

بازجستی در چرایی جرائم رایانه‌ای و راهکارهای مقابله با آن

سهیل معیری^۱

^۱ کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد زاهدان
dr.h.sh31@gmail.com

چکیده

با توجه به ویژگی‌هایی چون بدون مرز بودن فضای مجازی، کم‌هزینگی و پرتیری 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، بازتاب جهانی موفقیت، امکان جذب حامی و همکار برای ارتکاب جرم از سراسر جهان بدون حضور فیزیکی، امکان جذب منابع مالی و پول شویی آسان‌تر و هرگونه انجام فعالیت‌های مالی الکترونیکی در جهت اهداف مجرمانه و پیچیدگی جرائم رایانه‌ای، مطالعه و پژوهش بیشتر و نیز تصویب قوانین مورد نیاز در این زمینه، امری بسیار ضروری است. پیشنهادات در حال حاضر با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت آموزش بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرائم رایانه‌ای عبارتند از: ۱- از آنجا که پلیس به عنوان ضابط دادگستری و وظیفه کشف جرائم را بر عهده دارد، در کنار آموزش قضات و سایر مقدمات قضایی، آموزش پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد ۲- آموزش‌های عمومی در سطح کارمندان دولت و نظامیان و هم‌چنین مقامات قضایی ۳- تا حد ممکن عدم ذخیره‌سازی داده‌ها و اطلاعات طبقه‌بندی شده به شبکه‌های رایانه‌ای به خصوص شبکه جهانی اینترنت. ۴- مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به عنوان راهکاری سریع و کم‌هزینه و در عین حال مؤثر.

کلمات کلیدی: فضای سایبر، جرائم رایانه‌ای، فضای مجازی.

۱ مقدمه

بشر در طول حیات خود اعصار گوناگونی را پشت سر گذاشته و هریک از آنها را با الهام از تحول عظیمی که در آن عصر پدید آمده و گامی از رشد و تکامل بشری را رقم زده نام‌گذاری کرده است، مانند: عصر آتش، عصر آهن و عصر حاضر که عصر فناوری اطلاعات و ارتباطات نام گرفته است. می‌توان گفت به‌طور کلی تمام فعالیت‌های انسانی از گذشته تاکنون در حال پیشرفت بوده است همواره ابزاری ابداع و اختراع نموده است تا در ارتقاء رفاه و آسایش زندگی خود و خانواده مؤثر گردد، اما در اواخر سده بیستم، عصر فراصنعتی شاهد ظهور پدیده‌ای شگرف، پدیده‌ای که در حقیقت به معنای تولد جهانی دیگر با شرایط و ویژگی‌های جهان کنونی بود که این دنیای جدید، فضای مجازی یا فضای سایبر نام گرفت و هنوز نیم قرن از اختراع اولین

رایانه نمی‌گذرد که سرعت عمل آن از ابتدایی‌ترین ماشین حساب‌های دیجیتال امروزی نیز کمتر بود، اما به هر حال تحولی شگرف در دنیای علم و فناوری محسوب می‌شد و از همین رو رایانه‌ها در این مدت کم به خوبی توانستند جای خود را در تمامی شئون زندگی انسان باز کنند و به نوعی خود را در تمامی پیشرفت‌ها سهیم سازند اما بهره‌برداری روزافزون از سیستم‌های رایانه‌ای زمانی شتاب بیشتری به خود گرفت که امکان متصل گردیدن آنها به یکدیگر در سراسر جهان فراهم شد. این پیشرفت، به وسیله جامعه‌شناسان، دومین انقلاب صنعتی نامیده شده است اما نکته مهم اینجاست که هرچند این فضا با همه گستردگی و جهان شمول بودنش و تأثیرات مثبتی در زندگی انسان‌ها بر جای گذاشته است اما هرگز از نگاه قانون‌مداران علم حقوق خارج نبوده و به محض ظهور این فضا، علم حقوق و ابزارهای آن نیز به بررسی ابعاد این فضا از نگاه حقوقی پرداختند. به عبارت دیگر چون فضای سایبر از همان بدو تولد در دسترس همگان قرار گرفت، هر کس مطابق اغراض و مقاصد خود از آن سود می‌جست و آثار منفی و مخرب فرهنگی هم این محیط بر جای گذاشت که بعضی از این بهره‌برداری‌ها جنبه سوء استفاده به خود گرفت و بالطبع قانون‌گذاران را واداشت که تدابیری بیاندیشند، به همین علت دخالت علم حقوق، ضرورت یافت. این سوء استفاده‌ها که می‌توان گفت که در مجموع جرائم رایانه‌ای نام گرفته‌اند، طیف جدیدی از جرائم هستند. طبیعتاً مجازات‌های قوانین رایانه‌ای، امروزه برای مجازات مجرمین کافی اما کامل نمی‌باشد، چون هر روز جرایم جدیدی به وجود می‌آید که برای مجازات آنها نیاز به قوانین جدید داریم. همان‌گونه که جرایم اینترنتی همیشه در حال به‌روز شدن هستند، بایستی تلاش کرد تا بتوان با نو شدن جرایم، هر ساله قوانینی را که با جرایم جدید متناسب باشد ارائه کرد و از جهتی نیز بایستی سعی شود در زمینه جرایم رایانه‌ای مجازات‌ها بازدارندگی بیشتری داشته باشند تا امنیت و آسایش جامعه در پرتو همکاری مردم و مسئولیت توأم فراهم گردد.

بشر در طول حیات خود با دوره‌های گوناگونی از تحول و تکامل مواجه بوده است که از اوایل قرن بیستم، زمره‌های محوریت یافتن عنصر دیگری شنیده شد در این عنصر که در همان دوران صنعتی واجد ارزش بودن خود را به اثبات رسانیده بود، به تدریج با پا گذاشتن به سده بیستم موقعیت خود را تثبیت کرد و تا آنجا پیش رفت که به دوران صنعتی پایان داد و بشر را وارد عصر پسا صنعتی یا پسامدرن کرد. این عنصر با ارزش، اطلاعات نام دارد و حدود یک قرن است که بشر تلاش خود را صرف تجلی آن در تمامی عرصه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی کرده است. بی‌تردید هرکاری ابزاری می‌خواهد و ابزار فناوری اطلاعات و ارتباطات، تحقق یک جامعه به‌واقع اطلاعاتی است. دلیل اشاره به عامل ارتباطات، به لحاظ جایگاه ویژه آن در توسعه و تکامل اطلاعات است. ارتباط و به تبع آن ابزارهای ارتباطی، از همان ابتدا از عناصر حیاتی محسوب می‌شدند و می‌توان گفت اگر وجود نداشتند، بشر هیچ‌گاه نمی‌توانست به این حد از رشد و بالندگی برسد. دو فناوری در عرصه فناوری اطلاعات و ارتباطات نقش تعیین‌کننده‌ای به عهده داشته‌اند که عبارتند از: رایانه (هدف از اختراع رایانه، تسریع و تسهیل پردازش) و مخابرات اطلاعات بود که به خوبی به ثمر نشست و مخابرات نیز به عنوان مهم‌ترین ابزار ارتباطی در نشر این اطلاعات پردازش شده نقش بسزایی ایفا کرده است. به تدریج با کشف قابلیت‌های شگرف ناشی از تلفیق این دو فناوری، انقلابی در عرصه فناوری اطلاعات و ارتباطات رقم خورد. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که تحولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها فضایی با ویژگی‌های کاملاً متمایز از دنیای فیزیکی به وجود آورده‌اند

که عده‌ای آن را فضای مجازی نامیدند و برخی هم عنوان فضای سایبر را برای آن برگزیده‌اند. اما ناگفته پیداست که فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. به‌طور کلی، آنچه امروز تحت عنوان رفتار مجرمانه در این گروه جرایم قرار می‌گیرد، دو طیف می‌باشند: گروه اول جرایمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشان را تسهیل می‌کند. جرایم تحت شمول این حوزه بسیار گسترده‌اند و از جرایم حتی بین‌المللی گرفته تا جرایم علیه اموال و اشخاص را در بر می‌گیرند. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر این جرایم، به سوءاستفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست که جرایمی نظیر دسترسی غیرمجاز به داده‌ها با سیستم‌ها یا پخش برنامه‌های مخرب نظیر ویروس‌ها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرایم سایبری محض گفته می‌شوند. بنابراین، برای مقابله با چنین جرایمی و سوء استفاده از آن نیازمند تدوین قوانین جدیدی هستیم که حقوق سایبری نام دارد.

۲ ویژگی جرایم رایانه‌ای

در خصوص بیان ویژگی‌های جرایم رایانه‌ای نکته قابل توجه این است که کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون در نظر گرفتن اینکه این اطلاعات و خدمات در کدام نقطه دنیا واقع شده است. محیط سایبر زمینه فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیه معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده است. محدوده فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار و حتی مرزهای یک کشور محدود نبوده و در یک سطح کم هزینه هر کاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد. از بعد اقتصادی، سایبر را می‌توان یک بازار واحد جهانی دانست که از ثمره‌های موفق جامعه مبتنی بر تکنولوژی مدرن اطلاعاتی می‌باشد که با روند توسعه آن روابط اجتماعی و سنتی و فرهنگی حاکم بر روابط افراد را در سطح ملی دچار تحول نماید در واقع همواره چون ارائه تعریف دقیق و جامع و مانعی از فضای سایبری امکان‌پذیر نمی‌باشد اما با وجود این تفاوت‌ها نباید سه ویژگی اصلی را برای فضای سایبری دور از نظر داشت و آن هم به شرح ذیل است: نخست: پیچیدگی تکنولوژی (عدم توانایی در شناخت ابعاد پیچیده جرایم سایبری و فضای سایبر)؛ دوم: تنوع و گوناگونی جرایم سایبری (به دلیل تحول و توسعه فضای سایبر)؛ سوم: توان مرموز سازی جرایم سایبری در این راستا مراجع قانون گذاری کشورهای مختلف و اسناد بین‌المللی، اعم از ارشادی و الزام آور، هرکدام به فراخور نیازها و تهدیدات پیش رو تعاریف متفاوتی از این جرایم ارائه کرده‌اند که ویژگی‌هایی را نیز به همراه دارند.

۳ علت‌شناسی جرایم سایبری

ژان پیناتل در بیان علت جرم می‌گوید: «شرط لازمی که بدون آن رفتار مجرمانه بروز نمی‌دهد» علت‌شناسی از اصول بنیادین دانش جرم‌شناسی محسوب می‌گردد؛ به گونه‌ای که اهداف جرم‌شناسی در زمینه پیشگیری و درمان بزه، با شناخت علل ارتكابی آن مقدر می‌باشد. لذا جرم‌شناسان برای مقابله با یک جرم با ترسیم یک رابطه علت و معلولی، سعی در خنثی نمودن علل مؤثر در ایجاد نتیجه مجرمانه می‌نمایند همان گونه که در بررسی علل جرایم سنتی با دامنه گسترده‌ای از علل روبرو هستیم، در ارتباط با دنیای جدیدی به نام « فضای سایبر» نیز علاوه بر علل احصاء شده در جرایم سنتی، عوامل متعدد و جدیدی با توجه به ویژگی‌های خاص این فضا در شکل‌گیری جرایم سایبری تأثیرگذار می‌باشند. بنابراین، امروزه در کنار دنیای حقیقی با دنیای مجازی مواجه هستیم که دارای سه ویژگی عمده و اصلی می‌باشند: انعطاف‌پذیری عناصر تشکیل‌دهنده جرم در زمان و مکان، ناشناس ماندن نسبی مرتکبان در فضای مجازی که در واقع شناسایی آنان و محل ارتكاب جرم را دشوار می‌نماید و جهانی بدون گسترده ارتكاب بزه که به بزهکاران اجازه می‌دهد بتوانند جرم را بدون حضور در محل یا از اقصی نقاط جهان انجام دهند [۸]. در این گفتار، تمرکز روی علل کلی ارتكاب جرایم اعم از سنتی و سایبری قرار داده شده و در تبیین این علل ویژگی‌های خاص فضای مجازی به‌عنوان متغیری ویژه و تعیین‌کننده، مد نظر قرار خواهد گرفت.

۱.۳ علل فردی

جنس، سن، بدبینی، خودخواهی، نفرت، کینه، جنون، ثروت، جنون اخلاقی، پرخاشگری، عصبانیت آنی و انتقام از عوامل فردی است که با توجه به وضعیت زیستی - روانی فرد، وی را متمایل به انجام یک رفتار خلاف هنجار می‌کند. برای مثال، آنچه در خصوص سن مرتکبین جرایم سایبری به‌عنوان یکی از علل فردی قابل توجه است، وقوع جرایم مالی در سنین بالا و جرایم علیه عفت و اخلاق عمومی در سنین پایین است. در واقع، نوجوانان سهم عظیمی در جرایم نوع دوم به خود اختصاص داده‌اند. شخص نوجوان پس از ورود به مرحله بلوغ با تغییر و تحولاتی در وضعیت جسمی، روانی و شخصیتی خود مواجه می‌گردد که این تغییرات و وجود محیطی پرجاذبه و قابل دسترس به‌عنوان دنیای مجازی وی را به سوی این دنیای جدید متمایل می‌سازد. در این رابطه سوء استفاده‌کنندگان جنسی از اطفال با استفاده از فضای مجازی که قادر به بارگذاری و توزیع حجم بالایی از مسائل مربوط به پورنوگرافی می‌باشد، گروه‌هایی با افکار و عقاید یکسان تشکیل می‌دهند و به‌دنبال آن به سرعت ارائه سرویس‌های اینترنتی را به تشکیل گروه‌های روسپی‌گری و جنسی در میان کودکان و نوجوانان در دنیای حقیقی تبدیل می‌نمایند. امروزه کودکان و نوجوانان با دسترسی به فضای مجازی و حجم وسیعی از تبلیغات و فیلم‌ها و عکس‌ها و مطالب و شخصیت‌ها آشنا می‌گردند که این وضعیت در کنار آثار مثبتی که دارد، آثار منفی و مخربی نیز به بار آورده است. لذا جوامع جهت اصلاح و تربیت صحیح نسل‌های آینده خود همواره به‌دنبال مقابله با این عوامل بوده است. آنچه به‌عنوان علل گرایش کودکان و نوجوانان به محتویات مبتذل قابل ذکر است، در واقع وضعیت سنی، خواسته‌ها و ارزش‌های مورد تقاضای این قشر، جاذبه این محتویات و عدم وجود جایگزین مشروع می‌باشد. لذا افراد در سنین پایین

به دلیل شرایط خاصی که در آن قرار دارند و بیشتر تحت تأثیر عوامل محیطی قرار می‌گیرند. لذا اتخاذ تدابیر بازدارنده و پیش‌بینی جایگزین‌های مشروع و پرجاذبه در این زمینه می‌تواند کمک‌کننده باشد. از دیگر علل فردی که موجب شکل‌گیری جرایم بالاخص جرایم سایبری می‌گردد، ویژگی‌های روانی - شخصیتی افراد است. کینه‌توزی با یک جنون اخلاقی یا جنون ثروت یا عصبانیت آنی هر یک به نوبه خود، فرآیند ارتکاب جرم را سرعت می‌بخشد. بنابراین همان‌گونه که از مصادیق علل فردی مشخص است برخی ویژگی‌های روانی شخصیتی با تأثیر از محیط اطراف از علل اصلی گرایش به ارتکاب جرایم سایبری محسوب می‌گردد که البته ماهیت فضای سایبر و تساهل انجام اقدامات مجرمانه در آن نیز مزید بر علت است و خودنمایی و سرگرمی از دیگر علل فردی است که طی آن در اکثر موارد اشخاص صرفاً جهت نشان دادن توانایی و استعداد خود مرتکب این جرایم می‌گردند، به گونه‌ای که هک کردن یک سایت یا دسترسی به داده‌های دیگری یا مختل کردن یک داده را امری مطلوب و افتخارآمیز تلقی می‌کنند که البته مقابله با این‌گونه افراد مشکلات خاص خود را دارد.

۲.۳ علل اجتماعی

وضعیت فرهنگی حاکم بر فرد و جامعه، وضعیت خانوادگی و گروه هم‌سالان و محیطی که فرد در آن زندگی می‌کند، وضعیت اقتصادی، بی‌اعتقادی به هنجارها، نحوه فعالیت رسانه‌های جمعی و غیره از جمله عوامل اجتماعی هستند که در گرایش فرد به ارتکاب جرم، به‌ویژه جرایم سایبری، تأثیر بسزایی دارند. در این راستا به مهم‌ترین این عوامل اشاره می‌شود.

۱.۲.۳ ضعف فرهنگی

دین و مذهب و اعتقاد به ارزش‌های تعیین شده جامعه از ابزارهای مهم پیشگیری از جرم محسوب می‌گردد تا جایی که به‌طور مثال، در محدوده فضای سایبر، اعتقاد به ارزش‌های دینی، ناخودآگاه فرد را از ارتکاب جرایم سایبری به‌خصوص در زمینه محتویات مبتذل باز خواهد داشت. بنابراین، تضعیف این اعتقادات، بی‌تفاوتی فرد به ارزش‌های جامعه را به همراه داشته و این معضل تأثیر خود را در فضای مجازی که محیطی امن و آرام برای ارتکاب اقدامات معارض با قانون است، بروز می‌نماید. علاوه بر این مورد سطح تحصیلات و آگاهی در عین اینکه تأثیر مثبتی دارد، خود نیز می‌تواند از عوامل اصلی ارتکاب جرایم سایبری محسوب گردد. لذا برخلاف جرایم سنتی که گاهی اوقات بی‌سوادی از علل اصلی ارتکاب آن جرایم محسوب می‌گردد، در جرایم سایبری بی‌سوادی و ناآگاهی از مفاهیم سایبری موجب ارتکاب این جرایم نمی‌گردد بلکه داشتن سواد و تخصص حتی در برخی از جرایم سایبری خاص از علل اصلی ارتکاب آن جرایم خاص محسوب می‌گردد. در کنار این موارد فقدان فرهنگ استفاده صحیح از رایانه و فضای مجازی در کشورهای در حال توسعه و عدم آگاهی از خطرات و آسیب‌های دنیای مجازی می‌تواند از علل دیگر شکل‌گیری محیط مساعد برای ارتکاب جرایم سایبری محسوب گردد.

۲.۲.۳ شرایط نامساعد اقتصادی

تورم، فقر اقتصادی، فساد اقتصادی، بیکاری و وضعیت نابسمان زندگی از جمله عللی است که از گذشته تاکنون جوامع انسانی را تحت تأثیر قرار داده و همواره آثار خود را در زمینه سیاسی، اجتماعی، فرهنگی و حقوقی نشان داده است. جرایم اعم از سنتی و سایبری در پاره‌ای از موارد متأثر از شرایط اقتصادی فرد و جامعه قرار خواهند گرفت و به عبارتی دیگر ارتکاب جرم راه‌حلی جهت رهایی از فشاری است که طبق قاعده فشار رابرت مرتون از عوامل اقتصادی بر فرد تحمیل گردیده است تا جایی که امروزه طبق آمار اعلام شده در ایران حدود ۸۰ درصد جرایم رایانه‌ای را جرایم مرتبط با امور مالی و اقتصادی تشکیل می‌دهد. برای مثال، کلاهبرداری و سرقت داده‌ها جهت کسب مال تحت عنوان فیشینگ از جمله جرایم سایبری است که می‌تواند زیربنای اقتصادی داشته باشد. فقر اقتصادی یا جنون ثروت ممکن است فرد را به استفاده از ابزارهای نامشروع جهت کسب ثروت تحریک کند. و در این راستا از فضای مجازی به‌عنوان محیطی امن استفاده کرده و با استفاده از یک رایانه و فقط نشستن در خانه و مقداری تخصص، سیستم‌های رایانه‌ای را مختل کند. بنابراین آنچه در برخی موارد موجب ارتکاب یافتن این جرایم می‌گردد، شرایط نامساعد اقتصادی فرد یا جامعه است؛ چه بسا با ایجاد یک سیاست اقتصادی مناسب از میزان ارتکاب این جرایم کاست.

۳.۲.۳ خانواده‌های نابسامان

محیط خانواده محیطی است که فرد در آن به دنیا آمده و در آن به حیات خود ادامه می‌دهد و محققان بر این عقیده‌اند که فرد تحت تأثیر شدید والدین و اعضای خانواده‌اش قرار می‌گیرد و به‌همین دلیل وضع خانوادگی او در بروز رفتارهای خطرناک و ارتکاب جرایم تأثیری مستقیم دارد. این‌گونه تأثیر بر شکل‌گیری منش و شخصیت فرد و در نتیجه رفتارهای آتی آنها بسیار اثرگذار می‌باشد. دوگرف در این باره می‌نویسد: «اثرات سال‌های عمر بر تکوین و تحول آتی شخصیت افراد بسیار بدیهی بوده است و اگر خانواده به وظایف تربیتی عمل کند و اگر روابط بین والدین و فرزند طبیعی باشد و در محیط جو عاطفی محبت حاکم باشد و در نهایت اگر تمام نیازهای طبیعی فرد فراهم گردد، طفل به‌راحتی اجتماعی شده و همچنین در روابط خانوادگی و بیرون از آن رفتار متعادل خواهد داشت اما اگر شرایط و موقعیت به صورت دیگری باشد، یعنی خانواده از نظر تربیتی دچار نقیصه شده و اگر طفل از کمبود شدید عاطفی رنج ببرد و اگر والدین از هم جدا شده باشند، بدیهی است نتایج زیان‌بار آن دیر یا زود در طفل مشاهده خواهد شد. خانواده نقش تعیین‌کننده و قاطعی در انگیزه‌شناسی بزهکاری جوانان تعیین می‌نماید» [۵]. بنابراین خانواده به‌عنوان اولین نهاد اجتماعی که با آن سر و کار دارند، حسب وضعیت و شرایط حاکم بر آن، تأثیر زیادی بر جامعه‌پذیری یا اجتماع‌گریزی دارد. این‌گونه تأثیرات منفی، اختصاص به جرم خاصی ندارد و چه بسا شرایط حاکم بر یک خانواده به‌گونه‌ای باشد که در آن ارتکاب انحرافات سایبری امری قبیح محسوب نگردد و کودک و نوجوان با نوعی مشوق همراه بشوند. یقیناً فرد حاضر در این‌گونه شرایط، رفتارهای معارضی را بروز خواهد داد که متأثر از شرایط نابهنجار خانوادگی‌اش خواهد بود.

۴.۲.۳ همسالان معارض

گروه همسالان از دیگر نهادهای مرتبط با دنیای شخصی افراد می‌باشد که در رشد شخصیتی کودکان اهمیت بسیاری دارد. چرا که کودکان در میان همسالان خود احساس امنیت می‌کنند، برای رفتارهای خود هنجار مناسب می‌یابند و فهم و درک خود را شکل می‌دهند، مهارت بدنی - اجتماعی مناسب را کسب می‌کنند و انگیزه مشارکت و همیاری با دیگران را در خود می‌پروراند. طبق نظریه معاشرت ترجیحی ساترلند، افراد در معاشرت با دوستان و آشنایان و بخصوص کسانی که برای او اهمیت ویژه‌ای دارند، یکسری اقدامات را فرا می‌گیرد و با تجزیه و تحلیل آنها سعی در تقلید و الگوگیری از آنها می‌نماید. بنابراین، نوع گروه همسالانی که در آن، شخص عضویت دارد و ارزش‌ها و رفتارهای حاکم بر آن گروه، تأثیر مهمی در افکار اعضای آن گروه دارد. تا جایی که کودکان و نوجوانان با فراگیری آموزش‌های مخصوص ارتکاب جرم به خصوص جرایم سایبری که نیازمند تخصص برای ارتکاب می‌باشد، پس مرتکب این چنین جرایم می‌گردند. برای مثال در یک گروه که به ارتکاب جرم نشر سی‌دی‌های حاوی محتوای مبتذل مشغول می‌باشند این بسیار امر عادی می‌باشد. بنابراین، افراد با عضویت در این گروه‌ها الگوبرداری می‌کنند و مرتکب آن جرم می‌شوند حتی اگر نفعی برای آنها نداشته باشد.

۴ نقش بزه دیده سایبری

در علم جرم‌شناسی بزه‌دیده از دو منظر مورد مطالعه قرار می‌گیرد: ۱- بزه‌دیده‌شناسی اولیه ۲- بزه‌دیده‌شناسی ثانویه. در بزه‌دیده‌شناسی اولیه به بررسی نقش بزه‌دیده، در ارتکاب جرم پرداخته می‌شود. به عبارت دیگر در این نوع فرد بزه‌دیده، خود عاملی برای ارتکاب بزه محسوب می‌گردد. ولی در ثانویه فرد بزه‌دیده به عنوان شخصی می‌باشد که متحمل آسیب‌ها و خسارات مادی و معنوی و عاطفی شده است که سعی در جبران آنها شده است [۸]. فون هانتینگ در سال ۱۹۴۸ با انتشار کتاب «مجرم و قربانی او» بزه‌دیده‌شناسی علمی را پایه‌گذاری کرد و با ارائه سه مفهوم بزه‌کار، قربانی، بزه‌دیدگی مخفی و ارتباط خاص میان بزه‌کار و بزه‌دیده به بررسی تأثیر و نقش بزه‌دیده در ارتکاب جرم می‌پردازد [۷]. در ارتباط با جرایم سایبری نیز نقش بزه‌دیده اهمیت بسیار زیادی دارد و انکارناپذیر است. برای مثال: فردی که از ایمیل خود به‌طور کامل خارج نمی‌شود و امکان دستیابی دیگران به داده‌های شخصی‌اش را با این کار فراهم می‌کند. با اینکه اطلاعات شخصی خود را از طریق فیس‌بوک یا سایر شبکه‌های اجتماعی و حتی چت در اختیار دیگران می‌گذارد و حتی اینکه کامپیوتر شخصی خود را جهت تعمیر به افراد غیرمطمئن می‌سپارد، همه اینها می‌تواند فرد را به‌منزله یک طعمه در اختیار افراد سودجو قرار بدهد. جاذبه فضای سایبر خصایص و ویژگی فضای سایبری می‌تواند بر روی گرایش افراد به ارتکاب بزه بسیار تأثیرگذار باشد. ویژگی‌هایی نظیر تسهیل دسترسی به آخرین اطلاعات، گستره جهانی داشتن فضای سایبر، ریسک پایین دستگیری، ماهیت متفاوت جرایم سایبری جاذبه محتویات فضای اینترنت و آزادی اطلاعات و ارتباطات و خاص بودن بزه‌دیده سایبری، عدم نیاز به ارتباط نزدیک و فیزیکی با مجنی علیه، پراکندگی مجنی علیه سایبری و عدم کشف بسیاری از جرایم علیه افراد در عالم واقعی همگی می‌توانند دست به دست هم داده و ارتکاب افراد به‌سوی رفتار خلاف هنجار را تحریک

کنند. علاوه بر این موارد به این نکته نیز باید اشاره کرد که استفاده از سیستم‌های رایانه‌ای همانند گذشته در انحصار اقشار محدودی نمی‌باشد و چون فراگیر و دارای امکانات بی‌شماری است معمولاً گروه‌های جوان بیش از سایر اقشار در آن جذب می‌شوند. این در حالی است که تدوین‌کنندگان تدابیر پیش‌گیرانه اجتماعی با فضای مجازی رابطه عمیقی ندارند یا نمی‌توانند به اندازه جوانان و نوجوانان به فعالیت‌های شبکه‌ای بپردازند. این شکاف دیجیتال میان متولیان پیشگیری و بزه‌کاران و بزه‌دیدگان باید برطرف شود زیرا در غیر این صورت، به دلیل عدم درک متقابل نمی‌توان به تأثیرگذار بودن تدابیر پیش‌گیرانه امیدوار بود [۲].

۵ نتیجه‌گیری

جرائم رایانه‌ای به مثابه پدیده‌ای شگفت‌انگیز که با تولد آن تحولی شگرف در زندگی انسان‌ها پدید آمده است، گرچه برخی از جرائم آن شباهت‌هایی با جرائم سنتی دارد، اما تفاوت‌هایی در روش و ماهیت و نوع جرم دارد که از لحاظ جرم‌شناسی و کیفرشناسی و حقوق کیفری پژوهش‌های نو را می‌طلبد. یعنی می‌توان گفت که باتوجه به پیشرفت روزافزون زوایای مختلف این فضا و کارکردهای متنوع آن، شرایط هر روز فضا را برای ارتکاب اعمال مجرمانه نیز باز می‌کند؛ یعنی این فضا ضمن بر جای گذاشتن آثار مطلوب و توسعه خدمات به عموم مردم ولی از طرفی نیز می‌تواند زمینه بر جای گذاشتن آثار نامطلوب را نیز فراهم آورد. بدین ترتیب، به یقین می‌توان گفت حذف کامل این فضای فناوری ارتباطات و اطلاعات از صحنه زندگی انسان‌ها امکان ندارد ولی از طرفی هم منزه کردن این فضا از لوٹ وجود مجرمین هرگز ممکن نیست پس تنها راه حل این است که جامعه بشری را از ابتدایی‌ترین اقدام یعنی شناسایی علل بروز جرائم تا مکانیزم‌های حاکم بر فضا آگاه و سیر ارتکاب جرائم سایبری را مسدود کنیم. در این راستا اتخاذ تدابیر پیشگیرانه به شرحی که در بخش سوم رفت، بسیار ضروری است. واقعیت این است که مبارزه و کشف این‌گونه جرائم کاری بس دشوار است، چرا که به واسطه ویژگی‌های فضای مجازی که ظرفیت سوء استفاده از آن را بالا می‌برد، ویژگی‌هایی چون بدون مرز بودن فضای مجازی، کم‌هزینه‌گی و پرتیری 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، بازتاب جهانی موفقیت، امکان جذب حامی و همکار برای ارتکاب جرم از سراسر جهان بدون حضور فیزیکی، امکان جذب منابع مالی و پول‌شویی آسان تر و هرگونه انجام فعالیت‌های مالی الکترونیکی در جهت اهداف مجرمانه با توجه به پیچیدگی جرائم رایانه‌ای، مطالعه و پژوهش بیشتر و نیز تصویب قوانین مورد نیاز در این زمینه بسیار ضروری است.

پیشنهادها: در حال حاضر با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت آموزش بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرائم رایانه‌ای به خصوص جاسوسی رایانه‌ای و اینترنتی، این آموزش‌ها باید در مقاطع مختلف زمانی تکرار و روزآمد شوند. ۱- از آنجاکه پلیس به عنوان ضابط دادگستری وظیفه کشف جرائم را بر عهده دارد، در کنار آموزش قضات و سایر مقدمات قضایی، آموزش پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد، چون تعقیب و پیشگیری از جرائم سایبری مستلزم تربیت نیروهای متخصص می‌باشد. البته این توانایی را هم بایستی داشته باشند

که خود را به طور مستمر به روز نگه دارند و گرنه نمی‌توان با این جرایم مقابله کرد. ۲- آموزش‌های عمومی در سطح کارمندان دولت و نظامیان و همچنین مقامات قضایی؛ زیرا آنان برای یک قضاوت صحیح نیاز دارند که شناخت نسبی از ماهیت این فضا و نوع جرایم داشته باشند و برگزاری کلاس‌های تخصصی شدن محاکم این دسته از جرایم توصیه می‌گردد. ۳- تا حد ممکن عدم ذخیره‌سازی داده‌ها و اطلاعات طبقه‌بندی شده به شبکه‌های رایانه ای به خصوص شبکه جهانی اینترنت. ۴- مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به عنوان راهکاری سریع و کم‌هزینه و در عین حال مؤثر؛ در این روش تمامی درگاه‌های سیستم‌های رایانه‌ای از قبیل درایو، CD پورت‌های USB و ... از طریق سرور (شبکه) بسته شده و به این ترتیب کاربر رایانه نمی‌تواند هیچ داده و اطلاعاتی را وارد رایانه کرده و یا از آن خارج کند. در این حالت کاربر تنها به داده‌های مجازی که از سوی مسئولان و به منظور انجام وظیفه روی سیستم او قرار داده شده است، دسترسی خواهد داشت.

مراجع

- [۱] ابراهیمی، شهرام، جرم شناسی پیشگیری، ۱۳۹۰، جلد اول، چاپ اول، تهران، نشر میزان.
- [۲] جلالی فراهانی، امیرحسین و باقری اصل، رضا. پیش‌گیری اجتماعی از جرایم و انحرافات سایبری، ۱۳۸۶، مجله مجلس و پژوهش، شماره ۵۵.
- [۳] عالی‌پور، حسن، حقوق کیفری فناوری اطلاعات، ۱۳۹۰، چاپ اول، تهران، انتشارات خرسندی.
- [۴] فضل‌ی، مهدی، مسئولیت کیفری در فضای سایبر، ۱۳۸۹، چاپ اول، تهران، انتشارات خرسندی.
- [۵] قاسمی روشن، ابراهیم، عوامل اجتماعی و جرم، ۱۳۷۹، ماهنامه معرفت، شماره ۳۶.
- [۶] کی‌نیا، مهدی، مبانی جرم‌شناسی، ۱۳۸۶، جلد اول، چاپ هشتم، تهران، نشر دانشگاه تهران.
- [۷] مال‌میر، محمود و زرخ، احسان، پیشگیری از بزه‌دیدگی سایبری، ۱۳۸۹، فصلنامه مطالعات پیشگیری از جرم، شماره هفدهم.
- [۸] نجفی ابرندآبادی، علی حسین، تقریرات بزه‌دیده‌شناسی، ۱۳۷۴، تنظیم فاطمه قناد، دوره کارشناسی دانشگاه شهید بهشتی.
- [9] V. Shiva Kumar, Cyber Crime: prevention and detection, Asset, Director. A.P. Police Academy, 2008.
- [10] Michael Kunz and Patrick Wilson, computer crime and computer fraud, university of Maryland Department of criminology and criminal justice, 2004.
- [11] Marc D. Goodman and Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, I law info tech, 2010.
- [12] Ales Zavrsnik, Cybercrime Definitional Challenge and Criminological Particularities Masaryk, University journal of law and technology, 2008.

