علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

مجله علمی علوم اسلامی انسانی (سال چهارم)
شماره ۱۴/ تابستان ۱۳۹۷ / ص ۷۴- ۶۴

نقش فضای سایبر در ارتکاب جرایم با رویکرد پیشگیرانه

احسان اسمعیل زاده[۱]

[۱]کارشناسی حقوق، دانشگاه پیام نور ارومیه، ارومیه، ایران

نویسنده مسئول:
احسان اسمعیل زاده

چکیده

امروزه توسعه و گسترش علوم رایانه ای گذشته از اینکه موجب بروز یک تحول یا انقلاب تکنولوژیکی بعد از انقلاب رنسانس در جهان گردیده است، تواماً بستری را برای ارتکاب جرایم مختلف رایانه ای فراهم آورده که گسترش آن موجب بروز آسیب ها و خسارت های گوناگونی در جوامع گردیده است. مجرمان در برخی از جرایم، مبانی اخلاقی ، فرهنگی ، اقتصادی و حتی گاهی امنیت و روابط جامعه را هدف قرار می دهند. توسعه فزآینده فناوری اطلاعات و ارتباطات به تحول و دگرگونی در ابعاد مختلف مولفه های اقتصادی، اجتماعی ، فرهنگی ، سیاسی و دفاعی – امنیتی منجر شده است و مجموعه فعالیت ها در زمینه تولید، بهره برداری، بانکداری، برقراری ارتباط با رایانه های شبکه بندی شده را دستخوش تغییرات شگرف نموده است. محیط سایبر به عنوان یکی از محیط هایی است که می تواند در زمره محیط های اجتماعی شخصی، اتفاقی و انتخابی قرار گیرد و برای پیشگیری از اندیشه، اعمال و رفتار مجرمانه در این محیط باید اقداماتی صورت گیرد.

کلمات کلیدی: فناوری اطلاعات و ارتباطات، جرایم سایبری، حریم خصوصی، پیشگیری وضعی.

علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

مقدمه

مطالعه علمی علل و عوامل ارتکاب جرایم کلاسیک به کمک فناوری اطلاعات و ارتباطات یا در فضای سایبر، به ویژه اینترنت و جرایم جدید علیه سامانه های رایانه ای و مخابراتی، خود نیاز به رویکرد جدید جرم شناختی متناسب با این فضا دارد[۱].

بطور کلی روش های ارتباطی، به سه صورت انجام می شود:

۱) روش مبادله یک طرفه[۲]: در مبادله یک طرفه، مثل تلوزیون و رادیو، وسیله ارسال کننده، هرگز نیاز به دریافت جواب از وسیله دریافت کننده ندارد، در این حالت مبادله اطلاعات در یک جهت صورت می گیرد.

۲) روش مبادله دو طرفه بصورت غیر هم زمان[۳]: در مبادله دو طرفه غیر همزمان، مثل بی سیم ها و سامانه ها رایانامه[۴]، هر دو وسیله گیرنده و فرستنده با یکدیگر تبادل اطلاعات می نمایند. اما در این روش ارسال اطلاعات از طریق کانال ارتباطی در هر زمان فقط در یک جهت می تواند انجام شود که کاربر می تواند بوسیله آن در یک لحظه یا حرف بزند یا گوش دهد و یا متن را ارسال کند یا آن را دریافت کند. در هر صورت هر دو طرف نمی توانند بطور همزمان هم صحبت کنند و هم گوش بدهند.

۳) روش مبادله دو طرفه بصورت هم زمان[۵]: در مبادله دو طرفه هم زمان؛ مثل موبایل ، تلفن های ثابت و اتاق های گفتگو، هر دو وسیله می توانند ارسال و دریافت اطلاعات را بصورت هم زمان انجام دهند که هر دو استفاده کننده می توانند در آنِ واحد هم صحبت کنند و هم گوش دهند یا از طریق رایانه هم زمان داده ها را ارسال و دریافت کنند.

برای ارسال و دریافت داده ها و همچنین انجام مکالمه صوتی ، همانند فضای حقیقی نیازمند محیط هستیم، این محیط که توسعه ابزارهای فناوری اطلاعات و ارتباطات ایجاد می شود، دارای کانالی است که دو نقطه مبداء و مقصد را به همدیگر متصل می نماید. کیفیت این کانال تضمین کننده ارتباط سالم، سریع، امن و ارزان می باشد، بطوری که بیشترین آسیب پذیری فناوری اطلاعات و ارتباطات از این بخش می باشد و مجرمان حرفه ای نیز از این محیط که مسیر عبور و جریان داده ها و صدا می باشد، نهایت سوء استفاده را می برند. این کانال، دارای یک پهنا و عرض می باشد که به پهنای باند[۶] معروف است. یک پهنای باند، عبارت است از «مقدار اطاعاتی که می تواند در یک مدت زمان معین ارسال شود.»، در حال حاضر بیشترین آسیب های وارده و تهدیدات مجرمانه از طریق اینترنت و شبکه های وابسته به آن مثل تلفن همراه صورت می پذیرد. ظهور اینترنت زمانی کلید خورد که در اواخر دهه ۶۰ میلادی، وزارت دفاع ایالات متحده آمریکا علاقه مند به استفاده از شبکه های رایانه ای شد. به گونه ای که در سال ۱۹۶۸ وزارت دفاع ایالات متحده ، آژانس طرح های تحقیقات پیشرفته دفاعی به نام (DARPA) را تأسیس کرد. اینترنت مجموعه ای است از شبکه های موجود در سراسر جهان است که توسط دروازه هایی[۷] به یکدیگر متصل شده اند. به شکل امروزی در آمده و اغلب وسایل ارتباطی مانند؛ تلفن همراه ، تلوزیون ها، دوربین های مدار بسته و ... تحت این شبکه کار می کنند.

یک پروتکل ارتباطی عبارت است از «مجموعه ای از قوانین که توسط سامانه های پردازنده مورد استفاده قرار می گیرد تا سامانه ها بتوانند با یکدیگر ارتباط برقرار کنند.» پژوهشگران فناوری اطلاعات و ارتباطات از اینترنت به عنوان یک شبکه مجازی یاد می کنند و برای نشان دادن فضای اینترنت و هر گونه سامانه هماهنگ با آن از ابر دیتا بطور مجازی استفاده می نمایند.

---

[۱]. نجفی ابرند آبادی، ۱۴:۱۳۸۹) رک به : پیکا، جرج ، جرم شناسی ، ترجمه علی حسین نجفی ابرند آبادی ، دیباچه مترجم برای ویراست دوم « از جرم شناسی حقیقی تا جرم شناسی مجازی»

[2] .sipplex

[3] .Half-Duplex

[4] .Email

[5] .Full-Duplex

[6] .Bandwidth

[7] .Gateway

علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

تعریف فناوری اطلاعات و ارتباطات

فناوری اطلاعات و ارتباطات این گونه تعریف شده است:«مطالعه، طراحی، پردازش، تبادل، ذخیره سازی، توسعه، پیاده سازی، مدیریت و پشتیبانی از سامانه های مبتنی بر رایانه به ویژه کاربرد های نرم افزاری و سخت افزاری رایانه ای»(حسن بیگی، ۱۲:۱۳۸۴).

گرچه فناوری اطلاعات و ارتباطات به سرعت در جوامع در حال فراگیر شدن است و مزیت های زیادی را برای جامعه دارد. اما توسعه و بهره برداری از آن به توسعه زیرساخت های ارتباطی بویژه ارتباطات از راه دور منجر شده است که به نوبه خود در حملات گسترده به رایانه ها و زیر ساخت های دولتی و نیز هک کردن سایت ها بی تأثیر نیست. این عملیات با اندیشه های سود جستن، فعالیت های مجرمانه سایبری خطرناکی را به دنبال خواهد داشت، این محیط جدید که به اصطلاح «فضای مجازی یا سایبر» نامیده می شود. فضایی گسترده، وسیع و موثر است که در کلیه فعالیت های اجتماعی بشر گسترش یافته و گاهی انسان را به بعد غیر مادی جهان نزدیکتر می کند. فضایی که کاملاً متفاوت از فضای واقعی است. اصطلاح «فضای سایبری» که محصول فناوری اطلاعات و ارتباطات می باشد در دنیای اینترنت و شبکه های اجتماعی بسیار شنیده می شود.

جرایم سایبری

واژه سایبر از واژه یونانی «سایبرنتیک» به معنای سکاندار یا راهنما مشتق شده است. این واژه نخستین بار توسط ریاضیدان بنام نوربرت وینر[8] در کتابی با عنوان سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین در سال ۱۹۴۸ به کار برده شد(زندی ۳۸:۱۳۸۹).

البته برخی معتقدند برای اولین بار توسط ویلیام گیبسون در رمانی به عنوان (Neuromancer) در سال ۱۹۴۸ مورد استفاده قرار گرفته است(پاکزاد ۲۳:۱۳۸۸).

امروزه سایبر واژه ای است که به عنوان پسوند برخی واژه ها مانند فضای سایبر[9]، شهروند سایبر[10]، پول سایبر[11] و ... بکار می رود. ترجمه های صورت گرفته از لفظ سایبر دقیق نیست و هر چند بعضاً لفظ مجازی به عنوان معادل آن گرفته می شود. اما چون (Cyber) بیانی از موضوعات واقعی و قابل مشاهده و لیکن غیر قابل لمس است نمی تواند بر لفظ مجازی که به موضوعات ذهنی و تصوری اشاره دارد، حمل شود(پاکزاد ۲۳:۱۳۸۸).

امروزه با توسعه فضای سایبری و تولید برنامه های ارتباطی مختلف، شبکه های اجتماعی نیز به سرعت در حال توسعه هستند که بخش بزرگی از اوقات فراغت یا فعالیت های روزمره شغلی افراد را به خود اختصاص داده است، که از آن جمله می توان به تانگو، فیس بوک، واتس آپ، وایبر ، لاین ، تلگرام و ... اشاره کرد.

در تعریف جرم سایبری[12] می توان گفت: «استفاده از رایانه یا سایر وسایل الکترونیکی از طریق سامانه های اطلاعاتی مانند شبکه های یکپارچه یا اینترنت برای تسهیل در انجام رفتار های غیر قانونی.»

با توجه به عمومیت و گستردگی شبکه جهانی اینترنت، ورود به آن با کمترین هزینه ممکن و به راحت ترین شیوه و به صرف ارتباط از طریق تلفن ثابت یا همراه و یا اتصال به شبکه بصورت برخط (Online) می تواند انجام شود، برای نمونه فناوری اطلاعات و ارتباطات ابزاری برای تسهیل جعل و استفاده از سند مجعول را میسر نموده است و با تغییر در داده های مرتبط با اسناد موجود در فضای سایبری، می توان به راحتی هر چه تمام تر جرم جعل را مرتکب شد. بطور کلی، تخمین زده می شود که در حدود ۸۰/۰۰۰ وب سایت مختلف در اینترنت مشغول ارائه روش و نحوه ارتکاب جرایم رایانه ای می باشند و اطلاعات و یا ابزار نحوه انجام آن را بدون هیچگونه هزینه ای ارائه می کنند(زندی ۳۵۷:۱۳۸۹).

با گسترش فضای سایبری و وابستگی افراد به آن شکل زندگی مردم نیز تغییر یافته است که افراد با ورود به فضای سایبری با محاسن و معایبی رو به رو می شوند که بدین شرح است: (محمدی ۳۶-۴۰ :۱۳۸۵).

---

[8] .Norbert Wiener

[9] .Cyber Space

[10] .Cyber citizen

[11] .Cyber cash

[12] .cyber crime

ISSN: 2538-3671
http://www.johi.ir

۱- **فردگرایی خود آگاهانه:** یعنی آنچه در فضای سایبری بسیار مشهود است، گسترش اهمیت فرد و حریم خصوصی در برابر جمع و حوزه عمومی می باشد. افراد در فضای سایبری در عین حال که می توانند حضور داشته باشند، اما چون می توانند هویت واقعی خود را پنهان کنند، می توانند در همان حال خود را جدا از دیگران و تنها حس کنند. این ویژگی باعث تقویت توانایی و قابلیت های فردی شخص شده است و او را قادر می سازد تا پنهانی ترین زوایای روح و شخصیت خود را به فعلیت برساند.

۲- **آزادی بیان و عقاید:** حکومت ها و صاحبان قدرت همواره آزادی افراد را در جهت منافع خود محدود کرده اند. بنابراین، اولین پیام ، حذف اقتدار در فضای سایبری است. با این حال، در این فضا اندیشه ها و تفکرات به راحتی در مسیر شبکه ها منتقل و حرکت داده می شوند و به عبارتی صدور اندیشه ها آسانتر صورت می گیرد.

۳- **آزادی دسترسی به اطلاعات و ارتباطات:** با توجه به ویژگی های خاص محیط های سایبری و انتشار دادها و اطلاعات با عملیات آسان مثل کپی برداری و داده گذاری، افراد در جریان اطلاعات قرار می گیرند و دستیابی به اطلاعات آسانتر و آزادتر شده است. از این رو، هر نوع اطلاعاتی اعم از فرهنگی، سیاسی و اقتصادی، بدون محدودیت های حاکم بر دیگر رسانه ها، در فضای سایبر قابل دسترسی است. آزادی ارتباطی نیز از ویژگی های دیگر فضای سایبر است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست.

۴- **کاهش روابط اجتماعی واقعی:** جذابیت فضای سایبر به حدی است که کاربران در ابتدای دسترسی به اینترنت، ساعت ها وقت صرف گشت و گذار در اینترنت می نمایند. مطالعه انجام شده در مورد اینترنت نشان از این دارد که استفاده بیشتر از اینترنت منجر به کم شدن ارتباطات اجتماعی شده است و آسیب های جدی به کودکان در حال یادگیری در بخش تعامل اجتماعی بوجود می آورد که خود منجر به کشیده شدن کودکان به خرده فرهنگ های مجرمانه می گردد.

۵- **موقتی بودن ارتباط ها و پیوندها:** همه چیز در مورد افراد سایبری موقتی است. هیچ تضمینی برای ادامه فعالیت و کنش یک عضو در یک جمع سایبری وجود ندارد، به همین دلیل احساس مسئولیتی در قبال همدیگر وجود ندارد و تنها به شکل هیجانی و عاطفی و لحظه ای شکل می گیرد و تصمیم گیری می شود.

۶- **پنهان کاری و وجود بی نظمی:** عدم کنترل کاربران بطور پنهانی و ساماندهی (IP) ها و دامنه سرورها امکان بوجود آوردن هر گونه بی نظمی را ممکن می سازد. بطوری که هویت های غیر واقعی و چند گانه در تماس با حجم عظیمی از اطلاعات متنوع، فضای سایبری را به چالش می کشاند. این وضعیت فرصت هایی را در اختیار افراد سودجو، بویژه مجرمین مالی قرار می دهد تا با سرقت و شنود اطلاعاتی رمز کارت های اعتباری را بدست آورند.

۷- **هنجار شکنی در اینترنت:** در فضای سایبری نه هویت افراد بعضاً مشخص شده است و نه ارتباط چهره به چهره ای به مفهوم واقعی کلمه در آن وجود دارد و نه این که حاکمیتی که افراد را وادار به تبعیت از هنجار ها بکند. این موضوع فضای سایبری را به محیطی مساعد برای رشد انحرافات و کجروی ها بصورت مجرمانه هدایت می نماید.

۸- **جذابیت وتنوع: رسانه ها؛** از فیلم ، عکس، متن و یا هر هنر دیگری برای جذاب کردن محتوا استفاده می کنند و این ابزارها در فضای سایبر قابل دستیابی است؛ بویژه آن گاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی های منحصر به فردی که در تنوع و جذابیت فضای سایبری تأثیر به سزایی دارد، مشتری محوری محض است. در متون نوشتاری، ارتباط تنگاتنگی میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظر سنجی و ارزیابی در این فضا بسیار آسانتر و روزآمدتر است و این توانایی را به داده پردازان، فروشندگان و عرضه کنندگان محصولات اینترنتی می دهد که از آخرین خواسته های مشتریان و مخاطبان خود مطلع گردند.

۹- **جهانی و فرامرزی بودن:** از ویژگی های منحصر به فردی که فضای سایبر را از دیگر رسانه ها ممتاز می سازد، جهانی بودن آن است، هر فردی در هر نقطه از جهان می تواند از طریق آن به آسانی به جدیدترین اطلاعات دست یابد، مرزهای جغرافیایی تاکنون نتوانسته از گسترش روزافزون فضای سایبر جلوگیری کند. از این رو، هر نوع فیلتر و مرز بندی در برابر آن بسیار دشوار می نماید. بنابراین با وجود اینکه، فضای سایبری آسان ترین و سریع ترین روش ارتباطی را برای افراد ایجاد کرده است، در صورتی که قوانین و مقررات برای آن در نظر گرفته نشود، می تواند منجر به سوء استفاده تبهکاران شود که نه تنها موجب هرج و مرج و هنجار شکنی در ارتباطات می شود، بلکه افراد را در تعارض با هنجارهای اجتماعی در فضای حقیقی قرار می دهد که منجر به ورود افراد به خرده فرهنگ های مجرمانه در فضای سایبری و ارتکاب جرایم مختلف بویژه جرایم سازمان یافته و تروریستی می شود.

علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

نقش فناوری اطلاعات و ارتباطات در ارتکاب جرایم سازمان یافته

فناوری اطلاعات و ارتباطات در ایجاد تصمیمات مجرمانه بزرگ در سطح بین المللی و جرایم سازمان یافته، بویژه در سال های اخیر نقش به سزایی داشته است و امروزه در جرایم سازمان یافته به عنوان ابزار لاینفک این گروه ها محسوب می شود. گسترش شبکه های بی سیمی و تولید موبایل های ماهواره ای، رایانه های کوچک و قابل حمل بر سرعت اشتراک گذاری افکار و عقاید مجرمانه بویژه در زمان ترانزیت کالا یا انسان افزوده است. علاوه بر افراد عضو در گروه های مجرمانه، فناوری اطلاعات و ارتباطات این امکان را فراهم آورده تا مجرمان با شگرد های فریبکارانه از نظارت کاربران بی اطلاع در انجام مأموریت های خود بصورت گمنام کمک بگیرند. قابلیت جدیدی که در اینترنت ایجاد شده است، استفاده آزادانه همه افراد از فناوری «انتقال صوت بر روی داده ها» می باشد.

به عقیده استاد میر محمد صادقی، تبانی به دو صورت چرخشی و زنجیره ای صورت می گیرد، در تبانی چرخشی، یک نفر به عنوان رهبر گروه با افراد دیگری در تماس بوده و نظر همه آنها را به ارتکاب جرم جلب می کند، بدون اینکه آن افراد هیچ تماسی با یکدیگر داشته باشند. حالت دوم که می توان آن را تبانی زنجیره ای نامید، وقتی است که برای ارتکاب یک جرم، شخص «الف» با «ب»، «ب» با «ج» و «ج» با «د» در ارتباط بوده است. در هر دو حالت وجود هدف مشترک ضروری است که امکان به سرانجام رسیدن هر دو روش تبانی برای ارتکاب جرم در فضای سایبر امکانپذیر می باشد. در برخی از جرایم رایانه ای، انگیزه اصلی، کسب منفعت مالی است و لیکن انگیزه های دیگری چون انتقام جویی شغلی، سرگرمی، اثبات برتری قدرت، خودنمایی، علل روانی و ... وجود دارد(باستانی ۳۴:۱۳۸۶).

همانگونه که وقوع جنگ جهانی اول و دوم منجر به گسترش روش های مجرمانه جدید و افزایش انواع جرایم گردید، فناوری اطلاعات و ارتباطات نیز فرصت های جدیدی را در اختیار مجرمان و افراد غیر مجرم قرار داده است. این به نوبه خود، انگیزه ها را فعال نموده تا افراد به فضای سایبر روی آورند، همچنین به نظر می رسد، میان فعالیت های هک کردن و روان شناسی هک، پیوند طبیعی وجود دارد؛ زیرا آنها الگوهای رفتاری انگیزش یافته و آموخته هایشان را نشان می دهند(دالال و شارما۱۳۸۸:۴۳۱).

برخی از انگیزه های فعالیت در فضای سایبری عبارتنداز:

۱) انگیزه سیاسی – اجتماعی
۲) انگیزه اقتصادی
۳) انگیزه علمی
۴) انگیزه روان شناختی
۵) انگیزه مجرمانه

نقش جرایم سایبری در تجارت الکترونیکی

تجارت الکترونیکی از جمله فرآیندهای جامعه اطلاعاتی دنیای امروز است که در سال های اخیر با حضور اینترنت بسیار توسعه یافته است. تجارت الکترونیکی، شامل به اشتراک گذاشتن اطلاعات کسب و کار، برقراری ارتباطات تجاری و هدایت معاملات تجاری بوسیله شبکه های ارتباطی است. تجارت الکترونیکی شامل طیف گسترده ای از فعالیت ها و تخصص ها، از جمله امنیت در معاملات، اعتماد و اعتبار در معاملات، قانونگذاری، مکانیزم پرداخت، چگونگی تبلیغات، کاتالوگ های الکترونیکی، حضور واسطه ها، عملکرد فروشگاه های چند رسانه ای و ... است(Pivk,1999:79).

جرایم قراردادی و مصنوعی که با توجه به پیشرفت های بشری و نیاز جامعه ایجاد شده اند، ارتباط تنگاتنگی با فناوری روز دنیا دارند. برای نمونه پولشویی در دو دهه اخیر با توجه به پیشرفت های بانکداری الکترونیکی، توسعه پیدا کرده است. از این رو فناوری اطلاعات و ارتباطات، ارتکاب جرایم قراردادی را به شدت تسهیل نموده است. بطور مثال؛ ویژگی دقت و سرعت موجب شده تا جعل اسکناس کاملاً وابسته به فناوری اطلاعات و ارتباطات باشد. در نهایت می توان نتیجه گرفت که فناوری اطلاعات و ارتباطات در شکل گیری اندیشه مجرمانه و گذر از اندیشه به فعل مجرمانه و نیز تدارک مقدمات سخت افزاری و نرم افزاری جرایم سایبر نقش بسزایی را ایفا می کند.

علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

نقش فضای سایبر در ارتکاب جرایم

مجرمان امروزی به جذب افراد از طریق سایت های اینترنت به صورت علنی و غیر علنی فریبکارانه روی آورده اند و برای تسریع در انجام فعالیت های مجرمانه، در مواقعی، افراد متخصص در زمینه فناوری اطلاعات و ارتباطات را استخدام می نمایند و در دراز مدت مجرمان حرفه ای، فناوری مورد استفاده هکر ها را فرا خواهند گرفت یا هکر ها را ترغیب خواهند نمود که برای آنان کار کنند(زیبر ۳۸:۱۳۸۴).

در ارتباط با این موضوع، در تبصره ماده ۵۱۰ ق.م.ا (تعزیرات) هر گونه شناسایی و جذب جاسوسان را قابل مجازات می داند. با این وجود حتی جذب نیرو از طریق اینترنت و فضای سایبری برای جذب جاسوسی با ماده مذکور قابل مجازات است.

مجرمین آینده، احتمالاً بسیاری از انگیزه های بزهکاران امروزی را نظیر شادی، حرص و طمع، شهوت، انتقام و... خواهند داشت. اما شیوه های ارتکاب جرایم آنان اساساً متفاوت خواهد بود. با فناوری هایی که امروزه در حال توسعه است، مجرم خواهد توانست، منزل افراد را با استفاده از رایانه، تلفن، دوربین و ... مورد تجاوز قرار دهد(فتاح ۶۱:۱۳۷۷).

مجرمان با ورود به فضای سایبر با انبوهی از منابع آموزشی روبه رو می شوند. این منابع آنها را مستعدِ ارتکاب جرم می نماید. برخی سایت ها جرم را تبلیغ می کنند و برخی دیگر، راه های تهیه آسان ابزار جرم بصورت غیر مستقیم را تبلیغ می کنند و دیگری خودکشی بی درد را در گوشه ای از صفحه اصلی سایتش به نمایش می گذارد. این ها همه نشان از مهیا بودن فضای سایبر و توانایی آن می باشد. از این رو به نظر می رسد، آموزش و یادگیری جرم بیش از آنکه از فضای حقیقی به فضای سایبر منتقل شود، با شدت و سرعت زیاد از فضای سایبر به فضای واقعی در حال انتقال است.

فضای سایبر بطور بالقوه قابلیت ابزاری برای ارتکاب هر گونه جرایم سنتی مانند؛ قتل، سرقت و ... را دارد. بعضی از آنها مثل افتراء بدون نیاز به ابزار مادی اتفاق می افتد، ولی محیط و شرایط آن در فضای سایبر آماده است و مجرم تنها با ارسال یک رایانامه دارای متن افترا آمیز، مرتکب جرم می شود. ارتکاب برخی از جرایم مثل سرقت در فضای واقعی نیازمند ابزارهایی مثل اسلحه، نرده بان یا وسایل دیگری است. برخی شرکت های سایت های فروش اینترنتی، این ابزارها را بصورت تحویل پستی راه اندازی کرده اند که تهیه آن را تسهیل نموده است. بنابراین فناوری اطلاعات و ارتباطات می تواند ارتکاب جرایم سنتی در فضای واقعی را تسهیل نماید. حتی در ارتکاب جرم قوادی، جمع کردن افراد از طریق فضای سایبری نیز امکانپذیر است.

پیشگیری از بزهکاری

پیشگیری یا جلوگیری کردن هم به معنی «پیش دستی کردن، پیشی گرفتن و به جلوی چیزی رفتن» و هم به معنی «آگاه کردن هشدار دادن» است؛ از نظر علمی پیشگیری، یک مفهوم منطقی- تجربی است که همزمان از تاملات عقلانی و مشاهدات تجربی ناشی می شود و عنایت انحصاری آن تحدید امکان وقوع مجموع اقدام های مجرمانه از طریق غیر ممکن کردن، دشوار کردن یا کمتر محتمل کردن آنهاست.

پیشگیری شاخه ای از جرم شناسی است که دارای شاخصه و معیارهای خاص آن علم است که آن را از دنیای حقوق کیفری متمایز می سازد، پیشگیری زائیده تفکر پویای جرم است و آنکه علل جرم قابل مطالعه، شناخت، ارزیابی و قابل تجزیه و تحلیل است و لذا برای تثبیت علم پیشگیری نخستین گام وجود سیاستگذاری و مدیریت بررسی رضایت اجتماع می باشد تا سطوح و انواع مختلف پیشگیری تواماً بکار گرفته شود.

مطالعات و یافته های تحقیقات در قلمرو تاریخ حقوق کیفری نشان می دهد که جوامع بشری برای مقابله با جرم عمدتاً از مجازات، آن هم از انواع شدید آن(یعنی پیشگیری کیفری) استفاده می کرده اند، اما به حکایت یافته های حقوق کیفری و مکاتب مختلف فلسفی- کیفری، این شدت و حدت نظام کیفری نتوانسته است آن طور که انتظار می رفته است منحنی جرایم را مهار کند؛ از طرفی افزایش جرایم از حدود ۲۵ سال پیش به این طرف در پاره ای از کشورها به ویژه در جوامع صنعتی که با پدیده شهرنشینی روزافزون و توسعه افقی و عمودی شهرها و کلان شهرها و نیز نسل دوم و حتی سوم مهاجران خارجی دست به گریبان شده، علاوه بر خسارات مادی، موجب ظهور احساس ناامنی و ترس از بزه دیدگی در بین شهروندان شده است. در نتیجه، این قبیل جرایم کیفیت زندگی مردم را خدشه دار کرده است. در نهایت فضای فعالیتهای فرهنگی، اقتصادی و اجتماعی یعنی پیشرفت جامعه را نامطمئن و دستخوش اختلال می کند. با توجه به پیامدهای اخیر بزهکاری است که امروزه در کنار استفاده از نهادهای قهر آمیز و کیفری و با توجه به محدود بودن ظرفیت و کار این نهادها، بر پیشگیری و به ویژه پیشگیری مشارکتی تکیه می شود. برگزاری همایش های متعدد بین المللی، منطقه ای و داخلی در اغلب کشورها در مورد پیشگیری در دو دهه اخیر دلیل دیگری بر اهمیت آن است.

علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

پیشگیری از جرم در دو مفهوم پیشگیری کیفری و پیشگیری غیر کیفری بکار میرود. پیشگیری غیر کیفری در معنای علمی که در جرم شناسی پیشگیرانه به عنوان شاخه ای از جرم شناسی کاربردی بررسی می شود، قلمرو متنوع و گسترده ای دارد و براساس مدلهای خاصی قابل تقسیم است. چنانچه برخی از اساتید جرم شناسی با توجه به سه محور(شخصیت، اوضاع ما قبل جنایی و روند فعلیت یافتن) پیشگیری را در سطوح مختلفی قابل تقسیم می دانند، چرا که علی الاصول وقوع جرم نمی تواند خارج از آن سه محور باشد. با پذیرش محورهای یاد شده انواع پیشگیری را می توان تطبیق و صورت بندی نمود: در دسته نخست؛ تدابیر پیشگیری عمومی (پیشگیری اجتماعی) در جهت اصلاح و تربیت کلیه افراد جامعه که می توانند بزهکاران بالقوه باشند و تدابیر خصوصی برای افرادی که حالت خطرناک و روحیه ضد اجتماعی و ناسازگاری دارند متمرکز می شود(پیشگیری اولیه و ثانویه). دسته دوم فعالیتها در راستای از بین بردن وضعیت های پیش جنایی یا ماقبل جنایی صورت می گیرد و در آن تدابیری چون جلوگیری از تظاهر به فساد، منع حمل و نقل و خرید و فروش اسلحه یا مواد مخدر برای محور زمینه های مساعد جرم زا اتخاذ می گردد(پیشگیری وضعی)، دسته سوم فعالیتها در واقع برای خنثی سازی بزهکاری در مرحله فعالیت یافتن عمل مجرمانه به عنوان مثال حضور پلیس یا کنترل های مخفیانه صورت می گیرد.

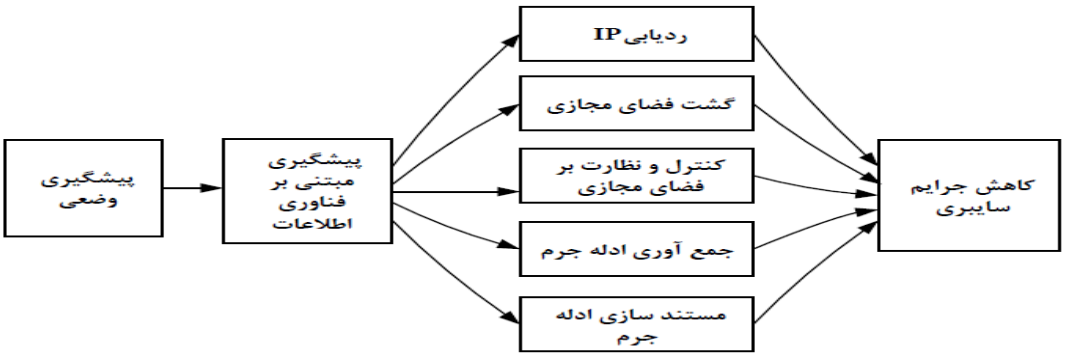
بدین ترتیب، تاثیرگذاری تیپ های مختلف پیشگیری یکسان نیستند، برخی از انواع پیشگیری زمینه و علل وقوع جرم را از بین می برد(پیشگیری اجتماعی) و دیگری فرصت و امکان آن را کاهش می دهد یا دشوار می سازد. (پیشگیری وضعی)، به عنوان مثال پیشگیری وضعی، هدفش از بین بردن و کاهش فرصتهای وقوع جرایم می باشد.

بنابراین با وجود تاثیر گذاری غیریکنواخت و متفاوت تیپ های پیشگیری، برنامه ریزی، تدابیر، اقدامات و فعالیتهای این علم، طیف کلان و گسترده ای دارد و لذا نمی توان انتظار داشت یک موسسه، نهاد و وزارتخانه بتواند عهده دار انجام پیشگیری از وقوع جرم در جامعه باشد. بدین ترتیب این نظر شکل می گیرد که به منظور پیشگیری از وقوع جرم بایستی «سیاستگذاری و مدیریت» نمود؛ به این معنی که با تعیین چارچوب های اجتماع هماهنگی، مشارکت و همکاری صورت پذیرد.

صور مختلف پیشگیری وضعی مبتنی بر فناوری اطلاعات و ارتباطات

۱- پیشگیری مبتنی بر فناوری اطلاعات درکاهش ارتکاب جرایم سایبری تأثیر دارد.
۲- پیشگیری مبتنی بر ردیابی IP (مهاجم) در کاهش ارتکاب جرایم سایبری تأثیر دارد.
۳- پیشگیری مبتنی بر گشت و کنترل و نظارت فضای مجازی در کاهش ارتکاب جرایم سایبری تأثیر دارد.
۴- پیشگیری مبتنی بر جمع آوری ادلهٔ الکترونیکی جرم در محیط اینترنت درکاهش ارتکاب جرایم سایبری تأثیر دارد.
۵- پیشگیری مبتنی بر مستند سازی صحنه جرم درمحیط اینترنت در کاهش ارتکاب جرایم سایبری تأثیر دارد.

(نمودار ۱)



نمودار۱ – صور مختلف پیشگیری وضعی مبتنی بر فناوری اطلاعات و ارتباطات

علوم اسلامی انسانی، شماره ۱۴، تابستان ۱۳۹۷، جلد دوم، ص ۷۴- ۶۴

ISSN: 2538-3671
http://www.johi.ir

نقش فناوری اطلاعات و ارتباطات در پیشگیری وضعی

بطور کلی برای ارتکاب یک جرم، وجود سه عامل مهم ضروری است تا مثلث جرم تشکیل شود. مهم ترین آنها که قاعده مثلث جرم را تشکیل می دهد، انگیزه مجرمانه[۱۳] است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد مجرمانه[۱۴] می شود. برای از بین بردن این عامل ضروری است تدابیر پیشگیرانه اتخاذ گردد. اما اگر به هر دلیلی مجرمان واجد انگیزه شوند، باید از اجتماع دو ضلع دیگر این مثلث یعنی فرصت[۱۵] و ابزار ارتکاب جرم[۱۶]جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد. زیرا متصدیان امر هر چه بکوشند ابزار های ارتکاب جرم را از سطح جامعه جمع آوری کنند، باز هم مجرمان با انگیزه به آنها دست خواهند یافت. هر چند در عین حال نباید اهمیت جمع آوری این ابزارها را در کاهش جرایم نادیده گرفت و باید کوشید تا از طریق انواع پیشگیری ها بویژه در حوزه فاوا و استفاده ابزاری از آن، نهایت حفاظت و حمایت از آماج ها و همچنین بزه دیدگان احتمالی صورت گیرد.

فناوری اطلاعات و ارتباطات از راه های مختلفی به کمک پیشگیری وضعی آمده و خطر ارتکاب جرم در دو محیط مادی و سایبر را مدیریت می کند. امروزه در سایه فناوری اطلاعات و ارتباطات، دستاوردهای چشمگیری برای متولیان پیشگیری وضعی از جرم بدست آمده است. امکان گردآوری، متمرکز سازی، پردازش، تحلیل و استخراج سریع و صحیح داده های جنایی، شناخت دقیق مکان ها و گروه های در معرض ریسک بالای بزه دیدگی و پاسخ به بزه از طریق دشوار نمودن دسترسی به آماج و تسهیل در شناسایی مجرم از جمله این دستاوردها محسوب می شود.

در واقع پیشگیری وضعی از جرم با کاهش فرصت، بر توانایی و در نهایت تمایل فرد مرتکب تأثیر می گذارد. این نوع پیشگیری، از طریق گرفتن فرصت از مجرمان بالقوه و افزودن بر مخاطرات و ضررهای ارتکاب جرم، به مبارزه با بزهکاری می پردازد. زیرا بطور معمول بزهکار در خصوص ارتکاب جرم و منافع و ضررهای احتمالی آن بررسی قبلی را انجام داده و سپس تصمیم به ارتکاب یا عدم ارتکاب آن می گیرد. فرآیندی که با استفاده از ابزارهای مجهز به فناوری اطلاعات و ارتباطات با کیفیت و سهولت بیشتری طی می شود. با این حال، چون ابتدا سامانه های رایانه ای ایجاد می شوند و به دنبال آن امنیت سامانه ها تأمین و برقرار می گردد، این وقفه می تواند در فضای سایبر، اثرات مخربی را به دنبال داشته باشد. همانطور که آمد، مشارکت و ایجاد امنیت شبکه از لایه کاربران و محل کار افراد به همراه آموزش مستمر به کودکان، در پیشگیری از جرایم سایبر از اهمیت بالایی برخوردار است. فناوری اطلاعات و ارتباطات با وجود مزایای زیاد در راستای پیشگیری از جرم، با اشکالات و کاستی هایی رو به رو می باشد که از آن جمله می توان به قطعی شبکه، بالا بودن هزینه ها، احتمال نقض حریم خصوصی و کاربرد مشابه آن از سوی تبهکاران اشاره نمود. البته به روز بودن فناوری فوق و استفاده صحیح و پایدار از آن می تواند مثمر ثمر باشد. سر انجام نیل به اهداف پیشگیری از جرایم، از سویی نیازمند کاهش فرصت های مجرمانه از طریق اعمال سیاست های حمایتی برای پیشگیری از بزه دیدگی یا ایجاد موقعیت های پر خطر برای مجرمان است.

بطور کلی یک مجرم زمانی تصمیم به ارتکاب جرم می گیرد که آماج مناسب و بدون حفاظت نظر او را جلب کند و با بررسی اوضاع و احوال و شرایط آن، احتمال عملی کردن آن را، فارغ از سنجش سود و زیان جرم، در حد زیاد پیش بینی کند. پس اگر بتوانیم با راهکار های پیشگیرانه فرد را از تصمیم خود منصرف کنیم و فرصت و آگاهی های لازم برای عدول از این تصمیم داده شود، مجرم دیگر به مرحله تهیه و تدارک مقدمات جرم وارد نمی شود. در فضای سایبر راهکار های امنیتی و پیشگیرانه زیادی از قبیل فیلتر کردن، ردیابی، دیوار های آتشین و ... برای جلوگیری از تدارک مقدمات جرم و ارتکاب آن ارائه شده است، اما همانطور که آمد، قصد و نیت فرد تا مرحله انجام مقدمات جرم بصورت پنهان در ذهن افراد وجود دارد، موارد زیر از جمله اقداماتی است که می تواند افراد را از تصمیم مجرمانه منصرف کند:

۱) در فضای سایبری از طریق اینترنت و رایانه، تلفن های همراه، تلوزیون و رادیو برای قشر های مختلف جامعه آموزش های لازم روان شناختی و جرم شناسانه، جهت رهایی افکار شر و مجرمانه ارائه شود، آموزش های شناخت بد افزار ها مثل ویروس ها، اسب تروا و ... در سطح مدارس، سازمان ها و حتی کشور می تواند از آسیب های جرایم در فضای سایبر بکاهد و از جرم پیشگیری نماید. همانطور که در مورد اعتیاد این اتفاق صورت می گیرد. البته آموزش روش های ارتکاب جرم طبق قانون جرایم رایانه ای مصوب ۱۳۸۸ جرم و قابل مجازات است.

---

[13] .Motive

[14] .Intention

[15] .opportunity

[16] .Means

ISSN: 2538-3671
http://www.johi.ir

۲) اگر در وب سایتی در مورد تصمیم سازی مجرمانه آموزش هایی ارائه شود، در مقابل، آموزش های رایگان برای خنثی سازی آن در فضای سایبر توسعه و گسترش یابد.

۳) تشویق هایی برای منصرف کردن افراد در نظر گرفته شود تا احساس نیاز او را برطرف نماید؛

۴) افرادی که قصد ارتکاب جرم بوسیله فضای سایبر را دارند، بوسیله نرم افزارهای ردیاب، مشخصات او را در مسیر ثبت و به رایانه او ارسال کنیم تا از تصمیم خود منصرف شود؛

۵) آگاهی های لازم به افراد دارای مقاصد مجرمانه در فضای سایبر که احتمال بزه دیده شدن آن ها وجود دارد، داده شود تا به گودال جرم نیفتند.

۶) یکی از راه های پیشگیری از انگیزه و ایجاد تصمیمات افراد، ایجاد مانع در سر راه برقراری تماس بین بزهکاران بالقوه و آماج یا هدف جرم (بزه دیده بالقوه) می باشد. برای نمونه، در صورت تغییر منظم کانال های ارتباط سایبر و رمز نمودن داده ها، از این ارتباط پیشگیری خواهد شد.

۷) نمونه دیگر ایجاد محدودیت در ساعت فعالیت است، برای نمونه در ایران، نیروی انتظامی به برخی اصناف، رستوران ها، اغذیه فروشی ها و... دستور داده است تا ساعت خاصی از شب فعالیت کنند. این اقدام، گذشته از وجاهت قانونی آن، به منظور پیشگیری وضعی از رو به رو شدن بزهکار بالقوه و بزه دیدگان بالقوه اعمال می شود. اگر دختر بچه ای از طلا و جواهرات استفاده کند، امکان ارتکاب جرم بر وی افزایش خواهد یافت. بنابراین با ایجاد مانع بر سر راه برقراری تماس میان دو کنش گر جرم، از ارتکاب جرم پیشگیری می شود(نجفی ابرند آبادی ۱۲۵۶:۱۳۸۲).

۸) راهکار بعدی، جاذبه زدایی است. اگر جاذبه مالی و روانی سیبل جرم کاسته شود، بطوری که منافع ارتکاب جرم کاهش یابد، طبق قاعده، جلوی تصمیم مجرمانه گرفته خواهد شد. به عنوان نمونه، استفاده از کارت های اعتباری به جای پول نقد، جاذبه مالی را از کیف قاپ می زداید.

حریم خصوصی در فضای مجازی

حیثیت و حریم خصوص، مقوله ای است که هم در احکام دینی و هم در موازین قانونی چه در سطح ملی و چه در سطح بین المللی مورد توجه و تأکید مکرر قرار گرفته شده است.

«حریم خصوص» معمولاً قرین عباراتی همچون آسودگی خاطر، امنیت اسرار، حیثیت و آبرو که روشن ترین نقطه شخصیت هر فرد در جامعه است، می باشد. حریم خصوصی از موضوعات بسیار مهم حقوق بشری است و تعریف آن نیز دشوارتر است. زیرا تعریف حریم خصوصی بستگی زیادی به فرهنگ و زمینه های اجتماعی و محیطی دارد.

در بسیاری از کشورها، این مفهوم با مقوله حفظ اطلاعات که حریم خصوصی را در فضای مدیریت اطلاعات شخصی تفسیر می کنند، پیوند خورده و در هم آمیخته است(EPIC&PI,2002:1).

طبق تعریفی، حریم خصوصی محدوه ای از زندگی شخص است که بوسیله قانون و عرف تعیین شده و ارتباطی با عموم ندارد، بنحوی که دخالت دیگری در آن ممکن است باعث جریحه دار شدن احساسات شخص یا تحقیر شدن وی نزد دیگران به عنوان موجود انسانی شود(رحمدل،۱۳۰-۱۲۹=۱۳۸۴).

با توجه به تعاریف مذکور می توان گفت مفهوم حریم خصوصی امری نسبی است که مفهوم آن از کشوری به کشور دیگر ممکن است متفاوت باشد و احترام به حریم خصوصی، بیان احترام به استقلال و اختیار دیگران است(Shostack and syverson-2004:36).

حریم خصوصی افراد در فضای سایبر را می توان در دو حوزه بررسی کرد:

۱) ارتباطات خصوصی یا غیر عمومی که به اشکال مختلف مکتوب، صوت، تصویر یا حتی چند رسانه ای بصورت همزمان یا غیر همزمان در سراسر جهان بر قرار می شوند و ...

۲) پایگاه های داده ای که حاوی اطلاعات شخصی اند یا حتی اطلاعات شخصی حساس افراد را نگهداری می کنند و دسترسی به آنها تقریباً با مشکلی مواجه نیست.

فناوری اطلاعات و ارتباطات این امکان را فراهم آورده که مجرم از طریق داده های کاذب، داده ها و اطلاعاتی را ایجاد نماید که به حریم خصوصی افراد لطمه وارد می نماید. برای مثال اگر بخشی از یک عکس در اختیار مجرم قرار گیرد او می تواند با استفاده از نرم افزار های پیشرفته آن را تبدیل به یک عکس مستهجن نماید که سایت های اینترنتی، صندوق های صوتی و پستی می توانند وسیله مناسبی برای تبلیغ، توزیع و عرضه تصاویر غیر اخلاقی باشند. با توجه به اینکه این نوع عمل مجرمانه ماهیتاً در

ISSN: 2538-3671
http://www.johi.ir

جرایم کلاسیک نیز وجود دارند، با توسعه فناوری اطلاعات و ارتباطات رشد قابل ملاحظه ای داشته است. بنابراین، جمع آوری، ذخیره، پردازش یا افشای اطلاعات کاذب حتی توسط دارنده قانونی آن ها ممنوع می باشد. این امر به دلیل عدم انعکاس واقعیت و کذب بودن، می تواند به نقض حریم خصوصی منجر شود و حیثیت فرد را خدشه دار نماید.

امروزه تهدید به افشای داده های شخصی بیش از بیش رواج پیدا کرده است و این مهم از طریق فضای سایبر و انتشار آن در سایت های گمنام بسیار سریع تر و آسانتر شده است. بطوری که بدون هیچگونه مقاومتی امکانپذیر است. میزان پولی که می توان از طریق گردآوری و فروش اطلاعات شخصی کسب کرد، انگیزه زیادی به شرکت ها و موسسات دست می دهد تا آن جا که مقدور باشد، از آن اطلاعات استفاده نمایند. اطلاعات مزبور غالباً بدون آن که خطر چندانی این شرکت ها یا موسسات ارائه کننده خدمات اطلاعاتی را تهدید کند، مورد استفاده قرار می گیرد. زیرا برای یک مشتری، اغلب دشوار و یا تقریباً غیر ممکن است که از سیاست یک شرکت در زمینه اطلاعات شخصی افراد آگاه شود(نورائی، بیدخت،۱۵:۱۳۸۷).

پس بدون تردید می توان گفت که منافع موجود در حریم خصوصی، به استفاده فناوری اطلاعات و ارتباطات مرتبط شده است. مسلماً فناوری اطلاعات و ارتباطات جمع آوری و استفاده از داده را بطور بالقوه و ناخواسته موجب نمی شود. اما در بسیاری از موارد، استفاده از آن را تسهیل می کند. در نتیجه، حفظ حریم خصوصی به عنوان یکی از مسائل مهم اخلاقی در فناوری اطلاعات و ارتباطات از اوایل بحث در مورد اخلاق، رایانه و اطلاعات مطرح شد، بلکه در مدیریت اطلاعات نیز این چنین است که در نتیجه آن ابزار گوناگون قانونی توسط کشور های مختلف توسعه داده شده اند، اما دولت ها علاوه بر توجه به قوانین فضای سایبر در خصوص حریم خصوصی، بایستی به اخلاق حرفه ای فناوری اطلاعات و ارتباطات از طریق رسانه بپردازند. چون حفظ حریم خصوصی، اخلاق خوب و حرفه ای را می پذیرد(Stahl.2007:2).

پیشنهادات

۱) قوه مقننه ، قضاییه و نیروی انتظامی با گسترش تعاملات دو جانبه و چند جانبه بین المللی و استفاده از تجارب فراملی، در خصوص هماهنگ سازی جرم انگاری سایبری، برطرف نمودن خلاء های قانونی، کشف جرایم و... در زمینه مبارزه با جرایم سیاسی اقدام نمایند.

۲) با توجه به نظریه تقلید و یادگیری اجتماعی و تأثیر بزهکاری افراد به ویژه کودکان و نوجوانان بر یکدیگر، والدین، آموزش و پرورش، نیروی انتظامی و قوه قضاییه نسبت به برنامه ریزی لازم با استفاده از آخرین روش های آموزشی و فنی در راستای پیشگیری از یادگیری رفتار مجرمانه از طریق فضای سایبر، اقدام نمایند.

۳) به جهت پیشگیری از اغفال کاربران و جلوگیری از بزه دیده شدن آنان، استفاده صحیح از فضای سایبر و رعایت امنیت کاربران و سامانه ها بویژه شبکه های اجتماعی، توسط رسانه ملی، سازمان های دولتی و غیر دولتی و آموزش و پرورش، آموزش و اقدام لازم به عمل آید.

۴) کارگروه متشکل از قوه قضاییه، وزارت ارتباطات و فناوری اطلاعات، نیروی انتظامی و شرکت های توانمند در حوزه فضای سایبر، نسبت به بررسی و توسعه شبکه های اجتماعی بومی به منظور تولید فرهنگ فاخر اسلامی – ایرانی اقدام نمایند.

۵) به منظور پیشگیری از جرایم سایبری، موسسات مالی، بانکی، سازمان ها و ... نسبت به افزایش و ارتقاء سامانه های فنی، اقدام و از تجربیات پلیس فتا در مقابله با جرایم، تهدید ها و آسیب های این حوزه استفاده نمایند.

۶) نیروی انتظامی با استفاده از ظرفیت رسانه ملی، نسبت به ارائه آموزش های عمومی مرتبط با فضای سایبر در جهت پیشگیری وضعی و اجتماعی اقدام نماید.

۷) انجام بررسی های فنی و تخصصی در خصوص خدمات پست های الکترونیک (رایانامه ها) و راه اندازی آن در داخل کشور برای هر فرد ایرانی با کد ملی مشخص.

ISSN: 2538-3671
http://www.johi.ir

نتیجه گیری

فناوری اطلاعات و ارتباطات این ظرفیت را دارد که در ابعاد مختلف پیشگیری وضعی از جرایم سایبری تأثیر گذار باشد. بنابراین از آنجا که استفاده از آن می تواند با ابزار کنترلی که فراهم می سازد از ارتکاب جرایم سایبری پیشگیری کند، با ابعاد نظارتی که دارد امکان شناسایی مجرمان سایبر را نیز می تواند فراهم سازد. در این مقاله، ضمن بیان گسترش جرم در فضای مجازی به دلیل ویژگی های خاص آن، ابتدا بـه تبیین جرایم سایبر و ذکر نمونه هایی از آن پرداخته شد. آنگاه با ارائه مفاهیم و دسته بندی پیشگیری از جرم، پیشگیری مبتنی بـر فناوری اطلاعات به عنوان یک نوع پیشگیری وضعی مورد بررسی قرار گرفت. سپس راهکارهایی مبتنی بـر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمین، گشت فضای مجازی، کنترل و نظارت بر فضای مجازی، جمع آوری ادلۀ الکترونیکی جرم، مستند سازی صحنه جرم برای پیشگیری از جرایم سایبر احصاء شـد. بنابراین پیشگیری مبتنی بـر ردیابی نشـانی هویت مجازی(مهاجم)، گشت فضای مجازی، کنترل و نظارت بر فضای مجازی و جمع آوری ادلۀ الکترونیکی جرم در محیط اینترنت، مستند سازی صحنۀ جرم در محیط اینترنت در کاهش ارتکاب جرایم سایبری تأثیر دارد.

منابع و مراجع

۱- آقابابایی، حسین، ۱۳۸۹، قلمرو امنیت در حقوق کیفری، پژوهشگاه فرهنگ و اندیشه اسلامی، تهران، چاپ نخست.

۲- اردبیلی، محمد علی، ۱۳۹۳، حقوق جزای عمومی، نشر میزان، جلد نخست، چاپ سوم.

۳- اصلانی، حمیدرضا، ۱۳۸۴، حقوق فناوری اطلاعات، حریم خصوصی در جامعه اطلاعاتی، با همکاری مرکز فناوری اطلاعات ریاست جمهوری، میزان، تهران، چاپ نخست.

۴- باستانی، برومند، ۱۳۸۸، جرایم رایانه ای و اینترنتی، جلوه ای نوین از بزهکاری، بهنامی، تهران، چاپ پنجم.

۵- زندی، محمدرضا، ۱۳۸۹، تحقیقات مقدماتی در جرایم سایبری، جنگل، تهران، چاپ نخست.

۶- حسن بیگی، ابراهیم، ۱۳۸۴، حقوق و اینترنت در فضای سایبر، انتشارات موسسه فرهنگ مطالعات و تحقیقات بین المللی ابرار معاصر، تهران، چاپ نخست.

۷- پیتر کری و جو ساندرز، ۱۳۸۴، حقوق رسانه، ترجمه حمیدرضا ملک محمدی، میزان، تهران، چاپ نخست.

۸- دالال، اِ. اس و راقا و شارما؛ ۱۳۸۸، حقوق فناوری اطلاعات و ارتباطات (مجموعه مقالات): نیم نگاهی به ذهن هکرها، برگردان: احسان زررخ، روزنامه رسمی ایران (معاونت حقوقی و توسعه قضایی قوه قضاییه)

۹- نجفی ابرند آبادی، علی حسین، ۱۳۸۱، تقریرات درس جرم شناسی، تهران، مجتمع آموزش عالی دانشگاه تهران.

۱۰- میر محمد صادقی، حسین، ۱۳۹۴، حقوق کیفری اختصاصی یک، میزان، تهران، چاپ سی ام.

۱۱- میر محمد صادقی، حسین، ۱۳۹۴، حقوق کیفری اختصاصی دو، میزان، تهران، چاپ سی ام.

۱۲- میر محمد صادقی، حسین، ۱۳۹۴، حقوق کیفری اختصاصی سه، میزان، تهران، چاپ سی ام.

13- Baelon, Dl. Choi and, YJ. Conaty. Tf, 2006. Computer crimes, American criminal law review, vol.43.

14- Tashankar. K,2011. Cyber criminology, crc press taylor and francis group, u.s.

15- Mc quade, S. 2006, understanding and manging cyber crime, Boston , ma:allyn and Bacon.