ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

شماره مجوز مجله:۸۰۴۰۰ زمان چاپ:۱۴۰۲/۰۵/۲۰

حمایت از بزهدیدگان سایبری در حقوق ایران و اسناد بین المللی

دکتر امین غنی زاده افشاری

دکتری حقوق بین الملل

چکیده

اینترنت و فضای اینترنتی علاوه برجنبه های مثبت، از قبیل جنبه های آموزشی و عرضه خدمات ارتباطی دارای جنبه های منفی است که استفاده کنترل نشده از آن به ویژه وقتی با دیگرفناوری ها از قبیل تلویزیون همراه باشد، افراد را در معرض خطر آثار مضر آن بر تکامل فیزیکی، اجتماعی و روانی قرار می دهد. با تدوین قوانین جرایم رایانه ای، تا حدودی جرایم کمتر شده است ولی در بسیاری موارد در فضای مجازی به خاطر نداشتن آگاهی و آموزش کافی، ناخواسته مورد بزه واقع می شوند. و باید دانست آیا نقش خود بزه دیده در فضای مجازی باعث مورد تعارض واقع شدن وی می باشد. البته به نظر می رسد کاربر به دلیل نداشتن اطلاعات کافی و نحوه استفاده فضای اینترنتی و ابزارهای موجود در این فضا به راحتی مورد جرم واقع می شود که باید به این افراد و کاربران آموزش های جامع و لازم داده شود و آنها نباید اطلاعات خصوصی خود را در اختیار دیگران قرار دهند و به هیچ کس اعتماد نداشته باشند. هم چنین امکان دارد کودکان و نوجوانان در معرض محتویات خشن و جنسی که در حد سن آنها نیست قرار گیرند. در این میان به خاطر نداشتن اطلاعات و عدم استفاده صحیح و بهینه از این فضا، افراد در معرض بزه دیده شدن واقع می گردند. اما واقعیت این است که مبارزه و کشف اینگونه جرایم کاری بس دشوار است، چرا که به واسطه ویژگی های فضای مجازی که ظرفیت سوء استفاده از آن را بالا می برد. ویژگی هایی؛ چون بدون مرز بودن فضای مجازی، کم هزینگی و پرثمری و پایین بودن احتمال دستگیری یا مجازات، امکان وارد آوردن خسارات، بالا بدون آسیب جسمانی مجرم، آسان بودن تهیه و امکانات و عوامل مورد نیاز جرم، امکان جذب منابع مالی و پولشویی آسان تر و هرگونه انجام فعالیت های مالی الکترونیکی در جهت اهداف مجرمانه و .... و به دلیل همین مشکلات و دشواری ها و با توجه به پیچیدگی جرایم رایانه ای، مطالعه و پژوهش بیشتر مورد نیاز است و همچنین قانونگذار با تدوین و تصویب قوانین جدید و مورد نیاز در این زمینه نقش به سزایی در کم کردن این گونه جرایم دارد.

واژگان کلیدی: بزهدیدگان، سایبری، حقوق، اسناد بین الملل، ایران

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

مقدمه

میل و اشتیاق به استفاده از رایانه و اینترنت و بهره مندی از مزایای آن یک تمایل جهانی است. این تمایل که با سرعت قابل توجهی در حال افزایش است اگرچه زمینه مشارکت جوامع را در فرآیند اقتصاد داده پردازی فراهم می سازد اما در عین حال شرایط و بستر مساعدی نیز برای ظهور پدیده های نوین بزهکاری به رد آورده است. جرائم ارتکابی در فضای مجازی یکی از این پدیده های نوین تلقی می شود. امروزه در اکثر جوامع کاربرد فناوریهای پیشرفته رو به گسترش .است از آنجا که این فناوریها در عرصه های مختلفی از جمله تجارت الکترونیک انجام خدمات بانکی توسط شبکه فروش محصولات، انجام خدمات مراقبتی و درمانی آموزش و تحقیقات رواج یافته است تمایل ویژه افراد مستعد برای بزهکاری، به استفاده از این فناوری، عامل بالقوه ای در گسترش جرائم مزبور بوده است. در حال حاضر جرائم سایبری به عنوان یکی از دغدغه های بزرگ هزاره سوم میلادی، آینده ی اجرای قوانین را در بسیاری از کشورهای جهان به مخاطره انداخته است. کشورهای توسعه یافته برای مبارزه با این جرائم، پیش قدم شده و قوانینی تدوین کرده اند که بسیاری از آنها از اسناد بین المللی سرچشمه می گیرند. این اسناد راهکارهای مناسبی پیش روی قانون گذاران کشورها قرار داده اند در عین حال از آنجاکه : نقش پلیس در پیشگیری از جرائم سایبری و کشف آنها مستلزم تبیین ماهیت این جرائم چالش های مرتبط با آن و واکنش های لازم به منظور تحول و دگرگونی اساسی در کیفیت سیاست گذاری هاست(بازوند، ۱۴۰۰: ۱۴).

جرایم سایبری

کلمه سایبر در لغت به معنای مجازی و غیر مادی است. Cyber پیشوندی در انگلیسی و پسوندی در فارسی است که به کلمات جدید و امروزی چسبانده شده است تا به آنها معنا و مفهوم بدهد. چه ارتباطی با کامپیوتر یا فضای آنلاین دارد. به عبارت دیگر، سایبر به مطالعه مکانیسم های مورد استفاده برای کنترل و تنظیم سیستم های پیچیده اعم از انسان یا ماشین اطلاق می شود. اصطلاح فضای مجازی یا دنیای مجازی آنلاین اصطلاحی است که برای اولین بار توسط ویلیام گیبسون در سال ۱۹۸۴ استفاده شد، بنابراین این شبکه ها را می توان به عنوان اتصال از طریق مسیرهای اطلاعاتی مانند اینترنت تعریف کرد که در آن تمام اطلاعات در مورد روابط، مردم، فرهنگ ها، ملت ها، دولت ها و به طور کلی وجود دارد. هر آنچه بر روی زمین به صورت فیزیکی و محسوس وجود دارد به صورت دیجیتالی در این فضا وجود دارد و برای کاربران قابل استفاده و دسترسی است و از طریق رایانه های اجزای آن و شبکه های بین المللی به هم متصل می شود. در این تحقیق همراه با تشریح ویژگی های فضای سایبری، به بررسی انواع جرایم در این حوزه پرداخته شده است(زندی، ۱۳۹۲، ۲۱).

کلمه سایبر در فارسی به مجاز و مجازی ترجمه می شود. اما این ترجمه بیان صحیح کلمه نیست، زیرا محیط اینترنت یک محیط واقعی و واقعی است نه جعلی و مجازی و فقط می تواند مادی و کاربردی باشد و ذکر این نکته کافی نباشد. این نیست. بصورت مجاز و مجازی. می گویند کارشان فرآیند محور است و بر اساس یک سیستم صفر و یک سیستم کار می کنند. البته پیدایش فضای اینترنت مدیون همین شبکه عظیم جهانی است و بخش مهم و حداقل بخشی از سطح عملی و کاربردی آن را تشکیل می دهد. جرایم سایبری در یک کلام جرمی است که در یک محیط غیر فیزیکی علیه فناوری اطلاعات اعم از شبیه سازی و مجازی سازی انجام می شود. امروزه با پیشرفت فناوری اطلاعات و ارتباطات،

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

بسیاری از جرایم سنتی به طور چشمگیری به جرایم سایبری تبدیل شده اند. به جرایم سایبری جرایم سایبری نیز گفته می شود(زندی، پیشین، ۴۰)

کلمه کامپیوتر نمی تواند به طور دقیق و شهودی وسعت این حوزه را نشان دهد زیرا امروزه بسیاری از ابزارها و وسایلی که با داده ها کار می کنند را می توان کامپیوتر نامید، بنابراین نمی توان از کلماتی مانند جرایم رایانه ای یا جرایم سایبری استفاده کرد. سرپوش گذاشتن بر نوعی جرم مربوط به این زمینه، به عنوان مثال، یک سیستم ضبط و پخش یک کامپیوتر الکترونیکی نیست. اما به طور کلی تحت دنیای سایبری قرار می گیرد. در جرایم سایبری تأکید بر رویه ها نیست، دستگاه های مختلفی ساخته شده است که هر کدام راه جدیدی برای دسترسی به این فضا بدون نیاز مستقیم به رایانه ایجاد می کنند، مثلاً تلفن همراه یکی از این وسایل است.

ویژگی های فضای سایبری

تفاوت محیط سایبری با سایر محیط ها در تعدادی ویژگی مهم نهفته است. این ویژگی ها که گاه از ویژگی های منحصر به فرد فضای مجازی به شمار می روند به شرح زیر است:

الف- نامحدود بودن در فضای سایبر: فضای مجازی محدودیت خاصی ندارد، در محیط واقعی با افراد خاص یا محدود سروکار داریم اما فضای مجازی محیطی بدون مرز است. این ویژگی مثبت که امکان استفاده خوب از محیط سایبری را برای تسهیل فعالیت ها فراهم می کند، در صورت سوء استفاده می تواند اثرات منفی بر جای بگذارد. این ویژگی فضای مجازی به مجرمان فرصت های زیادی برای تغییر یا پنهان کردن هویت خود می دهد. این نامحدود بودن این پرسش را مطرح می‌کند که آیا سرزمین‌های قضایی جدید می‌توانند در برابر این مجموعه منحرف زنده بمانند(ویلیامز، ۲۰۱۱، ۴۷).

ب- استفاده از محیط آنلاین: محیط سایبری یک محیط فیزیکی و باریک نیست، این ویژگی فضای سایبری را خطرناک‌تر از محیط واقعی می‌کند، زیرا در درجه اول نگهبان مثلا پلیس موقعیت بیرونی و باریکی برای کار در این محیط ندارد. . برای اینکه مجرم احساس آزادی کند، به صورت ذهنی در ارتکاب جرم شرکت می کند. وقتی خرابکاران آن را نمی بینند از آسیب جلوگیری کنید. دوم اینکه قربانیان جرایم سایبری اعم از هک و هک با مجرم روبرو نمی شوند و هیچ گونه صمیمیت بین این دو وجود ندارد. ۷۰ (از سوی دیگر، جرم ارتکابی در فضلی در سال ۱۳۸۹ نشان می دهد که با گذشت زمان، اثر جرم بر بزه دیده می شود و در نتیجه کمتر به اقدام سریع برای پیشگیری از جرم توجه می شود.

ج - تغییرپذیری و توسعه: با توجه به ماهیت فضای مجازی و پیشرفت های علوم مرتبط، هر روز شاهد ظهور برنامه ها، نرم افزارها و خدمات اینترنتی متنوعی هستیم که برای استفاده مناسب از این ابزارها نیاز به برنامه ریزی صحیح است. این فضا از این جهت منحصر به فرد است که در بسیاری از موارد روند برخورد با اثرات منفی این ابزارها را فلج کرده و منجر به استفاده از این ویژگی های نوآورانه به روش های غیرعادی شده است(امانی کلارجانی، ۱۳۹۶: ۷).

د- پیچیدگی و تخصص: از دیگر ویژگی های فضای مجازی، تخصصی بودن این فضا است. تخصص به معنای داشتن توانایی خاصی برای ورود به این فضا نیست زیرا یک فرد عادی با استفاده از کامپیوتر قادر به ورود به این فضا خواهد بود. با این حال، پیچیدگی این فضا فراتر از ورود به این جهان است. برنامه نویسی رایانه ای، تشخیص تخصصی مضرات در فضای مجازی، نحوه استفاده ایمن از این فضا، نحوه شناسایی و برخورد با منحرفان، تأثیر فضای مجازی بر فرهنگ و

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

بسیاری از سؤالات اساسی و کلیدی که باید در این زمینه تسلط یافت. وجود مهارت های کافی برای پیچیدگی این فضا. دسترسی آسان و سریع از دیگر ویژگی های فضای مجازی است، دسترسی آسان و سریع به این فضا به گونه ای است که افراد با استفاده از رایانه شخصی و یا اقامت در کافه ها قادر خواهند بود بدون محدودیت از تمامی امکانات این فضا استفاده کنند. و محیط های آسیب زا در فضای مجازی می تواند اثرات منفی مانند شکل گیری جرایم یا انحرافات اخلاقی به ویژه در بین جوانان داشته باشد. کاربران این دو شبکه ظرف یک هفته شکایت خود را به مقامات شبکه ارائه کردند و شکایت کردند که افراد به سیستم آنها دسترسی غیرمجاز داشته و مشکلاتی را ایجاد کرده اند زیرا سوء استفاده الکترونیکی فوق الذکر فراملی شده است. پلیس کانادا با پلیس همکاری کرد. آمریکا چهار نوجوان ۱۳ ساله را از مدرسه دالتون در نیویورک از طریق خطوط الکترونیکی شبکه دستگیر کرد(پاکزاد، ۱۳۸۸، ۱۸)

ه-**استفاده گسترده از فضای مجازی الکترونیکی**: یکی دیگر از ویژگی های فضای مجازی این است که بیشتر فعالیت های روزمره افراد به آن وابسته است. امروزه با توجه به توسعه فناوری و مکانیزه شدن کسب و کار و فعالیت های تولیدی اقتصادی، استفاده از فضای مجازی افزایش یافته و موجب تسهیل و تسریع توسعه شده است، به طوری که بسیاری از صنایع، کارخانه ها، ادارات، انبارها، بازارهای تجاری، تاسیسات نظامی و ... یک شبکه مجازی مدیریت می شود. این امر نقش فضای مجازی را در دنیای امروز حساس و مهم می کند.

ماهیت جرایم سایبری

با توجه به اینکه جرایم در فضای مجازی به اشکال مختلف صورت می گیرد، صحبت از شرایط، ارکان و طبقه بندی جرایم دشوار است. تعریف روشن و بدون ابهام از ماهیت این جرایم دو چندان شده است. متاسفانه در حال حاضر اطلاعات دقیق و موثقی از گستردگی و تاثیر جرایم سایبری نه تنها در کشور، بلکه در سایر نقاط جهان وجود ندارد و حجم زیادی از آن کشف نشده باقی مانده است.

یکی از مشکلاتی است که بازپرس در مرحله کشف و تعقیب جرایم گزارش شده با آن مواجه است(خداقلی،۱۳۸۳، ۳۵). عدم افشای جرایم ذکر شده در بالا تا حدی به این دلیل است که اطلاعات ممکن است بر اعتماد کاربران و سطح خدمات ارائه شده تأثیر منفی بگذارد. جنایت می تواند دلیل دیگری باشد.او می دانست. در عین حال، صرف نظر از دشواری هایی که در تبیین ماهیت جرایم سایبری وجود دارد، به نظر می رسد این جرایم را می توان به چهار دسته یا دسته کلی تقسیم کرد.

۱- جرایم کلاسیک (سنتی) با شرح جرایم سایبری در این دسته قرار می گیرند که جرایم سنتی محسوب می شوند اما در حال حاضر با توجه به پیشرفت تکنولوژی با ابزارهای جدید انجام می شوند. از جمله این جرایم می توان به جعل و کلاهبرداری سایبری اشاره کرد(راجی، ۱۳۹۴: ۱۳۹۵). در حال حاضر که شبکه های رایانه ای وسیله ارتکاب جرایم سنتی مانند کلاهبرداری و جعل از طریق اینترنت است، قاضی مجبور به عدم وجود جرایم مدون است. . و قانون خاص در این خصوص از قوانین سنتی مانند قوانین جزایی و قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای که آیین نامه آن مصوب ۹۷۳۱ است و نیز مجازات های مصوب «قانون تجارت الکترونیک»۱۳۸۲ موجود است، از آن استفاده کنید(دازیانی، ۱۳۸۴: ۱۲)

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

۲- جرایم علیه محرمانه بودن داده ها و سیستم های رایانه ای و مخابراتی، هر نماد موضوعی، مفهوم یا دستورالعمل اعم از متن، صدا یا تصویر که برای برقراری ارتباط بین سیستم های رایانه ای یا شخص یا پردازش توسط سیستم رایانه ای استفاده می شود. که توسط یک سیستم کامپیوتری استفاده و ایجاد می شود، محتوای داده نامیده می شود. از جمله جرایم کیفری متعلق به این دسته است. می‌توان به شنود غیرمجاز داده‌های مخابراتی در یک ارتباط خصوصی یا داده‌های محرمانه که برای امنیت داخلی و خارجی کشور مهم است، اشاره کرد.

۳- جرایم علیه صحت و سلامت داده ها و سیستم های رایانه ای و مخابراتی. یا توقف حذف داده های رایانه ای و مخابراتی به منظور کلاهبرداری، از کار انداختن، از بین بردن یا مختل کردن داده ها یا امواج الکترومغناطیسی، جلوگیری از دسترسی افراد مجاز با تغییر رمز ورود یا رمزگذاری از جمله جرایم مشمول این است(دزیانی، ۱۳۸۴: ۲۰).

۴- جرایم محتوایی این دسته شامل جرایمی است که رایانه توسط مجرم به عنوان ابزار و وسیله ارتکاب جرم مورد استفاده قرار می گیرد و تنها فناوری اطلاعات زمینه ارتکاب آنها را فراهم می کند، مثلاً انتشار مطالب ناپسند. این دسته شامل نمایش اندام تناسلی یا رابطه جنسی مرد یا زن، ترویج یا تشویق به انحراف جنسی یا خودکشی از طریق سیستم های رایانه ای یا مخابراتی است.

امروزه در نقاط مختلف دنیا اکثر صنایع و شرکت های تولیدی و خدماتی با رکود شدیدی مواجه هستند. درصد زیادی از این شرکت ها انواع مختلف آزار و اذیت و استفاده غیرمجاز از سیستم های کامپیوتری را تجربه کرده اند. در حال حاضر، این اختلالات عمدتاً بر سیستم بانکی و صنعت مالی متمرکز است. ذکر این نکته ضروری است که جرایم سایبری عمدتاً توسط نیروهای سازمان یافته و از پیش برنامه ریزی شده و همچنین رقبا یا اخراج شده از سازمان های مذکور انجام می شود، بررسی های انجام شده در سال های اخیر نشان دهنده افزایش چشمگیر تعداد اعمال مجرمانه و گرایش های مجرمانه در فضا مجازی است بر اساس این بررسی ها، خطر جرایم سایبری به طور غیرقابل کنترلی در حال افزایش است و خسارات مالی هنگفتی را در بخش های مختلف به بار آورده است. در سال‌های آینده شاهد رشد تصاعدی در استفاده از فناوری اطلاعات به‌ویژه استفاده از اینترنت خواهیم بود، قطعاً چنین تمایل و روند شگفت‌انگیزی که به موازات افزایش تعداد جرایم سایبری است.

انواع بزه دیدگی

بز ه دیده کسی است که یک خسارت قطعی، آسیبی به تمامیت جسمی او وارد کرده است و اکثر افراد جامعه هم به این مسئله اذعان دارند. هنتینگ پدر علم بزه دیده شناسی، بزه دیده را چنین تعریف نموده: که بزه دیده جرم، مانند کسی است که کالبد عمل مجرمانه را تشکیل داده است. هنتینگ بزه دیده را در مفهوم مضیق خود مطرح ساخت که ناظر بر مجنی علیه است.

بزه دیدگی اولیه

عمل مجرمانه ای که شخص قربانی آن می گردد؛ می تواند قتل، سرقت، تجاوز به عنف و بسیاری از جرایم دیگر باشد.

بزه دیدگی ثانویه

در صورتی که بزه دیده یک جرم برای بار دوم قربانی شود نشانه ای از آسیب پذیری است و نشان می دهد که بزه دیده بیش از حد در معرض خطر قرار دارد.

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

بزه دیدگی مکرر

یعنی کسی که چندین بار متحمل جرم شود و دائماً قربانی جرم می گردد. مطابق ماده ۱۰ آیین دادرسی کیفری، بزه دیده کسی است که از وقوع جرم متحمل ضرر و زیان می گردد، چنانچه شاکی تعقیب مرتکب را درخواست کند و هرگاه جبران ضرر و زیان وارده را مطالبه کند مدعی خصوصی نامیده می شود. به طور کلی، عمده انگیزه های جنایی سایبری را با عنایت به رایج ترین جرایم سایبری می توان به ترتیب زیر بر شمرد: انگیزه ی سرگرمی، انگیزه مالی، انگیزه انتقام جویانه یا خشونت بار و انگیزه جنسی.

انگیزه سرگرمی

ارتکاب بزه برای سرگرمی منحصر به فضای سایبری نیست. در دنیای فیزیکی نیز عمده ای هستند که برای خوش گذرانی مرتکب انواع افعال مجرمانه می شوند. هنگامی که سرگرمی جنبه نامشروع به خود می گیرد و از مسیر درست خارج می شود، می تواند دست آویزی برای سوء استفاده و تعرض باشد. طبق نظریه ی انریکو فری درباره طبقه بندی عمومی بزه کاران، آنها به پنج دسته تقسیم می شوند:

۱-مجرمان مادرزاد یا بالفطره که به لحاظ پیشینه ساختاری جسمی، مستعد ارتکاب جرم هستند(گرایش چهره شناسی).

۲-مجرمان حرفه ای یا به عادت که توانایی سازگاری با اجتماع را ندارند و به الحاظ استعداد شخصی و تاثیر سوئ عوامل روحی مرتکب جرم می شوند؛

۳- مجرمان دیوانه که به دلیل ببیماری هار=ی روانی مرتکب جرم می شوند(گرایش روان شناختی) این سه دسته به عنوان مجرمان اصولا خطرناک شناخته می شوند؛

۴- مجرمان اتفاقی که تحت تاثیر اوضوع و احوال و بر اساس سلسله موقعیت ها به طور اتفاقی مرتکب جرم و به ندرت مرتکب تکرار جرم می شوند.

۵- مجرمان هیجانی که بدون نقشه قبلی و بدون تفکر مبادرت به ارتکاب جرم می کنند و بلافاصله نیز پشیمان می شوند. دو گروه اخر مجرمان کمتر خطرناک به شمار می ایند(نجفی ابرند ابادی،۱۳۸۲: ۱۴۸۲). رفع نیاز های سرگرمی در میان هرکر ها جلوه های گوناگونی یافته که برای نمونه می توان آن ها را در ردیف های زیر طبقه بندی کرد:

شیفتگان سایبری

این گروه از یادگیری نحوه کارکرد سامانه ها با آزمون و خطا لذت می برند و صذفا برای یادگیری اقدام به هک می کنند.

بی آزاری سایبری

این نوع هکر ها بدون آن که صدمه ای به یک وب سایت وارد آوزند، به تن نفوذ می کنند و به هنگام خارج شدن از خود یک پیام عادی به جا می گذارند مانند جک اینجا بود.

بازی انگاران سایبری

هکر هایی که هک ردن سامانه را یک بازی تلقی می کنند. این گروه تدابیر امنیتی شبکه مورد نظر خود را هدف قرار می دهند و تلاش می کنند با شکستن ان ها به پیروزی دست یابند(جلالی فراهانی، ۱۳۸۴: ۳۳) برخی که به آنها کودک

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

دوستان[۱] منفعل می گویند، اینترنت را تنها برای دسترسی و پیاده کردن هرزه نگاری کودک و استفاده از عکس ها و داستان های کودکانی که به فعالیت جنسی مشغولند(معمولا بزرگ سالان) برای ارضای خود به کار می گیرند(رحیمی مقدم، ۱۳۸۸: ۲۱) در برابر، برخی دیگر کودک دوست فعال می شوند که اینترنت را برای یافتن قربانیان خود به کار می گیرند. این مجرمان معمولا مجموعه ای از تصاویر هرزه نگاری کودک را در اختیار دارند، اما به این کار بسنده نمی کنند. آنها غالبا در محیط های گپی که کودکان حضور می یابند پرسه می زنند و سعی می کنند با انها ارتباط برقرار کرده و با جلب اعتماد آن ها، برنام یک مقلاقات حضوری را تنظیم کنند. سپس ممکن است به کودک تجاوز کنند یا این که فقط با ان ها رفاقت کرده و ترجیح دهند به تدریج زمینه براقراری روابط جنسی را فراهم آورند(جلالی فراهانی، ۱۳۸۴: ۳۸-۳۹).

ویژگی های جمعیت شناختی -اجتماعی بزهکاران سایبری

چنانچه از ما پرسیده شود به نظر شما بزهکاران سایبری از چه ویژگی هایی برخوردار ند به احتمال زیاد پاسخ خواهیم داد که آنها برخلاف ویژگی های نوعیِ بزهکاران عادی، از هوش، دانش و سطح تحصیلات و نیز از تمکن مالیِ بیشتری نسبت به سایر بزهکاران برخوردارند(نجفی ابرندآبادی، ۱۳۸۸: ۹). البته چنانچه کمی افراطی تر باشیم ممکن است آنان را گونه ای از بزهکاران یقه سفید بدانیم.

سن

سن یک عامل جرمزای فردیِ گذرا و انتقالی است. این عامل در حقوق کیفری به منظور تمییز سن مسئولیت کیفری و در جرم شناسی و بزه دیده شناسی ازلحاظ تفکیک بزهکاری اطفال و بزرگسالان، موردتوجه قرار می گیرد. از منظر جرم شناسی، یافته های تحقیقاتی نشان می دهند که در هر رده سنی، گونه ای از بزهکاری یا بزهدیدگی در میان افرادآن طبقه وجود دارد. برای نمونه در دوران طفولیت، کودکان ممکن است بزه دیده جرایمی چون تکدیگری(در این موارد فرد بزهکار-بزه دیده است) ترک نفقه، آدم ربایی و غیره شوند. چنانکه وندالیسم یا خرابکاری در بین نوجوانان و جوانان شایع ترین جرم است و موارد معدودی از وندالیسمِ میانسالان و سالمندان گزارش شده است.[۲] یا برعکس، برخی جرایم مختص افرادی است که در طبقه سنی بالایی قرار دارند .بارزترین نمونه از چنین بزهکارانی، مجرمین یقه سفید هستند(قورچی بیگی۱۳۹۲: ۱۷).

اما به عنوان یک قاعده کلی باید گفت که میان بزهکاری و سن حداقل در فراوانی رابطه معکوسی وجود دارد؛ به گونه ای که با افزایش سن، بزهکاری کاهش می یابد. در ارتباط با کنشگران فضای سایبر نیز باید گفت در سنجشی که در سال۲۰۰۳ میان برخی کشورها پیرامون رده سنی کاربران اینترنت انجام شد، نشان داد که در کشورهایی نظیر کره ۹۵ درصد ایالات متحده امریکا ۹۱ درصد ژاپن ۸۱ درصد و انگلستان۸۰ درصد نوجوانان و جوانان ۱۶-۲۴ سال، بیشترین استفاده از اینترنت را داشته اند. بنابراین، می توان گفت که علی الاصول بیشترین فراوانی بزه سایبری نیز باید متعلق به آنان باشد.

---

[۱] Passive pedopholes

[۲] تحقیق های انجام شده در ایران نشان می دهند که در ترکیب سنیِ افراد درصد آنان در گروه سنی وندالِ دستگیرشده،۶۷/۵ درصد آنان در گروه سنی ۱۰ تا ۲۵ سال قرار داشته اندُ سهم گروه سنی کمتر از ۱۰ سال ۳/۶ درصد و بقیه متعلق به گروه ۲۶ سال به بالا است.

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

در ایران، از بررسی پرونده ۴۵ محکوم به تولید و انتشار تصاویر مستهجن مشاهده می شود است که کمترین سن ۱۹و بیشترین ۵۴ سال و درمجموع، میانگین سنی آن ها۲۶/۲ است(معاونت آموزش تحقیقات قوه قضاییه ۱۳۸۹: ۲۰۹-۲۳۸)(همچنین، آمار پلیس فتا پیرامون سن متهمان جرایم سایبری در بازه زمانی سال ۱۳۹۰ تا ۱۳۹۱ نشان ن می دهد که ۷۷/۶ درصد متهمین دارای میانگین سنی ۱۷-۳۵ است.

البته نباید پنداشت که کل جرایم سایبری را نوجوانان و جوانان مرتکب می شوند . بر اساس ، اعلام بخش جرایم رایانه ای و مالکیت معنوی وزارت دادگستری ایالات متحده ۳۴ درصد از مجرمین دورن سازمانی بین ۲۰-۲۹ سال سال ، ۳۶ درصد بین-۳۵-۳۰ مجرمین و ۲۷ درصد بیش از ۳۷ سال سن دارند. هرچند بیشتر مرتکبین بین۳۰ و۳۵ سال هستند، اما بیشترین آسیب، توسط افراد بیش از ۳۵ سال مانند راجردورونیو ۳ با ۶۰ سال سن متهم به سرقت ۳ میلیون دلار، تیموتی آلن لوید ۳۹ ساله متهم به بیش از ۱۰ میلیون دلار و کوین میتنیک ۳۷ ساله متهم به بیش از میلیون دلار شده اند.

جنسیت

آنچه واضح است، نسبت نابرابری از بزهکاری میان مردان و زنان وجود دارد. هرچند در سال های اخیر با رشد مسئولیت پذیری و مشارکت زنان در جامعه نرخ بزهکاری زنان رشد یافته است، اما هنوز در بسیاری از جرایم فاصله ارقام بزهکاری مردان با زنان زیاد است.

گونه ای که در سال ۲۰۰۹ اداره تحقیقات فدرال امریکا گزارش داد که از۳۰ میلیون متهم دستگیرشده۷۵ درصد مرد و تنها ۲۵ درصد آنها زن می باشند و ۸۱ درصد جرایم خشن از سوی مردان ارتکاب یافته است(britton,۲۰۱۱: ۳). اطلاعات زندانیان ایران نیز نشان می دهد که بیش از ۹۶ درصد محکومین به حبس، مرد هستند. ورای توجیهات زیست شناختی و جامعه شناختی پیرامون بزهکاری زنان انجام شده است، باید گفت رویکرد پلیس و برخورد دستگاه عدالت کیفری با بزهکاران زن نیز متفاوت از مردان است و بخشی از این نابرابریِ آماری می تواند ناشی از نگاه مسامحه گر دستگاه عدالت کیفری به جنسیت زنان باشد. وضعیت بالا تا حد زیادی در ارتباط با جرایم سایبری نیز صادق است. برخی پژوهش ها بیانگر وجود رابطه ی مستقیم میان جنسیت کاربران و میزان مراجعه به سایت های هرزه نگاری مواجهه با تصاویر هرزه نگارانه در اینترنت میان است. بر اساس یافته های پژوهشی با عنوان ۸۲ درصد سایت های هرزه نگاری را مردان جوان و تنها ۵ درصد از را زنان تشکیل می دهند(نگهی، ۱۳۹۱: ۵۶)

سطح مهارت فنی و استعدادهای درونی

معمولاً انتظار می رود که بزهکار سایبری، فردی دارای دانش تخصصی بالا از علوم رایانه ای باشد؛ کسانی که حداقل با چند زبان برنامه نویسی و نیز به طور تخصصی از امنیت رایانه ها و سامانه ها آشنایی دارند.

شاید بتوان این دیدگاه را در ارتباط با جرایم رایانه ای که در دهه های گذشته روی می داد، با اغماض بپذیریم. زمانی که دانش آموختگان دانشگاه ام.آی.تی[۳] بامهارت و تخصص دانشگاهی خود به برنامه نویسی و ویروس نگاری های پیشرفته اقدام می نمودند و جز اما امروزه با پیشرفت های خود آنها، کسی توان مقابله با آنها را نداشت سخت افزاری و نرمافزاریِ رایانه ای و نیز پیدایش اینترنت، بزهکاران سایبری به راحتی یک اشاره بر موشواره می توانند آنچه را پیشتر به دشواری

[۳] Massachusetts Institute of Technology (MIT)

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

انجام می شد را عملی سازند. اما تصور رایج نادرست تر آن است که سطح مهارت فنی [۴] تمامی بزهکاران سایبری، همگن و متجانس انگاشته شود. یافته های یک پژوهش نشان می دهد که از مجموع ۲۳۹ نفر مورد مطالعه، ۲۱ درصد مهارت فنی پایین، ۲۲ درصد مهارت بالا، ۲۴ درصد متخصص و در واقع، اگرچه هنوز برخی شیوه ها درصد توان فنی متوسط دارند.

ارتکاب[۵] نظیر حملات ممانعت از سرویس دهی توزیعی در گستره سایبر به جهت ایمن بودن سامانه ها و شبکه ها نیازمند مهارت های عالی رایانه ای است، اما امروزه بیشتر جرایم سایبری با حداقل مهارت و تلاش روی می دهند. در این زمینه می توان به مهارت حداقلی ریزه خواران... اشاره نمود. حتی در حملاتی که از پیچیدگی زیادی برخوردارند، افراد می توانند با مشورت پیرامون مشکل خود در شبکه اجتماعی هکرها یا با خرید نرم افزارهای خودکار و از پیش طراحی شده نفوذ، نسبت به آن اقدام کند. از روش های جدید جبران خلأ نداشتن مهارتلازم می توان به اجیر کردن نوجوانان به منظور طراحی حمله و برنامه نویسی اشاره کرد که به نوعی می توان آن را شکل جدیدی از کودکان کار دانست.

سطح تحصیلات

مطالعات گوناگون نشان می دهد که رابطه معکوسی میان سطح تحصیلات و بزهکاری وجود دارد؛ به این صورت که هرچه سطح تحصیلات بالاتر رود، فرد کمتر به ارتکاب جرم اقدام می کند. اما به نظر ما این فرضیه حتمی و غیرقابل رد نیست؛ زیرا اگرچه سطح سواد یک جامعه می تواند شاخصی برای توسعه یافتگی یک کشور تلقی شود، اما ضرورتاً کاهش بزهکاری را به دنبال ندارد.

حتی با لحاظ عواملی نظیر توسعه شهرنشینی، افزایش جمعیت شاخص های افزایندهی جرم در دو سده اخیر و در کنار آن پیشرفت های فناورانه و رشد علم در جوامع بشری و سطح تحصیلات مردم شاهد آن هستیم که به نسبت افزایش سطح سواد جوامع، نه تنها بزهکاری کاهش نیافته بلکه در اَشکال و فراوانی سیر صعودی داشته است. از سوی دیگر حتی با چشم پوشی از یافته هایی که رابطه معکوسی میان بزهکاری و سطح زمانی ۸۰ ساله اگرچه تعداد بی سواد ها تا ۹۰ درصد کاهش یافته، اما از نرخ جرم کاسته نشده است. ممکن است انتقاد شود که میزان افزایش جمعیت و رشد شهرنشینی در این دوره زمانی لحاظ نشده است، اما به نظر می رسد حتی باوجود چنین نقیص های، نباید نرخ کاهش جرم تا این اندازه ناچیز باشد.

باید گفت موضوع مطالعه اکثر این پژوهش ها جرایم خشن یا مبتنی بر زور می باشند. لذا حداقل دستاورد این یافته ها آن است که سطح سواد با بزهکاری خشن رابطه معکوس دارد و نمی توان آن را به تمامی اشکال جرایم تسری داد. یک پیمایش خود گزارشی در میان دانشجویان سال اول تا سال چهارم در کانادا نشان داد که ۸۸ درصد شرکت کنندگان در رفتارهای مجرمانه سایبری نظیر استفاده از رمز عبور دیگران بدون اجازه آنها، تغییر و جستجو در فایل های دیگران بدون اجازه آن ها، استفاده از ویروس های تألیفی یا ویروس نگاری به منظور اعمال خرابکارانه و به دست آوردن رمز کارت رجرز و اعتباری دیگران و غیره مباشرت داشته اند.

---

[۴] Technical Skills

[۵]

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

به شکل قابل توجهی با مورد پیشین همخوانی دارد. شاید دلیل اصلی این مشابهت، عدم لحاظ شرایط محدودکننده در جامعه آماری باشد؛ چراکه در مطالعه نخست، پژوهشگران جامعه آماری خود را تنها معطوف به دانشجویان نمودند. البته باید اشاره کرد که جرایم مورد بررسی مطالعه نخست در زمره جرایم سایبری محض می باشند و این جرایم نسبت به سایر جرایم سایبری، به دانش و مهارت بیشتری نیاز دارند. لذا بدیهی است که معمولاً افراد تحصیل کرده تر این جرایم را مرتکب می شوند. موردی دیگری که نباید از یاد برد، آن است که رشد تحصیلات در کشورهای مختلف، یکسان نیست و در جوامع توسعه یافته یا دانشگاهی نظیر هند و مالزی، نرخ بیشتری از جرم در میان تحصیل کردگان را شاهد هستیم. پس به طورکلی می توان گفت وضعیت تحصیل در تمامی بزهکاران ازجمله بزهکاران سایبری نیز همگن نیست.

برای نمونه پژوهشی که پنج سال به طول انجامید، نشان می دهد بزهکاران سایبری به مانند سایر بزهکارانی که به سایر جرایم نظیر ضرب وجرح و برگلری از سوی محکوم شده اند، از سطح تحصیلاتی متفاوتی برخوردار می باشند دیگر باید اذعان داشت در جرایم سایبری به دلیل آنچه در بالا آمد، اغلب افراد تحصیل کرده بیش از سایرین دست به ارتکاب جرم می زنند.

پیشینه خانوادگی و زمینه های شغلی

تصور رایج ما از خانواده ای که یک بزهکار سایبری-هکر در دامان آن پرورش یافته، خانوادهای محروم و سطح پایین است که پدر و مادر هیچ نظارتی بر فرزند خود ندارند، پدر و مادر از هم جداشده یا طلاق گرفته اند یا به دلیل مشکلات روانی یا رفتاری به طور مداوم در حال مشاجره با یکدیگر می باشند. گاه فرزند مدت طولانی از آغوش پر مهر یکی از والدین محروم می شود و یا به جهت الکل بارگی و دیگر رفتارهای انحرافی والدین، کودک در دوران رشد خود دچار اختلال می گردد. پس به طورکلی، هکرها به مانند بیشتر بزهکاران در دوران کودکی و نوجوانی از سوی والدین خود حمایت عاطفی و مورد مراقبت نبوده اند. ازاین رو، معمولاً هکرها به خاطر شخصیت ضد اجتماعی و درون گرای خود در مدرسه نیز دوستان زیادی ندارند. آنها با فرار از تمامیِ موج های ناایمن زندگی، به ساحل امنی چون فضای مجازی رسیده اند؛ جایی که می تواند اظهارنظر کنند، قدرت ازدست رفته خود را بازیابند و به عبارتی به تمامی آنچه در دنیای خاکی از آن محروم بوده اند، دست یابند. اما باید اشاره کرد که همواره وضعیت این گونه نیست. حتی در مواردی به جهت پیوند عمیقی که میان والدین و فرزند وجود دارد، کودک رفتار انحرافی را از والدین می آموزد. برای نمونه در یک پرونده، کودکی سه ساله توانست تحت آموزش و تشویق پدر و مادر خود با اجرای عملیات حملات ممانعت از سرویس دهی به داده های رایانه ای دیگر، دسترسی یابد

همانطور که در بالا اشاره شد بزهکاران سایبری ممکن است از هر قشری باشند و محصور کردن آنها به افرادی خاص، نادرست است. وضعیت اشتغال بزهکاران سایبری نیز از این حال خارج نیست. درواقع، برخلاف آنچه تصور می شود، بزهکاری سایبری منصرف به افراد بی کار ۶ درصد متهمین جرایم سایبری و فاقد درآمد نیست.

پیشینه مجرمانه

یکی از برجسته ترین شاخص های سنجش خطرناکی در مطالعات جرم شناختی، سابقه دار است. برای نمونه در ارتباط با کدامین بزهکاران باید از راهبرد اصلاح و بازپروری سود جست یا در ارتباط با گونه های خطرناک تر بزهکاران، با سرکوب آنان را از جامعه حذف نمود. اما گاه چنانچه این عامل را به عنوان تنها شاخص خطر مورد نظر قرار دهیم، ممکن است گمراه شویم. برای نمونه مرتکبین جرایم خیابانی برعکس بزهکاران یقه سفید اغلب دارای سابقه مجرمانه هستند. از طرف

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

دیگر، پژوهشی پیرامون جرایم یقه سفید نشان داد که هیچ یک از افراد تحت بررسی پیشتر دست به ارتکاب جرم نزده اند(قورچی بیگی،۱۳۹۲: ۱۶).

اما آیا به واقع گروه اخیر خطرناکتر نیستند؟ مطالعه ای که پیرامون بزهکاران سایبری صورت گرفت نیز نشان داد که بیش از ۸۰ درصد بزهکاران هیچ سابقه مجرمانه ای نداشتند و تنها کمتر از ۲۰ درصد آن ها پیشتر به جرایمی همچون خریدوفروش مواد مخدر، توزیع لوح های فشرده هرزه نگاری، سرقت جزئی، قمار و غیره محکوم شده بودند.

مسئولیت کیفری در قانون جرایم رایانه ای ایران

قانونگذار ایران در قانون جرایم رایانه ای فصل ششم از قانون را به موضوع مسئولیت کیفری اختصاص داده است، شاید بتوان گفت مهمترین تغییری که قانون فوق الذکر در رابطه با مسئولیت کیفری ایجاد نموده، شناسایی و ایجاد مسئولیت کیفری برای اشخاص حقوقی است، ماده ۱۹ و ۲۰ قانون فوق الذکر در رابطه با مسئولیت کیفری اشخاص حقوقی است.
ماده ۱۹ مقرر می دارد: در موارد زیر، چنانچه جرایم رایانه ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:
الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه ای شود.
ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای را صادر کند و جرم به وقوع پیوندد.
ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه ای شود.
د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه ای اختصاص یافته باشد.
ماده ۲۰ نیز اشاره داشته: اشخاص حقوقی موضوع ماده فوق، با توجه به شرایط و اوضاع واحوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:
الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.
ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم شخص حقوقی منحل خواهد شد(رضوی فرد و موسوی، ۱۳۹۵: ۴۱).

شرایط تحقق مسئولیت کیفری اشخاص حقوقی در فضای سایبر[۶]

در مسئولیت کیفری اصل بر مسئولیت شخص حقیقی است و شخص حقوقی در صورتی مسئول است که جرم به نام و در راستای منافع آن ارتکاب یابد؛ به عبارت بهتر شخص حقوقی باید از ارتکاب جرم منتفع شود و سود مادی یا معنوی ببرد، هم‌چنین جرم باید به نام شخصی حقوقی ارتکاب یابد یعنی برای مثال از امضا و مهر شرکت استفاده شود یا اینکه به اسم آن شرکت عمل مجرمانه تحقق یابد.برای روشن‌تر شدن موضوع به موارد زیر توجه کنید:

---

[۶] یکی از الگوهای ماده ۷۴۷ قانون مجازات اسلامی در پیش بینی معیارهای انتساب بزه به شخص حقوقی، ماده ۱۲ کنوانسیون بزه های محیط سایبر مصوب ۲۰۰۱ است که طبق این مقرره، چنانچه اشخاص حقوقی در راستای منافع خود مرتکب جرایم مصوب این

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

۱- مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود: برای مثال مدیر یک شرکت فروش کالا، به نام شرکت و جهت کسب اطلاعاتی که به نفع شرکت است، اقدام به نفوذ در سامانه و سرقت اطلاعات شرکت رقیب کند.
۲- مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند: در مثال فوق مدیر می‌تواند به جای اینکه خود اقدام به نفوذ و سرقت اطلاعات کند، این امر را به یکی از کارکنان شرکت بسپارد.
۳-هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود: برای مثال نویسنده یک نشریه الکترونیکی، اکاذیبی که باعث جذب مخاطب و فروش بیشتر نشریه است، نگارش کند و در اثر عدم نظارت سردبیر این اکاذیب منتشر شود؛ در اینصورت فارغ از مسوولیت کیفری که به شخص حقیقی تحمیل می‌شود، نشریه نیز به عنوان شخص حقوقی قابل مجازات است.
۴- هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد: این بند هم شامل زمانی می‌شود که شخص حقوقی از ابتدا فعالیت خود را ارتکاب جرم قرار داده و هم زمانی که فعالیت اولیه‌اش مشروع و قانونی بوده اما پس از مدتی به جای فعالیت قانونی صرفا به ارتکاب جرم می‌پردازد. برای مثال یک شرکت با هدف تعمیر رایانه‌ها تشکیل می‌شود و تا مدتی هم به این کار مشغول است اما پس از گذشت زمانی، از فعالیت قانونی خود منحرف شده و با پخش ویروس، به ایجاد اخلال در سامانه‌های رایانه‌ای می‌پردازد.
براساس ماده ۱۹ قانون جرایم رایانه ای، اشخاص حقوقی در صورتی دارای مسئولیت کیفری می باشد، که جرم ارتکاب یافته به نام اشخاص حقوقی و در راستای منافع آن رخ داده باشد، لذا در صورت حدوث هر یک از حالات ذیل، شخص حقوقی دارای مسئولیت کیفری می باشد؛
الف- هرگاه مدیر شخص حقوقی مرتکب جرم رایانه ای شود.
ب- هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه ای را صادر کند و جرم به وقوع بپیوندد.
ج- هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه ای شود.
د- هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه ای اختصاص یافته باشد.
نکته: باتوجه به تبصره یک این ماده، مدیر کسی است که اختیار نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی را دارد. شایان ذکر است، باتوجه به تبصره دو این ماده در صورتیکه شرایط فوق وجود نداشته باشد، مسئولیت کیفری بر اشخاص حقوقی در جرایم رایانه ای متحمل نمی شود، بلکه شخص حقیقی (فرد عادی) که مرتکب جرم شده است، مجازات می شود.

رایانه ای بودن بزه

اولین نکته در ایجاد مسئولیت کیفری برای شخص حقوقی این است که رفتار ارتکابی باید در زمره بزه های رایانه ای گنجانده شود اگر چه ماده ۷۴۷ با اشاره صریح به جرایم رایانه ای در وهله نخست به ذهن متبادر می سازد که منظور قانون گذار صرفاً جرایم رایانه ای احصاء شده در قانون مذکور می باشد اما بایدتوجه نمود ماده فوق به طور عام به واژه ی جرائم رایانه ای پرداخته و از قیودی مثل جرائم رایانه ای و جرائم موضوع این قانون استفاده نکرده است لذا در نتیجه بزه هایی همچون جرایم رایانه ای موجود در قانون تجارت الکترونیکی مصوب ۱۳۸۲ ، بزه های موضوع ماده ی ۱۳ قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه ای مصوب ۱۳۷۹ و ماده ی ۶۳۱ قانون مجازات نیروهای مسلح مصوب۱۳۸۲ (جرایم محض سایبری و جرایمی که رایانه و تجهیزات آن موضوع جرایم سنتی هستند) را نیز در بر گرفته که البته جرایمی که رایانه واسطه ارتکاب آنهاست مثل جعل اسناد و مدارک به طور قطع از قلمرو این بحث خارج می باشند(زیبر، ۱۳۹۰: ۱۰).

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

ماهیت رایانه ای داشتن جرم ارتکابی از سوی اشخاص حقوقی از جمله شرایط اساسی تحقق مسئولیت کیفری آنها به شمار می رود. جرم رایانه ای جرمی است که در فضای مجازی رخ می دهد. اعم از اینکه جرم مربوطه از نوع جرایم محض رایانه ای باشد، مثل هک یا ویروسی کردن و یا اینکه رایانه و تجهیزات آن موضوع جرایم سنتی مانند کلاهبرداری، سرقت، جاسوسی و... باشد. بر این اساس، جرایمی که رایانه واسطه ارتکاب آنهاست مثل جعل اسناد و مدارک از قلمرو این بحث خارج می باشند.

سؤال قابل طرح در این قسمت آن است که آیا منظور از جرایم رایانه ای، جرایم احصا شده در فصل ششم از بخش یکم از کتاب پنجم قانون مجازات اسلامی(تعزیرات)یا اینکه سایر جرایم رایانه ای مذکور در مقررههای دیگری چون قانون تجارت الکترونیک مصوب ۱۳۸۲، ماده ۱۳(۵) حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای مصوب ۱۳۷۹ ماده ۱۳۱(۶) قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲ را نیز شامل می شود؟

گرچه در بادی امر اطلاق عبارت جرایم رایانه ای مندرج در ماده (۷۴۷) قانون مجازات اسلامی(تعزیرات) برداشت دوم را تایید می کند؛ اما با توجه به این که فصل مربوط به مسئولیت کیفری اشخاص حقوقی خود، ذیل آن بخش از مقرره های موصف قراردارد که به احصاء پنج دسته از جرایم پرداخته است،[۷] برداشت دوم صائب تر به نظر می رسد، با این همه، سیاست دفاع اجتماعی در قبال گونه های جرایم ارتکابی در فضای مجازی اقتضا دارد که قانونگذار در فصل مختص به مسئولیت کیفری اشخاص حقوقی، به وضوح به دیگر مقرره های مربوط نیز اشاره نماید تا از بروز اینگونه برداشت های متهافت جلوگیری نماید.

ماهیت پیشگیری اجتماعی در فضای سایبری

از جمله مهمترین آن ها شناسایی هویت و خصوصیات مجرمان و منحرفان سایبری بر اساس انگیزه های هر یک و همچنین، شناسایی هویت و خصوصیات بزه دیدگان سایبری و ارزیابی خطرپذیری آن ها برای جهت دهی نوع و میزان آموزش های پیشگیرانه است. سپس با توجه به نتایج به دست آمده، می توان بر اساس الگوهای کلی پیشگیری از جرم، راهکارهای قابل اجرا و مؤثری را پیشنهاد داد. با این حال، این مباحث به مجال دیگری موکول می گردد.

پیشگیری اجتماعی جامعه مدار سایبری

در اینجا مباحث پیرامون پیشگیری جامعه مدار خاص با محوریت کدهای رفتاری مطرح می گردد. به طور کلی، با کدهای رفتاری می توان گروه های خاصی را که وظیفه ای به آن ها سپرده شده، در مقابل اعمال خود پاسخگو نگه داشت. از جمله آن ها، گروه های مشاغل هستند که در حوزه های مختلف به فعالیت می پردازند و چون که به متصدیان شبکه ای خود، داده های واجد ارزشی را واگذار کرده اند تا با رعایت سه اصل محرمانه بودن، تمامیت و دسترس پذیری در فضای سایبر منتشر کنند، ضروری است متناسب با حرفه، نوع و میزان اطلاعات آن ها و دیگر شرایط، کد رفتاری مربوط را برای آن ها تدوین کنند. شایان ذکر است، در این مورد تاکنون برای بعضی مشاغل و موضوعات حساس، از سوی مراجعه مهم و معتبر بین المللی، کدهای رفتاری نمونه ای منتشر شده است. برای مثال، به تازگی برای فعالان عرصه

---

[۷] دسترسی غیرمجاز، شنود غیر مجاز، جاسوسی رایانه ای، جرایم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی جعل رایانه ای، تخریب و اخلال در داده ها یا سامانه های رایانه ای و مخابراتی، سرقت و کلاهبرداری مرتبط با رایانه، جرایم علیه عفت و اخلاق عمومی، هتک حیثیت و نشر اکاذیب

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

تجارت الکترونیکی و بازاریابی شبکه ای، کدهای رفتار یکسانی تدوین شده تا از وقوع جرم و تخلف های مرتبط با پیام های تجاری ناخواسته الکترونیکی(اسپم) جلوگیری شود.

اما گروه دیگری که کدهای رفتاری برای آن ها از جمله ضروریات شغلی است، ارائه دهندگان خدمات شبکه های اطلاع رسانی رایانه ای هستند. آن ها در حقیقت پل ارتباطی میان دنیای فیزیکی با فضای سایبر محسوب می شوند و نسبت به بقیه دست اندرکاران این حوزه، افزون بر این که توانایی اقدامات بسیار متنوع و گسترده ای را دارند، مسئولیت های خطیری نیز بر دوش آن ها گذاشته شده است. این افراد به راحتی می توانند امکان نفوذ به پایگاه ها را فراهم کنند یا اطلاعات حساس و کلیدی راجع به آن ها را در اختیار افراد ناصالح قرار دهند. به دلیل وجود چنین شرایطی، چندی است بر نحوه عملکرد ارائه دهندگان خدمات شبکه ای نظارت بیشتری صورت می گیرد که از جمله مهم ترین آن ها اقدامات انجام شده در جهت نظارت بر حفظ حریم آنلاین افراد از سوی این ارائه دهندگان خدمات است۰ آن ها به راحتی می توانند علاوه بر امکان پذیری ساختن شنود و ردیابی ارتباطات الکترونیکی، دسترسی به پایگاه های داده ای که ورود افراد غیرمجاز به آن ها ممنوع است یا اطلاعات شخصی و حساسی را که خود آن ها برای پیشبرد فعالیت های شبکه ای جمع آوری کرده اند میسر سازند.

پیشگیری اجتماعی رشد مدار سایبری

به نظر نمی رسد کسی در این واقعیت تردید داشته باشد که نه تنها نسل جوان و نوجوان جامعه ما، بلکه بدون استثنا در تمامی جوامع، توانسته است تعامل بهتری را با فضای سایبر برقرار کند. البته چندان جای شگفتی نیست، زیرا نسل گذشته امور خود را در دنیای فیزیکی به پیش می برده و شاید لزومی ندیده با این فضای جدید انس بگیرد، در حالی که نسل جدید با این فضا رشد یافته و از همان ابتدا هر آنچه پیرامون خود مشاهده کرده، رنگ و بوی سایبری داشته است. به هر حال، این وضعیت بیم و امیدهایی را برانگیخته است. از یک سو، می توان امیدوار بود نسل جدید در برپایی هرچه سریع تر یک جامعه اطلاعاتی تمام عیار، مبتنی بر اصول و قواعد حاکم بر این فضا، همت لازم را داشته باشد. اما از سوی دیگر، باید آن ها را از خطرات و آسیب های فراوان این فضا مطلع کرد تا با گرفتاری در آن ها، نتیجه عکس حاصل نشود.

سازکار های حمایت از بزه دیدگان جرایم رایانه ای

بزه دیدگان جایم رایانه ای همانند سایر قربانیان جرائم نیازند توجه و حمایت ویژه مجامع بین المللی و قانونگذاران داخلی می باشد. به ویژه از این جهت که با توجه به ماهیت و خصوصیت فضای مجازی بزه دیدگان ان بیشترین صدمات را در مقایسه با قربانیان جرائم فضای سنتی محتمل می شوند. در این راستا در سطح بین المللی علاوه بر سند عام بین المللی راجع به بزه دیدگان تحت عنوان اعلامیه اصول اساسی عدالت برای بزه دیدگان و سوءاستفاده از قدرت ۱۹۵۸ که از آن تحت عنوان منشور بین المللی بزه دیدگان یاد شده است، سند خاصی تحت عنوان کنوانسیون جرایم سایبر مصوب شوای اروپا ، به عنوان مهم ترین سند در حوزه جرائم رایانه ای محسوب می شود(زرشکی و شیروی، ۱۳۹۹: ۹۰).

در سطح داخلی آنجه که موجود است قانون جرایم رایانه ای مصوب ۱۳۸۸است که عمدتا ملهم از کنوانسیون جرایم سایبر می باشد تصویب شده است و مقررات دیگری چه عام و خاص در این راستا پیش بینی نشده است. یکی از بزه دیدگان خاص که در محیط رایانه ای در معرض بزه دیده گی خاصی هستند کودکان و بهره برداری از آنها در هرزه نگاری است در این راستا مقن ایرانی در قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعایت غیرمجاز می نمایند(مصوب۱۳۸۶) در تبصره ۳ ماده ۳ مقرر نموده است:

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

استفاده صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارها و لوح های فشرده غیر مجاز موضوع این قانون موجب اعمال حداکثر مجازات های مقرر برای عامل خواهد بود.

در نگاه اول به نظر می رسد قانونگذار درصدد حمایت کیفری ویژه از کودکان در قبال هرزه نگاری بوده است در صورت که جنین نیست زیرا قانون گذار به آثار غیرمجاز اشاره کرده است نه آثار سمعی و بصری مستهجن و مبتذل . و بنابراین قانونگذار جرایم مذکور در متن، مواد ۱و ۲ این قانون را مد نظر داشته که جرایم نسبتا و غالبا به نقض حق نشر مربوط می شوند(زینالی،۱۳۸۷: ۲۹۰).

از سوی دیگر هرزه نگاری کودکان[۸] در لایحه پیشنهادی جرایم رایانه ای با تاسی از کنواسیون جرایم سایبر مورد توجه قرار گرفته بود ولی در تصویب نهایی قانون گذار ایران بر خلاف نظر تدوین کنندگان لایحه که همسو با معیار های جهانی بود، با عدم پذیرش، به رویکرد مطلق هرزه نگاری رایانه ای مبادرت کرده اند. ماده ۱۴ قانون جرایم رایانه ای که در ذیل فصل جرایم علیه اخلاق و عفت عمومی آمده است، ضمن کاهش مجازات های مقرره در قانون مجازات اشخاصی که در امور سمعی و بصری فعالیت های غیر مجاز می نمایند. هیچ گونه رویکرد افتراقی از رهگذر کیفر گذاری مشدد به دلیل کودکی بزه دیده اتخاذ نکرده است(زینالی،۱۳۸۷: ۲۹۳، پور قهرمانی،۱۳۸۸: ۱۲۰؛ محسنی،۱۳۹۰). در حالی که این رویکرد با اسناد خاص هرزه نگاری کودکان مغایرت دارد. که این اسناد خاص بیشتر مصوب سال ۱۹۹۹ می باشد که سال بااهمیتی در زمینه توجه جامعه جهانی به هرزه نگاری کودکان در فضای مجازی است. که از جمله آنها کنفرانس پکن(۱۹۹۹) در مورد مبارزه با استفاده از اینترنت برای استثمار کودکان می باشد. که بخشی از توصیه های گروه کاری این کنوانسیون به اقدامات قانون گذاری مربوط می شود بر اساس این توصیه ها:

-هر کشور باید اطمینان حاصل کند که قوانین آن زمینه هرزه نگاری کودکان و سوء استفاده جنسی از اطفال ، استفاده از اینترنت را برای ارتکاب یا تسهیل این جرایمم منع می کند .

-هرکشوری بابید هرزه نگاری کودکان را به گونه ای تعریف کند که تصاویری را که به صورت الکترونیکی ساخته یا تغییر داده شده است را در بر می گیرد.

-تصاویر ساختکی ایجاد شده الکترونیکی باید در حقوق کیفری هر کشور گنجانده می شود به گونه ای که توزیع و مالکیت هرزه نگاری را در بر می گیرد. کنوانسیون ۱۹۹۹ مبارزه با هرزه نگاری کودکان در اینترنت ۱۹۹۹ می شود که در این کنفرانس یکی از جالش های اصلی مبارزه با هرزه نگاری، تفاوت حقوق کیفری ماهوی کشور ها، راجع به اشکال ممنوعه هرزه نگاری کودکان و محتوای هرزه نگاری و سن کودک بیان شده است(حسینی۱۳۸۲: ۶۷؛ نگهی،۱۳۹۱: ۱۴۳).

اجلاس یونسکو در زمینه سو استفاده جنسی از کودکان، هرزنگاری کودکان و کودک دوستی در اینترنت ۱۹۹۹ اقدام دیگری در راستای حمایت از کودکان در محیط اینترنت است. در روز های هجدهم و نوزدهم ژانویه ۱۹۹۹ حدود ۳۰۰ نفر از متخصصان حوزه مراقبت و محافظت از کودکان ، متخصصان اینترنت و ارائه دهندگان خدمات اینترنتی[۹] نمایندگان

---

[۸] child pornography

[۹] intevnet service provider

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

رسانه ها، نهاد های مجری قانون و نمایندگان دولت به منظور بررسی را های مبارزه با کودک دوستی و هرزه نگاری کودکان در اینتر نت گردهم آمدند و اعلامیه ای صادر کردند که به برخی از مفاد آن اشاره می شود:

-قانونمند سازی هدفمند از سوی کسانی که علیه هرزه نگاری کودکان فعالیت می کنند، از جمله حمایت از قواینن ضد هرزه نگاری کودکان فعالیت می کنند، از جمله حمایت از قواین ضد هرزه نگاری کودکان که تصاحب ان ر نیز در بر می گیرند.

- در کنار قانون گذاری، یونسکو باید به ترویج هماهنگ سازی قانونی نیز بپردازذد. این اسناد زمینه سند الزام آور ویژه ای را در سطح جهانی فراهم می کنند(زینالی،۱۳۸۷: ۲۴۷). پروتکل الحاقی به کنواسیون حقوق کودک راجع به فروش، فحشاء و هرزه نگاری کودکان(۲۰۰۰) یک سند الزام اور جهانی دیگری است که بر نگرانی روند رو به افزایش و قابل توجه هرزه نگاری کودکان تایید شده است. این سند الزام اور بین المللی در بند ج ماده ۲ هرزه نگاری کودکان را چنین تعریف می کند:

هرزه نگاری کودکان به هر گونه نماش کودکان در گیر در فعالیت های واقعی یا مجازی بارز جنسی با هر وسیله یا هر گونه نماش اندام جنسی کودک برا ی اهداف جنسی اطلاق می شود.

سند های دیگر در این زمینه کنوانسیون جرایم سایبر ۲۰۰۱ و در نهایت کنوانسیون شوای اروپا راجع به حمایت از کودکان در برابر بهره کشی و سو استفاده جنسی اقامات دیگری در راستای حمایت از کودکان هستند(باقری وناشی و همکاران، ۱۳۹۶: ۷۷).

همان طور که ملاحظه می شود در اسناد بین المللی نسب به کودکان بزه دیده ماشی از جرایم رایانه ای رویکرد افتراقی در پیش گرفته شده است در حالی که در حقوق داخلی ایران به ویژه در قانون جرایم رایانه ای که در واقع قانون خاص محسوب می شود تفاوتی بین بزه دیدگان عادی و کودک ملاحظه نمی شود. با وجود این مساله قانون گذار در باب حمایت آیین دادرسی در ماده ۲۸ بند ت ماده۶۶۴. ق.آ. د، ک۱۳۹۲) بیان داشته است که دادگاه های ایران در موارد ذیل صالح به رسیدگی خواهند بود:

-جرایم رایانه ای متضمن سوء استفاده از اشخاص کمتر از هجده سال، اعم از انکه مرتکب یا بزه دیده ایرانی یا غیر ایرانی باشد.

نتیجه گیری

امروزه استفاده از وسایل نوین الکترونیک ارتباطی تغییرات گسترده ای در تمام جنبه های زندگی انسان ایجاد نموده است، بدیهی است عرصه حقوق جزاء نیز دچار تغییرات زیادی شده است، مهمترین تأثیری که تکنولوژی بر حقوق جزا گذاشته، ایجاد فرصت های جدید ارتکاب جرم برای بزهکاران و درنتیجه افق های نوینی از حمایت کیفری و ایجاد مسئولیت کیفری است، جرایم مختلفی ممکن است در محیط اینترنت به وقوع بپیوندند و در نتیجه مجرمین متعددی اقدام به ارتکاب جرم در محیط اینترنت می نمایند، عدم هماهنگی حقوق جزاء با این پدیده ها یعنی عدم جرم انگاری جرایمی که در محیط اینترنت به وقوع می پیوندند، عدم ایجاد مسئولیت برای بزهکارانی که از این محیط برای انجام رفتارهای بزهکارانه خویش بهره جویند و ... مطمئناً راه را برای ارتکاب جرایم بسیار زیادی در محیط اینترنت و سایبر فراهم خواهد نمود، بر این اساس باید اذعان داشت که پیشرفت فناوری نباید بتواند جلوی جلوگیری و مقابله با جرایم را

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

در حقوق جزا بگیرد، بنابراین مهمترین مسئله ای که در پیش روی نظام های کیفری مختلف وجود دارد ایجاد و پذیرش تغییرات در راستای مبارزه و مقابله با جرایم مختلفی است که با استفاده از اینترنت و یا در محیط مجازی به وقوع می پیوندند، مبحث شناخت مسئولیت کیفری برای مجرمینی که در این محیط اقدام به ارتکاب رفتارهای بزهکارانه می نمایند از مهمترین موضوعاتی است که باید پس از جرم انگاری یک رفتار مورد توجه قرار بگیرد در اکثر جرایم کامپیوتری عنصر مادی یکسان بوده و امروزه بستر فناوری این جرم ها نیز یکی شده است. شکل یکسان ارتکاب از حیث اجزای عنصر مادی یا یکسانی به واسطه بستر فناوری است که موارد ذیل نمونه ای از آن است: قوانین ماهوی و شکل یکسان دارند، رویه های یکسان برای مبارزه وجود دارد، الزامات یکسان داخلی/ بین المللی دارند و پلیس واحد برای آن نیاز است. در حالت سنتی برای جرم مراحل ذیل تصور می شود: قصد مجرمانه، تهیه مقدمات، عملیات اجرایی جرم. در تمام مراحل فوق گذشت زمان مشهود است و ممکن است قصد تا عملیات اجرایی جرم از چند ثانیه تا چند ماه زمان نیاز داشته باشد. لکن در جرایم رایانه ای این زمان به چند ثانیه یا کسر ثانیه تبدیل می شود. فرد مرتکب از لحظه ارسال تا دریافت مطالب افترا آمیز در کل شبکه کمتر از چند ثانیه زمان نیاز دارد. بعضی از عواملی که تعدد مکان جرم را موجب می شود عبارتند از: محل ارتکاب، محل وقوع نتیجه، محل وجود ادله، محل فرار مرتکب در حالت سنتی بزه دیده یا که هدف جرم است انسان می باشد و در جرایم علیه اشخاص، تمامیت جهانی و معنوی فرد هدف ارتکاب جرم است.

فهرست منابع

بازوند، وحید، نورمحمدی، مسئولیت کیفری در مفهوم انتزاعی و گستره حاکمیت آن بررفتار شخص حقوقی (از تحلیل نظری تا واکنش قضایی)، فصلنامه پژوهش های حقوقی، دوره ۲۰، شماره ۴۷. ۱۴۰۰

امانی کلارجانی، امرالله، فضای مجازی و واکاوی سیاست‌های پیشگرانه در کنترل آسیب‌های اجتماعی نوپدید، نشریه علمی تخصصی رهیافت پیشگیری، پیش شماره اول.۱۳۹۶

باقری وناشی، محسن، باقری توانی، محسن، مروری کوتاه بر نقش بزه دیده در بزه دیدگی فضای مجازی و جرایم رایانه ای، اولین کنفراس پژوهش در فقه، حقوق و علوم اسلامی.۱۳۹۶

زندی م، (۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری، چاپ اول، تهران: انتشارات جنگل.

ویلیامز ، فرانک پی، ماری لین دی، مک شین، (۱۳۸۶)، نظریه های جرم شناسی ، ترجمه ق حمید رضا ملک محمدی، تهران، نشر میزان.

زرشکی، محمد، شیروی، مهسا، تتبعی بر مسئولیت کیفری اشخاص حقوقی در فضای سایبر، ششمین کنفرانس ملی علوم انسانی و مطالعات مدیریت.۱۳۹۹

الهی منش، محمد حسن، قدیری، طاهره، فرجامی کیا، هادی، تأثیر فضای مجازی بر مشارکت سیاسی شهروندان جمهوری اسلامی ایران (مطالعه موردی شهر تهران)، فصلنامه علوم اجتماعی دانشگاه آزاد اسلامی واحد شوشتر، سال دوزادهم، شماره چهارم. ۱۳۹۷

نجفی ابرندآبادی، علی حسین، ، کیفرشناسی نو- جرم شناسی نو: درآمدی بر سیاست جنایی مدیریتی خطر مدار، تازه های علوم جنایی (مجموعه مقاله ها)، زیر نظر علی حسین نجفی ابرندآبادی، تهران، میزان. ۱۳۸۸

جلالی فراهانی، امیر حسین، پیشگیری از جرایم رایانه ای، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، تهران ، دانشگاه امام صادق.۱۳۸۴

قورچی بیگی، مجید، تحلیل و بررسی جرمشناختی جرایم یقه سفیدها، رساله دوره دکتری، دانشگاه تهران، دانشکده حقوق و علوم سیاسی، حقوق کیفری و جرم شناسی.۱۳۹۲

ماهنامه علمی تخصصی پایا شهر

۷۷۸۶-۲۹۸۰ISSN

رضوی فرد، بهزاد، موسوی، نعمت اله، مسئولیت کیفری در فضای سایبری در حقوق ایران، پژوهش حقوق کیفری، سال پنجم، شماره ۱۶. ۱۳۹۵

زیبر، اولریش، جرائم رایانه ای ترجمه محمد علی نوری و..... انتشارات گنج دانش تهران. ۱۳۸۳

زینالی، امیر حمزه، حمایت کیفری از کودکان در برابر هرزه نگاری : از واکنش های جهانی تا پاسخ نظام ها کیفری ملی، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات، چاپ اول ، تهران ، انتشارات روزنامه رسمی. ۱۳۸۹

بای، حسینعلی، پورقهرمانی، بابک، بررسی فقهی و حقوقی جرائم رایانه ای چاپ اول انتشارات پژوهشگاه علوم و فرهنگ اسلامی. تهران. ۱۳۸۸

محسنی، فرید، سهم کودکان و نوجوانان از حمایت کیفری در فضای مجازی و حقیقی، آموزه های حقوق کیفری، شماره ۱. ۱۳۸۹

نگهی، مرجان، مقابله با هرزه نگاری کودکان: بررسی تطبیقی اسناد بین المللی و - پژوهشنامه حقوق کیفری، قوانین کیفری ایران نشر میزان چاپ اول چاپ دوم کتاب. ۱۳۹۱

Littlefield Publishers Britton, Dana M. (۲۰۱۱)the Gender of Crime, New York: Rowman &Chiesa, Raoul, Ducci, Stefania and Ciappi, Silvio. (۲۰۰۹)Profiling