد. به عنوان مثال اگر ارسال پیام‌های ناخواسته تا حدی باشد که در قالب یک جرم حمله مانع ارائهٔ خدمات[۱۸] ظاهر گردد به نظر می‌رسد

---

۱۷. این اصل در قوانین کلاسیکی جزایی به عنوان اصل سرزمینی عینی (Objective Territoriality) شناخته شده و آن ناظر به موردی است که جرم در خارج از قلمرو حاکمیتی یک دولت اتفاق می‌افتد ولی تأثیر ابتدائی آن در داخل آن کشور محقق می‌شود که مثال معمول آن را به این صورت بیان می‌کنند: تفنگ‌داری در کانادا به سوی یک آمریکایی بر روی رود نیاگارا شلیک می‌کند و شخصی در نیویورک زخمی می‌شود و می‌میرد که تیر در کانادا شلیک شده و مرگ در آمریکا حاصل شده است بر اساس این اصل کشور آمریکا به خاطر وقوع تأثیر اولیهٔ تیر و مرگ در آن کشور خود را صالح می‌شناسد.

18. Denial of Service Attacks(DOS).

صالح دانستن محل استقرار ارائه دهندهٔ خدماتی که سرور آن آسیب جدی دیده که در واقع همان محل تأثیرگذاری و یا محل وقوع اثر جرم می‌باشد منطقی و عادلانه باشد.[۱۹] کما اینکه یک شخص خارجی که مالک یک سایت مربوط به قمار[۲۰] می‌باشد ممکن است در مقابل عملش، در کشورهایی که قمار ممنوع شده، پاسخگو باشد.[۲۱]

در یک قضیه‌ای که یک دانشجوی آرژانتینی از طریق اینترنت در خانهٔ خود در شهر بوئنس آیرس، به یک شبکهٔ نظامی آمریکایی دسترسی پیدا نمود عمل او نقض حقوق ایالات متحده محسوب شد و او به‌طور ضمنی در ایالات متحده حاضر تلقی شد.[۲۲]

برخی ایالت‌ها در آمریکا مانند ایالت ارکانزاس و ویرجینیای غربی بدون شناسایی محل وقوع اثر به عنوان محل وقوع جرم و به تبع آن محل صالح جهت رسیدگی، از اهمیت آن غافل نمانده‌اند و آن را به عنوان یکی از مبانی تشخیص صلاحیت دانسته‌اند.

در خصوص صلاحیت مراجع قضایی در زمینهٔ فضای سایبر در ایران قانون مجازات جرائم رایانه‌ای مصوب خرداد ماه سال ۱۳۸۸ در بخش دوم، تحت عنوان آیین دادرسی، به این موضوع پرداخته است. مادهٔ ۲۸ این قانون دادگاه‌های ایران را، در جایی که سیستم‌های رایانه‌ای دخیل در ارتکاب جرم در قلمرو حاکمیت ایران باشد، صالح دانسته و در این راستا می‌گوید: «علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند به هر نحو در

---

19 .Brenner.Suan&Koops.Bert.(2004)." *Approaches to Cybercrime Jurisdiction*". Journal of High Technology Law.p.40.

20. Gambling.

۲۱ . زهرا، تحریری؛ جایگاه فضای مجازی در حقوق بین‌الملل، پایان‌نامه کارشناسی ارشد، دانشگاه تهران، ۱۳۸۵، ص ۲۹.

۲۲ . همان.

سیستم‌های رایانه‌ای و مخابراتی یا حامل‌های دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد...». مادهٔ ۲۹ در خصوص نقش محل ارتکاب جرم در صلاحیت تصریح نموده: «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.» مادهٔ ۳۰ در ادامه می‌گوید:« قوهٔ قضاییه موظف است به تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه‌های عمومی و انقلاب، نظامی و تجدید نظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد.

تبصره ـ قضات دادسراها و دادگاه‌های مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب خواهند شد».

مادهٔ ۳۱ هم مقرر می‌دارد: «در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهد بود».

مشاهده می‌شود که قانون‌گذار ایران با عنایت به ویژگی خاص جرائم سایبری؛ یعنی فرامکانی بودن، بدون اهمیت گذاشتن به مکان وقوع جرم به عنوان ضابطهٔ تعیین مرجع صالح توجه خود را به محل کشف یا گزارش آن معطوف کرده است و دادگاه همان محل را صالح به رسیدگی دانسته است. اگرچه کماکان محل وقوع را معیار دانسته ولی به لحاظ صعوبت تشخیص آن محل، به شیوهٔ تعیین محل وقوع نپرداخته و فقط متذکر شده که در صورت مشخص بودن محل وقوع(به هر نحوی) مرجع همان محل صالح می‌باشد.

قانون تجارت الکترونیکی مصوب ۱۳۸۲ هم، که در مورد محل انجام یک عمل

تجاری در تجارت الکترونیکی در مادهٔ ۲۹ قواعدی را بیان کرده است[۲۳]، فصل چهارم آن به بحث صلاحیت جزایی اشاره و مقررات حاکم بر صلاحیت جزایی در خصوص جرائم تجارت الکترونیکی را به سایر قوانین احاله کرده است. در همین راستا با تصویب قانون جرائم رایانه‌ای در خرداد ماه ۱۳۸۸ قواعدی راجع به شیوهٔ اعمال صلاحیت در بخش دوم همین قانون پیش‌بینی شد.

مسألهٔ قابل ذکر این است که در سطح بین‌المللی، مقامات اجرا کنندهٔ حقوق، مانع شکلی، به‌ویژه در استرداد خارجیانی که حقوق داخلی را نقض نموده‌اند، دارند. بنابراین برخی نویسندگان برای فضای سایبر یک صلاحیت جداگانه در نظر گرفته‌اند و فضای سایبر را به عنوان یک فضای جدای از فضای جغرافیایی شناخته‌اند.[۲۴]

بند دوم: ضابطهٔ سیستم دولت متبوع اشخاص دخیل

مبنای اصلی این قاعده تابعیت دخالت کنندگان در جرائم است. در قواعد سنتی صلاحیت، در صلاحیت مبتنی بر تابعیت مرتکب[۲۵] گفته می‌شود که در یک کشور بر

---

۲۳. مادهٔ ۲۹ قانون تجارت الکترونیکی مقرر می‌دارد: «اگر محل استقرار سیستم اطلاعاتی با محل استقرار دریافت «داده‌پیام» مختلف باشد مطابق قاعده زیر عمل می‌شود: الف) محل تجاری، یا کاری اصل ساز (Originator) محل ارسال «داده‌پیام» است و محل تجاری یا کاری مخاطب محل دریافت «داده‌پیام» است مگر آنکه خلاف آن توافق شده باشد. ب) اگر اصل‌ساز بیش از یک محل تجاری یا کاری داشته باشد، نزدیک‌ترین محل به اصل معامله، محل تجاری یا کاری خواهد بود در غیر این صورت محل اصلی شرکت، محل تجاری یا کاری است».

اصل‌ساز: منشأ اصلی «داده‌پیام» است که «داده‌پیام» به وسیلهٔ او یا از طرف او تولید یا ارسال می‌شود اما شامل شخصی که در خصوص داده‌پیام به عنوان واسطه عمل می‌کند نخواهد شد. (بند ب مادهٔ ۱ قانون تجارت الکترونیکی).

۲۴. همان، ص ۳۰.

25. Nationality of Perpetrator.

اساس یک معیار مورد قبول خود قوانین و مقرراتی را وضع می‌کند و به تبع آن انتظار دارد این قوانین از سوی تبعهٔ خود صرف نظر از محل استقرار و یا اقامتش رعایت شود. بنابراین در این قاعده بحث قلمرو سرزمینی و محدودیت‌های فیزیکی ناشی از آن مطرح نیست. بلکه هرکس از تابعیت به مفهوم حقوقی آن برخوردار باشد تحت صلاحیت محاکم کیفری کشور خود قرار می‌گیرد.[۲۶]

امروزه بعضی کشورها به دلایلی حوزهٔ قواعد صلاحیت شخصی را گسترش داده و علاوه بر مرتکبین جرائم، نسبت به اتباع بزه‌دیدهٔ[۲۷] خود نیز اعمال صلاحیت می‌کنند. در این راستا گروهی صلاحیت شخصی نسبت به مجرمین را صلاحیت شخصی فعال[۲۸] و صلاحیت شخصی نسبت به بزه‌دیدگان را صلاحیت شخصی منفعل[۲۹] نامیده‌اند.[۳۰]

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[۳۱] محسوب می‌شود. این نوع صلاحیت در شق د از بند ۱ مادهٔ ۲۲ کنوانسیون بوداپست[۳۲] مربوط به جرائم سایبر به این صورت آمده است: «ماده۲۲(صلاحیت) ۱ـ هر یک از اعضا باید به گونه‌ای اقدام به وضع

26 . W. Brenner,op. cit., p24.

27. Nationality of The Victim.

28. Active Nationality jurisdiction .

29. Passive Nationality Jurisdiction.

۳۰. به همین خاطر نام‌گذاری این قاعده به «ضابطهٔ سیستم قضایی دولت متبوع اشخاص دخیل» مناسب‌ترین عنوان تشخیص داده شد.

31. Territoriality Principle.

۳۲. این کنوانسیون در شهر بوداپست مجارستان، به تاریخ ۲۳ نوامبر ۲۰۰۱ در راستای پیش‌بینی قواعدی در زمینه جرائم سایبر در ۴۸ ماده تهیه شد.

قوانین و مقررات نمایند که در صورت لزوم صلاحیت رسیدگی به هر یک از جرائم مندرج مصوب در مواد ۲ تا ۱۱ این کنوانسیون را در زمانی که جرم در موارد زیر به وقوع می‌پیوندد را به وجود آورند: الف-...ب-...ج-...د-«در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده و از سوی تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرائم واقع در حوزه صلاحیت جهانی حقوق جزا می‌باشد».

در کشور هلند مقرراتی متضمن صلاحیت مبتنی بر تابعیت مرتکب وجود دارد. جعل که شامل جعل کامپیوتری است وقتی که خارج از کشور هلند توسط یک مستخدم حکومت هلند یا مستخدم سازمان‌های بین‌المللی که در هلند مستقر هستند ارتکاب شود چنانچه عمل در کشور محل ارتکاب جرم باشد در هلند قابل مجازات است. و بالاخره هرزه نگاری کودکان[۳۳] وقتی توسط یک تبعهٔ هلند ارتکاب شود بر اساس قوانین هلند قابل مجازات است. و نکتهٔ جالب توجه این است که صلاحیت شخصی همچنین در این کشور در جایی قابل اعمال است که مرتکب جرم بعد از ارتکاب (و قبل از مجازات) تابعیت هلند را کسب کرده باشد.[۳۴]

اصل تابعیت، نسبت به اشخاص حقوقی نیز قابل اعمال است. همان گونه که شعبهٔ آلمانی کامپیوسرو به عنوان یک شرکت آلمانی، تابع حقوق آلمان تلقی و مسئول شناخته شد.[۳۵]

ب) صلاحیت شخصی منفعل یا صلاحیت مبتنی بر تابعیت مجنی‌علیه

این نوع صلاحیت در قلمرو جغرافیایی به دو دلیل، زیاد مورد توجه قرار نگرفته است. اولاً: اعمال صلاحیت نسبت به بزه‌دیده به معنی عدم کفایت قوانین دیگر کشورها در

33. Child Pornography.

34 . W. Brenner, op.cit., P24.

۳۵ . تحریری؛ پیشین، ص ۲۸.

محاکمهٔ مجرمین جرائم است. ثانیاً: مخاطب اصلی فرایند کیفری مجرم است نه بزه‌دیده و لذا حتی اگر یک کشور چنین حقی را برای خود قائل شود باید امکانات و نیروی کافی جهت برگزاری یک رسیدگی عادلانه و مناسب را تدارک دیده باشد. این موضوع اساساً در جایی مطرح می‌شود که محل ارتکاب جرم در خارج از کشور قرار دارد که در این صورت جمع‌آوری ادله و تحقیقات و یا استرداد متهم مشکل خواهد بود. به همین دلیل عده‌ای معتقدند ادعای صلاحیت شخصی تنها در مورد جرائم شدید[۳۶] توجیه‌پذیر است.[۳۷] ولی در نتیجهٔ جرائم سایبری به خاطر نبود برخی مشکلات مذکور و همچنین ماهیت ویژهٔ فضای سایبر، کشورها نسبت به صلاحیت در فضای مزبور رغبت بیشتری از خود نشان داده‌اند. کما اینکه کشور هلند در جرم سایبری مهم یعنی سابوتاژ کامپیوتری[۳۸] و تخریب داده‌ها [۳۹] در جایی که تبعهٔ خود، بزه‌دیده واقع شده است خود را صالح به رسیدگی شناخته است. ایالات متحده آمریکا این قاعده را در جایی قابل اجرا دانسته است که دولت آمریکا بزه‌دیده واقع شده باشد. در این راستا بخش (۳) (a) ۱۰۳۰ عنوان هجدهم قانون فدرال مقرر کرده است: «چنانچه هر شخص عالماً و بدون مجوز به کامپیوتر غیر عمومی[۴۰] یک نهاد یا عامل ایالات متحده دسترسی یابد، قابل پیگرد خواهد بود.» قسمت(b)(۶)(a) بخش مذکور نیز قاچاق متقلبانهٔ عمدی هر گونه گذرواژه‌ای[۴۱] را که امکان دسترسی به کامپیوتر مورد استفاده توسط یا برای دولت ایالات متحده را فراهم می‌آورد مشمول این قانون قرار داده است. شایان ذکر است بسیاری از ایالات آمریکا به تبع این قانون مقررات

36. Serious Offences
37 .Lixingan, op.cit., p.17.
38. Computer Sabotage .
39. Data Damage.
40. Non Public Computer.
41. Traffic In Password.

مشابهی را وضع کرده‌اند.[۴۲]

در بلژیک جرم ارتکابی علیه یک تبعهٔ بلژیک چنانچه جرم در کشور محل ارتکاب قابل مجازات باشد و حداقل مجازات ۵ سال حبس داشته باشد طبق قوانین بلژیک تعقیب می‌شود.[۴۳]

اگرچه با به‌کارگیری تکنولوژی بسیار پیشرفته و انجام تلاش‌های مضاعف امکان تشخیص محل جغرافیایی مرتکب ممکن است ولی مجرمین چنین جرائمی با به‌کارگیری ترفندهای فوق العاده و با استفاده از دانش فناوری بالا و با پیش‌بینی و احتمال چنین عواقبی گاهی محل تشخیص خود را خیلی مشکل و یا غیر ممکن می‌سازند. ولی با این حال همچون تا مجرم شناخته نشود سیستم قضایی دولت متبوع او قابل شناسایی نخواهد بود چالش تعیین مرجع قضایی صالح باقی خواهد ماند. بنابراین باید قاعدهٔ دیگری جستجو شود و یا اینکه در کنار این مبنا مبنای مکمل دیگری پیدا و شناسایی گردد.

بند سوم: ضابطهٔ سیستم قضایی دولت تهدید شده (صلاحیت حمایتی)[۴۴]

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 اگرچه مجرم تبعهٔ آن کشور نباشد و یا اینکه جرم در خارج از قلمرو حاکمیتی آن دولت ارتکاب شده باشد(پور بافرانی، ۱۳۸۲، ص ۴۲). توضیح اینکه یک سری جرائم هستند که به کیان کشورها لطمه وارد می‌آورند و این در حالی است که همانند دیگر جرائم نمی‌توان بزه‌دیده مشخصی را برای آن‌ها در نظر گرفت. همچنین چنین جرائمی

42 . W.Brenner, op.cit., p. 25.

43 . Ibid.

44. Protective Principle.

غالباً از جانب سیستم قضایی محل ارتکاب و یا سیستم دولت متبوع مرتکب جرم انگاری نمی‌شوند چون این جرائم امنیت و منافع یک کشور ویژه را تهدید می‌کنند و نسبت به سایر حاکمیت‌ها (دولت‌ها) متضمن هیچ گونه خطری نیستند و حتی ممکن است با رضایت آن دولت‌ها انجام شوند.[۴۵] بنابراین تعقیب چنین جرائمی بر اساس صلاحیت شخصی و یا صلاحیت سرزمینی قابل اجرا نیست و به نظر می‌رسد بهترین مبنا همان صلاحیت حمایتی باشد.[۴۶]

بنابراین این سؤال مطرح می‌شود که در فضای سایبر اجرای این صلاحیت باز ممکن است؟ و چنانچه اجرای چنین قاعده‌ای در فضای سایبر وجود داشته باشد تا چه میزان قدرت اجرایی آن نسبت به سایر ضوابط تعیین صلاحیت وجود دارد؟ در پاسخ به این سؤال باید گفت که وقتی امنیت کشورها و منافع حیاتی آن‌ها با این فضا گره خورده باشد و از طرف دیگر آسیب‌پذیری آن منافع در مقابل خطرهای جدی و سهل الارتکاب به‌ویژه تهدیدات تروریستی نمود خاصی پیدا می‌کند، دیگر تردیدی باقی نمی‌ماند که بهترین شیوهٔ تأمین امنیت این منافع اجرای قاعده مذکور است. از این حیث تفاوتی نمی‌کند که جرم سنتی باشد یا سایبری. چون در این نوع صلاحیت ملاک تعیین دادگاه صالح، تهدید منافع حیاتی یک کشور است با هر نوع جرمی(اعم از سایبری یا سنتی) که باشد: یعنی نوع جرم و محل ارتکاب و هویت مرتکب (تابعیت او) برای کشور مدعی صلاحیت ملاک نیست.

بنابراین سایبری بودن جرم مانع اجرای قاعدهٔ مذکور نمی‌شود و بلکه از این حیث بهترین نوع صلاحیت محسوب می‌گردد.[۴۷] ولی چالش‌هایی که این نوع صلاحیت با آن

---

۴۵. مثال بارز این گونه جرائم: جاسوسی، اقدام علیه امنیت ملی، جعل پول رایج و دیگر جرائم مشابه است.

46 . W.Brenner,op.cit.

47 . Trachtman. P. Joel. *"Global Cyberterrorism, Jurisdiction, and International Organization"*. P. 32.

مواجه شده است این است که اولاً: اگر جرائمی نظیر اقدامات تروریستی و تخریب رایانه-ای و ضد امنیتی، کشورهای متعددی را با خطر جدی مواجه کنند به گونه‌ای که چنین اقداماتی بر اساس قوانین آن کشورها قابل تعقیب باشند و همهٔ آن کشورها به صلاحیت مذکور در راستای حمایت از منافع خود استناد کنند، تعارض مثبت در صلاحیت به شکلی جدی ایجاد می‌گردد. ثانیاً: کشورهای محل ارتکاب اقدامات مذکور به‌ویژه اقدامات ضد امنیتی و حکومتی و یا دولت متبوع مرتکبین آن‌ها معمولاً چنین اقداماتی را جرم انگاری نمی‌کنند. بنابراین استناد به چنین قاعده‌ای در چنین مواردی با مشکل مواجه می‌شود مگر در موارد خیلی ضروری و در حد متعارف.[۴۸]

کشورهای مختلف چنین صلاحیتی را در قوانین سنتی و جدیداً در قوانین جرائم سایبری خود به رسمیت شناخته‌اند. به عنوان مثال ایالات متحده آمریکا در بخش ۱۰۳۰ عنوان هجدهم خود اصطلاح «کامپیوتر حمایت شده»[۴۹] آورده و در تعریف آن اشعار داشته «کامپیوتری است که در تجارت یا ارتباطات داخلی یا خارجی مورد استفاده قرار می‌گیرد. از جمله کامپیوتر واقع در خارج از ایالات متحده‌ای که استفاده از آن به نحوی است که تجارت یا ارتباطات داخلی یا خارجی ایالات متحده را تحت تأثیر قرار می‌دهد» که قسمت اخیر این تعریف یعنی اشاره به سیستم‌های رایانه‌ای خارج از کشور با تصویب قانون پاتریوت[۵۰] در اکتبر ۲۰۰۱ اضافه شده است تا صلاحیت فرامرزی محاکم این کشور نسبت به جرائم سایبری تقویت گردد.[۵۱]

48 . Lixingan, op.cit.,p. 22.

49. Protected Computer.

50. Patriot Act(Providing Appropriate Tools Required To Interceot And Obstruct Terrorism).

51 . W.Brenner, op.cit., p. 26.

در کشور ما در بند ج مادهٔ ۲۸ قانون مجازات جرائم رایانه‌ای مصوب ۱۳۸۸ صلاحیت واقعی پذیرفته شده است. مادهٔ مذکور در این خصوص مقرر می‌دارد: علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

«...

ج) جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سیستم‌های رایانه‌ای و مخابراتی و وب‌سایت‌های مورد استفاده یا تحت کنترل قوای سه‌گانه یا نهاد رهبری یا نمایندگی‌های رسمی دولت یا هر نهاد یا مؤسسه‌ای که خدمات عمومی ارائه می‌دهد یا علیه وب‌سایت‌های دارای دامنهٔ مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد».

بند چهارم: ضابطهٔ تقدم در تعقیب نسبت به جرائم با خطر جهانی

برخی جرائم متضمن رفتاری مغایر با نظم جهانی و نوع بشر هستند به گونه‌ای که صرف نظر از شخص یا دولت خاصی که جرم علیه او واقع شده علیه تمام ملت‌ها محسوب شده و از مرتکب آن به «دشمن نوع بشر»[۵۲] یاد می‌شود. اقتدار یک دولت بر عهده‌دار شدن تعقیب مرتکب چنین جرائمی را «صلاحیت جهانی»[۵۳] می‌گویند. این قاعده معمولاً مغایر با حقوق بین‌الملل است مگر برای جرائم علیه حقوق بین‌الملل[۵۴] نظیر دزدی دریایی[۵۵]،

52. Hostis Humani Gentium.
53. Universality Nexus.
54. Delicta Juris Gentium.
55. Piracy.

تجارت برده[۵۶]، تعرض به هواپیما یا هواپیما ربایی[۵۷]، نسل کشی[۵۸] و جنایات علیه بشریت.[۵۹و۶۰]

بنابراین هر جرمی را نمی‌توان تحت شمول این قواعد قرار داد بلکه می‌بایست یک توافق بین‌المللی در خصوص ضرورت مقابلهٔ همگانی با آن وجود داشته باشد.[۶۱] همان طور که طی سال‌های اخیر کنوانسیون‌های بین‌المللی متعددی از سوی اکثریت کشورها به تصویب رسید که نشان دهندهٔ شکل‌گیری یک عزم جهانی جدی برای مبارزه با برخی پدیده‌های شوم است. از مهم‌ترین آن‌ها می‌توان به کنوانسیون ملل متحد برای مبارزه با جنایات سازمان‌یافته فراملی که بسیاری از کشورها آن را امضاء کرده‌اند یا کنوانسیون مواد مخدر و روان‌گردان در سال ۱۹۸۸ میلادی اشاره کرد.[۶۲]

در خصوص اجرای این صلاحیت در فضای سایبر، کنوانسیون جرائم سایبری (۲۰۰۱ بوداپست) در مادهٔ ۲۲ صراحتاً بیان کرده است: «هر یک از اعضا باید به گونه‌ای اقدام به

---

56. Slave Commerce.

57. Hijacking.

58. Genocide.

59. Crimes Against Humanity.

۶۰. اگرچه اصولاً صلاحیت جهانی به معنای مداخله در حاکمیت سایر کشورها نیست. زیرا، اولاً: به‌طور کلی پذیرش اصول صلاحیت کیفری فراسرزمینی، در حقوق بین‌الملل منع نشده و عرف بین‌المللی هم آن را پذیرفته است. ثانیاً: توسعهٔ صلاحیت دولت‌ها به معنای داشتن قدرت اجرایی برای ورود به قلمرو حاکمیت کشورهای دیگر نیست، بلکه به این معنا است که دولت‌ها به خود حق می‌دهند که هرگاه جرمی... واقع شود و دستگیری مجرم از راه‌های قانونی ممکن باشد، صلاحیت رسیدگی به جرم ارتکابی او را داشته باشند. (برای مطالعه تفصیلی این موضوع رجوع شود به: فضل اله فروغی، منشاء و ماهیت حقوقی اصل صلاحیت جهانی، مجله مطالعات حقوقی دانشگاه شیراز، دور اول، شماره سوم، زمستان ۱۳۸۸).

61 . Ibid, p. 26.

۶۲ . جلالی فراهانی؛ پیشین، ص ۱۱۵.

وضع قوانین و مقررات نماید که در صورت لزوم صلاحیت رسیدگی به هر یک از جرائم مندرج در مواد ۲ تا ۱۱ این کنوانسیون را در زمانی که جرم در موارد زیر به وقوع می‌پیوندد را به‌وجود آورند: ...د) در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده و از سوی تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرائم واقع در حوزهٔ صلاحیت جهانی حقوق جزا می‌باشد».[۶۳]

اگرچه کنوانسیون مذکور به صلاحیت‌های سرزمینی و شخصی و جهانی پرداخته است و کشورها را مکلف به وضع قوانین در راستای همان صلاحیت‌ها بدون در نظر گرفتن ماهیت فضای سایبر و جرائم ارتکابی در آن کرده است و در واقع شیوه‌های سنتی صلاحیت را بدون به‌کارگیری ملاکی برای اجرای آن‌ها به‌کار برده است. ولی در صلاحیت جهانی(در مقایسه با صلاحیت شخصی و سرزمینی) فضای سایبر با ماهیت ویژهٔ خود نتوانسته است چالش جدی جدیدی به‌وجود آورد. چون در این نوع صلاحیت ملاک و ضابطه، میزان خطری است که به نظم کل جهان و بشریت وارد می‌شود خواه جرم منتج به چنین نتیجه‌ای در فضای غیر ملموس سایبر شده باشد خواه در فضای فیزیکی دریای آزاد و خواه در قلمرو جغرافیایی و حاکمیتی یک کشور معین.

بنابراین ارتکاب جرم مشمول صلاحیت جهانی در فضای سایبر نه تنها بر قابلیت اجرایی قاعدهٔ مذکور تأثیر منفی نگذاشته است بلکه به لحاظ ویژگی‌های خاص چنین جرمی از جمله سهولت در ارتکاب، فراملی بودن، گسترده بودن و صبغهٔ جهانی داشتن آن، حفظ نظم و انسجام جهانی اقتضاء می‌کند که تعقیب آن در سریع‌ترین و راحت‌ترین شکل تدابیر کیفری لازم صورت گیرد. به نظر می‌رسد قاعدهٔ صلاحیت جهانی نسبت به چنین جرائمی که در فضای سایبر اتفاق می‌افتد قابلیت اجرایی جدی‌تر و بیشتری پیدا می‌کند.

---

۶۳. امیر حسین، جلالی فراهانی؛ *ترجمهٔ کنوانسیون جرائم محیط سایبر بوداپست ۲۰۰۱*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوهٔ قضائیه، ۱۳۸۳، ص ۱۱۵.

البته تأکید بر این نکته خالی از لطف نخواهد بود که اجرای این صلاحیت به‌طور کلی و به‌ویژه در خصوص جرائم سایبری در صورتی امکان‌پذیر است که تمام مؤلفه‌های لازم برای اعمال صلاحیت جهانی وجود داشته باشد از قبیل اینکه بایستی در مورد شمولیت آن جرم در صلاحیت جهانی یک اجماع و توافق بین‌المللی به‌وجود آمده باشد مبنی بر اینکه چنین جرمی آن قدر شدید و جدی تلقی گردد که تمامی کشورها می‌توانند با استفاده از صلاحیت جهانی به آن رسیدگی کنند یا مرتکب آن را تعقیب نمایند. به همین علت است که تعداد این جرائم در قلمرو قواعد سنتی صلاحیت، محدود به چند جرم می‌باشند و در فضای سایبر هم به لحاظ جدید بودن آن محدودتر است. چون اجماع و توافق بین‌المللی بر جهانی بودن یک جرم مستلزم گذشت زمان و ایجاد رویهٔ خاص و یا تصویب کنوانسیون ویژه است.

با این حال تاکنون در فضای سایبر نسبت به برخی جرائم نظیر هرزه نگاری کودکان[۶۴] این اجماع و توافق به‌طور نسبی محقق شده ولی هنوز قدرت اجرایی چندانی پیدا نکرده است. همچنین جرم نفوذ غیر مجاز[۶۵] که مادر جرائم سایبری محسوب می‌شود به عنوان یک جرم موضوع صلاحیت جهانی مورد توجه قرار گرفته ولی هنوز یک جرم جهانی محض پذیرفته نشده است. البته جرائم دیگری نظیر انتشار ویروس در برخی موارد و پول‌شویی الکترونیکی[۶۶] به عنوان جرم جهانی مورد توجه کشورهای متعددی قرار گرفته است.

در قانون مجازات جرائم رایانه‌ای ایران مصوب خرداد ماه ۱۳۸۸ در همین راستا و با قبول جرم هرزه نگاری کودکان به عنوان جرم بین‌المللی مشمول صلاحیت جهانی، در مادهٔ

64. Child Pornography.
65. Hacking.
66. Electronic Money Laundering .

۲۸ مقرر شده است که: «علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود... د) جرائم رایانه‌ای متضمن سوء استفاده از اشخاص کمتر از ۱۸ سال، اعم از آنکه مرتکب یا بزه‌دیده ایرانی یا غیر ایرانی باشد».

در پایان باید گفت که با رشد روز افزون تکنولوژی اطلاعات و به تبع آن رشد جرائم سایبری با حدت و شدت و خطرناکی بیشتر و گسترش دایرهٔ بزه‌دیدگی[۶۷] آن‌ها و لزوم مقابلهٔ جهانی با چنین جرائمی تعداد جرائم مشمول صلاحیت جهانی افزایش خواهد یافت. ولی از آنجا که اجرای این نوع صلاحیت صرفاً ناظر به برخی جرائم با ویژگی‌های خاص می‌باشد به گونه‌ای که قسمت اعظم جرائم ارتکابی در فضای سایبر مشمول چنین جرائمی و به تبع آن چنین صلاحیتی نمی‌شوند، بدیهی است که اجرای این صلاحیت راهکار شامل و کاملی در خصوص صلاحیت نسبت به جرائم ارتکابی در فضای سایبر نمی‌باشد. بنابراین سعی در پیدایش یک راهکار مناسب در این زمینه اجتناب ناپذیر است که در مطالب آتی به تئوری‌های مطرح شده در این راستا پرداخته خواهد شد.

گفتار دوم: رویکرد فضای سایبر به عنوان یک فضای آزاد بین‌المللی[۶۸]

با بررسی شیوهٔ اعمال صلاحیت در فضاهای بین‌المللی از آنجا که در این تئوری فضای سایبر به عنوان یک فضای بین‌المللی محسوب می‌شود این نکته باید بررسی شود که تا چه حد می‌توان از روش‌های اعمال صلاحیت در فضاهای مذکور در فضای سایبر

67. Victemizing.

۶۸. این رویکرد توسط Darrel C.Menth در سال ۱۹۹۸ در یک مقاله‌ای تحت عنوان *"Jurisdiction In Cyberspace: A Theory of International Space"* مطرح شده است. این مقاله در سایت زیر قابل دسترسی می‌باشد:

http://www.mttlr.org/volfour/menthe.pdf.

استفاده کرد؟ اگرچه یقیناً دزدی دریایی در یک دریای آزاد خیلی متفاوت از دزدی ادبی و مالکیت فکری در اینترنت است. در یکی در جایی که عمل اتفاق می‌افتد جرم اتفاق افتاده محسوب می‌گردد در حالی که در دیگری یعنی فضای سایبر اینترنت چگونه می‌توان زمان و مکان ارتکاب جرم را مشخص کرد و حتی برخی گفته‌اند که صلاحیت در این فضا بی معنی و بی مورد می‌شود. [۶۹] (Yeargain.John.w,1995:). ولی به‌طور کلی در فضاهای بین‌المللی جغرافیایی، تابعیت اشخاص، عامل اساسی جهت تعیین صلاحیت محسوب می‌شود. و شیوهٔ اعمال صلاحیت حسب محل ثبت یا پایگاه دولت متبوع پایگاه یا کشتی و یا سفینهٔ فضایی اعمال می‌شود.

در زمینهٔ فضای سایبر این عامل دچار بحران می‌شود. چون هرچند الزام ثبت شخصی تمام فایل‌ها و پیام‌ها به موجب معاهدات بین‌المللی غیر ممکن نیست لیکن در حال حاضر چنین نیست و آن زمان هنوز فرانرسیده است. بنابراین باید بر اساس قواعد موجود مسائل را فیصله داد. علی ای حال اشخاص در فضای سایبر از طریق اعمال و افعال‌شان هویت می‌یابند. یک بار گذار، صفحه وب[۷۰] متعلق به خودش را با تابعیت خود ممهور می‌کند اگرچه موقعیت صفحهٔ مذکور ممکن است (در فضای جغرافیایی) مشخص نباشد ولی مسئول یا صاحب آن مشخص است.

تابعیت موضوعات در فضای سایبر را می‌توان از روی تابعیت شخصی یا مجموعه‌ای که آن‌ها را قرار داده یا حتی آن‌ها را کنترل کرده است شناسایی کرد.[۷۱] این بررسی می‌تواند با سازماندهی صفحات وب همخوانی داشته باشد چون شناسایی تابعیت یک

---

69 . Yeargain. John.w, Juisdiction In Cyberpace: Whose LawControls?, Southeastern Louisiana University Zhu Jing, Southeastern Louisiana University p. 5.

70. System Operator.

۷۱ . جلالی فراهانی؛ پیشین، ص ۹.

صفحه وب نسبتاً آسان می‌نماید که عادتاً نام ایجاد کنندهٔ آن در خود صفحه درج شده که یک فرد یا سازمان است. ولی آن‌چه که باید به آن توجه کرد وضعیت افراد یا سازمان‌هایی است که چنین صفحاتی را برای دیگران ایجاد می‌کنند. در واقع بسیار اتفاق می‌افتد مالکان واقعی سایت‌ها، حتی در جریان بارگذاری محتوای مورد نظرشان نیستند و کلیهٔ امور توسط متخصصان فنی و حرفه‌ای مربوط انجام می‌شود.[۷۲] بنابراین وقتی می‌خواهیم بر روی فاعل یک وب سایت متمرکز شویم تا بر این اساس صلاحیت شخصی را پیاده کنیم اولین سؤالی که مطرح می‌شود این است که مالک واقعی وب سایت کیست؟ آیا ایجاد کنندهٔ محتوا و ساختار وب سایت است یا حامی و سفارش دهندهٔ آن یا بالاخره کسی که بارگذاری می‌کند یا حتی متصدی سرور و پشتیبان فنی آن.[۷۳]

اتخاذ هر کدام از این موارد نقش مؤثری در دسترس پذیر کردن محتوای یک وب سایت دارد و به آسانی می‌توان به آن‌ها به مثابهٔ یک فاعل نگریست و بالتبع قواعد صلاحیت شخصی را اعمال کرد هرچند باید دید این قاعده تا چه اندازه قابل اجرا است. به‌طور قطع ابداع‌کنندگان این نظریه به هدفی که از محدود کردن حوزهٔ تعارضات صلاحیت یا انتقال آن از سرزمینی به تابعیت اشخاص دنبال می‌کردند، نائل شده‌اند اما باز هم واقعیات فنی و اجرایی حاکم بر این فضا به گونه‌ای است که معضلات جدی همچنان پا برجا می‌ماند. علاوه بر این، وب سایت‌ها حداکثر یک پنجم فضای سایبر را اشغال می‌کنند و این قاعده بر فرض قبول تنها برای گسترهٔ محدودی از محتویات فضای سایبر راهگشا است.[۷۴]

تئوری بین‌المللی بودن فضای سایبر، آن را از یک مکانی که مورد اعمال

---

72 .Ibid. p. 93.

73 .Ibid. p. 94.

۷۴. همان، ص ۱۰.

صلاحیت‌های متفاوت و متعدد است به یک مکانی که بررسی‌های عادی صلاحیت در آن قابل اعمال است تبدیل کرده است.[۷۵]

پیوندها[۷۶] نسبت به صفحات وب هم نیازمند چنین تحلیلی در خصوص صلاحیت است. شخصی که یک پیوند ایجاد می‌کند نسبت به محتوایی که دسترس‌پذیر می‌سازد موضوع قوانین لازم‌الاجرای کشورش خواهد بود و اشخاصی که از آنجا بارگذاری اطلاعات را انجام می‌دهند موضوع صلاحیت سرزمینی خود قرار می‌گیرند. همچنین دنبال کننده پیوندها که پیاده ساز است[۷۷] موضوع صلاحیت محل استقرار سیستم رایانه‌ای خود قرار می‌گیرد اگرچه رفتار او می‌تواند موضوع صلاحیت شخصی و قوانین حاکم در دولت متبوع خود نیز قرار گیرد. آنچه که تئوری فضاهای بین‌المللی را در این خصوص با مانع مواجه می‌کند این است که پیاده ساز برای اینکه موضوع صلاحیت محل حضور بارگذار قرار بگیرد باید از غیر قانونی بودن پیوندها برای بارگذار[۷۸] آگاه باشد به همین ترتیب مبنایی برای این تئوری باقی نمی‌ماند که دولت متبوع بارگذار قواعدی را نسبت به افعال پیاده ساز خارجی تجویز کند.[۷۹]

تئوری فضای سایبر به عنوان یک فضای بین‌المللی، نمی‌تواند یک روش کاملی برای تعیین دادگاه صالح در زمینهٔ جرائم سایبری باشد و این خود معلول عواملی چند می‌باشد از جمله اینکه فضای سایبر خیلی فراتر از شبکهٔ جهانی گسترده (www) می‌باشد و حتی شامل

---

75 . Ibid.

76. Links.

77. Downloader.

78. Uploader.

79. Uploader State.

تابلوی اعلانات رایانه‌ای[۸۰] میل‌های الکترونیکی[۸۱] گروه‌های یوزنت[۸۲] هم می‌شود و فرستادگان ایمیل هم ممکن است بدون اسم و نشانی باشد که این برای حقوق بین‌الملل مشکل ساز است چون قبلاً اشخاص هویت می‌یابند و بر اساس تابعیت‌شان عمل می‌شد.[۸۳] در حالی که در فضای سایبر یکی از چالش‌های حقوقی موجود صعوبت تشخیص هویت کاربران و وسعت دخالت کنندگان چه به صورت بزه‌دیده و چه به صورت مجرم می‌باشد. مشکل دیگر زمانی بروز می‌کند که ارتباط میان فضای سایبر و وسایل ارتباطات از راه دور نامشخص باشد. وقتی مثلاً یک ایمیل خصوصی از شخصی به دیگری فرستاده می‌شود از خطوط[۸۴] حوزه‌های صلاحیتی مختلفی می‌گذرد و تحت صلاحیت‌های متفاوتی قرار می‌گیرد به گونه‌ای که در یک زمان یک فعل می‌تواند موضوع چندین و چند حوزهٔ صلاحیتی قرار بگیرد و مشکلات صلاحیتی به این ترتیب بدون حل باقی می‌مانند. این مسأله به خاطر ویژگی منحصر به فرد فضای سایبر است که قواعد سنتی حاکم بر فضاهای بین‌المللی فیزیکی را دچار بحران کرده است و خود مقتضی وضع قواعد جدید و حتی امکانات جدید جهت اجرای قواعد مذکور شده است. به همین جهت برخی حقوق‌دانان تئوری دادگاه سایبر یا دادگاه دیجیتالی را مطرح کرده‌اند که به عنوان یک دادگاه کلی و ویژهٔ سایبری با صلاحیتی واحد به تمام جرائم سایبری و یا حداقل فقط نسبت به جرائمی که در خصوص صلاحیت رسیدگی به آن‌ها به‌طور مؤثری اختلاف ایجاد شده باشد، عمل می‌کند. این تئوری در مبحث آتی به تفصیل خواهد آمد.

80. Bulletin Board.
81. Electrnic Mail.
82. Usenet Groups.
83 . Ibid. p. 96.
84. Links.

گفتار سوم: رویکرد دادگاه سایبری(دیجیتالی)[۸۵]

در خصوص دادگاه سایبری و روند حاکم بر آن یکی از محققین و متخصصین در زمینهٔ فضای سایبر و حقوق انفورماتیک[۸۶] در یک مصاحبه‌ای در مورد چگونگی رسیدگی به جرائم ارتکابی در فضای سایبر از جمله مسائل صلاحیت دادگاه‌ها و اقدامات انجام شده در همان راستا بیان کرده است:

«من فکر می‌کنم نهایتاً روزی به این نقطه برسیم که همان طور که جرائم در فضای مجازی (سایبری) و بدون مرز اتفاق می‌افتند دادگاه‌های سایبر و بدون مرز رواج بیابد. هر چیزی که نیاز آن موجود باشد، دیر یا زود به‌وجود خواهد آمد. اگر قرار است که بسیاری از فعالیت‌های مردم در فضای بدون مرز و سایبر انجام بگیرد، چرا رسیدگی به این امور در دادگاه‌های این چنینی انجام نشود، طبیعتاً این دادگاه‌ها هم باید تابعیت‌های فراملیتی داشته باشند یعنی دادگاهی باشد بین‌المللی، با قوانین و مقررات بین‌المللی و لزومی هم ندارد که حتماً محل فیزیکی خاصی داشته باشد. می‌توان از طریق اینترنت و یک تجمع سایبری، دادگاهی برقرار نمود، رسیدگی، انجام و حکم صادر کرد و در نهایت پلیس هم با تجهیز به امکانات انفورماتیکی می‌تواند ضابط این دادگاه باشد من پیش‌بینی می‌کنم این امکانات در آینده ایجاد خواهد شد».[۸۷]

بنابراین می‌توان به قابلیت ایجاد یک دادگاه بین‌المللی در فضای سایبر پی برد که بتواند به تمام جرائم ارتکابی در آن فضا رسیدگی کند و با استفاده از سازوکارهای فضای سایبر و به‌کارگیری کادر متخصص بدون ورود در عالم فیزیکی در تحقیقات و رسیدگی

---

۸۵. المحکمة الرقمیة یا Digital court.

۸۶. دکتر امیر صادقی نشاط استاد در دانشگاه تهران، رئیس کمیسیون حقوقی شورای عالی انفورماتیک و نمایندهٔ سازمان برنامه‌ریزی و مدیریت در کمسیون حقوقی شورای عالی اطلاع رسانی بوده است.

۸۷. نشریهٔ شبکه، ص ۱۱۵.

در همان فضا مبادرت به صدور حکم کند و مجازات آن جرم را اعمال کند. البته ایجاد چنین دادگاهی مستلزم همکاری ویژهٔ بین‌المللی است به گونه‌ای که غالب کشورها در خصوص ایجاد چنین دادگاهی مشارکت داشته باشند و از طریق یک اساسنامه یا معاهده‌ای مساعی خود را با یکدیگر مشترک کنند و برای تمام لوازم دیگر این دادگاه راه‌کارهایی را پیشنهاد دهند و بر آن‌ها توافق کنند و حتی نوع مجازات بایستی سایبری باشد.

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

البته برخی حقوق‌دانان[۸۸] برای رسیدگی به جرائم سایبری در هر کشور پیشنهاد ایجاد یک دادگاه دیجیتالی با ماهیت و سازوکاری متفاوت از دادگاه سایبری مذکور در فوق را داده‌اند و دادگاه دیجیتالی را به این گونه تعریف کرده‌اند:«دادگاه دیجیتالی که ویژهٔ جرائم دیجیتالی[۸۹] 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 می‌باشد».[۹۰]

این دادگاه به جرائم رایانه‌ای خواه جرم به وسیلهٔ رایانه خواه علیه آن ارتکاب شود

---

۸۸ دکتر محمد رضوان کارشناس تحقیقاتی در وزارت دادگستری مصر.

89. Digital Crimes.

۹۰ . محمد رضوان، هلال؛ *المحکمة الرقمیة- مفهوم‌ها و مقومات‌ها*، الطبعة الاولی، القاهره، دار العلم للنشر و التوزیع، ۲۰۰۶، ص ۱۳.

همچنین به جرائم شبکه‌ای و اینترنتی از جمله شبکهٔ جهانی اینترنت و جرائم تلفن‌های سیار یا موبایل رسیدگی می‌کند.

دادگاه دیجیتالی همچنین علاوه بر تجهیزات انسانی و کادر فنی به مکان و جای خاصی جهت استقرار سیستم رایانه‌ای پیشرفته جهت نمایش آنچه بر دیسک‌ها[۹۱] و سی دی‌ها[۹۲] است در سالن دادگاه نیازمند می‌باشد.[۹۳]

تئوری دادگاه سایبری یا دیجیتالی به هر دو شکل آنچه به شکل یک دادگاه فراملی بین‌المللی با کادری مشترک و چه به صورت دادگاه داخلی در هر کشور، با نقص و مشکل مواجه می‌شود. به این توضیح که شکل اول یک تئوری آرمان گرایانه و بلند پروازانه است و از اندیشه و تئوری آن تا محقق ساختن و عملی نمودن آن فاصله نسبتاً دوری وجود دارد. همان طور که در عالم فیزیکی و ملموس و جرائم ارتکابی در آن با آن همه سابقه و قدمتی که دارد کشورهای جهان بعد از تلاش‌های زیاد و پیوسته در ده سال اخیر توانستند یک دادگاه کیفری با ماهیت بین‌المللی[۹۴] ایجاد کنند آن هم:

اولاً: نسبت به تعداد محدودی از جرائم که عبارتند از: نسل کشی[۹۵]، جرائم علیه بشریت[۹۶]، جرائم جنگی[۹۷]، جرم تجاوز[۹۸] قدرت اجرایی و تعقیب دارد.[۹۹]

---

91. Disks.

92. CD.

۹۳. همان، ص ص ۱۷ و ۱۸.

۹۴. اساسنامهٔ این دادگاه در هفدهم ژوئیهٔ ۱۹۹۸ در شهر روم به تصویب ۱۲۰ کشور از مجموع ۱۶۰ کشور شرکت کنندهٔ در کنفرانس دیپلماتیک روم رسید و با الحاق حداقل تعداد لازم از دولت‌ها(۶۰ دولت) از اول ژوئیهٔ سال ۲۰۰۲ لازم الاجرا گشت و قریب یک سال پس از آن عملاً کار خود را در شهر لاهه هلند آغاز کرد.(میر محمد صادقی؛ پیشین، ص۱۳).

95. The Crime of Genocide.

96. Crimes Against Humanity .

97. War Crimes.

ثانیاً: تاکنون از جانب بسیاری از کشورها به‌ویژه قدرتمندترین کشور جهان یعنی ایالات متحده آمریکا مورد امضا و قبول قرار نگرفته است.

ثالثاً: طبق اساسنامهٔ آن راه‌های نفوذ و سنگ اندازی بر روند تعقیب و رسیدگی به کرات مشاهده می‌شود.[۱۰۰]

همچنین اختیاری که برای شورای امنیت در مادهٔ ۱۶ اساسنامهٔ دادگاه مذکور- بر اساس فصل هفتم منشور سازمان ملل متحد- در خصوص امکان به تأخیر انداختن تحقیقات یا تعقیب افراد به مدت دوازده ماه، پیش‌بینی شده است[۱۰۱]، مبین امکان به‌کارگیری اهداف سیاسی در تعقیب متهمان و یا مجرمان از سوی شورای امنیت می‌باشد که این خود حاکی از ضعف دادگاه مذکور جهت رسیدگی به تمام مصادیق و عناوین مجرمانهٔ مصرح در اساسنامهٔ آن است.

بنابراین تشکیل یک دادگاه بین‌المللی در فضای غیر ملموس و فرامرزی و کاملاً

←

98. The Crime of Aggression.

99. Rome Statute of The International Criminal Court, Crimes within the jurisdiction of the Court, Article 5.

۱۰۰. برای مثال دادستان دادگاه کیفری بین‌المللی (ICC) آقای «لوئیز مورینو اوکامبو» اخیراً بنا به درخواست شورای امنیت سازمان ملل متحد شروع به جمع‌آوری ادله و تنظیم کیفرخواست علیه «عمر حسن البشیر» رئیس جمهور سودان به خاطر جنایت‌هایی که در جنوب سودان علیه مخالفین جنوبی از جانب نظامیان دولتی ارتکاب می‌شد، کرده است. در حالی که همان وقت جرائم جنگی و نسل کشی و سایر جرائم بین‌المللی از جانب اسرائیلیان علیه مردم غزه در فلسطین اشغالی ارتکاب می‌شد و همان دادگاه دعاوی بسیاری از وکلا و حقوق‌دانان خواهان محاکمهٔ رهبران اسرائیل را قبول نکرده است و یا در رسیدگی به آن تعلل به خرج داده است.

۱۰۱. مادهٔ ۱۶ اساسنامهٔ دادگاه مذکور در خصوص به تأخیر انداختن تعقیب و تحقیق مقرر می‌دارد: بعد از درخواست شورای امنیت طی یک قطعنامه تحت فصل هفت از منشور سازمان ملل متحد از دادگاه(کیفری بین‌المللی) مبنی بر توقف تحقیق به مدت ۱۲ ماه هیچ تحقیق یا تعقیبی بر اساس این اساسنامه قابل شروع یا پیگیری نیست. درخواست مذکور ممکن است همراه شرایطی باشد.

جدید سایبر که بتواند به تمام جرائم ارتکابی در آن فضا رسیدگی کند و رسیدگی آن مبتنی بر عدالت و اصول پذیرفته شدهٔ حقوقی باشد می‌تواند صرفاً یک آرزو باشد و عملی شدن یا کارایی داشتن آن بعد از ایجاد به گذشت زمان بسیار و تلاش‌های بین‌المللی مضاعف نیاز دارد و شاید غیر ممکن باشد. کما اینکه مسائل مجازات کردن مجرمین و شیوهٔ استرداد آن‌ها و سایر عملیات فیزیکی در چنین دادگاهی دچار بحران می‌شود. اگرچه در خصوص مجازات هم راه‌هایی از قبیل تغییر ماهیت مجازات و سایبری کردن آن مانند محرومیت از یک سری خدمات شبکه‌ای و یا مجازات مالی برای دارندگان حساب مالی وجود دارد. البته در عملی کردن چنین دادگاهی، کشورهای محل سرورهای اصلی اینترنت و شبکه که غالباً در ایالات متحده آمریکا هستند می‌توانند نقش به سزایی داشته باشند.

شکل دوم دادگاه دیجیتالی از آنجا 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. و سؤال اصلی ما را که عبارت است از اینکه دادگاه صالح به رسیدگی به جرائم ارتکابی در فضای سایبر کدام دادگاه است؟ را پاسخ نمی‌دهد چون اگر در یک کشور چندین شعبه دادگاهی از این نوع وجود داشته باشد، حال این سؤال مطرح می‌شود که:

اولاً: در آن کشور کدام یک از این دادگاه‌های مذکور صالح به رسیدگی خواهد بود؟ (صلاحیت محلی)

ثانیاً: میان کشورهای مختلف، نظام حقوقی کدام کشور صالح به رسیدگی می‌باشد؟

بنابراین، این سؤال بر اساس تئوری دادگاه دیجیتالی به شکل دوم بی پاسخ می‌ماند اگرچه این طرح یک نظر بسیار مفید و با ارزشی است ولی در بحث صلاحیت کیفری نمی‌تواند نقش مؤثری داشته باشد.

گفتار چهارم: رویکرد ارتباط حداقلی[۱۰۲] یا ارتباط منطقی[۱۰۳]

به لحاظ اینکه در تئوری‌های پیش گفته همان طور که در جای خود بحث شد به دلیل وجود مشکل تعیین محل ارتکاب جرم و همچنین تابعیت مرتکب و تعدد دخالت کنندگان در یک جرم سایبری اعم از مرتکبان و بزه‌دیدگان ایرادات به جایی مطرح شد به گونه‌ای که به‌کارگیری آن تئوری‌ها دچار بحران و چالش گشت. برای خروج از این بحران و پاسخ گویی به مشکل تعیین حوزهٔ قضایی صالح، برخی ضابطهٔ رابطهٔ حداقلی را مطرح کرده‌اند که در آن معمولاً رفتارهای مختلف بایستی در نظر گرفته شود و بررسی شود که کدام حوزه قضایی حداقل ارتباط لازم جهت رسیدگی به اختلاف را دارد. در این صورت، یک رفتار منفرد و یا یک معامله چنین رابطه‌ای را مشخص می‌سازد.[۱۰۴] 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[۱۰۵] و نه اثر آن در آنجا اتفاق افتاده باشد[۱۰۶] ارتباط حداقلی حاصل نشده است. برای مثال در یک مورد در ایالات متحدهٔ آمریکا عملی را به دلیل ضعف ارتباط حداقلی، صلاحیت ایالت مدعی صلاحیت رد شده است و همچنین در مورد دیگر تلاقی و گفتگوی مدیران شرکت‌ها در یک ایالت کافی شناخته نشده است.[۱۰۷] برخی اصل ارتباط حداقلی را ناتوان از پاسخگویی به صلاحیت

---

102. Minimum Contacts.

103. Reasonable Contact.

104 . Koepsell. David.R, an emerging ontology of jurisdiction in cyberspace, ethics and information technology, luwer ecodemic publishers. 2000, P100.

105. Executed.

106. Deliverd.

107 . Ibid. p101.

مراجع قضایی در شبکهٔ جهانی دانسته‌اند.[۱۰۸] در حالی که برخی دیگر از نویسندگان، تئوری رابطهٔ حداقلی که بیشتر در موارد مدنی مورد استفاده قرار می‌گیرد را به گونه‌ای دیگر و تحت عنوان «ارتباط منطقی» در خصوص موارد کیفری بیان کرده‌اند. این تئوری اگرچه بیشتر در کشورهای پیرو حقوق کامن لا به لحاظ اینکه این نظام حقوقی در استناد به قواعد عرفی بیش از هرچیز مسألهٔ انصاف و منطق را مد نظر قرار می‌دهد قابلیت اجرایی پیدا می‌کند ولی می‌تواند یک تئوری عامی باشد که در تمام نظام‌های حقوقی کاربرد داشته باشد.

در بحث «ارتباط منطقی» مرجع قضایی این مسأله را بررسی می‌کند که متهم در جرائم واقعه در فضای سایبر تا چه اندازه موفق به برقراری ارتباط اینترنتی با بزه‌دیده شده و آیا این میزان برقراری ارتباط کافی است تا دادگاه یا مرجع قضایی محل اقامت یا شکایت بزه‌دیده صالح به رسیدگی به اتهام مزبور باشد یا خیر؟ برای نمونه اگر در ایالت کالیفرنیا صدها شهروند کالیفرنیایی در اثر ارتباط با یک وب سایت و مانورهای متقلبانهٔ گردانندگان آن سایت اقدام به واریز مقادیر در خور توجهی پول به حساب‌های معرفی شده در سایت کرده و بزه‌دیدهٔ کلاهبرداری شده باشند، چنانچه مرجع قضایی این برقراری ارتباط میان سایت یادشده و کاربران یعنی مال‌باختگان را از نظر منطقی مبنای رسیدگی خود قرار دهد، خود را صالح به رسیدگی به اتهام کلاهبرداری علیه شهروندان مال‌باختهٔ کالیفرنیایی دانسته و شروع به رسیدگی خواهد کرد. ولی چنانچه در مقابل شهروندان کالیفرنیایی بدون توجه به تبلیغات فریبنده وب سایت مزبور یا با وجود همهٔ تلاش مدیران سایت جهت جلب نظر مخاطبان خود ارتباطی در خور توجهی با این سایت برقرار نکنند، دادگاه به این نتیجه

108 . M.juliut." *A Separate Jurisdiction For Cyberspace*". Journal of Computer-Mediated Communication. Volume 2 Issue 1.[online].< http://www.blackwell-synergy.com/doi/full/10.1111/j.1083-6101.1996.tb00186.x.[18 sep 2008].2006.p.3.

خواهد رسید که عدم برقراری ارتباط میان سایت مخاطبان (شهروندان کالیفرنیایی) یا حتی اندک ارتباط موجود میان آن‌ها، به اندازه‌ای نیست که بتوان بر مبنای آن دادگاه کالیفرنیا را حائز صلاحیت برای رسیدگی قضایی به جرم مذکور دانست.

تشخیص این امر که ارتباط پدید آمده در چه حد از اهمیت است و این اندازه ارتباط برای احراز صلاحیت دادگاه محل اقامت بزه‌دیدگان کافی است یا خیر؟ بر عهدهٔ خود دادگاه است و ملاک و معیار این تشخیص عرف، منطق و رویهٔ قضایی خواهد بود.

در این تئوری آن‌چه مهم ارزیابی می‌شود احراز رابطهٔ معنادار و منطقی و متعارف میان سیستم‌های رایانه‌ای و مخابراتی مربوطه و جرم ارتکابی و دخالت کنندگان در جرائم با مرجع قضایی ذی صلاحی است که می‌خواهد به آن رسیدگی کند.[۱۰۹]

بنابراین در این تئوری سایر تئوری‌های مطرح شده طریقیت پیدا می‌کنند و به عنوان یک وسیله جهت تعیین درجهٔ ارتباط جرم با کلیهٔ ارکان آن و همچنین دخالت‌کنندگان در آن با محل مورد نظر جهت رسیدگی به آن جرم نمود پیدا می‌کنند. برای مثال محل استقرار کامپیوترهای تأثیرگذار در وقوع جرائم دیگر نه به عنوان محل ارتکاب جرم و در نتیجه اجرای قواعد سنتی صلاحیت-یعنی شایستگی محل وقوع جرم-بلکه صرفاً از آن جهت مورد توجه قرار می‌گیرد که جرم بیشترین ارتباط و یا ارتباط منطقی را با این مکان برقرار کرده است و در نتیجه به عنوان محل صالح برای رسیدگی به جرم سایبری شناخته شود. همان طور که برخی ایالت‌های آمریکا نظیر ایالت کانکتیکات[۱۱۰] در خصوص رسیدگی به پرونده‌های جرائم سایبری خود مقرر کرده «چنانچه کامپیوترهای واقع در ایالت در تحقق

---

۱۰۹. محمد حسن، دزیانی؛ *مبانی صلاحیت کیفری در فضای سایبر*، کار پژوهشی شورای عالی انفورماتیک، ۱۳۸۴، ص ۱۶.

110. Connecticut .

جرم تأثیر قابل توجهی[۱۱۱] داشته باشد، محاکم این ایالت صالح به رسیدگی خواهند بود.[۱۱۲]

مادهٔ فوق صلاحیت ایالت مذکور را نه به دلیل وقوع جرم در محل استقرار سیستم کامپیوتری-یعنی خود ایالت-تعیین کرده است بلکه از آن لحاظ این ایالت را صالح به رسیدگی شناخته است که جرم مذکور ارتباط منطقی با آن داشته است. چون یکی از مشکلات و چالش‌های حقوق کیفری در فضای سایبر تعیین محل ارتکاب جرم است به همین خاطر این ایالت همانند برخی از ایالت‌ها یا دولت‌های دیگر در قانون خود بدون پرداختن به محل ارتکاب جرم، ضوابطی از قبیل تأثیر قابل توجه، گستردگی خسارت‌ها و یا تعدد قربانیان تبعهٔ یک حوزهٔ قضایی را مطرح کرده‌اند که این خود مبین رعایت ضابطهٔ «ارتباط منطقی» می‌باشد.

این ضابطه از نظر رویهٔ عملی هم در آمریکا جایگاه ویژه‌ای دارد. در یک مورد[۱۱۳] یک شرکت توزیع کنندهٔ نرم افزار در ایالت آریزونا علیه یک شرکت نرم افزاری در نیومکزیکو اقامهٔ دعوی نمود که علت آن هم انقضای توافق‌نامهٔ مابین شرکت‌ها و اظهارات آشکار خوانده پیرامون انقضای قرارداد بوده است. خواهان مدعی توهین و افترا در چارچوب قانون و نقض حقوق مارک تجاری بود. تماس‌ها و ارتباط خوانده با آریزونا، که بر اساس معیار «بهره مندی عمومی»[۱۱۴] تجزیه و تحلیل شد، باعث پذیرش صلاحیت ایالت مذکور گردید.[۱۱۵]

همان‌طور که در ابتدای بحث گفته شد اگرچه این تئوری غالباً در نظام حقوقی کامن

---

111. Impact.

112 . Neal Kumar katyal, op.cit., p.106.

113. Edias Software International V.Basis International.ITD.

114. Perposeful Availment.

115 . George m.Perry & others, Personsl Jurisdiction In Cyberspace, Were Can You Be Sued. And Whose Laws Apply? New York,NY. 1998. P.8.

لا و در کشورهایی از جمله ایالات متحده آمریکا قابلیت اجرایی پیدا می‌کند و به لحاظ اینکه کشورهای تابع نظام حقوقی نوشته بیشتر بر اساس نصوص قانونی از پیش تدوین شده عمل می‌کنند تا عرف و منطق حقوقی و لذا این قاعده کمتر قابل اجرا می‌باشد، ولی با توجه به اینکه اولاً: فضای سایبر یک فضای جدیدی است که نیازمند وضع قواعد جدید در زمینهٔ حقوق به‌ویژه حقوق کیفری است. ثانیاً: کشورهای پیرو نظام حقوقی نوشته می‌توانند با وضع قوانین جدید این ضوابط را به صورت مکتوب در آورند و بر اساس آن‌ها عمل نمایند. بنابراین به‌کارگیری این ضابطه با رعایت شرایط مزبور، خلاف اصول کلی در این نظام حقوقی محسوب نمی‌گردد.

نتیجه‌گیری

با بررسی قواعد سنتی حاکم بر شیوهٔ تعیین مرجع قضایی کیفری صالح نسبت به جرائم ارتکابی در فضای جغرافیایی و امکان تسری آن قواعد نسبت به جرائم ارتکابی در فضای سایبر دیده شد که اگرچه برخی قواعد از قبیل قاعدهٔ «صلاحیت دولت متبوع اشخاص دخیل در ارتکاب جرم»، « صلاحیت دولت با منافع تهدید شده» و یا «صلاحیت دولت مقدم در تعقیب در جرائم با خطر جهانی» به لحاظ تأثیر کم ماهیت فضای محل ارتکاب جرم در اجرای آن‌ها، در این مورد قابلیت اجرا دارند. ولی از یک طرف در فضای سایبر مرزی وجود ندارد تا به روشنی بتوان به قاعدهٔ صلاحیت سرزمینی استناد کرد. از طرف دیگر امکان بهره‌مند شدن از هویت‌های چندگانهٔ متفاوت در فضای سایبر، اعمال صلاحیت تابعیت را در هاله‌ای از ابهام فرو می‌برد. وجود بزه‌دیدگان بی شمار و امکان آسیب رساندن به تأسیسات حیاتی چندین کشور در یک زمان، استناد به قواعد میان بری نظیر صلاحیت حمایتی را با مشکلات بسیار مواجه ساخته است. در نهایت با این‌که معضل جرائم سایبری فراگیر شده، ولی هنوز اما و اگرهای بسیاری در خصوص آن مطرح است که این خود تمسک به صلاحیت جهانی را نیز مشکل می‌سازد. بنابراین طرح راهکارها و تئوری‌های جدید اجتناب ناپذیر می‌نماید و ناچار باید به فکر قواعد تازه‌ای بود که با ماهیت این فضا سازگاری داشته و قابل اجرا باشند. در همین راستا برخی دانشمندان و نویسندگان تئوری‌های جدیدی را از قبیل «*تئوری فضای سایبر به عنوان یک فضای آزاد بین‌المللی*»- به گونه‌ای که هم عرض با سایر فضاهای بین‌المللی دیگر، از قبیل دریاهای آزاد و فضای ماورای جو و قطب‌ها، باشد-، «*تئوری دادگاه دیجیتالی یا سایبری*»- که به صورت مجازی به تمام جرائم ارتکابی در فضای مذکور رسیدگی می‌کند- و یا «*تئوری حداقل ارتباط لازم*» و یا به عبارتی داشتن ارتباط منطقی جرم با یک کشور، با ادعای سازگار بودن آن‌ها با فضای سایبر، مطرح کرده‌اند که هر کدام از زاویه‌ای دارای ایراد و چالش می‌باشد.

به عنوان راهکار می‌توان گفت تئوری سوم می‌تواند با اقدامات تکمیلی دولت‌های مختلف راهکاری برای خروج از چالش باشد. برخی جرائم معدود دیگر، علی‌رغم وجود ابهام در اجرای صلاحیت‌های سنتی، بر اساس صلاحیت حمایتی یا جهانی قابل رسیدگی هستند. اگرچه در اجرای آن مسألهٔ استرداد مجرمین می‌تواند به عنوان چالشی بر سر راه آن محسوب گردد ولی اشکال در اجرای صلاحیت منافاتی با قبول اصل آن ندارد. بنابراین صلاحیت واقعی و جهانی بدون در نظر گرفتن محل وقوع جرم می‌توانند نسبت به جرائم سایبری اجرا شوند. در جایی که ملاک تعیین صلاحیت بر اساس قواعد سنتی مکان وقوع جرم باشد به لحاظ عدم قابلیت اجرایی صلاحیت سرزمینی به ناچار باید قاعدهٔ دیگری را جایگزین آن کرد که به نظر می‌رسد با عنایت به مشکل و یا غیر قابل تشخیص بودن محل وقوع جرم در فضای سایبر بهترین نوع صلاحیت، صلاحیت مبتنی بر *تئوری ارتباط حداقلی یا منطقی* میان جرم و یک دولت (تئوری سوم مذکور در فوق) باشد. در این صورت باید تئوری مذکور را به عنوان اصل در راستای تشخیص صلاحیت مراجع قضایی دانست و سایر تئوری‌ها از قبیل محل بارگذاری و یا پیاده سازی، محل استقرار اشخاص یا سیستم‌های دخیل و یا محل تحقق اثر و نتیجه و...-که در راستای تعیین مکان وقوع جرم مطرح شده‌اند- می‌توانند در خدمت این تئوری جهت تعیین حداقل ارتباط لازم و منطقی میان یک مکان و جرم واقعه به‌کار گرفته شوند. با این توضیح که قواعد حاکم بر تعارض صلاحیت‌ها همچنان در خصوص تعارض صلاحیتی نسبت به جرائم سایبری باقی می‌باشد ولی در این‌جا دیگر به عنوان ضابطه‌ای مستقل محسوب نمی‌شوند بلکه در راستای تشخیص ارتباط بیشتر جرم یا نتایج حاصل از آن با یک مکان(حوزهٔ قضایی) خاص به‌کار می‌آیند و به این ترتیب نظام قضایی و حوزهٔ قضایی صالح را مشخص می‌کنند. این امر نیازمند همکاری بین‌المللی دولت‌ها به‌طور جدی و پیش‌بینی کنوانسیون‌های ناحیه‌ای و جهانی و تثبیت قواعدی مقبول می‌باشد. همان‌طور که در بند ۵ مادهٔ ۲۲ کنوانسیون جرائم سایبری بوداپست مجارستان بر این مسأله، یعنی به شور نشستن کشورهای ذی‌نفع جهت تعیین

مناسب‌ترین و شایسته‌ترین عضو صالح به تعقیب و رسیدگی، تأکید شده است.

در کشور ایران، قانون جرائم رایانه‌ای مصوب خرداد ۱۳۸۸ مطالبی را در مواد۲۸، ۲۹، ۳۰ و ۳۱ به مسألهٔ صلاحیت اختصاص داده است. در بندهای الف و ب مادهٔ 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 دامنهٔ مرتبهٔ بالای کد کشوری ایران، قاعدهٔ 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 صلاحیت جهانی را برای رسیدگی به جرائم سایبری پیش‌بینی کرده است.

در خصوص تعارض صلاحیت در حوزه‌های قضایی داخلی اگرچه مادهٔ ۳۱ قانون مارالذکر مقرر کرده است که حل اختلاف در خصوص صلاحیت مطابق مقررات قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی خواهد بود. ولی برای سهولت رسیدگی می‌توان با تصویب قانونی و تأسیس یک هیئت یا شعبه مرکزی در پایتخت، در خصوص رسیدگی به جرائم سایبری در نقاط مختلف کشور، به همهٔ مراجع قضایی داخلی تکلیف کرد تا در صورت دریافت هرگونه گزارش از مقام صلاحیت‌دار یا دریافت شکوائیه و یا مشاهدهٔ هر نوع جرم از جرائم سایبری بلافاصله شعبهٔ مرکزی را در جریان امر قرار داده و منتظر تعیین تکلیف از آن باشند.

منابع

الف: فارسی و عربی

۱. برنر، سوزان (۱۳۸۴)؛ *صحنهٔ جرم سایبری*، ترجمه داریوش باقریان، شورای عالی انفورماتیک.

۲. پور بافرانی، حسین(۱۳۸۲)؛ *اصل صلاحیت واقعی در حقوق جزای بین‌الملل و ایران*، مجلهٔ حقوقی دادگستری، شماره ۴۲.

۳. پور بافرانی، حسن (۱۳۸۱)؛ *ماهیت و انواع صلاحیت در حقوق جزای بین‌الملل*، ص ۱۶۵، مجلهٔ مجتمع آموزش عالی قم، شماره ۱۲.

۴. تانن بام، اندوراس(۱۳۷۶)؛ *شبکه‌های کامپیوتری*، ترجمهٔ محمدقدسی، شورای عالی انفورماتیک.

۵. تحریری، زهرا؛ جایگاه فضای مجازی در حقوق بین‌الملل، پایان‌نامه کارشناسی ارشد، دانشگاه تهران، ۱۳۸۵.

۶. جاوید نیا، جواد (۱۳۸۷)؛ جرایم تجارت الکترونیکی، چاپ اول، تهران، انتشارات خرسندی.

۷. جعفر پور، ناهید(۱۳۸۲)؛ ترجمهٔ توصیه‌نامهٔ آر(۹۵) ناظر به مشکلات آیین دادرسی کیفری مربوط به فناوری اطلاعات و گزارش توجیهی مصوبه کمیته وزرای اروپا: سپتامبر ۱۹۹۵، خبرنامهٔ انفورماتیک، شماره ۸۱

۸. جلالی فراهانی، امیرحسین(۱۳۸۴)؛ *پول‌شویی الکترونیکی*، فصلنامهٔ تخصصی فقه و حقوق، سال اول، شمارهٔ چهارم.

۹. جلالی فراهانی، امیر حسین(۱۳۸۳)؛ *ترجمهٔ کنوانسیون جرائم محیط سایبر بوداپست ۲۰۰۱*، چاپ اول، تهران، مرکز مطبوعات و انتشارات قوهٔ قضاییه.

۱۰. جلالی فراهانی، امیر حسین (۱۳۸۵)؛ *صلاحیت کیفری در فضای سایبر*»، نشریهٔ فقه و حقوق، سال سوم، شماره ۱۱.

۱۱. جلالی فراهانی، امیر حسین (۱۳۸۵)؛ *تروریسم سایبری*، فصلنامهٔ تخصصی فقه و حقوق، شماره ۳۵.
۱۲. حسن بیگی، ابراهیم (۱۳۸۴)؛ حقوق و امنیت در فضای سایبر، چاپ اول، تهران، مؤسسهٔ فرهنگی تحقیقات ابرار معاصر تهران.
۱۳. خبرنامهٔ انفورماتیک، (۱۳۸۴) شماره ۸۱.
۱۴. دزیانی، محمد حسن (۱۳۸۴)؛ *صلاحیت سایبری*، بخش اول، شورای عالی انفور ماتیک.
۱۵. دزیانی، محمد حسن (۱۳۸۴)؛ *مبانی صلاحیت کیفری در فضای سایبر*، کار پژوهشی شورای عالی انفورماتیک.
۱۶. دزیانی، محمد حسن (۱۳۷۷)؛ گزارش توجیهی جرائم رایانه‌ای. شورای عالی انفورماتیک.
۱۷. دولت شاهی، شاهپور (۱۳۸۳)؛ *صلاحیت قضایی در محیط مجازی* مجموعهٔ مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات توسط معاونت و توسعه قضایی قوهٔ قضاییه.
۱۸. ریک، کاسپرسن (۱۳۷۶)؛ تعقیب بین‌المللی جرم کامپیوتری، ترجمه محمد حسن دزیانی، شورای عالی انفورماتیک.
۱۹. عبابنه، محمود احمد(۲۰۰۵)؛ جرائم الحاسوب و ابعادها الدولیه، الطبعه الأولی، عمان، دارالثقافه للنشر والتوزیع.
۲۰. فروغی، فضل الله (۱۳۸۷)؛ *مطالعه تطبیقی اصل صلاحیت جهانی در حقوق کیفری آلمان و آمریکا*، ص ص ۲۶۱-۲۸۳، فصلنامهٔ حقوق، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، دوره ۳۸، شماره دوم.
۲۱. فروغی، فضل الله (۱۳۸۸)؛ منشاء و ماهیت حقوقی اصل صلاحیت جهانی»، ص ص ۲۱-۴۷، مجله مطالعات حقوقی دانشگاه شیراز، دور اول، شماره سوم.

۲۲. فوریستر، توم(۱۹۸۹)؛ التقنیة العالمیة، قصه ثوره تقنیه المعلومات، الطبعه الإولی، عمان، منشورات مرکز الکتب الأردنی.
۲۳. گزارش توجیهی قانون مجازات جرائم رایانه‌ای، شورای عالی انفورماتیک، ۱۳۸۳.
۲۴. میر محمد صادقی، حسین (۱۳۸۳)؛ دادگاه کیفری بین‌المللی، چاپ اول، تهران، نشر دادگستر.
۲۵. میر محمد صادقی، حسین (۱۳۷۷)؛ حقوق جزای بین‌الملل (مجموعه مقالات)، تهران، نشر میزان.
۲۶. نشریه شبکه، ۱۳۸۵.
۲۷. هلال، محمد رضوان(۲۰۰۶)؛ المحکمة الرقمیة- *مفهومها و مقومات‌ها*، الطبعه الإولی، القاهره، دار العلم للنشر والتوزیع.

ب: لاتین

28. Darrel.C.menthe.(1998). "jurisdiction in cyberspace:A Theory Of International Spaces". 4 Mich. Telecomm. Tech. L. Rev. 69, available at <http://www.mttlr.org/volfour/menthe.pdf>.
29. Geist. Michael."Globol internet jurisdiction".[on line].<Http://www.anescap.org/tid/ Projects/ ecom o4-s6ageist.pdf[12 dec 2008]
30. George m.Perry & others.(1998)."Personsl Jurisdiction In Cyberspace, Were Can You Be Sued. And Whose Laws Apply? "New York,NY.
31. Henry. Hand Perritt. J ." the internet is changing. the Public internation leyal system" .chicago kent Collye of low.[online].http://www. kentlaw. edu / cyber law / perrthe po Tchg . htm.[7 nov 2008].

32. Koepsell. David.R. (2000) an emerging ontology of jurisdiction in cyberspace, ethics and information technology, luwer ecodemic publishers.

33. Li.xingan.(2004)."Theories And Practices Of International jurisdiction of cybercrime".lex publication.

34. Mark A.Lemley,"Place and cybersPace".UCBerkeley School of Law ,publilaw and legal theory Research PaPer no , 102 , 2003..[online].< http://papers.ssrn.com/ sol3/ papers.cfm?abstract_id=349760.[25 nov 2008]

35. M.juliut.(2006)." A Separate Jurisdiction For Cyberspace". Journal of Computer-Mediated Communication. Volume 2 Issue 1.[online].< http://www.blackwell-synergy.com/doi/full/10.1111/j.1083-6101.1996.tb00186.x.[18 sep 2008]

36. Nauss.E.Susan." Personal jurisdiction:lost in cyberspace".2003 .p23[on line]. <http: www.sum.edu/scr/articles/2003/fall/exon-pdf.[14 sep 2008]

37. Neal kumar katyal,(2001) Criminal law in cyberspace, university of Pennsylvania law rteview vol,149.p.1003.

38. Trachtman. P. Joel.(2004)." Global Cyberterrorism, Jurisdiction, and International Organization", This paper was prepared in connection with the Conference on the Law and Economics of Cybersecurity, George Mason University School of Law. [online]:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=566361[16 Jul 2008]

39. W.Brenner.Susan."Cybercrime Jurisdiction".Crime Law Soc Change .2006.46: 189–206 DOI 10. 1007/s 10611-007 -9063-7. [online]. < 46 http://www. springerlink.com/content/e115601u0337ug25/fulltext.pdf.[20 Feb 2009]

40. W.Brenner.Suan&Koops.Bert.(2004)." Approaches to Cybercrime Jurisdiction".

Journal of High Technology Law.[online].< http://papers.ssrn.com/ sol3/ papers. cfm? abstract_id=786507.[19 sep 2008]

41. Yeargain.John.w.(1995)."Juisdiction In Cyberpace: Whose LawControls?". Southeastern Louisiana UniversityZhu Jing, Southeastern Louisiana University.p5 [online]: http://calbar.ca.gov/calbar/pdfs/sections/buslaw/2001-spring-meeting_ rice_ jurisdiction-in-cyberspace.pdf[18 feb 2008].