مطالعات علوم سیاسی، حقوق و فقه

دوره ۲، شماره ۴، زمستان ۱۳۹۵

صفحات ۲۳۰- ۲۱۹

Online ISSN: ۲۴۷۶-۴۴۶۹

Print ISSN: ۲۵۳۸-۲۰۳۹

www.irijournals.com

پیشگیری غیر کیفری در جرایم اینترنتی

سام اکرمی [۱]، سعیده اکرمی [۲]

[۱] دانشجوی دوره دکتری حقوق کیفری و جرم شناسی دانشگاه آزاد قم

[۲] دانشجوی کارشناسی ارشد جزا و جرم شناسی واحد تهران جنوب

چکیده

تحقیق حاضر با بررسی وارائه راهکارهای مناسب برای پیشگیری از وقوع جرم به صورت توصیفی-تحلیلی صورت گرفته است. فضای سایبر با تمام اثرات و نتایج مطلوب و مثبتی از قبیل آسان شدن امور، کم هزینه شدن امور و...که دارد به همان نسبت نیز آثار نامطلوب و مخربی نیز با خود همراه. جرایم سایبری در فضای صورت میگرد که شرایط و اوضاع احوال خاصی دارد از قبیل گمنامی کاربران، عدم امکان شناسایی هویت مجرمان، بدون مرز بودن این فضا، سهولت ارتکاب جرم، کثرت بزه دیدگان. همه گیر شدن این تکنولوژی به گونه ای است که امکان حذف این فناوری از زندگی روزمره افراد وجود نداشته و به همین دلیل نیز امکان پاک سازی جوامع از حیث وجود جرایم سایبری نیز امکان پذیر نیست. لذا علاوه بر اقدام های کیفری که قانونگذار برای این مجرمین در نظر میگیرد باید به روش هاو اقدامات غیر کیفری نیز در جهت پیشگیری از این جرایم و جلوگیری از تکرار اینگونه جرایم نمود. توجه به تدابیر پیشگیرانه غیر کیفری و کیفری مناسب به جای مجازات های بی فایده از اهمیت بالایی برخوردار است. در تلاش هستیم با ارایه پیشنهاداتی به سیاست گذاران جنایی کشور جهت مقابله و پیشگیری از جرایم سایبری کمک شایانی شود.

واژه‌های کلیدی: پلیس فتا، فضای سایبر، پیشگیری کیفری، پیشگیری وضعی.

۱- مقدمه

با جهانی شدن اینترنت و ارتباطات همواره جهان فناوری و اطلاعات به مانند جهان خاکی از بزه و بزهکاری در امان نمانده است. برای ارتکاب جرم و بزهکاری چه در دنیایی فیزیکی و چه در دنیایی اینترنتی عوامل فردی و محیطی بسیاری تاثیر گذار هستند؛ اما در این بین مجرمین سایبری ویژگی های خاص و منحصر به فردی نسبت به بزهکاران دنیایی فیزیکی دارند از قبیل هوش بالاتر و قابلیت انطباق پذیری بیشتر که به آنها در پیشبرد اهداف شومشان کمک میکند و خود فضای سایبر نیز ویژگی ها و بسترهای جرم خیزی نیز دارد که انگیزه مجرمین را تقویت کرده و به آنان در رسیدن به اهداف شومشان کمک خواهد کرد. امروزه با همه گیر شدن اینترنت و فضای سایبر و پیشرفت امور به وضوح روشن است که تمامی امور خرد و کلان زندگی بشر تحت تایر این تکنولوژی قرار گرفنه است که شاهد آن هستیم تمامی اقشار جامعه از قبیل مردان، زنان، نوجوانان و حتی خردسالان، پیران و کم سوادان به این دنیا پا گذاشته و این فضا باعث حذف محدودیت های مکانی و مرزی میشود و افراد میتوانند با ایجاد شبکه جهانی که به وجود آمده است به راحتی در سراسر دنیا با یکدیگر ارتباط برقرار کنند

ما شاهد این هستیم کشور ما در بحث پیشگیری اعم از پیشگیری کیفری و غیر کیفری در مورد جرایم رایانه ای موفق نبوده و با توجه به پیشرفت روزافزون این تکنولوژی و فراوانی وسایل نوین در جهت ارتکاب جرایم سایبری لازم است که اهداف بلند مدتی از قبیل پیشگیری اجتماعی و وضعی و حتی تهیه قوانین مفید و کارآمد اقدام کرده تا به دنبال ارایه راهکارهای پیشگیری برای جلوگیری از تکرار این جرایم باشیم تا با نهادینه سازی فرهنگ و اخلاق شاهد فضای مثبت وکارآمد این تکنولوژی در آینده باشیم و همانگونه که در برخورد با جرایم فیزیکی سیاست های جنایی و تقنینی متفاوت و ویژه ای را اتخاذ میکنیم لازم است در مورد جرایم سایبری نیز از اینگونه تدابیر نیز استفاده شود زیرا در واقع در جهان کنونی تمامی افراد دارای دو نوع زندگی هستند یکی زندگی واقعی و دوم زندگی مجازی هستند و با توجه به شرایطی که در این تحقیق نسبت به جرایم سایبری ذکر خواهد شد ارتکاب اینگونه جرایم در فضای سایبر بسیار آسان تر و کم خطر تر برای مجرمین میباشد.

۲. پیشگیری غیر کیفری در جرایم رایانه ای

در خصوص مفهوم پیشگیری و خصوصیات آن تعاریف متعددی ارایه گردیده است. در یک تعریف، موریس کوسن جرم‌شناس کانادایی پیشگیری را چنین تعریف نموده: «مجموعه اقدام‌ها و تدابیر غیرقهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم و کاهش وخامت جرم پیرامون علل جرایم اتخاذ می‌شود» (ابراهیمی، ۱۳۹۰: ۳۸). با توجه به تعاریف متعددی که از پیشگیری صورت گرفته است، به طور کلی می‌توان چند ویژگی عمده برای پیشگیری احصاء نمود: ۱. غیرقهرآمیز بودن تدابیر ۲. اختصاصی بودن اقدامات ۳. کاستن آثار جرم ۴. درنظرگرفتن عوامل خطر و محیط اجتماعی (جعفری، مجتبی ۱۳۸۷: ۱۴۷).

از میان تقسیم‌بندی‌های مختلفی که در خصوص تدابیر پیشگیرانه صورت گرفته است دو نوع پیشگیری اجتماعی و پیشگیری وضعی از مقبولیت بیشتری برخوردارند. به همین دلیل، در بررسی شیوه‌های پیشگیری از جرایم سایبری از این نوع تقسیم‌بندی استفاده می‌گردد. پیش از پرداختن به جزییات این دو نوع پیشگیری، مناسب است به قطعنامه هشتمین کنگره سازمان ملل متحد در خصوص پیشگیری از جرم و اصلاح مجرمان که در سیزدهمین اجلاس سازمان ملل متحد توسط مجمع عمومی سازمان در قالب قطعنامه شماره ۴۵/۱۲۱ تأیید گردید، اشاره گردد. در این قطعنامه از کشورهای عضو خواسته شده است که در صورت لزوم با مدنظر قرار دادن موارد زیر تلاش‌های خود را در مبارزه با جرایم رایانه‌ای شدت بخشند:

۱ .مدرنیزه کردن قوانین و دادرسی کیفری

۲ .ارتقای ضوابط پیشگیرانه و امنیتی رایانه

۳ .گزینش راه‌هایی برای حساس کردن عامه مردم و قوه قضاییه و مجریان قوانین نسبت به این مسأله و اهمیت پیشگیری از ارتکاب جرم‌های رایانه‌ای

۴. دادن آموزش‌های کافی به دادرسان، مأموران و عوامل مسئول در زمینه پیشگیری، تحقیقات، تعقیب و احقاق حق در جرم‌های اقتصادی و زیربنایی

۵ .مطالعات دقیق با همکاری سازمان‌های ذینفع در مورد قواعد اخلاقی مربوط به استفاده از رایانه و تعمیم این قواعد به منزله بخشی از مواد درسی و آموزش انفورماتیک

۶ .اتخاذ سیاست‌های مربوط به بزه‌دیدگان جرم‌های رایانه‌ای بر اساس اعلامیه سازمان ملل متحد در مورد اصول بنیادی عدالت برای بزه‌دیدگان و قربانیان سوءاستفاده از قدرت

لازم به ذکر است که توسل به تدابیر پیشگیرانه، توجیهی جهت ایجاد اخلال در امنیت و آزادی مردم محسوب نمی‌گردد. لذا این تدابیر باید با حفظ حریم خصوصی اشخاص و صرفاً جهت پیشگیری از جرایم سایبری صورت گیرد و مفاد ماده ۱۲ اعلامیه حقوق بشر همواره باید مدنظر قرار گیرد. مطابق این ماده «احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخله خودسرانه واقع شود و شرافت و اسم و رسمش مورد حمله قرار بگیرد، هرکس حق دارد که در مقابل این گونه مداخلات و حملات مورد حمایت قرار بگیرد». (اکبر وروایی، حسین مومنی پور ۱۶:۱۳۹۰)

۲-۱ پیشگیری وضعی در جرایم اینترنتی

نگاهی گذرا به ادبیات حقوقی موجود نشان می‌دهد که قانونگذار در اکثر قریب به اتفاق موارد از واژه پیشگیری استفاده نموده است (ر.ک: زینالی، مدیریت پیشگیری از جرایم و آسیب‌های اجتماعی در حقوق ایران و چالش‌های فراروی آن: ۵۴). جوهره ذاتی جرم‌شناسی به عنوان شاخه‌ای از علوم جنایی بر پیشگیری از جرایم استوار بوده که به بررسی علل، آثار و نتایج پدیده بزهکاری می‌پردازد (گلدوزیان، بایسته‌های حقوق جزای عمومی: ۲۴). معانی تازه برای پیشگیری از جرم با تأکید بر عوامل فردی و اجتماعی مختلف که بر وقوع جرم مؤثرند، راهکارهایی را پیش روی جرم‌شناسان قرار داده است. به تعبیر ساده، پیشگیری هر اقدام سیاست جنایی بدون تأکید بر تهدید کیفری یا اجرای آن است که با هدف تحدید امکان پیشامد جنایی از راه‌های گوناگون انجام می‌شود. با این وصف قلمرو جرم‌شناسی امروزه بسیار گسترده شده و بزهکاری نیز تا کنون مورد مطالعه رشته‌های مختلفی قرار گرفته است (اردبیلی، حقوق جزای عمومی، ج ۱: ۵۲).

در این میان پیشگیری وضعی به عنوان راهکار جدید پیشگیرنده از بزهکاری و جانشین گونه‌های متعارف پیشگیری از جرم به ویژه پیشگیری اجتماعی مطرح می‌شود (نجفی ابرندآبادی، پیشگیری عادلانه از جرم: ۵۸۰). کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند؛ به عبارت دیگر، این نوع پیشگیری دربرگیرنده مجموعه تدابیر غیرکیفری است که از طریق از بین بردن یا کاهش فرصت‌های مناسب از ارتکاب بزه جلوگیری می‌کند (چاله چاله، اصول و مبانی پیشگیری از جرم: ۶). طرح پیشگیری وضعی از جرم به عنوان یک نظریه علمی اصالتاً تأسیسی انگلیسی است که توسط سه دانشمند مطرح و توسعه یافته است (ر.ک: صفاری، مبانی نظری پیشگیری از وقوع جرم: ۲۹۰).

توجه به مثلث جرم می‌تواند به درک این موضوع کمک نماید. با این توضیح که برای ارتکاب یک جرم، اجتماع سه عامل ضروری می‌باشد. مهم‌ترین آنها که قاعده مثلث جرم را تشکیل می‌دهد، انگیزه مجرمانه است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد مجرمانه می‌شود. برای از بین بردن این عامل، ضروری است تدابیر پیشگیرانه اجتماعی اتخاذ گردد؛ اما اگر به هر دلیل مجرمان واجد انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت و ابزار ارتکاب جرم جلوگیری کرد. از اینان این دو هم سلب فرصت از مجرمان اهمیت بیشتری دارد؛ زیرا متصدیان امر هر چه بکوشند ابزارهای

ارتکاب جرم را از سطح جامعه جمع‌آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آنها دست یابند. هر چند در عین حال نباید اهمیت جمع‌آوری این ابزارها را در کاهش جرایم نادیده گرفت (خلفی، مبانی حقوقی پیشگیری از جرم: ۲۱).

رکن اصلی پیشگیری وضعی، حفظ آماج‌ها و بزه‌دیدگان از تعرض مجرمان است. آنچه در این نوع پیشگیری دنبال می‌شود، این است که با جاذبه‌زدایی از جرم، بالا بردن هزینه و کاهش احتمال نتیجه‌گیری از جرم، زمینه ارتکاب آن را از بین ببریم یا تا حد قابل قبولی پایین بیاوریم. این نوع پیشگیری اساساً بزه‌دیده‌مدار تلقی می‌شود و بنابراین با پیشگیری اجتماعی که بزهکار را در کانون توجه خود قرار می‌دهد، متفاوت است. هر چند اینجا نیز مجرم به صورت غیرمستقیم مطرح می‌باشد.

در زمینه پیشگیری وضعی از جرایم رایانه‌ای بایستی اذعان داشت با این که مشکلات بسیاری بر سر راه آن وجود دارد، اما باز هم از جایگاه خاصی برخوردار است. یکی از دلایلی که می‌توان جهت تویجه پیشگیری وضعی از این جرایم نمود، همین قابلیتی است که فضای تبادل اطلاعات فراهم آورده است. همان طور که گفته شد، ماهیت جرم رایانه‌ای به گونه‌ای است که نمی‌توان با دست تهی مرتکب آن شد و باید علاوه بر صرف اندیشه کافی، ابزارها و لوازم مورد نیاز را هم در اختیار داشت؛ اما این بدان معنا نیست که برای ارتکاب قسمت عمده‌ای از این جرایم باید تخصص و مهارت فوق‌العاده داشت، بلکه اگر افراد از دانش کافی جهت بهره‌برداری ابتدایی از سیستم‌های رایانه‌ای برخوردار باشد زمینه برای وقوع جرم مساعد می‌شود. از این رو آنچه در پیشگیری وضعی از جرایم رایانه‌ای دنبال می‌شود، این است که با اتخاذ تدابیر فنی، از بهره‌برداری از این گونه قابلیت‌های جرم‌برانگیز این فضا جلوگیری شود؛ به عبارت دیگر، مخاطبان اصلی پیشگیری وضعی از جرایم رایانه‌ای کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی می‌کنند با امکاناتی که فضای تبادل اطلاعات در اختیار آنها قرار می‌دهد، مرتکب جرم شوند، نه این که خود دست به ابتکار عمل بزنند که در این صورت همان طور که در ادامه توضیح خواهیم داد، از پیشگیری وضعی کاری ساخته نخواهد بود.

دلیل مهم دیگری که باعث شده پیشگیری وضعی در جرایم رایانه‌ای با تمام کاستی‌های آن دنبال شود، بحث شبکه‌های اطلاع‌رسانی رایانه‌ای است. تقریباً می‌توان گفت هر گونه اقدامی در فضای تبادل اطلاعات مستلزم این است که از طریق شبکه‌های اطلاع‌رسانی رایانه‌ای بدین فضا وارد شویم، آن هم شبکه‌هایی که در دنیای امروز به طور تخصصی فعالیت می‌کنند و هر یک به ارائه یک نوع خدمات در فضای تبادل اطلاعات می‌پردازند و از همه مهم‌تر این که تحت نظارت دولت و مقررات قانونی لازم‌الاجرا هستند. در حقیقت، این شبکه‌ها پل ارتباطی ما با فضای تبادل اطلاعات هستند و به این ترتیب اگر در این پل ارتباطی اقدامات پیشگیرانه اقدامات پیشگیرانه وضعی مؤثری اعمال شود، می‌توان امیدوار بود که تا حدودی از وقوع جرایم در فضای تبادل اطلاعات جلوگیری می‌شود. این وضعیت مزیتی برای پیشگیری وضعی از این جرایم محسوب می‌شود که پیشگیری وضعی از جرایم سنتی از آن بی‌بهره است. چرا که در آنجا هیچ عامل مؤثری را نمی‌توان میان جرم و مجرم قرار داد. آنچه امروزه در قالب نصب دیوار آتشین یا پالایه در این شبکه‌ها انجام می‌شود، چیزی جز پیشگیری وضعی نمی‌باشد (جلالی فراهانی، پیشگیری از جرایم رایانه‌ای: ۱۱۰). لذا در اینجاز به مجرمان اجازه داده نمی‌شود که به راحتی به مقصود خود نایل شوند.

همچنین با پیدایش پدیده‌هایی چون پلیس گشت اینترنت، پیشگیری وضعی در این فضا جلوه دیگری نیز به خود گرفته است که البته با الهام از نتایج مثبت پلیس گشت پیاده به عنوان یک اقدام وضعی پیشگیرانه به اجرا درآمده است.

آخرین دلیلی که می‌توان جهت پیشگیری وضعی از جرایم رایانه‌ای ذکر کرد، به ویژگی منحصر به فرد فضای تبادل اطلاعات مربوط می‌شود. در این فضا شخص می‌تواند برخلاف دنیای فیزیکی در یک زمان در چند نقطه ظاهر شود و با انجام یک عمل بر چند نقطه تأثیر بگذارد. به عنوان مثال یک مجرم می‌تواند از طریق شبکه به تعداد بسیاری کامپیوتر میزبان متصل شود و به طور همزمان در فعالیت تمامی آنها اختلال ایجاد کند یا با آنها ارتباط زنده برقرار کرده و مرتکب اشکال مختلفی از عناوین مجرمانه شود. البته باید توجه داشت که این خصیصه سوای از حوزه تأثیرگذاری فضای تبادل اطلاعات است که نسبت به دنیای

فیزیکی، حوزه بسیار گسترده‌تری را در برمی‌گیرد. به عنوان مثال، گستره تأثیرهای مخرب نشر مطالب تحریک‌آمیز علیه امنیت ملی یا مطالب توهین‌آمیز نسبت به مقدسات مذهبی یا تصاویر حاوی هرزه‌نگاری در این فضا بر کسی پوشیده نیست.

ناگفته نماند که پیشگیری وضعی در کنار این قابلیت‌ها، در فضای تبادل اطلاعات با محدودیت‌های فنی و قانونی نیز مواجه است که البته بخشی از این محدودیت‌ها در فضای فیزیکی هم وجود دارند. با این توضیح که متعاقب اجرای یک طرح فنی پیشگیرانه وضعی، راه‌های خنثی‌کننده آن فوراً در فضای تبادل اطلاعات در اختیار همگان قرار می‌گیرد و عملاً پیشگیری وضعی مزبور کان لم یکن می‌شود. همچنین وجود ابزارها و فناوری‌هایی در فضای تبادل اطلاعات، این امکان را در اختیار اشخاص قرار می‌دهد که در نهایت با ناشناس ماندن و پنهان کردن محتوای فعالیت‌های خود به بهره‌قرداری از این فضا بپردازند. کما این که از نظر قانونی نیز پیشگیری وضعی از جرایم رایانه‌ای موجب به خطر افتادن حریم خصوصی افراد در فضای تبادل اطلاعات و اصل آزادی جریان اطلاعات و حق بهره‌برداری مشروع اشخاص از اطلاعات می‌شود (برای مطالعه بیشتر ر.ک: همان: ۱۱۶-۱۱۲).

۲-۲ مصادیق پیشگیری وضعی در جرایم رایانه‌ای

از جمله اقدامات پیشگیرانه وضعی در خصوص جرایم رایانه‌ای می‌توان به موارد ذیل اشاره نمود:

۱-شناسایی بسترهای جرم‌خیز: اولین گام جهت ایجاد یک برنامه پیشگیری‌کننده، شناسایی تهدیدها می‌باشد؛ به عبارت دیگر، اتخاذ هر نوع اقدام جرم‌شناختی در راستای پیشگیری از جرایم رایانه‌ای، بررسی عوامل موجد جرم می‌باشد که اقدامات بعدی پیشگیری‌کننده نیز بر این اساس بایستی استوار گردد.

۲-دشوار ساختن ارتکاب جرم: این امر از طریق حفاظت از اهداف و قربانیان جرم، کنترل و ایجاد محدودیت در دسترسی به موقعیت‌های ارتکاب جرم، خنثی سازی و منحرف کردن مجرمان و برچیدن ابزار ارتکاب جرم میسر می‌گردد. خیلی از ویروس‌ها و کرم‌های اینترنتی هنگامی که وارد کامپیوتر می‌شوند، سیستم امنیتی را از کار می‌اندازند و اقدام به دادن اطلاعات شخص دریافت‌کننده به شخص فرستنده ویروس می‌نمایند که از طریق نصب آنتی ویروس‌ها و ضد کرم‌های اینترنتی که به روز شده‌اند می‌توان از ورود آنها و سرقت داده‌ها پیشگیری نمود (بوستان‌چی، پیشگیری از جرایم رایانه‌ای).

این تدابیر در زمره مهم‌ترین تدابیر پیشگیرانه وضعی از جرایم اینترنت قرار دارند. بر این اساس سعی می‌شود با نصب سیستم‌ها یا برنامه‌های خاص بر روی گروه‌های دسترسی به شبکه یعنی کامپیوترهای شخصی، مسیریاب سیستم‌های ارائه‌دهندگان خدمات شبکه‌ای و از همه مهم‌تر ایجادکنندگان نقطه تماس بین‌المللی، از ورود یا ارسال برخی داده‌های غیرمجاز یا غیرقانونی جلوگیری شود. این سیستم‌ها و برنامه‌ها عمدتاً در سه قالب دیوارهای آتشین، فیلترها و پراکسی‌ها هستند. این ابزارها حاوی فهرستی از موضوع‌های مجاز یا غیرمجاز هستند و بر اساس فرآیند انطباق عمل می‌کنند. بعضی از آنها مانند فیلترها و دیوارهای آتشین یک سویه عمل می‌کنند، یعنی فقط از ورودی‌های غیرمجاز جلوگیری می‌کنند؛ اما بعضی دیگر دوسویه عمل می‌کنند و علاوه بر ورودی‌ها از خروجی‌ها هم مراقبت می‌نمایند.

بر اساس ماده ۲۲ قانون جرایم رایانه‌ای، کمیته تعیین مصادیق محتوای مجرمانه شامل وزیر یا نماینده وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر نماینده مجلس شورای اسلامی به انتخاب کمیسیون حقوقی و قضایی و تأیید مجلس شورای اسلامی می‌باشد که البته ریاست آن کمیته هم به عهده دادستان کل کشور است.

این کمیته در دی ماه ۱۳۸۸ فهرستی از مصداق‌های محتوای مجرمانه را ارائه داد. این فهرست در پنج فصل در بخش‌های محتوای خلاف عفت و اخلاق عمومی، محتوای علیه مقدسات، محتوای علیه امنیت و آرامش عمومی، محتوای علیه مقامات و نهادهای دولتی و عمومی و محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم تهیه شده است. هر چند بخشی از این فهرست به مواردی اشاره دارد که در قانون مجازات اسلامی نیز آمده است، لیکن در برخی از موارد مصادیق ارائه شده تازگی دارد.

در این راستا پیش‌بینی مسئولیت کیفری آن هم به صورت صریح برای اشخاص حقوقی یکی از نوآوری‌های قانون جرایم رایانه‌ای است، چرا که ماده ۱۹ (۷۴۷ قانون مجازات) این قانون مقرر می‌دارد: «در موارد زیر چنانچه جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود: الف) هر گاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود. ب) هر گاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع پیوندد. ج) هر گاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود. د) هر گاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

مطابق تبصره ۱ ماده ۲۰ (۷۲۰ قانون مجازات) این قانون هم مدیر شخص حقوقی که طبق بند ب این ماده منحل می‌شود تا ۳ سال حق تأسیس یا نمایندگی یا تصمیم‌گیری یا نظارت بر شخص دیگری را نخواهد داشت. بدیهی است که شناخت مسئولیت کیفری برای شخص حقوقی و ایجاد محدودیت در دسترسی به موقعیت‌های جرم‌زا و برچیدن ابزار ارتکاب جرم برای مدیر شخص حقوقی به لحاظجرم‌شناسی در حوزه پیشگیری وضعی دارای اهمیت فراوان می‌باشد.

۳-تدابیر مراقبتی و نظارتی: از این روش تحت عنوان کنترل دسترسی یاد می‌شود که شامل استفاده ازرمز و کد عبور می‌باشد که باید در اختیار دیگران قرار نگیرد. نظارت شبکه‌ای شاید بیش از آن که یک اقدام پیشگیرانه باشد، از لحاظ بازدارندگی مورد توجه قرار می‌گیرد. این اقدام به دو شکل فنی و انسانی قابل اجراست. در حالت فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیه فعالیت‌های شبکه‌ای اشخاص حتی ضرباتی که بر روی صفحه کلیدشان زده‌اند یا نقاطی را که به وسیله ماوس بر روی آنها کلیک کرده‌اند، ضبط می‌کنند. سپس مأمور موردنظر می‌تواند با بررسی این سوابق، موارد غیرقانونی را تحت پیگرد قرار دهد. در خصوص این مصداق پیشگیری وضعی ماده ۲۱ (۷۲۱ قانون مجازات) قانون جرایم رایانه‌ای مقرر می‌دارد: «ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کمیته تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرایم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند.«...

وانگهی، تدابیر سازمانی مشتمل بر انتخاب پرسنل متخصص و آموزش امنیت نیز از جایگاه ویژه‌ای برخوردار می‌باشد (باستانی، جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری: ۱۱۶).

۴-رمزنگاری در رایانه: رمزنگاری‌ها به صورت رمز درآوردن اطلاعات و داده‌ها در شبکه‌های رایانه‌ای برای محدود نمودن دسترسی افراد به اطلاعات محرمانه ضرورت دارد. این روش بیشتر در مراکز نظامی کاربرد دارد. این دو اقدام پیشگیرانه تا حدی از لحاظ کارکرد با یکدیگر تفاوت دارند، اما از آنجا که یک هدف را دنبال می‌کنند، لذا آن دو را در اینجا با هم بررسی نموده‌ایم.

همان گونه که از نام این اصطلاحات پیداست، این ابزارها ماهیت اصلی یک مفهوم را پنهان یا غیرقابل درک می‌کنند تا غیر قابل شناسایی و تشخیص گردد. ابزار ناشناس‌کننده، هویت اشخاص را در فضای اینترنت پنهان می‌کنند و از این طریق به آنها امکان می‌دهند تا با ایجاد حریم بیشتر به فعالیت شبکه‌ای بپردازند. این اقدام به ویژه برای زنان و کودکان یا به طور کلی اشخاصی که به هر دلیل آسیب‌پذیرند، سودمند است؛ زیرا بی‌آن که فرصت شناسایی خود را به مجرمان اینترنت بدهند، می‌توانند به فعالیت‌های شبکه‌ای بپردازند؛ اما از ابزارهای رمزنگاری بیشتر برای محتوای ارتباطات استفاده می‌شود. در اینجا بر

اساس کدهای خاصی متن اصلی به رمزنوشته تبدیل می‌شود و گیرنده در مقصد به وسیله کلیدی که در اختیار دارد، آن را رمزگشایی می‌کند. متأسفانه ابزارهای متنوع و بسیاری در فضای اینترنت برای شنود و دستیابی به ارتباطات افراد وجود دارد که بهره‌گیری از برنامه‌های رمزنگاری می‌تواند خطر این گونه تعرض‌ها را کاهش دهد.

۵-کاهش جاذبه از آماج‌ها و قربانیان جرم: در این گونه پیشگیری با حذف آماج‌های جرم، علامت‌گذاری بر رایانه‌ها، تقلیل فرصت‌های وسوسه‌انگیز و وضع قواعد خاص در این حوزه می‌توان از بزه‌دیدگی مجدد اشخاص آسیب‌پذیر نیز پیشگیری نمود. در این رابطه معاونت آگاهی نیروی انتظامی اواخر سال ۱۳۷۸ شروع به جمع‌آوری اطلاعات پیرامون اطفال بزه‌دیده جرایم رایانه‌ای نموده است که در نتیجه بررسی‌های متعدد کارشناسی، تشکیل واحدهای پیشگیری و مبارزه با جرایم رایانه‌ای را در این حوزه ضروری دانسته است. چرا که با شناسایی پیشگیرانه علایم کودکان در معرض خطر جرایم رایانه‌ای و وضع قواعدی برای استفاده آنها از اینترنت و رایانه می‌توان امنیت این قشر آسیب‌پذیر را به هنگام وب‌گردی تأمین نمود (حسینی، جرایم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن: ۹۴).

۲-پلیس فتا و نقش آن در پیشگیری از جرایم رایانه ای

پلیس فتا بر اساس ماده ۴ قانون نیروی انتظامی جمهوری اسلامی ایران درباره وظایف این نیرو به وجود آمده است: اولین وظیفه نیروی انتظامی در این ماده استقرار نظم و امنیت و تامین آسایش عمومی و فردی است و پلیس فتا مسوول استقرار این نظم در فضای مجازی شناخته شده است. با تاسیس پلیس فضای مجازی در بهمن ۱۳۸۹ فرماندهی پلیس فتا به سرعت در تمام استان های کشور تشکیل گردید. این پلیس، جرایم بسیار متنوع و وسیعی را پیگیری میکند که تعدادی از آن ها اینترنتی و رایانه ای است اما برخی نیز مخابراتی و تکنولوژیک است. به طور کلی هر نوع جرمی که با فن آوری انجام شود به پلیس فتا مربوط میشود. ماهیت اصلی پلیس فتا عملیاتی است به ان معنا که به صورا کاملا تخصصی و از طریق تجهیز به منافع ارزشمند نیروی انسانی، دانش و تجهیزات با توان عملیاتی قابل قبول نیست به تامین امنیت معنای تولید و تبادل اطلاعات با رویکرد مقابله با جرایم از طریق پیش بینی، پیشگیری و کشف جرم اقدام می نماید.

۱-وظایف پلیس فتا:

۱-ایجاد امنیت و کاهش مخاطرات برای فعالیت علمی، اقتصادی

۲-ممانعت از تعرض به ارزش ها و هنجارهای جامعه

۳-مراقبت و پالایش از فضای تولید و تبادل اطلاعات برای پیشگیری از تبدیل شدن این فضا به بستری برای انجام هماهنگی و عملیات غیر قانونی و مجرمانه

۴-حفاظت و صیانت از هویت دینی و ملی

۲-اهداف پلیس فتا:

۱-حفظ حریم خصوصی کاربران و آزادی های مشروع

۲-صیانت از منافع، اسرار و اقتدار ملی در فضای تولید و تبادل اطلاعات

۳-صیانت از هویت دینی، ملی و ارزش های انسانی جامعه در فتا

۴-تامین امنین فضای تولید و تبادل اطلاعات (سایت رسمی پلیس فتا)

۳-بررسی رویکرد های پیشگیرانه قابل اتخاذ از سوی پلیس سایبری:

امروزه حوزه جرایم رایانه ای علاوه بر آن که حوزه جرایم سنتی را تحت تاثیر خود قرار داده است از جرایم علیه امنیت ملی گرفته تا جرایم سازمان یافته، جرایم علیه اموال و مالکیت افراد و تمامیت جسمی و حیثیتی آن ها یک سری جرایمی که منحصراً به فضای تبادل اطلاعات تعلق دارد را هم در بر می گیرد.

پیشگیری و مبارزه با جرایم رایانه ای در دنیا و ایران به علت پذیرش کنوانسیون بوداپست در سال ۲۰۰ میلادی، اغلب توسط یک نهاد تخصصی و انتظامی و امنیتی بنام پلیس سایبری انجام می گیرد. بنابرایت در ذیل به بررسی تدابی پیشگیرانه پلیس سایبری در فضای مجازی پرداخته می شود.

۲-۴ پیشگیری وضعی قابل اعمال توسط پلیس سایبری:

با توجه به ویژگی پیشگیری وضعی که با جاذبه زدایی از سیبل جرم، بالا بردن هزینه و کاهش احتمال نتیجه گیری از جرم، زمینه ارنکاب آن را از بین میبرد یا تا حد چشم گیری پایین می آورد (صفاری، علی،۵۲)

جرم رایانه ای به گونه ای است که نمی توان با دست تهی مرتکب آن شد و باید علاوه برصرف اندیشه کافی، ابزارها و لوازم مورد نیاز را هم در اختیار داشت؛ اما این بدین معنا نیست که برای ارتکاب قسمت عمده ای از ان جرایم باید تخصص و مهارت فوق العاده دانست، بلکه اگر از دانش کافی جهت بهره برداری ابتدایی از سیستم های رایانه ای برخوردار باشید. خود فضای تبادل اطلاعات امکاناتی در اختیار شما قرار می دهد که زمینه برای وقوع جرم مساعد می شود.

آنچه در پیشگیری وضعی از جرایم رایانه ای دنبال می شود، این است که با اتخاذ تدابیر فنی از بهره برداری از این گونه قابلیت های جرم انگیز این فضا جلوگیری شود؛ به عبارت دیگر، مخاطبان اصلی پیشگیری وضعی از جرایم رایانه ای کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی میکنند با امکاناتی که فضای تبادل اطلاعات در اختیار آنها قرار می دهد مرتکب جرم شوند، نه اینکه خود دست به ابتکار عمل بزنند که در این صورت، از پیشگیری وضعی کاری ساخته نخواهد بود.

دلیل مهم دیگری که باعث شده پیشگیری وضعی در جرایم رایانه ای با تمام کاستی های آن دنبال ود، بح شبکه های اطلاع رسانی رایانه ای است. تقریبا می توان گفت هرگونه اقدامی در فضای تبادل اطلاعات مستلطم این است که از طریق شبکه های اطلاع رسانی رایانه ای بدین فضا وارد شویم، آن هم شبکه هایی که در دنیایی امروز به طور تخصصی فعالیت می کنند و هریک به ارایه یک نوع خدمات در فضای تبادل اطلاعات می پردازند و از همه مهم تر اینکه تحت نظارت پلیس و مقررات قانونی لازم الاجرا هستند و به این ترتیب اگر در این پل ارتباطی اقدامات پیشگیرانه وضعی از این جرایم محسوب می شود که پیشگیری وضعی از جرایم سنتی از آن بی بهره است. چرا که در آنجا هیچ عاملی موثری را نمی توان میان سیبل وجود قرار دارد. آنچه امروزه در قالب فیلترینگ و یا گشت سایبری انجام می شود. چیزی جز پیشگیری وضعی نمی باشد.

۲-۵ پیشگیری اجتماعی قابل اعمال توسط پلیس سایبری:

هدف پیشگیری اولیه کل جامعه است و این نوع پیشگیری تلاش دارد تا ک جامعه راد در مقابل خطر بزهکاری و بزه دیدگی تقویت کند و این هدف در سطوح و شیوه های مختلف محقق می شود.

این شیوه ها شامل: آموزش همگانی، مقالات و پژوهش های علمی، فرهنگ سازی سایبری، کارگاه های آموزشی در جهت کلاهبرداری رایانه ای، کارگاه آموزشی امنیت تلفن همراه، برگزاری و شرکت در نمایشگاه ها و همایش های مرتبط با حوزه قضایی مجازی، اطلاع رسانی از طریق وب سایت تخصصی پلیس فتا، تیزرها و تبلیغات تلویزیونی با محتوای جرایم سایبری میشود که میتواند تاثیر به سزایی در پیشگیری از این سری جرایم دارد.

۲-۶ پیشگیری اجتماعی در جرایم اینترنتی

این نوع پیشگیری به طور کلی به دو دسته پیشگیری اجتماع‌مدار و رشدمدار تقسیم می‌گردد؛ که به ارایه راهکارهای در جهت بهتر انجام شدن این پیشگیری میپردازیم:

۱-آموزش فرهنگ استفاده مفید از فضا اینترنت

یکی از تدابیر پیشگیرانه جامعه‌مدار از بروز تبعات نامطلوب یک ابداع جدید، استفاده از ابزارهایی در جهت نهادینه کردن کاربری صحیح و مشروع از آن می‌باشد. در این راستا، فضای مجازی به عنوان دستاورد بشری همواره آثاری اعم از مثبت و منفی در جامعه به وجود آورده است که به دنبال آن سیاستگذاران جنایی کشورها به دنبال ارایه تدابیر لازم جهت تبدیل استفاده‌های نامشروع از این فضا به کاربری‌های مفید و مطابق با اهداف اساسی و ابتدایی این نوع‌آوری بوده‌اند. تبیین فرهنگ استفاده صحیح از این فضا و ترویج و نهادینه کردن این فرهنگ در جامعه از اقدامات اساسی محسوب می‌گردد که باید با تمسک به ابزارهای اطلاع‌رسانی به آن جامه عمل پوشاند. منظور از استفاده صحیح و مناسب از فضای سایبر صرف اشاره به تدابیر و اقدامات حفاظتی برای در امان ماندن از مخاطرات فضای سایبر نیست. در واقع تدابیر فوق ابزاری در جهت پیشگیری از بزه‌دیدگی و منفعل واقع شدن در مواجهه با جرایم سایبری است. در حالی که مفهوم نهادینه کردن فرهنگ استفاده صحیح از این فضا امری فراتر از این بوده و به معنای نهادینه کردن افکار و عقاید مثبت و مشروع نسبت به این فضا در جامعه است که نتیجتاً منجر به ظهور کاربری مفید و مؤثر از این فضا گردد. به عبارتی دیگر، باید با استفاده از ابزارهای تبلیغاتی و آموزشی، ماهیت فضای سایبر را به گونه‌ای تعریف نماییم که جامعه، دنیای مجازی را به عنوان ابزاری جهت کمک به بشریت در راستای فعالیت‌های روزمره خود شناخته و همواره به دنبال این باشد که از فضای سایبر برای تسهیل و تسریع در امور خود استفاده نماید. (اکبر وروایی، حسین مومنی پور ۱۳۹۰:۱۷)

۲-آموزش خانواده محور

این نوع تدابیر جهت اعمال نوعی پیشگیری رشدمدار و نیز جامعه‌پذیرکردن کودکان و نوجوانان صورت می‌گیرد. در این راستا جهت بهنجار نمودن شخص و پیشگیری از ارتکاب جرایم سایبری توسط این شخص در فضای مجازی باید اقداماتی با تمرکز بر وظایف خانواده انجام گیرد. این اقدامات در دو مرحله انجام می‌گیرد.

در مرحله اول، جامعه در مقابل خانواده‌ها وظایفی را بر عهده دارد. این وظایف، اقدامات حمایتی و آموزشی را شامل می‌شود. به عبارتی دیگر، نهادهای اجتماعی و به ویژه دولت بایستی با مهیا کردن امکانات رفاهی و آگاه‌سازی خانواده‌ها، آنها را در انجام وظیفه خطیر خود در تربیت صحیح فرزندان یاری رسانند. در مرحله

دوم، والدین باید با درک صحیح از نقش و اهمیت خانواده بر اقدامات فرزندان وظایف اساسی خود را در این زمینه انجام دهند. اقداماتی که مناسب است توسط والدین به منظور پیشگیری از قربانی شدن فرزندان در فضای سایبر صورت گیرد می‌تواند به شرح ذیل باشد.

والدین باید از طریق نصب نرم‌افزارهای فیلترکننده بر روی کامپیوتر، فرزندانشان را از مبتلا شدن به اموری از قبیل، گرایش به سوی تصاویر و صحنه‌های مستهجن بازدارند. همچنین می‌توانند با نصب نرم‌افزارهای کنترل‌کننده بر روی کامپیوتر و با ایجاد محدودیت زمانی برای استفاده از آن، نظارت خودر ا بر فعالیت‌های رایانه‌ای فرزندانشان اعمال کنند.

۳- تدوین و وضع قوانین مناسب و به روز

جرم‌انگاری و تعیین واکنش‌های تأدیبی و کیفری متناسب با جرایم سایبری نه تنها مجرمین و محکومان را با اعمال اقدامات ترهیبی و ترذیلی از ارتکاب مجدد این جرایم باز می‌دارد، بلکه صرف جرم محسوب گردیدن یک اقدام و پیش‌بینی واکنش متناسب در مقابل آن، خود می‌تواند عاملی مؤثر در منصرف نمودن افراد مستعد به ارتکاب جرم باشد. در تدوین نوع قوانین همواره باید این امر را مدنظر قرار داد که مطابق با نظریه الگوی اقتصادی جرمِ گری. س بکر مجرمین بالقوه، بسته به نتایج برآورد هزینه و نفع، فعالیت‌های مشروع یا نامشروع را مرتکب می‌شوند. طبق این نظریه، این افراد هنگام تصمیم‌گیری برای ارتکاب اعمال نامشروع، خطر دستگیری و میزان مجازات را به عنوان هزینه جرم در نظر می‌گیرند و میزان آن را نسبت به منافع اقتصادی رفتار مورد نظر، در صورتی که با موفقیت انجام شود، می‌سنجند و اگر منافع بر هزینه‌ها برتری یابد مرتکب جرم می‌گردند (سلیمی و داوری، ۱۳۸۷: ۲۸۰).

در ارتباط با جرایم سایبری نیز، با توجه به این که منافع حاصل از این جرایم به تناسب گستردگی این فضا و گمنام بودن مجرمین سایبری زیاد می‌باشد، باید در مقابل آن سیاست تقنینی متناسب ایجاد گردد تا بتوان با بالا بردن هزینه ارتکاب جرم به عنوان عاملی بازدارنده در مقابل مجرمین بالقوه این جرایم قرار گرفت.

۴-آموزش همگانی

هرچند کوشش‌ها برای دستیابی به آمار جرایم مرتبط با رایانه به دلیل نبود سازوکارهای گزارش‌دهی و ثبت سوابق دشوار است، لکن، تهیه آمار و ارقام جرایم سایبری ارتکابی، تعیین نوع جرایم پرتکرار، شیوه و نحوه ارتکاب این جرایم و در اختیار عموم قرار دادن این اطلاعات با حفظ حریم خصوصی اشخاص از ابزارهای دیگری است که می‌توان جهت آگاه‌سازی جامعه از تهدیدات این فضا استفاده کرد. رسانه‌های جمعی از جمله روزنامه و نشریات، صدا و سیما و اینترنت و ماهواره از جمله ابزارهایی هستند که می‌توان از آنها جهت اطلاع‌رسانی عمومی استفاده کرد. جهت عملی کردن این هدف باید نهادها و محققینی در این زمینه برای انجام فعالیت‌های تحقیقی و آمارگیری اختصاص یابند تا بتوانند با همکاری مراجع قضایی و نهادهای اجرایی میزان جرایم ارتکابی، نوع جرایم، نحوه ارتکاب و سایر مشخصات مربوط به جرایم سایبری را استخراج کرده و با استفاده از یافته‌های جرم‌شناسی و نظر به ماهیت فضای سایبر علت ارتکاب این جرایم را شناسایی و راه‌های مقابله با آن را مشخص کنند. سپس از طریق رسانه‌های عمومی یافته‌های خود را به اطلاع عموم رسانده و در اختیار نهادهای ذیربط قرار داده تا بتوان بر اساس این آمار سیاست جنایی متناسب با آن را تدوین نمود. برای مثال، اطلاعیه‌های پلیس فتا در مورد استفاده صحیح از کارت‌های بانکی عضو شبکه شتاب که به دنبال شیوع کلاهبرداری‌های مرتبط با رایانه صورت گرفت، تأثیری شگرف در کاهش بزه‌دیدگی ناشی از این نوع کلاهبرداری‌ها را به دنبال داشت.

نتیجه گیری:

امروزه گسترش فناوری و زیرساخت‌های ارتباطی و اطلاعاتی در حال گسترش است و سیاست دولت‌ها گسترش و توسعه هر چه بیشتر دسترسی مردم به رایانه و اینترنت است. بدیهی است که رشد کمی و کیفی این شبکه، زمینه را برای وقوع جرایم رایانه‌ای و گسترش دامنه این جرایم مهیا می‌سازد و این فضا را یک فضای پرآماج برای مرتکبین می‌کنند. جدید بودن این فناوری در کنار مزایای آن سبب شده که سیاستگذاران و قانونگذاران به زمینه‌های جرم‌شناسی موجود در این فضا توجه کافی ننمایند. لذا لازم است این نقصان با یاری گرفتن از اصول و مبانی حاکم بر پیشگیری از جرایم به ویژه از طریق مصادیقی که برای پیشگیری وضعی از جرایم رایانه‌ای عنوان نمودیم، البته با کمک سازمان‌های غیردولتی نظیر انجمن صنفی کارفرمایان شبکه‌های اینترنتی در ایران برطرف شود، چرا که برای شناسایی الگوهای متجاوزان کامپیوتری و ارایه برنامه‌های پیشگیری در خصوص سوء استفاده از رایانه نیازمند اتخاذ سیاست جنایی مشارکتی هستیم. جرایم رایانه‌ای به ویژه در قالب یک جنایت سازمان‌یافته فراملی، مسائل حقوقی مختلفی را در کشورهای مختلف جهان و از جمله در کشور ما مطرح کرده است. تلاش‌های زیادی هم در ابعاد حقوقی و جرم‌شناختی این جرایم صورت گرفته ولی هنوز حقوق پیشگیری از جرایم رایانه‌ای رشد کافی

نیافته و در حال شکل‌گیری است. به هر حال جرایم رایانه‌ای هم مثل سایر جرایم همیشه وجود خواهند داشت و وقوع آنها غیرقابل تصور نیستند؛ بنابراین می‌توان با گونه‌های مختلف پیشگیری به کنترل و کاهش آنها مبادرت نمود. در رابطه با جرایم سایبری نیز اصل فرعی بودن حقوق جزا اقتضا می کرد مقابله کیفری با تعرضات رایانه ای و یا به عبارت دیگر جرم شناختن این عمل و اعمال مجازات به عنوان آخرین راه حل صورت می پذیرد و در درجه اول اقدامات غیر کیفری اولویت داشته باشد. البته گسترش جرایم رایانه ای در اغلب کشورها سبب گردید تا نارسایی غیر کیفری آشکار شود و بر همین اساس برخی از کشورها با استفاده از ابزارهای کیفری به عرصه مبارزه با تعرضات رایانه ای وارد شوند. در حال حاضر پلیس فتا با اتخاذ طیفی مختلف از تدابیر پیشگیرانه اجتماعی و وضعی و اقداماتی که در رسانه های عمومی به جهت افزایش آگاهی اقشار مختلف اجتماع نسبت به چگونگی جرایم سایبری و طرق مبارزه با آن بعمل آورده است و از لحاظ حقوقی و فنی و افکار عمومی به مهمترین و تخصصی ترین مرجع پیشگیری از جرایم رایانه ای تبدیل شده است هرچند در این راه نیازمند همکاری و تعاون با سایر نهادهای متولی در پیشگیری از جرایم مزبور می باشد تا بتواند رسالت خود را به نحو احسن انجام داده باشد.

منابع:

۱. ابراهیمی، شهرام. (۱۳۹۰). جرم‌شناسی پیشگیری. جلد اول. تهران: انتشارات میزان.
۲. اردبیلی، محمدعلی. (۱۳۸۵). حقوق جزای عمومی. تهران: انتشارات میزان.
۳. باستانی، برومند. (۱۳۸۶). جرایم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزهکاری. تهران: انتشارات بهنامی.
٤. بوستانچی، مهرداد. پیشگیری از جرایم رایانه‌ای. قابل دسترسی در سایت: http://law1390.blogfa.com/post-4aspx
۵. جعفری، مجتبی. (۱۳۸۷). مختصر جرم‌شناسی (خلاصه‌ای از مباحث درس جرم‌شناسی دکتر نجفی ابرندآبادی).
۶. جلالی فراهانی، امیرحسین. (۱۳۸۹). کنوانسیون جرایم سایبر و پروتکل الحاقی آن (به همراه گزارش‌های توجیهی آنها). معاونت حقوقی و تاوسعه قضایی قوه قضاییه. تهران: انتشارات خرسندی.
۷. جلالی فراهانی، امیرحسین، باقری اصل، رضا. (۱۳۸۶). پیشگیری اجتماعی از جرایم و انحرافات سایبری. مجله مجلس و پژوهش. شماره ۵۵.
۸. چاله چاله، فرشید. (۱۳۸۷). اصول و مبانی پیشگیری از جرم. ماهنامه حقوقی، فرهنگی و اجتماعی دادرسی. شماره ۶۸.
۹. حسینی، بیژن. (۱۳۸۳). جرایم اینترنتی علیه اطفال و زمینه‌های جرم‌شناسی آن. تهران: انتشارات افراز.
۱۰. خلفی، مسلم. (۱۳۸۸). مبانی حقوقی پیشگیری از جرم. تهران: انتشارات نورالسجاد.
۱۱. سایت رسمی پلیس فتا:http://www.cyberpolice.ir
۱۲. سلیمی، احسان. (۱۳۹۱). خطر مضائف جرائم رایانه‌ای. مجموعه مقالات اولین کنگره فضای مجازی و آسیب‌های اجتماعی نوپدید. تهران: انتشارات وزارت رفاه و تأمین اجتماعی.
۱۳. صفاری، علی. (۱۳۸۰). مبانی نظری پیشگیری از وقوع جرم. مجله تحقیقات حقوقی. شماره ۳۴-۳۳.
۱۴. نوربها، رضا. (۱۳۸۴). زمنه حقوق جزای عمومی. تهران: انتشارات گنج دانش
۱۵. وروایی، اکبر، مومنی پور، حسین (۱۳۹۰). از علت شناسی تا پیشگیری جرایم سایبری

مطالعات علوم سیاسی، حقوق و فقه

دوره ۲، شماره ۴، زمستان ۱۳۹۵، صفحات ۲۳۰- ۲۱۹

Non-criminal Prevention in Cyber Crimes

Sam Akrami[1], Saeideh Akrami[2]

1 . PhD candidate of criminal law and criminology, Islamic Azad University, Branch of Qom

2 . PhD candidate of criminal law and criminology, Islamic Azad University, South Tehran Branch

Abstract

This study has been conducted using a descriptive-analytical method with the aim of investigating and offering appropriate strategies to prevent crimes. While cyberspace has many positive effects and results such as helping do the affairs easier and with lower cost, it has adverse and destructive effects as well. Cybercrimes occur in a space with certain conditions and circumstances, such as user anonymity, the impossibility of identifying the criminals, the space's having no boundary, ease of committing the crimes, and the large number of victims. This technology becomes so common that it is not possible to remove it from everyday life, nor is it easily possible to clean up the communities from cybercrimes. Therefore, in addition to the criminal actions and punishments that the legislator should consider for cybercriminals, non-criminal procedures and measures also need to be taken in order to prevent these crimes and their repetition. It is also very important to consider appropriate precautionary criminal and non-criminal measures instead of useless punishments. We try to offer suggestions to help policy makers to encounter and prevent cybercrimes.

Keywords: Cyber Police, cyber space, criminal prevention, substantive prevention.