ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

شماره مجوز مجله:۸۰۴۰۰ زمان چاپ:۱۴۰۳/۰۲/۲۵

حل و فصل اختلافات ناشی از جرائم سایبری در حقوق بین الملل

مهرداد فلاحی[۱]، اکبر رجبی[۲]

۱-دانش آموخته PHD حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد خمین

۲-استاد یار و مدیر گروه دانشگاه آزاد اسلامی واحد خمین

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

چکیده

در عصر دیجیتال و شکل گیری یک جامعه اطلاعاتی بزرگ ناشی از حرکت به سمت کسب و کارهای الکترونیکی مسئله حفاظت امنیت اطلاعات و داده های امری است حیاتی که متاسفانه با سامانه های امنیت شبکه و... به طور کامل پوشش داده نمی شود و اینجاست که تهدیدات سایبری به عنوان یک راه حل نقش پر رنگ تری به خود می گیرد. امروزه فضای مجازی و جرایم ناشی از آن به معضل مهم جوامع بشری تبدیل شده مزاحمان سایبری برای کاهش ریسک اعمال مجرمانه خود، بسترهای فضای مجازی را به عنوان حقیقی و سنتی ترجیح می دهند انجام امور مجرمانه در شبکه های اجتماعی ممکن است غیر واقعی (فیک) باشند، تبه کاران نسبت به انجام امور مجرمانه و تروریستی در فضای علاقه بیشتری نشان می دهند.

فناوری اطلاعات روز به روز در حال تکامل و پیشرفت بوده و تا لایه های پایین و جزئی جوامع بشری نفوذ پیدا کرده است. فضای سایبری زاییده این فناوری است. فضایی که با دارا بودن ویژگی های منحصر به فرد، می تواند بستر سازی جرایم خاص و پیچیده ای همانند جرایم علیه تمامیت و صحت داده ها باشد.

باید توجه داشت که اطلاعات دیجیتال نه تنها مزایای را ارائه می دهد، بلکه تهدیدهای امنیتی نیز ایجاد می کند. در مدیریت این تهدیدات، امنیت سایبری از اهمیت بالایی برخوردار است.

کلید واژه : حل و فصل اختلافات سایبری – جرایم سایبری - مفهوم سایبر و مبانی جنگ سایبری – قواعد حاکم در بعد بین الملل ، ماهیت بین الملل جرائم سایبری

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

مقدمه

جرایم سایبری را می توان به عنوان فعالیت های رایانه ای در نظر گرفت که یا غیر قانونی هستند یا توسط طرف های خاصی غیر قانونی تلقی می شوند و این فعالیت ها می توانند از طریق شبکه های جهانی انجام شوند .

فناوری اطلاعات مدرن به خوبی توسعه یافته است و تقریباً همه از ویژگی های فناوری اطلاعات و خدمات در اینترنت استفاده می کنند. با این حال مردم به دلیل تحقیقات امنیت سایبری تحت تاثیر قرار می گیرند. مردم می توانند به دستورالعمل های توصیه شده امنیت سایبری، قوانین، استانداردهای اتخاذ شده و اقدامات پیشگیرانه از جرایم سایبری برای کاهش تا حد زیادی این تهدیدات پایبند باشند. ناآگاهی یا فقدان دانش امنیت سایبری نیز باعث ایجاد یک مشکل اساسی در رابطه با محرمانگی و حریم خصوصی می شود. نمی توان به طور کامل از جرایم سایبری چه اغلب منجر به زیان تجاری کافی و انتشار مضامین ممنوع (انزجار، افراط گرایی، پورن کودکان و غیره) می شود، اجتناب کرد.

باید توجه داشت که در حوزه ی جرایم سایبری، مرز جغرافیایی چندان محلی از اعراب نداشته و به طور عمده مجرمان به صورت بین المللی دست به اقدامات مجرمانه می زنند. بنابراین مشخص بودن سیاست های داخلی یک کشور در مبارزه با جرایم سایبر، در مجموع راهگشا نبوده و اجماع جهانی در این زمینه لازم است. تا زمانی که اختلافات بین رویه های کشورها در قبال برخورد با جرایم سایبری ادامه داشته باشد، مجرمان با شناسایی و درک خلاهای قانونی موجود جهت انجام فعالیت مجرمانه خود، از این خلاء های قانونی موجود بهره خواهند برد. بنابراین حل و فصل اختلافات ناشی از جرایم سایبری در بستر حقوق بین الملل می توان رویه ی عملکرد کشورها در قبال برخورد با جرایم سایبری را بهبود بخشیده و گامی موثر در جهت کاهش جرائم سایبری، به ویژه در سطح بین المللی باشد.

همکاری های بین المللی حقوقی، با هدف جلوگیری از فرار مجرمان بین کشورها در زمینه های مختلف مجرمانه از دهه های گذشت انجام می شده است. ویژگی فضای سایبر، نداشتن مرز و عدم اهمیت مکان فیزیکی مجرم است. کما اینکه مجرمانه سایبری در برخی موارد از مکانی بسیار دور اقدام به انجام اعمال مجرمانه می کنند و همکاری بین المللی حقوقی برای جلوگیری از جرم در فضای سایبر و پیگیری و دستگیری مجرمان، بسیار پیچیده تر از سایر جرایم به ویژه جرائم سنتی می باشد.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

فصل اول

۱-۱-مبانی نظری حل و فصل اختلافات ناشی از جرایم سایبری

۲-۱-۲ ماهیت و خصایص جرائم ارتکابی در فضای مجازی

در واقع از عمر رواج اصطلاح «جرم» سایبری کمتر از دو دهه می گذرد و پیش از آن نمی توان چنین واژه ای را در هیچ لغت نامه ای امروز همه در همه لغت نامه های به روز آمد شده اعم از اینترنتی و معمولی می توان چنین واژه ای را به راحتی پیدا کرد اما بدیهی است جرم سایبری به رفتارهایی که ضد این فضا یا بستر بی مرز و بیکران یا توسط آن ارتکاب می یابد اطلاق می گردد.

در تعاریف گوناگونی که از جرائم سایبری یا جرائمی که در فضای مجازی به وقوع پیوسته وجود دارد می توان به برخی ویژگی های مشترک آن ها دست یافت اما برای روشن تر شدن ماهیت فضای سایبر و جرائم قابل ارتکاب در آن معرفی انواع این جرائم ضروری است؛ جرائم که می توان در یک دسته بندی کلی آنها را به دو دسته جرائم رایانه ای وسیله محور و «جرائم رایانه ای موضوع محور » تقسیم کرد؛ جرائم رایانه ای وسیله محور شامل جرائم ضد اشخاص، ضد عفت و اخلاق عمومی و جرائم مخابراتی جرائم ضد صحت و تمامیت داده و سامانه های رایانه ای و مخابراتی و جرائم ضد قابلیت دسترسی می شود، طرق ارتکاب این جرم راه برای تعریف جامع و مانع از آن بسته است؛ این امر به علت طبع این گونه جرائم است.

۲-۲-۲ ماهیت بین المللی جرائم ارتکابی در فضای مجازی

متتمایز و مهم ترین ویژگی دنیای سایبر از دنیای خاکی یا فیزیکی، برچیده شدن مفهوم ماده و مختصات مکانی آن است همین توانمندی سبب شده همه چیز یک جا باشد و همزمان به کاربری های متفاوتی پرداخته شود. برای مثال در کنار آموزش الکترونیکی، مایحتاج خود را خریداری امور بانکی را انجام گفت و گوی روزانه را در محیط های ارتباطی خصوصی و شبکه های اجتماعی غیر عمومی و عمومی براقر و با همه این ها پایگاه های خبری و سرگرمی های مورد علاقه را هم مرر و بررسی کنیم .

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

۲-۲-۳ ارتباط بدون مرز

در دنیای مجازی افراد می تواند فارغ از محدودیت هایی چون مرزهای ملی، حاکمیت سیاسی و نظارت سازمان ها، مراجع مختلف، زبان، ملیت، نژاد، جنسیت و... از هر کجای دنیا و در هر زمان با جوامع مختلف ارتباط برقرار کنند؛ با آن ها وارد گفتمان شوند و از نظرهای آن مطلع شوند. پس از انقلاب صنعتی که با بهره گیری از ابزارها و وسایل پیشرفته صنعتی، در امر تولید کالا تحولات شگرفی در سطح دنیا به دنبال داشت و عصر صنعتی را رقم زد، اکنون پس از گذشت قرن ها دچار انقلاب اطلاعات شده ایم که تاثیرات آن نسبت به انقلاب صنعتی بیشتر است که در مقابل عواقب این دگرگونی اطلاعات شامل یک ایالت یا یک سرزمین مشخص نیست بلکه شامل تمام جوامع ملل می گردد.

۲-۲-۴ تحول مفهوم زمان ومکان در دنیای مجازی

مفهوم زمان و مکان به صورت ساختاری و در فضای سایبری و فیزیکی با یکدیگر متفاوت است . در جرائم رایانه ای علاوه بر طرف مختلف ارتکاب یک جرم جهان بعضاً با جرائم جدیدی رو به رو می شود که حتی شناخت مفهومی این جرائم برای حقوقدانان وقضات دشوار است. این امر ناشی از سرعت بالا پیشرفت فناوری و تکنولوژی اطلاعات و ارتباطات است. شاید بتوان گفت به دلیل سرعت بالای این پیشرفت ها و همچنین سرعت بالای این گونه ابزارها، قانون گذار کیفری همیشه یک گام عقب تر از فناوری است و پس از قربانی شدن شهروندان بسیار توسط مجرمین با هوش رایانه ای به پیشگیری یا جرم انگاری می پردازد. از این رو فضا سایبر، فضای یک محل در همه جهان و همه جهان در یک محل است. وسعت آن به اندازه تمام جهان است و لامکان و بدون مرز بودن آن را به بزرگی جهانی که سرعت و فرامرزی بودن آن را کوچک کرده تبدیل ساخته است. زمان در این فضا معنایی نو یافته و مکمل معنای نو و جدید مکان در فضای سایبری شده است؛ بدین نحو که در زمانی نا چیز می توان با دورترین نقاط جهان ارتباط برقرار کرد.

۲-۲-۵ موقعیت متفاوت مجرمان در فضای مجازی

مجرمان تبادل اطلاعات بر خلاف مجریان قانون برای ارتکاب انواع جرائم خود با حدی و مرزی مواجه نیستند وبه راحتی می تواند از هر نقطه این کره خاکی سیستم های و داده های رایانه ای مورد نظر خود را مورد تعرق قرار دهند یا دیگر جرائم تبادل اطلاعات را مرتکب شوند. این دسته از جرائم بعضاً از لحاظ مرتکبان هم با جرائم سنتی تفاوت دارند؛ برخلاف جرائم سنتی که معمولا حضور

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

مجرم در محل وقوع جرم ضروری است. در فضای مجازی چنین ضرورتی وجود ندارد و شاید مجرم فرسنگ ها با محل وقوع جرم یا نتیجه آن فاصله داشته باشد به طور مثال در جرمی مانند انتشار ویروس می توان گفت با پخش ویروس، جرم در تمام جهان انجام شده است. همچنین «جرم سایبری » مستلزم مجاورت فیزیکی میان قربانی و مرتکب نیست . برعکس جهان واقعی، در جهان سایبر جرم به صورت اتوماتیک از طریق فناوری واقع می شود چون جرم در جهان واقعی اتفاق نمی افتد از محدودیت های جهان فیزیک هم برخوردار نیست.

فصل دوم

سایبری و جنگ سایبری فضای سایبر

فضای مجازی[۱] عبارتی است که در دنیای اینترنت، رسانه وارتباطات بسیار شنیده می شود. به نظر می رسد 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 می دهد که این واقعیت، وجوه و جنبه های متنوعی از جمله خصلت های روانشناختی قابل توجه نیز دارد. در منابع موجود آمده است که : واژه سایبر از لغت یونانی کیبرنتیس[۲] به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح سایبرنتیک توسط ریاضیدانی به نام نوربرت وینر[۳] در کتابس با عنوان سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم ها درسیستم های انسانی، ماشینی (و کامپیوترها) 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 واژه های ترکیبی بسیار از این کلمه سایبر بوجود آمده است که تعدادی از آن ها:

۱ .Cyberspace
۲ .Kybernetes
۳ .wiener Norbert

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

فضای سایبر، شهروند سایبر[۱]، پول سایبر[۲]، فرهنگ سایبر[۳] راهنمایی فضای سایبر[۴]، تجارت سایبر[۵]، کانال سایبر[۶] فضای سایبردر معنا به مجموعه هایی از ارتباط درونی انسان ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیایی فیزیکی گفته می شود. یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند.

برخلاف فضای واقعی، در فضای سایبری نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می گیرد. معادل فارسی فضای سایبر همان فضای مجازی می باشد فلذا این دو هیچ تفاوتی به لحاظ معنا با هم ندارند و فقط یکی انگلیسی و دیگری معادل فارسی آن می باشد.

ویژگی های فضای سایبر

محیط سایبر با فضای سایبر دارای ویژگی های خاصی است که آن را از سایر فضاها رسانه ای متمایز ساخته و امتیاز خاص و تقریبا منحصر به فرد به آن می بخشد از مهم ترین ویژگی های محیط سایبر می توان به موارد زیر اشاره نمود :

۱- استفاده از مولتی مدیا : در محیط سایبر می توان از امکانات نوشتاری، دیداری و شنیداری دیگر رسانه ها یعنی صورت، تصویر، اینشمیشن، متن و... استفاده نمود.

۲. سرعت به روز رسانی : آن لاین بودن و به روز رسانی لحظه ای اخبار و اطلاعات منتشره در فضای سایبر

۳. سنجش و بازخوردگیری : به کمک ابزارهای مدیریت شبکه ای رایانه ای، هر شبکه اطلاع رسانی این توانایی را دارد که تعداد افراد مراجعه کننده به یک پایگاه وب را در طول شبانه روز مشخص کرده و با بررسی ویژگی های رفتاری مخاطبین برنامه ریزی کارآمدتری انجام دهد. وجود فرامتن از بدیع ترین ویژگی های و محاسن فضای

---

۱. Cybercitizen
۲. Cybercash
۳. cyberculture
۴. cyber Coach
۵. Cyberussiness
۶. Cyberchannel

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

۴. استفاده از فرامتن: سایبر است که با کلیک کردن بر روی برخی کلمات، صفحات دیگری حاوی اطلاعات بیشتر در مورد آن واژه بوده و به نمایش در می آید.

۵. داشتن قابلیت تعاملی : در فضای سایبری، فاصله ها از بین رفته و ارتباط واسطه ای بین رسانه و مخاطب ایجاد می شود.

۶. توزیع افقی اطلاعات : ارتباطات جمعی از آغاز حالتی یک طرفه داشته ولی در فضای سایبری گیرنده یک مشارکت کننده فعال بوده و از طریق لینک دادن به مطالب مورد علاقه خود مثل فرستنده در توزیع اطلاعات شرکت دارد.

۷. تمرکز زدایی: محیط سایبر در تمام مراحل تولید و انتشار اطلاعات از ویژگی تمرکز زدایی بهره می برد و هر فرد می تواند به عنوان یک پایگاه تولید اطلاعات عمل کرده و محصولات خود را منتشر کند و تمام حاضرین در فضای سایبر، به این اطلاعات دسترسی خواهند داشت.

۸. قابلیت دسترسی: فضای سایبری با استفاده از تکنولوژی ها و تکنیک های نوین در دسترس همگان قرار دارد.

۹- فقدان محدودیت انتشار :بر خلاف سایر رسانه ها، فضای سایبر محدودیتی از نظر حجم مطلب ندارد.

۱۰- فقدان سلسله مراتب : اغلب سایت های سایبری فاقد سلسله مراتب مرسوم در سایر رسانه های شنیداری، دیداری و نوشتاری بوده و به همین دلیل فرایندهای اداری در آن ها بسیار سریع و بدون بوروکراسی صورت می گیرند.

۱۱- عدم سانسور : در مقایسه با سایر رسانه ها، ممیزی و دروازه بانی خبر و فیلترینگ در فضای سایبر در کمترین شکل وجود دارد و این میزان در آیند نیز کمتر خواهد بود.

۱۲. تازه و دایمی بودن : تن در فضای سایبر هرگز کهنه نمی شود می توان در هر زمان به آن افزود

۱۳. حذف واسطه های ارتباط با مخاطب

۱۴. آزادی از زمان و مکان بنابراین فضای مجازی رایانه ای مکانی الکترونیکی که در آن گروهی از افراد با یکدیگر دیدار و گفتگو می کنند اطلاق می گردد. از نظر فنی نیز مجازی به معنی فضای اطلاعاتی به وسیله سیستم های رایانه ای شبکه های دیجیتالی که

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

نهایتاً با (مادر) همه شبکه ها یعنی اینترنت ارتباط پیدا می کند می باشد. به عبارت دیگر هر زمینه غیر فیزیکی که به وسیله سیستم های رایانه ای «آن لاین» به وجود می آید می تواند به عنوان فضای مجازی تلقی گردد (جنگ و دفاع سایبر، پیشین)

تعریف جرم سایبری

اولین مشکل در ارائه ی، تعریف ماهیت جرم سایبری است. در مورد تعریف و ماهیت جرایم، الگوی یکسانی مورد تبعیت قرار نگرفته است برای درک مفهوم جرم سایبر و تفاوت آن با سایر جرایم رایانه ای درک تعریف محیط سایبر و ویژگی های آن ضروری است . سایبر از لحاظ لغوی در فرهنگ های مختلف به معنی مجازی و غیر ملموس است. بدون وجود تعریفی از جرم سایبر در فرهنگ لغت ها، قانون گذاران و مجریان قانون در سراسر جهان جرم سایبر را درک کرده اند. وقتی آن را می بینند می شناسند. انتشار ویروس ها و کرم های رایانه ای، انجام حملات الکترونیکی و به طور کلی هر گونه فعالیتی که سبب ایجاد اخلال در شبکه های رایانه ای و ویتی که سبب امور مبتنی بر آن شود، جرایم سایبری نامیده می شوند. جرایم سایبری را در معنی جامع می توان به هر گونه فعالیتی که به منظور انجام تبهکاری در شبکه های رایانه ای به خدمت میگیرد، اطلاق نمود. براساس تعریف فوق اقداماتی چون حمله الکترونیکی به زیر ساخت های حیاتی و ملی کشورها، کلاهبرداری، پولشویی الکترونیکی استفاده جنایت کارانه از اینترنت، جعل آیدی و حتی استفاده از رایانه و مفاهیم فناوری اطلاعات در جریان جنایات غیر سایبری مصداق هایی از جرایم سایبری است. در کل می توان گفت که جرم سایبری زیر مجموعه جرم رایانه ای است

ویژگی های جرایم سایبری

الف)جرایم کلاسیک با توصیف سایبری

جرایمی در این دسته قرار می گیرند که جرایم سنتی تلقی می شوند؛ اما در حال حاضر به علت پیشرفت فناوری با وسایل طبقه بندی جرایم سایبری را در چهار دسته یا طبقه کلی می توان جای داد. از جمله این جرایم می توان به کلاهبرداری سایبری جعل سایبری، تخریب سایبری جاسوسی سایبری و... اشاره نمود.

جرایم علیه محرمانه بودن داده ها و سیستم ها هر نمادی از موضوع ها مفاهیم یا دستور العمل ها از جمله متن، صوت یا تصویر را که برای برقراری ارتباط میان سیستم های رایانه ای یا پردازش توسط شخص یا سیستم رایانه ای به کار گرفته شده و به وسیله ی

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

سیستم رایانه ای ایجاد می گردد، داده ی محتوا گویند. از جمله جرایمی که در این دسته جای می گیرند می توان به شنود غیر مجاز داده های مخابراتی در یک ارتباط خصوصی یا داده های سری اشاره کرد که واجد ارزش برای امنیت داخلی و خارجی کشور می باشند.

ب) جرایم علیه صحت و تمامیت داده ها و سیستم ها

تغییر، ایجاد محو یا متوقف کردن رایانه ای و مخابراتی به قصد تقلب، غیر قابل استفاده کردن تخریب یا اختلال در داده ها یا امواج الکترومغناطیسی، ممانعت از دستیابی اشخاص مجاز به داده ها با تغییر رمز ورود و یا رمز نگاری از جمله جرایمی هستند که در این دسته قرار می گیرند.

ج) جرایم مرتبط با محتوا

این دسته جرایمی را تحت شمول خود قرار می دهد که در آن ها، رایانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می شود و صرفاً فناوری اطلاعات، زمینه ی ارتکاب آن ها را فراهم می سازد. برای مثال، انتشار محتویات مستهجن از قبیل اندام جنسی زن و مرد یا نمایش آمیزش جنسی انسان، تبلیغ یا تحریک یا تشویق به انحرافات جنسی یا خودکشی از طریق سیستم رایانه ای یا مخابراتی در این دسته قرار می گیرند.

قواعد حاکم در بعد بین المللی

حقوق داخلی مبتنی بر ضرورت های جامعه شناختی داخلی کشورها است. حقوق بین الملل هم مبتنی بر ضرورت های زیست بین المللی کشورها است به عبارت دیگر، مبنای حقوق داخلی جامعه شناسی داخلی است و مبنای حقوق بین الملل هم جامعه شناسی بین المللی تصویب قانون در هر یک از این نظام های حقوقی هنگام ضرورت پیدا می کند که نشانه های جامعه شناسی بین المللی تصویب قانون در هر یک از این نظام های حقوقی هنگامی ضرورت پیدا می کند که نشانه های جامعه شناختی و فرهنگی برای تصویب آن قانون وجود داشته باشد (الکترونیک، ۲۰۱۱ :۷۶) از این منظر جرم انگاری جرایم سایبری در نظام حقوقی داخلی و مبتنی بر ضرورت های زیست جمعی بشر احساس شده فلذا کشورها در حوزه صلاحیت خود اقدام به تصویب قوانینی در این زمینه کردند

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

همین ضرورت در عرصه زیست بین المللی هم تشخیص داده شد فلذا در حوزه حقوق بین الملل هم قوانینی در این باره روی کار آمدند که این ضرورت را پاسخگو باشند.

آنچه که خاصه در این حوزه برای جرایم بین المللی حائز اهمیت است، نحوه تعیین دولت صالح برای رسیدگی به این جرایم است. از سوی دیگر، بحث همکاری دولت ها برای مقابله با این دسته جرایم هم شایان توجه است که ذیل عنوان معاضدت قضایی بحث می گردد

صلاحیت کیفری

صلاحیت در لغت به معنای «شایستگی»، «اهلیت» و «توانایی یک مقام در انجام یک عمل» آمده است. صلاحیت در معنای اصطلاحی و فنی ناظر است به توانایی به کارگیری و اعمال قانون در مورد موضوعاتی که به موجب قانون در قلمرو صلاحیت یک مرجع مشخص قرار می گیرد. از این رو صلاحیت به لحاظ کیفری عبارت است از شایستگی و اختیاری که به موجب قانون برای جمع کیفری به منظور رسیدگی به موضوعات کیفری پیش بینی شده است. به طور کلی قاعده اصلی در مورد تعیین مرجع صالح در امور کیفری توجه به محل قوع جرم است؛ چنانچه که یکی از ویژگی های برجسته حقوق کیفری درون مرزی بودن آن است بدین معنا که قواعد آن به مرزهای یک کشور محدود می گردد و ناظر به روابط اشخاص یک جامعه در محدود سرزمینی واحد است. در این باره، قانون مجازات اسلامی مصوب ۱ اردیبهشت ۱۳۹۲ (زین پس : ق. م.ا) چنین مقرر کرده است : «قوانین جزایی ایران درباره کلیه اشخاصی که در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران مرتکب جرم شوند اعمال می شود» لازم به ذکر است که اگر محل وقوع جرم نامعلوم باشد، اصولا به اعتبار محل کشف جرم، محل دستگیری متهم، محل اقامت متهم هم مرجع قضایی می تواند اقدام به رسیدگی کند. افزون بر معیارهای پیش گفته، گاه عنصر خارجی به صلاحیت کیفری جنبه بین المللی می بخشد چنان که گاه تبعه یک کشور باشد، علیه منافع عالی کشور یعنی نظم و امنیت آن صورت می گیرد و نیز گاه شدت جرم به حدی است که فارغ از معیار سرزمینی، تابعیت و منافع عالی کشورها مد نظر قرار گرفته و مرتکب آن در هر کشوری که یافت شود قابل تعقیب و رسیدگی در محاکم همان کشور خواهد بود. با توجه به معیارهای گفته شده، افزون بر صلاحیت سرزمینی، صلاحیت مبتنی بر تابعیت متهم، صلاحیت مبتنی بر تابعیت بزده دیده، صلاحیت مبتنی بر منافع عالی کشور و صلاحیت جهانی تشکیل دهنده مجموعه معیارهایی است که به موجب آن می توان مرجع صالح کیفری برای رسیدگی به جرمی را تعیین نمود. اما در مورد موضوع مسئله یعنی جرایم

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

سایبری با توجه به ویژگی های مورد اشاره این از جرایم باید با بررسی و تحلیل هریک از این معیارها صلاحیت کیفری سایبری را توضیح و تبیین نمود. به بیان دیگر، از آنجایی که کنش های انجام یافته مجازی غیر مادی و غیر ملموس بوده و در فضای مکانی مشخص و معینی صورت نمی گیرد باید با تحلیل معیارهای ناظر به صلاحیت کیفری ضمن توجه به ویژگی جرایم سایبری، معیار صلاحیت کیفری را معلوم نمود.

صلاحیت سرزمینی

قاعده اصلی در تعیین صلاحیت محل ارتکاب جرم است و از این روست که مرجه قضایی محل ارتکاب صالح به رسیدگی است. اما همانطور که پیش تر مورد بحث قرار گرفت، جرم سایبری به لحاظ ماهیت مجازی و غیر واقعی خود همانند جرایم سنتی قتل، سرقت وجز این ها در بستر مکانی مشخص رخ نمی دهد و از این جهت گفت که به طور دقیق محل وقوع محل سایبری کجاست تا بدین سان مرجع صالح هم تعیین شود. با وجود این، می توان به بستر ارتباطات و مبادلات الکترونیکی اشاره نموده که در واقع همین بستر تشکیل دهنده فضای سایبری بوده و داده های مختلف در آن مورد پردازش قرار می گیرند.

بدین سیان می توان گفت مراکز تولید بسترهای الکترونیکی که به عنوان مراکز داده به ارایه خدمات میزمانی می پردازند محلی است که جرم سایبری در آن واقع شده و محل این مراکز در قلمرو حاکمیت هر کشوری که باشند تابع قوانین کیفری آن کشور بوده و از این رو بنا به معیار صلاحیت سرزمینی مراجع قضایی آن کشور صالح به رسیدگی خواهند بود. در این باره ماده ۶۴۴ قانون آیین دادرسی کیفری (زین پس : ق . آ . د.ک) چنین مقرر کرده است که علاوه بر موارد پیش بینی شده در دیگر قوانین، دادگاه های ایران صلاحیت رسیدگی به موارد زیر را دارند: الف- داده های مجرمانه یا داده هایی که برای ارتکاب جرم به کار رفته اند که به هر نحو در سامانه های رایانه ای و مخابراتی یا حامل های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شود . این نکته را هم باید افزود که به استناد ۶۵۵ ق. آ. د.ک چنانچه جرم رایانه ای در صلاحیت دادگاه های ایران در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. در صورتی که محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار و در صورت اقتضاء صدور کیفر خواست می کند و دادگاه مربوط نیز رای مقتضی را صادر می کند.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

صلاحیت مبتنی بر تابعیت متعم

یکی دیگر از معیارهای درخور توجه در صلاحیت کیفری سایبری ناظر به معیار قرار دادن تابعیت متهم است. بنابراین دولت ها می تواند قوانین خود را نسبت به اتباع خود فارغ از اینکه محل ارتکاب جرم کجا بوده است، اعمال کنند. در این باره ماده ۷ ق . م. ا چنین مقرر نموده است که هریک از اتباع ایران در خارج از کشور مرتکب جرمی شود، در صورتی که در ایران یافت و یا به ایران اعاده گردد، طبق قوانین جمهوری اسلامی ایران محاکمه و مجازات می شود. بنابراین، با توجه به جرم بودن برخی رفتاری سایبری در قوانین جمهوری اسلامی ایران (بند الف ماده ۷ ق.م.ا) و نیز تعزیری بودن این دسته از جرایم (بند ب ماده ۷ ق.م.ا)و لحاظ باقی شرایط مقرر یعنی اینکه متهم در محل وقوع جرم محاکمه و تبرئه نشده یا در صورت محکومیت، مجازات کلا یا بعضا درباره او اجراء نشده باشد (بند ب ماده ۷ق. م.ا) و اینکه طبق قوانین ایران موجبی برای منع یا موقوفی تعقیب یا موقوفی اجرای مجازات یا سقوط آن نباشد (بند پ ماده ۷ق . م. ا) پس از یافت شدن متهم در جرایم موجب تعزیر در محل وقوع جرم، محاکمه و تبرئه نشده یا در صورت محکومیت، مجازات کلاً یا بعض درباره او اجراء نشده باشد (بند الف ماده ۸ ق م.ا) پس از یافت شدن یا اعاده متهم به کشور فارغ از اینکه تابعیت او چیست و در نهایت با توجه به مقررات قانون آیین دادرسی کیفری، مرجع قضایی محل دستگیری یا محل اقامت متهم صالح به رسیدگی خواهد بود.

لازم به ذکر است که در یک مورد ویژگی بزه دیده به لحاظ سن و نه تابعیت می تواند معیار صلاحیت محاکم ایران باشد. بند(ت) ماده ۶۴۴ ق. آ. د. ک چنین مقرر کرده است که اگر «جرایم رایانه ای متضمن سوء استفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه دیده یا مرتکب ایرانی یا غیر ایرانی باشد و مرتکب در ایران یافت شود» در این صور توقف صدر ماده ۶۴۴ دادگاه های ایران صلاحیت رسیدگی خواهند داشت. بنابراین، اگر جرایم رایانه ای متضمن سوء استفاده از اشخاص کمتراز هجده سال باشد، در این صورت تابعیت مد نظر نبوده و به صرف همان ویژگی سنی، محاکم ایران دارای صلاحیت خواهند بود. درفرض اخیر اگرم جرم در بستر سامانه های رایانه ای و مخابراتی یا حامل های داده موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ارتکاب یافته باشد، مراجع قضایی مستقر در محل این سامانه ها به عنوان محل ارتکاب جرم صلاحیت خواهند داشت. در غیر اینصورت، به شرط یافت شدن یا اعاده متهم به کشور، با توجه به مقررات قانون آیین دادرسی کیفری، مرجع قضایی محل دستگیری یا اقامت متهم صلاحیت رسیدگی خواهد داشت.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

صلاحیت حمایتی

در برخی موارد جرایم سایبری می توان قائل به صلاحیت حمایتی بود. در واقع، به موجب اصل صلاحیت حمایت هرگاه جرم ارتکابی فارغ از تابعیت مرتکب و محل ارتکاب منجر به لطمه به منافع عالی کشور شود؛ در این صورت، مراجع قضایی کشور نسبت به چنین جرمی صلاحیت خواهند داشتند. از این رو، در خصوص ارتکاب برخی از جرایم سایبری نظیر تروریسم سایبری می توان با توجه به این نوع از صلاحیت، برای مراجع قضایی قائل به صلاحیت بود. البته وصف سایبری برای جرایم خصوصیتی ندارد و کافی است که یکی از منافع عالی نظیر امنیت داخلی و خارجی مورد لطمه باشد (ماده ۵ق. م . ا)

بنابراین ، در فرض ارتکاب جرم سایبری که به منافع عالی لطمه می زند با حصول سایر شرایط یعنی ارتکاب جرم خارج از قلمرو حاکمیتی ایران و فارغ از اینکه مرتکب تابعیت ایرانی و فارغ از اینکه مرتکب تابعیت ایرانی یا غیر ایرانی داشته باشد (ماده ۵ ق. م. ا) امکان استناد به صلاحیت حمایتی برای رسیدگی به جرایم سایبری در محاکم داخلی فراهم می شود. در این باره بند(پ) ماده ۶۴۴ ق. آ. د. ک هم چنین مقرر کرده است:

«جرم توسط تبعه ایران یا غیر آن در خارج از ایران علیه سامانه های رایانه ای و مخابراتی و تارنماهای مورد استفاده یا تحت کنترل قوای سه گانه یا نهاد رهبری یا نمایندگی های رسمی دولت یا هر نهاد یا موسسه ای که خدمات عمومی ارائه می دهد یا علیه تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران درسطح گسترده ارتکاب یابد.» در این صورت با توجه به مقررات قانون آیین دادرسی کیفری مرجع قضایی محل دستگیری یا اقامت مرتکب صالح به رسیدگی خواهد بود.

صلاحیت جهانی

برخی جرایم حسب شدت به عنوان جرم علیه تمام بشریت تلقی می شوند که در این صورت مراجع قضایی همه کشورها فارغ از محل ارتکاب جرم، تابعیت متهم، تابعیت بزه دیده، صالح به رسیدگی خواهند بود. برای نمونه جرایمی نظیر نسل کشی و جنایات علیه بشریت قابل اشاره است که به لحاظ شدت قابل رسیدگی توسط تمام کشورهاست.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

در این باره باید گفت کمینه امکان استفاده از صلاحیت جهانی امکان استناد به آن در حالتی است که مرتکب در سرزمین کشور باشد بدون در نظر گرفتن اینکه ملیت مرتکب چیست و مکان ارتکاب جرم کجاست. در این راستا، برخی بر این باورند که اجرای بدون محدودیت اصل صلاحیت جهانی ناقض اصل حاکمیت سایر کشورها خواهد بود. به ویژه در مورد کشوری که مرتکب تابع آن است و یا جرم در سرزمین آن رخ داده است. فراوری آن، برخی در رد این استدلال این گونه پاسخ گفته اند که جرایمی همانند نسل کشی و جنایات علیه بشریت تمام جامعه بین المللی را متاثر می کند، از این رو، چنین جرایمی در پیوند با امور داخلی کشورها نبوده و ناقض حق حاکمیت آنها نخواهد بود، بلکه چنین جرایمی آنچنان سرزنش پذیر هستند که مرتکب آن دشمن تمام ملل فرض شده و از این جهت هر دولتی حق تعقیب این جرایم را خواهد داشت. با توجه به نکته پیشین، محدود ماندن در سایر گونه های صلاحیت پذیرفتنی نبوده و همه دولت ها بدون لحاظ اینکه ارتباطی با جرم داشته باشند، نسبت به پیگرد جرایم بین المللی بنابر اصل صلاحیت جهانی زمانی امکان پذیر است که اجماع یا توافقی بین المللی در مورد شدید بودن جرم وجود داشته باشد چنان که پذیرفته شود همه کشورها می تواند بنابر صلاحیت جهانی اقدام به رسیدگی کنند. گفتنی است بر خلاف جرایمی نظیر نسل کشی، هنوز در مورد جرایم سایبری چنین اجماع و توافقی ایجاد نشده و کنوانسیونی در این باره به تصویب نرسیده است. با این همه، باید توجه داشت که صلاحیت جهانی در دو مفهوم موسع و مضیق به کار رفته است. صلاحیت جهانی در مفهوم موسع بدین معناست که مراجع قضایی همه کشورها فارغ از محل ارتکاب جرم، تابعیت متعم، تابعیت بزه دیده و بدون هیچ قید دیگر می توانند رسیدگی کنند. اما صلاحیت جهانی در مفهوم مضیق بدین معناست که مراجع قضایی کشورها زمانی می توانند فارغ از محل ارتکاب جرم، تابعیت متهم، تابعیت بزه دیده اقدام به رسیدگی کنند که متهم در قلمرو حاکمیت کشور اقدام کننده یافت شود. بنابراین، به نظر میرسد در فرض پذیرش جرایم سایبری به عنوان جرایم بین المللی قابل تعقیب براساس اصل صلاحیت جهانی، با توجه به مسائلی نظیر اصل حاکمیت دولت ها، استناد به اصل صلاحیت جهانی زمانی امکان پذیراست که متهم در قلمرو حاکمیتی یافت شود. قانون مجازات اسلامی هم مفهوم مضیق صلاحیت جهانی را پذیرفته است.

نتیجه گیری

همان گونه که فناوری رایانه و ارتباطات سهولت روابط بین افراد و بسیاری از نیازهای جامعه بشری را برآورده کرده و در هر زمینه ای رفاه و راحتی را به ارمغان آورده است، از طرفی راه سوء استفاده را برای افراد بزه کار و مجرمان هموار کرده است.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

با توجه به رشد بسیاری سریع فناوری رایانه و گسترش فناوری ارتباطی و تبادل اطلاعاتی به کمک رایانه و اجزای وابسته به آن در ارتباط و وابستگی تنگاتنگ جامعه امروزی به این فناوری از بعد حقوق کیفری اقدامات خاص قضایی یکسان با جامعه جهانی چه در زمینه تدوین قوانین جدید و کارآمد و چه در زمینه اقدامات امنیتی در حفاظت از سیستم های رایانه ای و شبکه ای و آموزش نیروی متخصص ،ضروری و لازم می آید.

تبادل اطلاعات تامین دلیل و جمع آوری ادله، شناسایی متهمان اعمال صلاحیت کیفری تعقیب مجازات و استرداد مرتکبان آن ها و بالاخره شناسایی و اجرای دستورها و احکام کیفری در پرونده های جرائم سایبری فراهم نمی شود جرائم سایبری در این دسته از جرائم جای می گیرند. این نوع جرائم به سبب ویژگی ها ومختصاتی که دارند ضرورت این گونه همکاری ها را هر روز بیش از قبل جهانیان گوش زد می کنند جرائم فضای سایبر علیه تمامیت محرمانگی و دسترس پذیری سیستم های رایانه ای یا شبکه های مخابراتی ارتکاب می یابند یا اینکه از خدمات چنین شبکه هایی برای ارتکاب جرائم سنتی استفاده میشود ویژگی فرامرزی این گونه از جرائم با سرزمینی بودن اختیارات مجریان قانون تعارض دارد از این رو کشورهای مختلف با همکاری و مذاکره به این نتیجه رسیده اند که این عرصه را تحت قاعده در آوردند و بر آن اعمال نظارت کنند.

منابع و ماخذ

منابع فارسی

افق یک (۱۳۸۱). اطلاعات فناوری قضا، تهران: دفتر همکاری فناوری ریاست جمهوری

امیریان فارسانی، امین، عبدالصمدی ، راضیه حیدری فارسانی، فاطمه (۱۳۹۹). علت شناسی ارتکاب جرایم سایبری و ساز و کارهای پیشگیری از آن، علوم خبری سال نهم.

آشوری ، داریوش، (۱۳۹۸)، دانشنامه سیاسی، چاپ بیست و هشتم، انتشارات مروارید، تهران.

باستانی، برومند (۱۳۸۳). جرایم کامپیوتری و اینترنتی، تهران: انتشارات بهنامی.

جاوید نیا، جواد،(۱۳۸۸)، جرایم تجارت الکترونیکی، انتشارات خرسندی، چاپ دوم، تهران.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

جلالی فراهانی، امیرحسین (۱۳۹۴). درآمدی بر آیین دادرسی کیفری جرایم سایبری، تهران: انتشارات خرسندی، چاپ دوم.

حسینی خواه ، نوراله (۱۳۹۸)، پلیس و جرایم رایانه ای، تهران، انتشارات معاونت، تربیت و آموزش ناجا.

زندی، محمدرضا (۱۳۹۴)، تحقیقات مقدماتی در جرایم سایبری، انتشارات جنگل .

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

گرگی، مارکو جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، انتشارات پلیس امنیت فضای تولید و تبادل اطلاعات ناجا، ۱۳۹۴.

منابع انگلیسی

Adel Azzam saqf Al Hait,''Jurisdiction in Cybercrimes: A Comparavtive study'' Journal of law , Policy and Globelization .

Bonafe .Beatric, The Relattion Between state and Individual Responsibility for International crimes Hague, martinus nijhoff pub: ۲۰۰۹ ,p۲۴.

Crawford , and Martin Koskenniemi(eds).The Cambridge companion to International law, Cambridge university Press, ۲۰۱۲.

Coleman, C(۲۰۰۳).Seeurity Cyberspace –New Laws and Developing Strategies, Computer law and

Gabrys E (۲۰۰۲).The International Dimension of Cyber –Grime, part ۲:A look at the council of.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

Title: Resolving disputes caused by cyber crimes in international law

Corresponding author: Dr. Mehrdad Fallahi, Ph.D. in criminal law and criminology, Islamic Azad University, Khomein branch

Supervisor of the second author: Dr. Akbar Rajabi, assistant professor and head of the department of the Islamic Azad University, Khomein branch

Abstract

In the digital era and the formation of a large information society due to the movement towards electronic businesses, the issue of protecting information and data security is vital, which unfortunately is not fully covered by network security systems, etc., and this is where Cyber threats are taking on a more colorful role as a solution. Nowadays, cyberspace and the crimes resulting from it have become an important problem of human societies. Cyber intruders prefer cyberspace platforms as real and traditional to reduce the risk of their criminal acts. Doing criminal things in social networks may be unreal (fake). However, criminals are more interested in doing criminal and terrorist activities in the space.

Information technology is evolving day by day and has penetrated to the lower and partial layers of human societies. Cyberspace is the product of this technology. A space that, with its unique features, can be a breeding ground for specific and complex crimes such as crimes against the integrity and accuracy of data.

It should be noted that digital information not only provides benefits, but also poses security threats. In managing these threats, cyber security is of great importance

Key word : Resolving cyber disputes - cyber crimes - the concept of cyber and the basics of cyber war - the governing rules in the international dimension and the international nature , cyber crimes