مجله علمی پژوهش در علوم انسانی ومطالعات اجتماعی (سال پنجم)
شماره ۱۵ / بهار ۱۳۹۸ / ص ۲۲۲-۲۰۱

راهبردهای پیشگیری از جرایم سایبری با نگاهی بر سیاست جنایی ایران و رهنمودهای سازمان ملل متحد

فهیمه بهرامی پور[۱]
[۱] دانشجوی کارشناسی ارشد[۱]، گروه حقوق بین الملل ، واحد قم ، دانشگاه دولتی ، قم ، ایران

نویسنده مسئول:

فهیمه بهرامی پور

چکیده

با شیوع استفاده از رایانه در زندگی شخصی و روابط اداری، بزهکاری و تخلف در استفاده از رایانه نیز، واقعه‌ای اجتناب ناپذیر است. پیشگیری از جرایم سایبری به جهت خصایص و ویژگی‌های آن و نیز خطر مضاعف این جرایم نسبت به جرایم سنتی از اهمیت دوچندان برخوردار است. از همین‌رو، پیشگیری و مقابله با این جرایم محور اصلی سیاست جنایی کشورها تلقی می‌شود. در سیاست جنایی تقنینی ایران در قوانین و مقررات مختلف از جمله قانون جرایم رایانه‌ای مصوب ۱۳۸۸ قانونگذار جنبه‌های ماهوی حقوق کیفری فناوری اطلاعات و ارتباطات را مورد توجه قرار داده و اقدام به جرم‌انگاری جرایم علیه محرمانگی داده‌ها، صحت و تمامیت داده‌ها، اموال و عفت عمومی نموده است. اما باتوجه به شیوه‌های نوین جرایم سایبری سیاست‌های کیفری به تنهایی نمی‌تواند پاسخگوی آسیب‌های ناشی از جرایم سایبری باشد. از همین‌جهت تمسک به راهبردهای پیشگیری غیرکیفری امری اجتناب ناپذیر است. بنابراین برای پیشگیری همه جانبه از جرایم سایبری به اقتضای عوامل جرم‌شناختی موثر بر این جرایم مستلزم بهره‌مندی از روش‌های مختلف پیشگیری (وضعی-اجتماعی) و نیز رهنمودهای سندهای پذیرفته شده‌ی بین‌المللی است. در این راستا سیاست قضایی ایران با همکاری نهادهای دولتی و غیردولتی از جمله معاونت اجتماعی پیشگیری از جرایم قوه قضاییه، پلیس فتا و نیز مراکز امداد و آگاهی رایانه‌ای، اقدام به مقابله با جرایم سایبری نموده است. اما علیرغم این تلاش‌ها روزآمد نبودن قوانین، رقم سیاه، فقدان نیروهای متخصص و فقدان ابزارهای نظارتی کارآمد امر پیشگیری را با مانع مواجه ساخته است. لذا در این پژوهش ضمن بررسی شیوه‌های پیشگیری‌های وضعی و اجتماعی جرایم سایبری و سیاست جنایی ایران در قبال این جرایم راهبردهای پیشگیری از جرم سایبری با تاکید بر رهنمودهای سازمان ملل متحد مورد مداقه قرار خواهد گرفت.

واژگان کلیدی: جرایم سایبری، پیشگیری وضعی، پیشگیری اجتماعی، سازمان ملل متحد، کنوانسیون بوداپست

مقدمه

امروز همگام با توسعه‌ی جامعه‌ی جهانی بحث ارتباطات نوین و فن‌آوری اطلاعات که تجلی روشن آن فضای سایبری است بستر ارتکاب جرایم بیشماری را فراهم آورده است.

با شیوع استفاده از رایانه در زندگی شخصی و روابط اداری، بزهکاری و تخلف در استفاده از رایانه نیز، واقعه‌ای اجتناب ناپذیر است. آنچه امروز تحت عنوان جرایم رایانه‌ای نام برده می شود، مجموعه ای از همین تخلفات و بزهکاری‌هاست که از طریق رایانه یا مؤثر بر رایانه اتفاق می‌افتد و مصادیق متعددی از آن نیز در ذهن ما نقش بسته است.چه بسا ساده‌ترین مصادیقی که به جهت کثرت اتفاق در ذهن داریم، مواردی مانند هک پایگاه های اینترنتی یا انتشار داده‌های محرمانه از طریق وب سایت‌هاست که اغلب با تصور تخلف در خلأ قانون و عدم امکان تعقیب اتفاق افتاده است. این خلأ قانونی یا عدم شناخت قوانین مرتبط در حدی است که قربانیان این تخلفات همواره در یافتن پناهی برای تظلم خواهی، عاجز می‌مانند.(شاهبندرزاده و همکار، ۱۳۹۱، ۱۳۸)

بدین‌ترتیب،جرایم سایبری-کامپیوتری دارای چند دسته یا طبقه کلی هستند که عبارتند از: ۱. جرایم کلاسیک با توصیف سایبری شامل جعل سایبری، کلاهبرداری سایبری و...؛ ۲. جرایم علیه محتوا شامل جرایم علیه کودکان و نوجوانان، افتراهای اینترنتی، پورنوگرافی، ترویج ایدئولوژی‌های مضر و....؛ ۳. جرایم صرف تکنولوژی اطلاعات شامل جرم دستیابی غیرمجاز، شنود و...؛ ۴. جرایم مخابراتی شامل جرایم ماهواره، شنود مخابراتی، جرایم موبایل و..؛ ۵. جرایم یا مبنای غیرجزایی شامل مالکیت فکری، جرایم بانکداری الکترونیک، جرایم تجارت الکترونیک، جرایم حمایت از داده و...

البته، با توجه به این که در کشور ما کاربرد رایانه از ابتدای ورود آن تا دهه ۱۳۷۰ بسیار محدود بوده است، لذا جرم رایانه ای سابقه چندانی در نظام حقوقی ایران ندارد. اگر احیاناً جرمی در این خصوص واقع شده باشد، گزارشی از آن منتشر نشده است. وقوع جرم رایانه ای به تدریج از دهه ۱۳۷۰ در ایران شروع شد.

یکی از جلوه‌های بررسی جرم‌شناختی یک پدیده، بررسی راهبردهای مناسب پیشگیری در برابر آن است. همان‌گونه که پیش از این هم گفته شد، هنگامی که پیشگیری سودمندتر از سرکوبی دانسته شود، به صورت اصلی راهبردی در سیاست‌های جنایی یک کشور در برابر بزه‌کاری در می‌آید. باید به یاد داشت که بسیاری از کشورهای توسعه‌یافته، به جای مجازات و بازپروری مجرمین، به ترسیم راهکارهایی مبادرت می‌ورزند تا قبل از وقوع آسیب و جرائم، هزینه‌های جرم را در جامعه کاهش دهند. (حسینی تبار کریمی، ۱۳۹۲،۵۶)

بدین‌ترتیب، تدابیر پیشگیری وضعی حتی در شکل حداقلی خود، موجب محدودسازی آزادی های فردی می‌گردند. بارزترین نمونهٔ این امر در فضای سایبر، فیلترینگ نامناسب و غیر کارشناسی است که صرفاً به خاطر استعمال یک یا چند واژه‌یغیر مجاز در یک متن علمی، بخشی از جامعه از یافته های آن اثر محروم می شوند. این امر، علاوه بر اینکه ناشی از کاربستِ غیر اصولی و بی برنامه است، به ماهیت تدابیر وضعی نیز میان بزهکار و ناکرده بزه تفکیک قائل نیست، برمی گردد. البته نباید تصور شود که تنها با کاربستِ تدابیر وضعی می توان از جرایم سایبری پیشگیری نمود؛ زیرا این اقدامات مصون از محدودیت و ایراد نیستند. به همین‌جهت باید برای پیشگیری از جرایم راهبردهای اجتماعی نیز مورد توجه قرار گیرد.

در سال‌های ۱۹۹۵ تا ۲۰۰۲ دو رهنمود در خصوص پیشگیری از جرم از طرف شورای اقتصادی و اجتماعی سازمان ملل متحد به تصویب رسیده است؛ نخستین مورد «رهنمود همکاری و کمک‌های فنی در خصوص پیشگیری از جرایم شهری» و دومین مورد «پیشگیری از جرم» است که تاکید این پژوهش بر مورد دوم است.

بدین‌ترتیب،از آنجایی که جرایم سایبری از جمله مسائل مهمی است که امروزه در جوامع آحاد مردم با آن روبرو هستند و روز به روز بر آمار ارتکاب این دست از جرایم افزوده می‌شود، نگارنده بر خود لازم و ضروری دانسته است که راهبردهای پیشگیری از جرایم سایبری را مورد مطالعه قرار دهد.لذا سوالات، فرضیه‌ها، اهداف،روش تحقیق و سامان تحقیق در این پژوهش به شرح ذیل خواهد بود:

- **سوالات**

۱. راهکارهای پیشگیری وضعی از جرایم سایبری کدام است؟
۲. مهم‌ترین راهکار پیشگیری اجتماعی از جرایم سایبری چیست؟

- **فرضیه‌ها**

۱. باتوجه به ماهیت جرایم سایبری، نظارت رسمی، کنترل دستیابی به اهداف، کاهش عوامل مجرم و نیز افزایش موانع ارتکاب می‌تواند از جمله راهبردهای وضعی برای پیشگیری از جرایم سایبری تلقی شود.
۲. از آنجا جامعه‌ی آماجی جرایم سایبری آحاد مردم هستند آموزش همگانی و فرهنگ‌سازی در جهت جلوگیری از بزه‌دیدگی و نیز پیشگیری از حرم در فضای سایبر و همچنین سازوکارهای تقویتیِ کدهای رفتاری و نیز منشور اخلاقی برای این افراد می‌تواند به عنوان مهم‌ترین راهکار پیشگیری اجتماعی باشد.

- **اهداف**

۱. بررسی مفاهیم و عوامل جرم شناختی جرایم سایبری
۲. بررسی راهکارهای وضعی پیشگیری از جرایم سایبری
۳. بررسی راهکارهای اجتماعی پیشگیری از جرایم سایبری
۴. بررسی راهبردهای سازمان ملل متحد و کنوانسیون بوداپست

- **روش تحقیق و شیوه گردآوری اطلاعات**

روش انجام این تحقیق با توجه به موضوع و اهداف و شیوه گردآوری اطلاعات که به شیوه‌ی کتابخانه‌ای و مراجعه به پایگاه های داده و جستجوی اینترنتی، مقالات دارای درجه علمی معتبر و به روز رسانی شده می‌باشد، به صورت توصیفی – تحلیلی خواهد .

- **سامان تحقیق**

این پژوهش در ۴ بخش نگارش شده است. در بخش اول به بررسی مفاهیم واژگان مرتبط پرداخته‌ایم. بخش دوم عوامل جرم‌شناختی موثر بر جرایم سایبری است؛ بخش سوم راهبردهای پیشگیری وضعی و اجتماعی از جرایم سایبری مورد بررسی قرار گرفته است؛ در بخش چهارم راهبردهای پیشگیری از جرایم سایبری با تاکید بر رهنمودهای سازمان ملل متحد و اسناد بین‌المللی آورده شده است.

۱.مفاهیم

برای فهم درست مباحث در هر زمینه و رشته‌ی علمی، پیش از هر اقدامی‌لازم است به مفهوم شناسی واژگان کلیدی آن توجه کافی و وافی داشته باشیم. چراکه؛ شکل‌گیری منطق و ادبیات مشترک و مورد توافق برای گفتمانی علمی‌و کارآمد از جمله ضروریات نتیجه بخش خواهد بود. لذا در این پژوهش نخستین گام به اریه‌ی مفهوم لغوی و اصطلاحی واژگان کلیدی این موضوع اختصاص داده خواهد شد.

۱-۱.فضای سایبر

منظور از فضای سایبر یا فضای مجازی ترکیبی از ده ها هزار رایانه به هم پیوسته، سرویس دهنده‌ها، شبکه‌های ارتباطی، سویچ‌ها، و کابل‌های فیبر نوری است که امکان برقراری ارتباطات را در سامانه‌ای جامع فراهم می‌آورد. (حسینی و همکار، ۱۳۹۲، ۴۳)

بنابراین، «می‌توان فضای سایبر را محیطی مجازی و غیرملموس و موجود در شبکه‌های بین المللی تعریف کرد که همه‌ی اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها، و به طور کلی هر آنچه به صورت فیزیکی و ملموس در کره‌ی خاکی در این فضا به شکل دیجیتالی وجود دارد و قابل استفاده و در دسترسِ کاربران است که از طریق رایانه، اجزای آن، و شبکه‌های بین‌المللی به هم مرتبط است. از جمله ویژگی‌های فضای سایبر می توان به ارتباطات سریع، قابلیت ارسال پیام، ارایه‌ی سرویس‌های ارتباطی، و تبادل اطلاعات با فرمت‌های گوناگون اشاره کرد. »(احمدی ناطور و همکار، ۱۳۹۵، ۴)

۲-۱. جرایم سایبری

جرم سایبری، یکی از اصطلاحاتی است که بر استفاده از فناوری رایانه در پرداختن به یک فعالیت غیر قانونی دلالت دارد . جرم فناوری های پیشرفته[۱] و جرم عصر اطلاعات[۲] نیز همین پدیده را توصیف می‌کند . اغلب جرایم سایبری که تا به حال شاهد آنها بوده ایم چیزی نیست جز مهاجرت جرایم از دنیای واقعی به فضای اینترنت . امروزه جرایم سایبری با سرعت نگران کننده‌ای، بدون کنترل رو به تکثیر و افزایش است و به عنوان فعالیت‌های به واسطه‌ی رایانه که هم غیر قانونی و هم نامشروع هستند، می‌توانند از طریق شبکه‌های الکترونیک جهانی هدایت شوند جرم سایبری را هر جرمی می‌دانند که شامل رایانه‌ها و شبکه‌ها باشد، ولو آنکه خیلی متکی به رایانه نباشد در حالی که برخی جرم سایبری را جرایمی می‌دانند که دسته‌های مختلفی از جرایم را در فضای سایبر و شبکه‌ی جهانی اینترنت در بر می‌گیرند و شامل جرایم ارتکابی به کمک رایانه و جرایم متمرکز بر رایانه نیز نامیده می‌شود. (شاه محمدی و همکار، ۱۳۹۳، ۱۰۵)

همچنین، سازمان همکاری و توسعه اقتصادی[3]در تعریف جرایم سایبری اعلام می‌دارد: « سوءاستفاده از کامپیوترها شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش خودکار انتقال داده‌ها است»و نیز برخی از متخصصان کمیته اروپایی اظهار داشته‌اند: «هر عمل مثبت غیرقانونی که کامپیوتر در آن ابزار یا موضوع جرم باشد، جرم کامپیوتری است.» (سازمان ملل، ۱۳۷۶، ۱۱۸)

۳-۱. پیشگیری وضعی

پیشگیری به معنای "جلوگیری، دفاع، صیانت و مانع شدن" است در واقع ، تعریف علمی پیشگیری از جرم "مجموعه اقدام‌های سیاست جنایی به استثنای اقدام‌های کیفری است که هدف انحصاری یا لااقل جزیی از این اقدام‌ها، محدود کردن وقوع مجموعه‌ای از جرایم باشد. (نجفی ابرندآبادی، ۱۳۹۱، ۷۴۱)

در عصر حاضر نیز صحبت از پیشگیری از جرم، غالبا مفاهیمی چون تغییر در جامعه، دگرگون‌سازی بافت شهری، تعارضات موجود میان گروه‌های مختلف اجتماعی، تعارضات میان کنش‌گران دستگاه‌های مختلف، توسعه ی تکنولوژی و طراحی شهری را به ذهن متبادر می‌سازد. در حقیقت می‌توان گفت امروزه سیاست پیشگیری از جرم، بیش از گذشته با تغییرات اجتماعی همراه بوده است؛ این سیاست در شناسایی انواع مختلف تدابیر موجود برای بررسی جرم نقش مهمی ایفا می‌نماید. (بابایی و همکار، ۱۳۹۰، ۱۴۹)

نخستین تعریف پیشگیری وضعی، توسط کلارک صورت گرفته است. در این تعریف، پیشگیری وضعی عبارت است از: « اقدامات معطوف به اشکال بسیار خاص جرم که متضمن مدیریت، طراحی یا دست کاری محیط به‌طور مستقیم، نظام‌مند و دائمی به منظور کاستن از فرصت‌های جرم است. به طوری که توسط اکثریت مجرمان ادراک و فهم شود.» «نایجل ساوت» نیز آن را متکی بر اداره، طراحی و کنترل محیط فیزیکی می‌داند که فرصت‌های ارتکاب جرم را کاهش یا خطر پیگرد متهم را درصورت موثر واقع نشدن بازدارندگی، افزایش می‌دهد. (صفاری، ۱۳۸۰، ۲۸۳)

۴-۱.پیشگیری اجتماعی

«طبق بند الف ماده‌ی یک لایحه‌ی پیشگیری از وقوع جرم، پیشگیری اجتماعی عبارت است از: تدابیر و روش‌های آموزشی، فرهنگی، اقتصادی و اجتماعی دولت، نهادها و سازمان های غیردولتی و مردم نهاد در زمینه‌ی سالم سازی محیط اجتماعی و محیط فیزیکی برای حذف یا کاهش عوامل اجتماعی وقوع جرم.» (محمدنسل، ۱۳۹۲، ۳۴) مرکز بین المللی پیشگیری از جرم، موضوع پیشگیری اجتماعی از جرم را به این نحو تعریف کرده است: هر چیزی که بزهکاری، خشونت و ناامنی را از طریق هدف گیری موفقیت آمیز علل شناخته شده‌ی جرم از طریق علمی کاهش دهد. پیشگیری اجتماعی از جرم، مجموعه‌ی اقدامات و تدابیری است که هدف آن حذف یا کاهش خطر عوامل اجتماعی و اقتصادی و محیطی جرم است. (همان، ۳۵)

---

[1]. High Tech Crime
[2]. Information Age Crime
[1]. Organization For Economic Co-Operation And Development.

بنابراین می‌توان گفت: «پیشگیری اجتماعی مجموعه اقداماتی است که مهار عوامل اثرگذار در شکل‌گیری جرم را دنبال می‌کنند و از آنجا که گذشته از محیط اجتماعی بر فرد و انگیزه‌های او تاثیر می گذارد به آن پیشگیری فردمدار نیز می‌گویند.... پیشگیری اجتماعی به دو نوع است: جامعه‌مدار و رشدمدار. شاید بهترین راهبرد برای پیشگیری، غلبه و یا دست کم کاهش جرایم، در نظر گرفتن اثر تعاملی علل و عوامل جرم‌زا باشد. زمانی که عوامل جرم‌زا ناشی از محیط‌های پیرامون انسان مورد نظر باشد از آن به پیشگیری جامعه‌مدار یاد می‌شود. و آنگاه که عوامل جرم‌زا ناشی از مراحل مختلف رشد کودک و نوجوان است آن را پیشگیری فردمدار می نامند. لذا متداول ترین عوامل خطر بزهکاری مانند اختلالات رفتاری در گروه پیشگیری رشدمدار بررسی می‌شود و آنجا که نابسامانی‌های خانوادگی ممکن است طلیعه بروز بزه را نوید دهند از پیشگیری جامعه مدار گفتگو خواهد شد.» (صبح دل، ۱۳۹۶، ۹۶-۹۵)

۲. عوامل موثر بر جرایم سایبری

ژان پیناتل در بیانِ علت جرم می‌گوید: « شرط لازمی که بدون آن رفتارمجرمانه بروز نخواهد کرد.» (کی‌نیا، ۱۳۸۶، ۵) علت شناسی ازاصول پایه‌ای دانش جرم‌شناسی محسوب می‌گردد. به گونه‌ای که اهداف جرم‌شناسی در زمینه پیشگیری و درمان یک بزه، با شناخت علل ارتکابی آن مقدور می‌باشد. لذا جرم‌شناسان برای مقابله با یک جرم با ترسیم یک رابطه‌ی علت و معلولی، سعی در خنثی نمودن علل موثر در ایجاد

نتیجه مجرمانه می‌نمایند. همانگونه 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 درجرایم سنتی، عوامل متعدد و جدیدی با توجه به ویژگی‌های خاص این فضا در شکل‌گیری جرایم سایبری تاثیرگذار می‌باشند. بنابراین، امروزه در کنار دنیای حقیقی با دنیایی مجازی مواجه هستیم که دارای سه ویژگی اصلی و عمده است: سیالیّت و انعطاف‌پذیری عناصرتشکیل دهنده جرم در زمان و مکان، ناشناس ماندن نسبی مرتکبان درفضای مجازی که در واقع شناسایی آنان و محل ارتکاب جرم را دشوار می‌نماید و جهانی بدون گستره ارتکاب بزه که به بزهکاران اجازه می‌دهد بتوانند جرم را بدون حضور در محل یا از اقصی نقاط جهان انجام دهند. (نجفی ابرندآبادی، ۱۳۹۰، ۱۳)

بدین‌ترتیب، جرایم سایبری نیز مانند جرایم سنتی تحت تاثیر عوامل گوناگونی به وقوع می‌پیوندد . برهمین اساس، در این مبحث علل زیستی، اجتماعی و روانی موثر بر جرایم سایبری به صورت مختصر شرح داده خواهد شد.

۱-۲. علل زیستی

«پس از افول دیدگاه‌های زیستی و تسلط نگرش جامعه‌شناسانه شاید کمتر کسی تصور می‌کرد عقاید زیستی بار دیگر در محافل جرم‌شناسی مورد توجه قرار گیرد، اتفاقی که برخلاف جریانِ غالب جرم‌شناسی به صورت نظام یافته با انتشار کتابِ جنجالی» زیست شناسی اجتماعی، تلفیقی جدید»[۴]اثر ادوار ویلسون[۵]در سال ۱۹۷۰ به‌واقعیت پیوست و مجددا مباحث زیستی مورد توجه جرم‌شناسان قرار گرفت البته این بدین معنا نیست که در دوران افول زیست‌شناسی جنایی، عقاید زیستی به طور کامل فراموش شده بود، بلکه به نظر می‌رسد تنها اثربخشی آن تا حدود فراوانی کاهش یافته بود. تجربه تلخ زیست‌شناسان جنایی از به استهزاء گرفته شدن عقاید زیستی سنتی عاملی بود تا اینبار با دیدگاهی علمی و واقع‌بینانه به رابطه بین بزهکاری و عوامل زیستی بپردازند و از زوایای مختلفی موضوع را به بحث گذارند که غالبا در طبقه‌بندی سه‌گانه‌ی رابطه رفتار مجرمانه با ژنتیک، زیست شیمیایی و فیزیولوژی عصب بیان می‌شوند.» (محمدی جورکویه و همکار، ۱۳۹۴، ۱۳۱)

سه حوزه‌ی مطالعاتی فوق هر یک به نوعی به دنبال کشف رابطه‌ی میان عوامل زیستی و جرایم هستند که به اختصار مطرح می‌گردند:

الف) ژن‌ها

در جرم‌شناسی، ژن‌ها از یک‌سو از طریق انتقال ویژگی‌های زیستی (وراثت و جرم) و از سوی دیگر به وسیله‌ی دگرگونی‌های احتمالی‌شان (اختلال‌های ژنتیکی) در وقوع رفتار مجرمانه اثرگذار می‌باشند.

---

1. Sociobiology: The New Synthesis.
2. Edward Wilson.
1. Neurophysiology
2. Neurocriminology

ب) زیست شیمایی

تاثیر عوامل زیست شیمایی بر وقوع جرم گاه از طریث «تغییرات هورمونی در بدن» (برای نمونه تغییر میزان تسترون در مردان و سندروم پیش قاعدگی در زنان)و گاهی به وسیله‌ی چگونگی «تغذیه» و یا حتی «میزان آلودگی‌های محیطی» مثل میزان سرب، جیوه، سم دفع آفات در هوا و نقش آنها بر وقوع جرایم است

ج) فیزیولوژی عصب[۶] و جرم

فیزیولوژی عصب، از رشته‌هایی است که با پیشرفت علم، جایگاه ویژه‌ای را کسب کرده است. در جرم‌شناسی می‌توان به گرایشی نسبتا نوپا در شاخه زیست‌شناسی، به نام « جرم‌شناسی عصب» [7] اشاره کرد.در خصوص فیزیولوژی عصب و جرم زیست‌شناسان جنایی به دنبال کشف ارتباط بین اختلال‌های عصبی و مواد شیمایی مغز با جرایم و به طور خاص رفتارهای پرخاش‌گرایانه می‌باشند. این گرایش زیستی با پیشرفت روزافزون علم، جایگاه ویژه‌ای را در جرم‌شناسی کسب کرده است. (حسینی وهمکار، ۱۳۹۶، ۱۶۸)

در خصوص علل زیستی جرایم سایبری تا کنون مطالعه‌ی دقیقی صورت نگرفته و در آثار علمی موجود نیز بیشتر به شرح مباحث تئوری استناد شده است. تنها آماری که از مشتقات علل زیستی جرایم سایبری در دسترس می‌باشد، بحث جنسیت این مجرمین است. طبق آخرین آماری که سردار هادیان فر رییس پلیس تولید و تبادل اطلاعات ناجا ارائه داده است، از سال ۹۰ تا ۹۶ در ایران جرایم سایبری ۹۰۰ درصد افزایش داشته است. طبق گزارش ارائه شده در این سالیان به ۱۲۰ هزار فقره پرونده رسیدگی شده و بیش از ۸۶ درصد پرونده‌ها در حوزه جرایم سایبری کشف و بیش از ۷۰ هزار مجرم سایبری دستگیر که ۷۷ درصد آقایان و ۳۳ درصد خانم ها بوده‌اند.[8]

۲-۲. علل روانی

«رفائل گاروفالو (۱۹۷۸) از معتقدان تاثیر عوامل روانی در ارتکاب بزه است. بررسی و شناخت عوامل روانی جرم مربوط به دانش روان شناسی جنایی است. از جمله رسالت‌های این دانش بررسی منش و شخصیت بزهکار و ارزیابی گرایش‌های ضداجتماعی و مطالعه روان خودآگاه و ناخودآگاه آنان به منظور تعیین مسئولیت اخلاقی و اجتماعی شان است. عوامل درونی بزهکاری با ویژگی‌های خود قابل تفکیک به دو گروه ارثی و اکتسابی هستند. عوامل ارثی شامل خودآوردهایی است که کودک از پدر، مادر و نیاکان خود گرفته و هنگام زادن با خود به دنیا آورده است. تأثیر وراثت را در تکوین شخصیت کودک نمی‌توان انکار کرد. پژوهش‌های سال‌های اخیر در زمینه علم وراثت نشان می‌دهد که پاره‌ای از نابهنجاری‌های کروموزومی تأثیر ژرفی در عواطف، هیجان‌ها و به‌طور کلی رفتار انسان دارد. ویژگی‌های اکتسابی شخصیت انسان سبب می‌شود، پاره‌ای از استعدادهای بالقوه ارثی شکوفا شود، یا به عکس سد راهی برای بالندگی آن فراهم شود.» (نبوی، ۱۳۹۱، ۱۲-۱۱)

باتوجه به طیف گسترده جرایم سایبری، مجرمان هریک از این جرایم ویژگی‌های خاص خود را دارند. بارزترین این تفاوت‌ها در بحث ویژگی‌های روانی آشکار می‌گردد زیرا به عناصر شخصیتی، رفتاری و روانی افراد مربوط می‌شود که هریک، گرایش به جرم خاصی را درپی دارد. البته در کشور ایران در این زمینه تحقیقات مستدل . متقنی صورت نگرفته است. در سایر کشورها نیز به این موضوع به صورت پراکنده پرداخته شده است که ما در ذیل به برخی از این تحقیقات اشاره می‌کنیم.

به طور مثال تحقیقی در آمریکا توسط کاترین سیگفرد و همکارانش در سال ۲۰۰۸ صورت گرفت. در این پژوهش ۳۰۷ نفر مورد به صورت اینترنتی به پرسش‌نامه‌ها پاسخ دادند که از بین این ۳۰۷ نفر ۲۷۷ نفر کسانی بودند که از اینترنت برای پورنوگرافی استفاده می‌کردند و ۳۰ نفر افرادی بودند که چنین استفادای نداشتند. این تحقیق نشان داد که استفاده‌کنندگان محتوای پورنوگرافی سطح بالاتری از استثمار اخلاقی و همچنین سطح پایین تری از کاربرد طرق انتخاب اخلاقی را نشان دادند. این افراد این عمل را گرچه از نظر اجتماعی غیرقابل پذیرش و غیراخلاقی می‌دانند ولی نسبت به خود این عمل را غیراخلاقی تلقی نمی‌کنند. همچنین، مشخص شد که زنان بیشتر در معرض استفاده از اینترنت هستند. (Seigfried, 2008)

همچنین ولک و همکارانش در سال ۲۰۰۹ در باب پورنوگرافی کودکان تحقیق گسترده‌ای انجام دادند که این تحقیق از طریق ایمیل و مصاحبه‌ی تلفنی صورت گرفته است. در این مصاحبه ۱۶۶۳ نفر از طریق ایمیل و ۶۱۲ نفر مصاحبه تلفنی به سوالات پاسخ دادند. این تحقیق

[8] http://www.irna.ir/fa/News/82900640

نشان داد که سوءاستفاده‌گران جنسی فضای مجازی معمولا افراد خشن و سادیستیک نیستند، بلکه آنان افرادی صبور هستند که روابطشان را با قربانیانشان به مرور گسترش می‌دهند و در موارد بسیارکمی، خشونت در رفتارها و الفاظ آنها دیده می‌شود. (Wolak,2009)

«مک فارلند و بوسیج، عقیده دارند که ارتکاب این جرم به دلیل اختلال روانی در فرد می‌باشد. آنان به این نتیجه رسیدند که مجرمین آزار و مزاحمت سایبری دارای سایکوز عاشقانه که نوعی اختلال ناشی از توهمات شهوانی فرد است، می‌باشند که معمولا در راهنمای تشخیص و آماری اختلالات روانی تعریف می‌شود. این سندروم برای توضیح رفتارهای وسواسی و اجبارگونه در افرادی که واقعا اعتقاد دارند روابطی صمیمانه با قربانیانشان برقرار کرده‌اند، کاربرد دارد.(Mcfarlane , 2003,18-22)

۳-۲. علل اجتماعی

انحراف از هنجارهای رسمی و پذیرفته شده یک پدیده جهانی است، اما نوع میزان شدت و سطح آن از جامعه ای به جامعه دیگر متفاوت است . آسیب های اجتماعی پدیده هایی زمانمند، مکانمند و به عبارتی نسبی و متغیراند. جنایت پرخاشگری، اعتیاد، روسپیگری، سرقت، قاچاق مواد مخدر .... نمونه‌های از این آسیب‌ها محسوب می‌شوند و آنچه که در یک بستر زمانی، مکانی، فرهنگی و اجتماعی آسیب تلقی می شود ممکن است در آینده در همان بستر و شرایط یا در مقطع زمانی مشابه در بستر و شرایطی متفاوت یا جامعه ای دیگر آسیب یا کج‌روی شناخته نشود. (ایار و همکاران، ۱۳۹۳، ۴۰)

«به زعم کارل مارکس بیشتر بزهکاری‌ها و رفتارهای قانون‌شکنانه به وسیله طباقات پایین انجام می‌شود و این نه به دلیل تمایل و علل روانشناختی مربوط به فقرا و طبقات پایین است بلکه به علت محدودیت‌هایی است که از طریق طبقه مسلط بر ابزار و نهادهای قدرت بر طبقات پایین و فقرا اعمال می‌شود. به زعم این نظریه وجود تضادهای گسترده در جامعه و طبقاتی شدن انسان‌ها، باعث می‌شود تا افراد طبقه پایین دچار از خودبیگانگی شوند و از خود بیگانگی که به معنی احساس از دست دادن کنترل برزندگی اجتماعی است احتمال اعمال قانون‌گریزانه را برای فرد فراهم می‌آورد که به طور جاری انجام می‌شود. از نظر مارکس در چنین فرآیندی افراد فقیری که دچار از خود بیگانگی می‌شوند به احساس پوچی، بی‌قدرتی، بیزاری از خود، بی‌اعتمادی و خشونت می‌رسند که پیامد چنین وضعیتی باعث اخلاق‌زدایی و بی‌توجهی به ارزش‌های هنجار بخش جامعه می‌شود. تا جایی که افراد طبقه پایین و فقیر به انکار ارزش‌های اساسی جامعه، هنجارهای اجتماعی و استانداردهای تثبیت شده رفتار می‌پردازند. زیرا جهت‌گیری قوانین و نظام وضع آن را به خود نسبت نمی‌دهند و با قوانین هنجاربخش به عنوان، بیگانه برخورد می‌کنند. »(وروایی و همکاران، ۱۳۹۵، ۸)

همچنین، «رابطه اقتصاد و جرم در نظریه پارسونز مورد بررسی قرار گرفته است. مسأله اساسی نظریه تحلیل کنش پارسونز ،مساله نظم اجتماعی است. پارسونز چهار شکل کارکردی عام را برای هر نظام اجتماعی در هر سطحی مطرح می‌نماید : انطباق با محیط، دستیابی به هدف، انسجام و حفظ انگاره‌های فرهنگی. پارسونز مشکل اساسی نظام اجتماعی را عمدتا در بعد انسجامی می‌بیند بحث اصلی پارسونز در تبیین انحرافات اجتماعی بر مبنای پیش فرضی که در مورد خرده نظام‌های چهارگانه: فرهنگ ، اجتماع، سیاست و اقتصاد مطرح کرده، شکل گرفته است. کارکردهای مناسب هر یک ازاین خرده نظام‌ها و ارتباط و کنش متقابل بین آنها، عامل کنترل کننده جامعه و همچنین ، عامل بقا و پایداری نظام اجتماعی است. در مقابل، عدم تعادل و بی سازمانی در هر یک از خرده نظام‌ها، حیات جامعه را تهدید کرده ، زمینه را برای رفتار انحرافی فراهم می‌سازد.» (نوغانی و همکار، ۱۳۹۴، ۸۸)

ونیز، یک قاعده‌ی کلی و شناخته شده است که جرم در نواحی شهری بیشتر از نواحی روستایی اتفاق می‌افتد. مکتب شیکاگو در این زمینه پژوهش‌های زیادی انجام داده است. پژوهش‌های مکتب شیکاگو بدین نتیجه رسیده که نرخ انحراف و جرایم، یک الگوی جغرافیایی خاصی دارد که ثباتی نسبتا طولانی داشته است. نظریه‌پردازان این مکتب بر این باور بودند که زندگی اجتماعی در برخی مناطق و مکان‌ها، چهره‌ای سامان‌گریز و دارای آسیب به خود می‌گیرد و در چنین وضعیتی، وقوع جرم قابل انتظار است. اما باید توجه داشت که در محیط سایبری؛ پراکندگی جغرافیایی صحنه جرم بسیار زیاد و معمولا دور از هم و در محدوده مرزی کشورهای مختلف است. بنابراین در این جرایم ترکیب جمعیتی و اقتصادی جای خود را به ویژگی‌های فنی و تراکم امکانات موجود برای ورود به فضای سایبر داده است. در واقع، گسترش زیرساخت‌های فناوری اطلاعات و ارتباطات در برخی از مناطق و لذا افزایش کاربران و استفاده‌کنندگان اینترنت از دلایل افزایش مجرمان در برخی مناطق می‌باشد. (ابوذری، همان، ۱۴۸-۱۴۵)

۳. راهبردهای پیشگیری از جرایم سایبری

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 تایید 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 مساله و اهمیت پیشگیری از ارتکاب جرم‌های رایانه‌ای؛

۴- دادن آموزش‌های کافی به دادرسان، ماموران 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. (اکرمی و همکار، ۱۳۹۵، ۲)

لذا در این مبحث به راهبردهای پیشگیری وضعی و اجتماعی جرایم سایبری پرداخته خواهد شد.

۱-۳. پیشگیری وضعی

همان‌طور که پیش از این گفته شد، کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. توجه به مثلث جرم می‌تواند به درک این موضوع کمک کند. برای ارتکاب کی جرم، سه عامل باید جمع شوند. مهم‌ترین آنها که قاعده‌ی مثلث جرم را هم تشکیل می‌دهد، انگیزه‌ی 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 پیشگیرانهٔ اجتماعی اتخاذ شود؛ 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 میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد؛ زیرا متصدیان امر هرچه بکوشند ابزارهای ارتکاب جرم را از سطح جامعه جمع آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آنها دست یابند؛ در عین حال نباید اهمیت جمع آوری این ابزارها را در کاهش جرایم نادیده گرفت. به هر حال، آنچه در پیشگیری وضعی از جرایم اولویت دارد، حفظ آماج ها و بزه دیدگان از تعرض مجرمان است.(شاهمحمدی، ۱۳۹۵، ۱۱۰)

بنابراین، هدف از اعمال تدابیر پیشگیری در فضای سایبر، مصونیت داده‌ها و حفظ آنها از عوامل مختلفِ مخرب در این فضا می‌باشد که علی القاعده ابتدا بایستی عوامل مذکور به شیوه‌های علمی مورد شناسایی قرار گیرند تا نحوه ورود و نفوذ عوامل مرتبط به وسیله کشف علمی، ابتدا شناسایی شده و متعاقبا به پیشگیری از وقوع جرایم سایبری بی‌انجامد. به اعتقاد برخی کارشناسان، امنیت در محیط سایبر بدین معنا است که دسترسی به منابع اطلاعاتی تحت کنترل کاربر قرار گیرد و هیچ کس بدون مجوز وی قادر به دسترسی به این منابع نباشد.

برخی از راهبردهای راهبردهای وضعی پیشگیری از جرایم سایبری عبارتند از: سخت کردن آماج جرم، کنترل ورودی ها به اماکن مختلف یا کنترل دسترسی به اماکن یا آماج جرم، تجهیزات و اهداف مربوط، کنترل خروجی ها، منحرف کردن بزهکاران از آماج و کنترل و ایجاد محدودیت برای استفاده از ابزارهای تسهیل‌کننده ارتکاب جرم.از همین‌رو؛ در ذیل به راهبردهای وضعی پیشگیری از جرایم سایبری پرداخته خواهد شد.

۱-۱-۳. افزایش موانع ارتکاب جرم

«مراد از مانع ایجاد سد یا دیواری مقابل بزهکار است تا با تغییر وضعیت وی از ارتکاب جرم توسط فرد مصمم به انجام آن جلوگیری کند. به طور مثال، یکی از راه های پیشگیری از وقوع جرم، پنهان نمودن آماج جرم یا بزه‌دیده‌ی احتمالی از دید بزهکاران است. در فضای مجازی، مخفی نمودن آماج به کمک ناشناس کننده ها و رمزنگارها امکان پذیر است. این دو اقدام با آنکه با یکدیگر تفاوت دارند، یک هدف را دنبال

می کنند. کارکرد اصلی آن ها این است که با پنهان کردن هویت یا محتوای اطلاعات افراد، از بزه‌دیدگی آنها جلوگیری کنند.» (خانعلی پور و همکار، ۱۳۹۰ ۱۲۹)

همچنین، برخی روش‌ها، منافع حاصل از جرم را از بین می برند. بنابراین تدابیر وضعی باید تا جای ممکن معادلات را به ضرر بزهکار رقم زند. جابه جا کردن آماج، حمله را برای بزهکاران بی جاذبه جلوه می دهد و آن ها را از انجام آن باز می دارد؛ برای نمونه هکرها می توانند به آسانی از طریق امواج الکترومغناطیسی منتشرشده در محیط، خود را به عنوان عضوی از شبکه تلقی کنند و از این طریق به شنود اطلاعات در حال انتشار اقدام نمایند. بنابراین تا جایی که ممکن است، باید از ارتباطات سیمی برای برقراری ارتباط بین سامانه‌های رایانه‌ای و مخابراتی استفاده نمود.

۲-۱-۳. کاهش عوامل محرک

گاهی عوامل مساعد بزهکاری به قدری تحریک کننده‌اند که افراد زیادی را به ارتکاب بزه وسوسه می‌کنند. همان طور که اشاره شد، این حالت در فضای سایبر به وضوح دیدنی است. پس، طبق این راهبرد باید در اوضاع و احوال ناظر به جرم، به گونه‌ای دخالت نمود که عوامل محرک را حداقل بزهکاران اتفاقی به کمترین حد ممکن رساند. پنج راهکار پیش بینی شده در این راهبرد که بیشتر بر کنش‌های روان شناختی بزه‌دیدگان احتمالی تکیه دارد به ترتیب عبارت‌اند از: کاهش استرس، اجتناب از اغتشاش، کاهش برانگیختگی خنثی کردن فشار گروه همسالان و ممانعت از تقلید ارتکاب جرم. (بهره‌مند و همکاران، ۱۳۹۳، ۱۶۷)

۳-۱-۳. نظارت

نظارت بر محیط سایبر پس از اتفاقات ۱۱ سپتامبر با جدیت بیشتری اعمال شد. بسیاری از حکومت ها و مردم جهان پس از این واقعه به این نتیجه رسیدند که میزان خاصی از نظارت و کنترل بر ارتباطات اینترنتی با هدف حمایت از مردم در برابر تروریسم، کلاهبرداری و دیگر جرایم اینترنتی، امری بسیار مهم است. (داتن،۱۳۸۴، ۱۵) چرا که اینترنت و ابزارهای سایبری، ماهیت و ریسک حملات احتمالی را تغییر داده و نیاز به امنیت در آن موجب شده است تا راه کارهای امنیتی جدید و استانداردهایی به وجود آیند. (گروه کار اقتصادی اروپا،۱۳۸۴، ۱۴۴)

برهمین اساس، «نظارت در محیط سایبر همچون نظارت در محیط مادی از جمله راهکارهایی است که علاوه بر کشف سریع جرم، از ارتکاب آن نیز جلوگیری می‌کند. تدابیر مراقبتی را می توان از دو طریق اعمال کرد: شیوه‌ی نخست، کاربستِ تدابیر فیزیکی در دنیای فیزیکی آن گونه که در سایر جرایم اعمال می شود می باشد؛ برای مثال، نصب دوربین‌های مداربسته در کافی نت‌ها و سازمندی صفحه‌ی نمایش رایانه‌ها به صورتی که در معرض دید عموم باشد. اما روش دیگر، نظارت الکترونیکی است که با ویژگی‌های این محیط، سازگاری بیشتری دارد. در این شیوه با به کارگیری تجهیزات و برنامه‌های خاص، فعالیت‌های شبکه ایِ افراد تحت نظر قرار می‌گیرد. بنابراین، استفاده از ابزارهایی که تحت محافظت بودن شبکه و تحت نظارت بودن کاربر را اعلام کنند، می‌تواند ابزارهای نظارتی را تکمیل نماید.» (بهره‌مند، همان، ۱۶۴)

بنابراین، تدابیر متنوعی برای حفظ سیستم‌های رایانه‌ای در برابر حملات وجود دارد و از جمله آنها، تدابیر نظارتی است که در فضای فیزیکی مشاهده می‌شوند که نمونه‌هایی از آن در قالب دوربین‌های مدار بسته جهت کنترل اماکن استفاده می‌شوند. اما آنچه در فضای سایبر به کار می‌رود، مجموعه‌ای از برنامه‌های رایانه‌ای است که بر حسب نوع برنامه ریزی که برایشان صورت گرفته، کلیه داده‌هایی را که با مبادلات الکترونیکی کاربرانِ در مظان ارتکاب جرم، مرتبط هستند را جمع‌آوری می‌کند تا مسئولان ذیربط به صورت زنده آنها را بررسی کنند. این اقدام تا حدی مورد توجه مجریان قانون کشورها قرار گرفته که برخی از آنها پلیس گشت سایبر نامیده شده‌اند، زیرا به گونه‌ای اوضاع سایبری را تحت کنترل دارند که هر گونه وقوع جرم یا دیگر ناهنجاری‌ها را به اطلاع مراجع ذیربط می‌رسانند.(وروایی، همان، ۷۰)

۴-۱-۳. کنترل دستیابی به اهداف

راه‌های گوناگونی برای کنترل ورودی‌ها وجود دارد که ساده‌ترین آنها، استفاده از رمز عبور در رایانه است. بدیهی است که بالا بردن ضریب کنترل می‌تواند به مثابه‌ی مانعی در برابر مجرمان باانگیزه عمل کند و آنها را در دستیابی به آماج جرم ناکام بگذارد. از دیگر راهکارهایی که می تواند به عنوان کنترل ورودی عمل کند، استفاده از شبکه‌های مجازیِ کاوشگرهای الکترونیک است. این کاوشگرها که از آنها به پلیس مجازی تعبیر می‌شود. وظیفه‌ی تشخیص هویت‌های مجازی، اعتبارسنجی امضاهای الکترونیک، کنترل دسترسی‌های مجاز به محتوای محرمانه‌ی داده‌ها و حتی تشخیص مصادیق محرمان‌ی منتشرشده را به عهده دارند. (خالقی پوستچی، ۱۳۸۸، ۴۶) تجهیز شرکت‌ها و سازمان ها به این سیستم‌های نظارتی و کنترلی، شیوه‌ی مناسبی برای پیشگیری از جرم است.

۵-۱-۳. نقش ICT در پیشگیری وضعی

امروزه، عموم روش‌های پیشگیری وضعی مبتنی بر فناوری است . بنابراین، ضروری است همگام با پیشرفت‌های فنی، این روش‌ها نیز به روز شوند این پیشگیری در زمان حاضر تحت تاثیر ابزارهای مختلفی قرار گرفته است. متخصصان این پیشگیری دریافتند که به منظور ارائه‌ی یک راهکار موثر و یک شیوه‌ی تکامل یافته از این نوع پیشگیری، نیازمند بازبینی در آن هستند.

امروزه در کنار کنش‌گران انسانی فناوری نوین هم در قالب سیستم‌های هشداردهنده‌ی خطر، سیستم‌های نظارت و مراقبت تلویزیونی، دوربین‌های نظارتی و سیستم‌های کنترل ورودی‌ها با کارت‌های مغناطیسی به کمک این نوع پیشگیری آمده و به آن جنبه‌ی فنی بخشیده است از این فناوری می‌توان برای شناسایی گروه‌های خطردار، دسته‌بندی خطر، وضعیت‌ها و محیط‌های خطرزا به منظور کاهش فراوانی خطر ارتکاب جرم و افزایش فراوانی خطر شناسایی، خنثی‌سازی، دستگیری و دور کردن مجرمان بالقوه و بالفعل از جامعه استفاده کرد. در واقع، پیشگیری وضعی به کمکICT از طریق شناسایی، مصون سازی و کنترل موقعیت‌های دارای خطر جرم به مدیریت خطر جرم می‌پردازد.(خانعلیپور و همکار، ۱۳۸۹، ۲۲۳-۲۲۲)

از همین‌جهت،در دهه گذشته استفاده از دوربین‌های مدار بسته به عنوان ابزار مراقبت و پیشگیری از جرم گسترش فراوانی در جهان بـه ویژه در اروپا و آمریکا داشته است . مراکز خرید ، پارکینگ‌ها و اماکن عمومی و خدماتی فراوانی به این تکنولوژی مجهز شده‌اند . به عنوان مثال در بریتانیا این دوربین‌ها پر هزینه‌ترین استراتژی پیشگیری از جرم غیر قضایی هستند . در سال ۲۰۰۴ در حـدود ۴۰۰۰۰ دوربین در انگلـیس و ولز نصب شده است و در طی سه سال از ۱۹۹۹تا ۲۰۰۱ دولت بریتانیا در حدود ۲۵۰ میلیون دلار برای طرح‌های دوربین‌های مدار بسته عمومی هزینه کرده است.(welesh, 2006,497)

البته تنها دوربین‌های مداربسته نیستند که به منظور کنترل مکان‌های جرم‌خیز به کار می‌روند بلکه، دستگاه‌های ردیاب GPS نیز از ابزارهایی است که ICT به منظور مدیریت مناسب ریسک جرم در اختیار متخصصان امر قرار می‌دهد. مجهز کردن اتومبیل‌های شخصی و عمومی به این سیستم باعث پایین آمدن میزان جرم می‌شود. همچنین در صورتی که اتومبیلی مورد سرقت قرار گیرد با کمک این سیستم سارق سریعتر دستگیر خواهد شد. همچنین با برچسب‌گذاری الکترونیک روی کالاها می‌توان از خطر سرقت آنها کاست. در کنار موارد یاد شده، پیشرفت‌های فنی مخابراتی را نیز می‌توان از جمله ابزارهای موثر در مدیریت ریسک جرم شناخت. خلاصه آنکه فناوری اطلاعات و ارتباطات کنترل مناطق جرم‌خیز و مدیریت ریسک جرم را با استفاده از دو روش زیر که به پیشگیری وضعی می‌انجامد به اجرا در می‌آورند:

۱. با تقویت نظارت و رویت‌پذیری با نصب دوربین‌های مدار بسته و...؛

۲. بالابردن هزینه ارتکاب جرم با افزایش احتمال شناسایی و دستگیری مرتکب از طریق به کارگیری دوربین‌های مداربسته، حسگرهای ورودی، دستگاه‌های هشداردهنده، زنگ‌های خطر و...(مغازه ئی و همکاران ۱۳۹۳، ۷۳-۷۰)

بدین ترتیب می‌توان گفت: فناوری اطلاعات و ارتباطات بر کارکرد پیشگیری وضعی به عنوان مهم‌ترین نوع پیشگیری در مدیریت ریسک جرم تاثیرگذار بوده است. در حال حاضر این پیشگیری با به کارگیری ابزارهای فناوری اطلاعات و ارتباطات، خود را به روز می‌کند تا بتواند به عنوان قدیمی‌ترین نوع پیشگیری همچنان به حیات خود ادامه دهد. این نوع پیشگیری با وجود محدودیت‌ها و ضعف‌هایی که دارد، به طور گسترده‌ای مورد توجه قرار گرفته است، به گونه‌ای که شورای اقتصادی و اجتماعی سازمان ملل متحد نیز در برنامه‌ی توسعه‌ی پیشگیری موثر از جرم ،دولت‌ها و جامعه‌ی مدنی را ترغیب کرده است تا از برنامه‌های توسعه‌ی این نوع پیشگیری حمایت کنند.

۲-۳. پیشگیری اجتماعی

پیشگیری اجتماعی با مداخله در محیط اجتماعی عمومی و شخصی افراد از قبیل محیط‌های فرهنگی، اقتصادی، سیاسی، و خانواده تلاش دارد تا ساز و کارهای خودکنترلی و مهارت‌های اجتماعی را افزایش دهد. این نوع از پیشگیری اجتماعی بر اساس مداخلات و تاثیراتی که بر فرایند شکل‌گیری شخصیت فرد یا محیط‌های پیرامون او صورت می‌گیرد به "پیش گیری جامعه مدار" و "پیشگیری رشد مدار" تقسیم می‌شود. پیشگیری جامعه‌مدار با هدف حذف عوامل جرم‌زا در محیط، در جستجوی کاهش انگیزه‌ی با اتخاذ تدابیر پیشگیرانه در طول رشد افراد و همین‌طور با مداخله زودرس در مورد اطفالی که مظاهر بزهکاری را بروز می‌دهند، فرآیند جامعه‌پذیری افراد را اصلاح می‌نمایند. در واقع هدف از این نوع پیشگیری اصلاح شخصیت کودکان و نوجوانان مساله‌دار است و از تبدیل آنها به بزهکار مزمن جلوگیری می‌نماید. برنامه‌های پیشگیری زودرس شامل برنامه‌های خانواده‌مدار، برنامه‌های مدرسه‌مدار، و برنامه‌های اجتماع‌مدار می‌باشد. (ساریخانی و همکار،

۱۳۹۵، ۱۴۴) بنابرآنچه گفته شد، در این مبحث به شرح پیشگیری رشدمدار و جامعه‌مدار به عنوان شاخه‌های اصلی پیشگیری اجتماعی پرداخته خواهد شد.

۱-۲-۳. پیشگیری اجتماعی رشدمدار

«پیشگیری رشد مدار، به‌دنبال بهبود وضعیت افرادی است که در معرض خطر به بزهکاری قرار دارند. این گونه از پیشگیری، بزهکاری را نه یک واقعه، بلکه یک فرآیند می‌داند که زمینه‌های آن در دوران رشد فرد یعنی از لحظه تشکیل نطفه تا بزرگسالی (جوانی) بروز پیدا می‌کند. این رویکرد بر این فرض مبتنی است که داشتن شخصیت متعادل، همنوا شدن با ارزش‌ها و هنجارها پذیرفته شده در جامعه و رشد و جامعه‌پذیری صحیح منوط به گذران طبیعی دوران رشد است و هر گونه انحراف و اختلال در نهادهای که در رشد، جامعه‌پذیری و کنترل کودک یا نوجوان مؤثر هستند وی را در معرض خطراتی قرار می‌دهد که ممکن او را به سمت دنیای بزهکاری بکشاند. بنابراین، پیشگیری رشد مدار با شناسایی عوامل خطر در محیط‌های جامعه پذیریِ نخستین اطفال و نوجوانان که عبارتند از : خانواده، مدرسه، گروه همسالان و رسانه‌ها سعی در احیای اوضاعی که از لحظه شکل‌گیری جنین تا شکل گیری کامل شخصیت طفل مفقود بوده و عاملی برای بزهکاری محسوب می‌شوند، توسط عوامل حمایتی دارد. در واقع پیشگیری رشد مدار بر این فرض مبتنی است که وجود اختلال در نهادهای جامعه پذیری که اطفال و نوجوانان در آن قرار می‌گیرند به شدت کودک را در معرض بزهکاری در آینده قرار می‌دهد. به همین جهت این گونه از پیشگیری تمرکز خود را بر این نکته قرار داده که با شناسایی عوامل خطر و بکارگیری ساز و کارهای حمایتی مناسب در محیط‌های جامعه پذیرسازی انسان، کودکان و نوجوانان در معرض خطر را به سوی همنوایی با قواعد اجتماعی سوق دهد و از احتمال وارد شدن فرد در رفتارهای مجرمانه جلوگیری کرده و در نهایت جامعه ی سالم و امن برای افراد جامعه فراهم سازد.» (پاشائی وحید، ۱۳۹۱، ۳-۲)

بدین ترتیب، پیشگیری رشدمدار، به معنی پیشگیری از رشد و شکل گیری عوامل بالقوه در این زمینه می‌باشد.

این پیشگیری‌ها در قالب رویکردهای پیشگیرانه ذیل، به اجراء گذاشته می‌شوند:

۱- پیشگیری اجتماعی به معنای مداخله، به منظور تغییر شرایط اجتماعی است.

۲- پیشگیری وضعی که منجر به کاهش فرصت‌های ارتکاب جرم می‌گردد.

۳- پیشگیری عدالت کیفری که با استفاده از اصلاحات و راهکارهای باز پرورانه تحقق می‌یابد. (محسنی، ۱۳۹۳، ۱۶۲)

بنابراین، یکی از مهم‌ترین ارکان جرم شناسی رشدمدار، شناخت عوامل خطرساز در جریان فرآیند رشد است. پیشگیری از وقوع جرم به‌ویژه پیشگیری رشدمدار در گستره سیاست جنایی ایران مورد توجه سیاستگذاران کیفری قرار گرفته است. به نحوی که اصول قانون اساسی از جمله اصل هشتم و بند ۵ اصل ۱۵۶ ، قوانین و مقررات عادی، بخشنامه‌ها و دستورالعمل‌های متعددی به اهمیت این امر پرداخته و سازوکار و تدابیر مختلفی را در راستای همنواسازی و اجتماع‌پذیری افراد ارائه نموده‌اند. همچنین در سطح اجرایی نهادها و سازمان‌هایی نظیر پلیس، سازمان بهزیستی کشور، کمیته امداد امام خمینی(ره) و غیره در خصوص آموزش مهارت‌های ارتباطی، زندگی و اجتماعی، ساماندهی اطفال و نوجوانان بی‌سرپرست یا بدسرپرست، ایجاد مراکز مشاوره و مددکاری و ارائه مشاوره‌های روانشناختی و انتظامی و غیره فعالیت دارند. (قهرمانی افشار و همکاران، ۱۳۹۵، ۸۷)

بنابراین در ارتباط جرایم سایبری نیز می‌توان با تکیه بر کارکرد آموزش خانواده‌محور و مدرسه محور و نیز افزایش مهارت‌های ارتباطی و اجتماعی و همچنین، توجه به رسانه‌ها در جهت آگاه‌سازی آحاد جامعه نسبت به اثرات مخرب جرایم سایبری و نیز بازشناسی گونه‌های جرایم سایبری، گامی موثر در جهت پیشگیری از بزه‌دیدگی افراد جامعه برداشت.

۲-۲-۳. پیشگیری اجتماعی جامعه‌مدار

پیشگیری‌جامعه‌مدار یا پیشگیری محیطی، کهن‌ترین گونه پیشگیری‌فردمدار است که با تکیه بر ظرفیت محیط‌ها، به ویژه محیط‌های پیرامون افراد به دنبال پیشگیری از جرم است. این نوع پیشگیری با به کارگیری اقدام‌های غیرقهرآمیز اجتماعی، فرهنگی، اقتصادی در محیط‌های مختلف در صدد ازبین بردن عوامل محیطی جرم‌زا یا دست کم کاهش تاثیر آنها برافراد است. بسیاری از تحقیقات صورت گرفته در حوزه جرم و فرصت‌های محیطی در اصل بخشی از دستورالعمل پیگیری محیطی از جرم محسوب می شود. به عبارت دیگر می‌توان ادعاکرد تمام نظریات

ارائه شده در خصوص فرصت‌های محیطی ارتکاب جرم، اساس نظریه پیشگیری جرم از طریق طراحی محیطی را تشکیل می‌دهند. همین موضوع باعث شده است تا این نظریه جایگاهی ارزشمند و قابل توجه در میان جرم شناسان پیدا کند. (کلارک،۱۳۸۷، ۳۴۶)

به این ترتیب، پیشگیری جامعه مدار با توجه به این انگاره که گونه‌های مختلف محیط بر نظام رفتاری افراد تأثیرگذار هستند بر استفاده از اقدام‌های غیرقهرآمیز محیط مدار به منظور زدودن یا کاهش تأثیر عوامل جرم زا تمرکز می‌کند. ازاینرو، اقدام‌های ناظر بر آموزش و پرورش، اشتغال زایی، فقرزدایی، تهیه مسکن برای شهروندان، ایجاد رفاه اجتماعی و اقتصادی که نقش موثری در فرآیند شکل‌گیری شخصیت افراد ایفا می‌نمایند، در چارچوب این نوع پیشگیری جای می گیرند. (ابراهیمی، ۱۳۹۰، ۶۱)

« پیشگیری جامعه مدار در کنار دو محیط خانواده و مدرسه به ظرفیت‌های اوقات فراغت نیز برای کاهش گرایش افراد به سمت بزهکاری توجه نشان می‌دهد.ایجاد امکانات مناسب برای اوقات فراغت شهروندان بخصوص کودکان، نوجوانان و جوانان می‌تواند سهم بسزایی در تربیت و پرورانیدن درست شخصیت آنان ایفا کند. به همین جهت، مطابق بند ۳ اصل سوم قانون اساسی «...تربیت بدنی رایگان» برای همه شهروندان به عنوان یکی از اصلی ترین تکالیف دولت‌ها پیش بینی شده است تا اوقات فراغت افراد در راستای رشد نظام‌مند رفتار آنان ساماندهی شود. در عرصه پیشگیری جامعه‌مدار، بهبود وضعیت مالی - اقتصادی نیز در کاهش تمایل شهروندان به ارتکاب جرم تاثیرگذار است. شماری از افراد، تحت تاثیر ناتوانی مالی - اقتصادیِ ناشی از بیکاری، فقر، نداشتن مسکن به بزهکاری و انحرافات اجتماعی رو می‌آورند» (نیازپور، ۱۳۹۳، ۹۷)

۳-۲-۳. آموزش همگانی و فرهنگ‌سازی

امروزه، نقش و اهمیت آموزش همگانی برای ایجاد امنیت فردی و عمومی در سطح جامعه به خوبی درک شده است. یکی از دلایل اولیه‌ی رشد انحرافات سایبری آن است که عموم مردم از ممنوعیت این دسته اعمال آگاهی ندارند. از این رو، شاید مهم ترین ابزار مبارزه با جرایم سایبری، آموزش همگانی باشد. همان طور که اشاره شد، با توجه به عدم درک پیامدهای گرانبار تهدیدات سایبری و تقبیح نکردن ارتکاب این قبیل جرایم از سوی جامعه، ضرورتِ نقش آموزش در پیشگیری از جرایم سایبری، بیش از سایر جرایم احساس می‌شود. ساده‌ترین نوع آموزش در ارتباط با این جرایم، همان تدابیری است که برای سایر انحرافات اجتماعی به کار می‌روند.

بدین‌ترتیب، یکی از راه کارهای کاهش جرایم فضای مجازی، پرداختن به آموزش های پیشگیری از وقوع جرم در فضای مجازی برای کارکنان است. به طور حتم، از این طریق می توان کارایی کارکنان را افزایش داد. وضعیت فضای مجازی و نوع استفاده مجرمان از این فضا در گسترش جرایم، در کنار ضعف آموزش‌های کارکنان، غافلگیری در پیشگیری و مقابله با آنها را به دنبال خواهد داشت. آشکار شدن اهمیت فضای مجازی برای فرماندهان و روسا، باعث به کارگیری و تهیه تجهیزات مدرن و پیشرفته در این حوزه و برنامه ریزی ارائه آموزش‌های نوین به کارکنان خواهد شد. برای بالابردن کارایی کارکنان در محیط مجازی و به منظور پیشگیری از وقوع جرم می بایست جایگاه آموزش در این حوزه را مشخص کرد. (کوچی و همکار، ۱۳۹۴، ۷۱)

در عرصه‌ی بین‌الملل نیز برای پاسخگویی به نیازهای روزافزون در زمینه پیشگیری از جرم، دوره‌های آموزش تخصصی همراه با مدرک رسمی افزایش یافته است. اکثرا موسسات و مراکز دانشگاهی برگزار کننده این دوره‌ها هستند، ولی در برخی از موارد مراکز آموزشی پلیس نیز اقدام به برگزاری دوره‌های آموزشی پیشگیری کرده است. (International Centre for the Prevention of Crime,2010)

البته باید خاطر نشان کرد که آموزش به آحاد مردم نیز می‌تواند نقش چشمگیری در پیشگیری از جرم و بزه‌دیدگی این افراد داشته باشد.

۴-۲-۳. کدهای رفتاری و منشور اخلاقی

«یکی از ابزارهای نوین و اثبات شده در امر پیشگیری اجتماعی، کدهای رفتاری یا کردارنامه‌ها هستند که با توجه به رویکرد و ماهیت تخصصی‌شان می‌توانند در پیشگیری از بزهکاری نقش مطلوب خویش را ایفا کنند. همگام با آموزه‌های پیشگیری اجتماعی از جرم، شالوده و زیربنای کدهای رفتاری بر محور آگاهی بخشی، هشداردهی و آموزش استوار است. در این راستا، رسالت اصلی کدهای رفتاری به عنوان یک سازوکار پیشگیرانه این است که می‌توانند با تقویت رفتار اخلاقی و ایجاد تحول درونی نقش پلیس باطن را برای بزهکاران بالقوه ایفا کنند. پلیس باطن موانع اخلاق درونی در فرد ایجاد می کند که با روش‌های مستقیم یا غیرمستقیم بر روی شخصیت فرد اثر گذاشته و موجب ترویج رفتارهای مسئولانه در محیط‌های اجتماعی و شغلی می‌شود. این کدها میتوانند به صورت بیانیه‌های حرفه ای وارد عمل شوند و چون از نوع مسائل ارزشی هستند، بهترین ضمانت اجرای آن ایجاد تحول درونی در افرادست که آنها را تشویق و ترغیب در پاسداری از بایدها و نبایدها می‌نماید.»(منفرد و همکار، ۱۳۹۱، ۱۱۳)

همچنین، روشن است که بزه‌دیده هم می‌تواند با فراهم نمودن فرصت یا ابزار ارتکاب جرم از روی ناآگاهی یا سهل انگاری موجبات بزهدیدگیاش را ایجاد کند و هم با ناآگاهی از شگردهای مجرمانه خود را در مسیر رویارویی با آنها قرار دهد و با واکنش نامناسب، بزهکار را به غایت مجرمانه خویش برساند. بی‌تردید، ناآشنایی، سهل انگاری و ناآگاهی بزهدیدگان بالقوه از موقعیتهای جرمساز بر آسیب‌پذیری بیشتر آنها می افزاید. در اینجا رسالت اصلی کدهای رفتاری شناساندن این آسیب‌پذیری‌ها و آموزش نحوه‌ی رویارویی و واکنش درست دربرابر آنهاست. امروزه پیشبینی و تدوین کدهای رفتاری برای حفاظت از گروه‌های آسیب‌پذیرتر، مانند کودکان و زنان، یکی از راهکارهایی است که رواج بسیاری یافته است. برای مثال،برای افزایش آگاهی کودکان از خطرهای فضای سایبر و لزوم کنترل خطرپذیری آنها در گشت وگذارهای سایبری به والدین توصیه می شود که نحوه کاربری فرزندان خود از ابزارهای رسانه‌ای، ارتباطی و رایانه‌ای را در قالب یک کد رفتاری تنظیم و راجع به قواعد و انتظارات استفاده از اینترنت در منزل به بحث و تبادل نظر بنشینند. (همان، ۱۲۶)

۳-۳. پیشگیری کیفری

در پیشگیری کیفری به نقش مجازات در پیشگیری از ارتکاب جرم پرداخته می شود. به نحوی که اگر مجازات مناسب و بازدارنده باشد، مانع وقوع جرم توسط اشخاص خواهد شد. به این دلیل که کسانی که قصد ارتکاب بزه دارند؛ قاعدتا بی‌توجه به مجازاتی که مقنن برای آن پیش بینی کرده نیستند و چنانچه هزینه آن را از سود و فایده بیشتر بدانند، قصد خود را عملی نمی کنند. این نوع از پیشگیری به اندیشه ژرمی بنتام که از پایه گذاران مکتب اصالت سودمندی است، نزدیک است. (خلفی، ۱۳۹۵، ۲۵)

بی‌شک باتوجه به گستردگی دامنه‌ی جرایم سایبری برای پیشگیری مناسب از این نوع جرایم باید به انواع پیشگیری تمسک جست. در این میان پیشگیری کیفری نیز می‌تواند به عنوان ضمانت اجرای مناسب و بازدارنده در جهت خنثی سازی آثار مخرب جرایم سایبری نقش بسزایی داشته باشد. بنابراین لازم و ضروری است که حقوق کیفری در این زمینه همگام با پیشرفت‌های جرایم سایبری تغییر پیدا کند. در غیر اینصورت بی‌شک بزهکاران زیادی باقی خواهند ماند.

از همین‌رو، برخی از محققان معتقدند: «مهم‌ترین ابزارهایی برای مبارزه با جرایم نوین در برابر حقوق جزا وجود دارد؛ راهکارهایی مانند جرم‌انگاری، ایجاد و توسعه مسئولیت کیفری، استفاده از راهکارهای نوین حل اختلاف و مجازات‌های نوین و... است. در رابطه با مسئولیت کیفری در جرایم سایبری قانونگذار ایران اقدام به توسیع و گسترش مسئولیت کیفری اشخاص حقوقی نموده است. در قانون جرایم رایانه‌ای نخستین بار این موضوع را مورد پذیرش قرار داده است؛ می‌دانیم بسیاری از جرایم سایبری اغلب توسط اشخاص حقوقی واقع می‌شوند و این اقدام قانونگذار در رابطه با ایجاد مسئولیت کیفری برای این اشخاص کاملا امری طبیعی بوده و در واقع استفاده از ابزار گسترش مسئولیت کیفری برای مبارزه با جرایم جدید است. البته باید اذعان داشت که:

الف) مسئولیت کیفری اشخاص حقوقی به معنای نفی مسئولیت اشخاص حقیقی نیست؛

ب) مسئولیت کیفری شخص حقوقی مانعی بر سر راه اعمال مجازات بر اشخاص حقیقی ایجاد نمی‌کند.» (رضوی فرد و همکار، ۱۳۹۵، ۴۳)

در کشور ایران نیز به طور خاص در خصوص جرایم رایانه‌ای، قانونی در سال ۱۳۸۸ با ۵۴ ماده تصویب شد. قانون مذکور اگرچه از حیث تدوین قوانین خاص در این زمینه در نهایت می‌تواند از حیث پیشگیری کیفری، موثر واقع شود، لیکن موارد قابل تاملی در آن ملاحظه می‌شود که ممکن است متناسب با جرایم رایانه‌ای نباشد. مثلا ماده ۱۳ آن در مورد کلاهبرداری رایانه‌ای، مدت حبس یک تا پنج سال را به عنوان یکی از مجازات‌ها مقرر داشته است. در حالی که در کلاهبرداری سنتی که از حیث خطرات و آثار زیانبار، نمی‌تواند هم‌سطح با کلاهبرداری رایانه‌ای باشد، مجازات حبس در کلاهبرداری غیرمشدد یک تا هفت سال می‌باشد. همچنین یکی دیگر از معضلاتی که در پیشگیری کیفری جرایم سایبری ایران با آن روبرو است، این است که همواره قانونگذار از پیشرفت این جرایم عقب‌تر بوده و نمی‌تواند آنگونه که شایسته است در این زمینه ایفای نقش کند، به گونه‌ای که طبق گزارشات رسمی پیش گفته شده، طی شش سال این جرایم ۹۰۰٪ افزایش پیدا کرده است.

۴. راهبردهای پیشگیری از جرایم سایبری با تاکید بر رهنمودهای سازمان ملل متحد

ریشه لغوی راهبرد یا استراتژی به کلمه استراتژو یونانی برمیگردد که در زمان حکومت کلیسا آتن در سال ۵۰۸ قبل از میلاد متداول شد. (لطیفیان،۱۳۸۳، ۱) راهبرد، فرآیند کلی تصمیم‌گیری درباره مقصد و چگونگی دستیابی به آن است. راهبرد یا استراتژی تعیین کننده زمینه‌های فعالیت در محیطی پیچیده و پویا بوده و ابزاری است که به عنصر انسانی در یک نظام سازمانی حیات بخشیده، افراد را به حرکت وامی‌دارد.

در تعریفی دیگر، راهبرد یا استراتژی الگویی بنیادی از اهداف فعلی و برنامه ریزی شاده، بهره برداری و تخصیص منابع وتعاملات یک سازمان با بازارها، رقبا و دیگر عوامل محیطی است.(پورصادق و همکار،۱۳۹۵، ۵)

بدین‌ترتیب، در این مبحث به ارائه‌ی اساسی‌ترین راهبردهای برون رفت از چالش‌های پیشگیری از جرایم سایبری که در مبحث پیشین برشمردیم پرداخته خواهد شد.

۱-۴. حمایت از بزه‌دیدگان جرایم سایبری

«بزه‌دیده‌شناسی علمی در حقیقت مکمل مباحث جرم شناسی علت شناختی است. بر این پایه؛بزه‌دیده می‌تواند به عنوان یکی از عوامل پیش جنایی، نقش مهمی را در فرایند جنایی ایفا کند چراکه او علاوه بر تسریع فرایند گذار از اندیشه به عمل مجرمانه از طریق تحریک و ترغیب بزهکار بالقوه، ممکن است به خاطر خصوصیات و ویژگی‌های خاص فردی و یا موقعیتی فرصت و زمینه ارتکاب عمل مجرمانه را برای بزهکار بالقوه فراهم کند. به عبارت دیگر، اگر بزهکاری معلول عوامل مختلف فردی و اجتماعی است، بزه‌دیدگی نیز معلول عوامل مختلف مانند جسمی، جنسی، روانی و موقعیتی است و بزه‌دیدگان آسیب‌پذیر به دلایل مذکور نوعی پیش زمینه و استعداد قبلی برای بزه‌دیده شدن دارند. به همین دلیل بزهکاران بالقوه قربانیان خود را اغلب از میان افرادی انتخاب می‌کنند که ارتکاب جرم بر روی آنان دارای خطر و هزینه بالایی نباشد. بنابراین، اشخاص آسیب پذیر به دلیل وضعیت و موقعیت خاص و ویژه شان موجبات تحریک و ترغیب بزهکاران بالقوه به ارتکاب رفتارهای مجرمانه علیه خودشان را تسهیل و فراهم می‌کنند.» (حاجی‌تبار، ۱۳۹۰، ۲۱)

در سال ۱۹۷۶ ، شورای اروپا بر ماهیت بین المللی جرایم رایانه‌ای و حمایت از بزه‌دیدگان آن تاکید داشت و در کنفرانسی بر روی جنبه‌های جرایم اقتصادی این موضوع بحث کرد. در سال ۱۹۸۵ شورای اروپا کمیته کارشناسی را برای بحث در مورد جنبه‌های قانونی جرایم رایانه‌ای تعیین کرد. در سال ۱۹۸۹ ، کمیته اروپایی در بررسی مشکلات جرایم با گزارش کارشناسان در جرایم رایانه‌ای با تجزیه و تحلیل عناصر قانونی کیفری لازم برای مقابله با اشکال جرایم الکترونیک، ا زجمله کلاهبرداری رایانه‌ای و جعل رایانه‌ای موافقت کرد. کمیته وزیران در سال ۱۹۸۹ با پیشنهادی موافقت کرد که به طور ویژه بر ماهیت جرایم رایانه‌ای تاکید داشت: « کمیته وزیران بر اساس مفاد تبصره۱۵ اساسنامه شورای اروپا، با درنظر گرفتن این که جرایم رایانه‌ای غالبا خصوصیت فرامرزی دارند، با آگاه بودن از نتایج مورد نیاز برای یکسان‌سازی بیشتر قانون و اجرا، و برای بهبود همکاری قانونی بین‌المللی، به کشورهای عضو توصیه‌هایی نمود.» در سال ۱۹۹۵ ، شورای اروپا در توصیه اصولی بیان می‌دارد که کشورها و مقامات تحقیق در حوزه فناوری اطلاعاتی باید سرلوحه کار خود قرار دهند. این اصول مواردی مثل تحقیق، تفتیش و تصرف، نظارت فنی، تعهد به همکاری با مقامات تحقیق کننده، ادله الکترونیکی، استفاده از رمزنگاری، آمارها و آموزش و همکاری بی ن المللی و حمایت از بزه‌دیدگان را در بر می‌گیرند. این سند موضوعات مزبور را از منظر تحقیق در مورد جرایم سنتی و جرایم سایبری بحث می‌کند. (اسلامی، ۱۳۹۵، ۱۶۷)

در نظام حقوقی ایران، گونه‌های سیاست جنایی دولت در حمایت از بزه‌دیدگان اصولا در سه حالت حمایت از بزه‌دیده، بلافاصله پس از تحقق جرم ، در مرحله دادرسی و صدور حکم و مآلاً در مرحله اجرای احکام و تامین ضرر و زیان وی می‌باشد.برخی از حقوق بزه‌دیدگان در فرآیند رسیدگی به دعاوی کیفری، در قانون آیین‌دادرسی کیفری مصوب ۱۳۹۲ اجرایی ۱۳۹۴ مورد تصریح قرار گرفته و برخی نیز متاسفانه مغفول مانده است، این حقوق عبارت است از:

۱. حق شناسایی و تکریم بزه‌دیده: بدین معنا که بزه‌دیده باید بتواند صدای خود را به گوش دیگران برساند. در همین راستا مشارکت بزه‌دیده به ویژه در آغازگری دعاوی کیفری نباید به صورت تشریفاتی و تصنعی باشد بلکه ترافعی بودن در دادرسی باید این فرصت را برای بزه‌دیده ایجاد کند تا بزه‌دیده مکنونات قلبی خود و نیز آلامِ پس از بزه‌دیدگی را بیان نماید. (لعل علیزاده، ۱۳۹۶، ۱۰۱)

۲.حق دسترسی فوری و آسان به نظام عدالت کیفری؛ فراهم ساختن سهولت دسترسی برای بزه‌دیدگان یکی دیگر از حقوق آنان شناخته می‌شود. برهمین اساس، قانونگذاری ایران در ماده ۱۷۵ قانون آیین‌دادرسی کیفری آورده است: « استفاده از سامانه‌های (سیستم‌های) رایانه‌ای و مخابراتی، از قبیل پیام‌نگار (ایمیل)، ارتباط تصویری از راه دور، نمابر و تلفن، برای طرح شکایت یا دعوی، ارجاع پرونده، احضار متهم، ابلاغ اوراق قضایی و همچنین نیابت قضایی با رعایت مقررات راجع به دادرسی الکترونیکی بلامانع است.» بنابراین با تمسک به این ماده تا حد زیادی، چالش مربوط به وسعت جغرافیایی و نیز عدم دسترسی به امکانات قضایی مرتفع می‌گردد.

۳. حق آگاهی یافتن از حقوق: در این راستا در ماده ۶ این قانون آمده است: « متهم، بزه‌دیده، شاهد و سایر افراد ذی‌ربط باید از حقوق خود در فرآیند دادرسی آگاه شوند و سازوکارهای رعایت و تضمین این حقوق فراهم شود.»

۴. حق مکتوم ماندن هویت و نشانی بزه‌دیده؛ در این راستا ماده ۴۰ قانون مزبور مقرر داشته است: « افشای اطلاعات مربوط به هویت و محل اقامت بزه‌دیده، شهود و مطلعان و سایر اشخاص مرتبط با پرونده توسط ضابطان دادگستری، جز در مواردی که قانون معین می‌کند، ممنوع است.»

۵. حق حفاظت از بزه‌دیده و خانواده‌ی وی؛ این حق یکی از اساسی‌ترین حقوق بزه‌دیدگان می‌باشد. نقض این حق ضمن ایجاد خسارت‌های جبران ناپذیر بستر بزه‌دیدگی ثانویه را نیز فراهم می‌سازد. در همین راستا، ماده ۹۷ قانون آیین دادرسی کیفری آورده است: « بازپرس به‌منظور حمایت از بزه دیده، شاهد، مطلع، اعلام کننده جرم یا خانواده آنان و همچنین خانواده متهم در برابر تهدیدات، در صورت ضرورت، انجام برخی از اقدامات احتیاطی را به ضابطان دادگستری دستور می‌دهد. ضابطان دادگستری مکلف به انجام دستورها و ارائه گزارش به بازپرس هستند.»

۶. حق اطلاع از محتویات پرونده؛ آگاه کردن بزه‌دیده از محتویات و تحولات پرونده، بدون لزوم مراجعه‌ی حضوری وی موجب افزایش اعتماد و تمایل وی به مشارکت در فرآیند رسیدگی می‌شود. (آشوری و همکار، ۱۳۹۰، ۱۷) قانون آیین‌دادرسی کیفری برای تضمین این حق در ماده ۱۰۰ مقرر داشته است: « شاکی می‌تواند در هنگام تحقیقات، شهود خود را معرفی و ادله‌اش را اظهار کند و در تحقیقات حضور یابد، صورتمجلس تحقیقات مقدماتی یا سایر اوراق پرونده را که با ضرورت کشف حقیقت منافات ندارد، مطالعه کند و یا به هزینه خود از آنها تصویر یا رونوشت بگیرد.»

۷. حق برخورداری از وکیل و معاضدت حقوقی؛ این حق متاسفانه علیرغم ضرورت آن در خصوص بزه‌دیده در قانون آیین‌دادرسی کیفری مورد توجه واقع نشده است. بنابراین ضابطان یا کارگزاران قضایی نیز در خصوص تبیین و تفهیم این حقوق تکلیفی نداشته و ضمانت اجرایی نیز ندارد.

۸. حق برخورداری از حمایت‌های پزشکی و روانی؛ متاسفانه این حق نیز در قانون آیین‌دادرسی کیفری در خصوص بزه‌دیدگان مغفول مانده است.

۹. حق جبران خسارت؛ در قانون جرایم رایانه‌ای کشورمان راجع به حمایت بزه‌دیدگان سایبری از حیث جبران خسارت وارده و شیوه‌های آن موضوعی پیش‌بینی نشده است اما با توجه به اطلاق ماده ۱۴ قانون آیین دادرسی کیفری که مقرر داشته شاکی می‌تواند در صورت وقوع خسارت جبران ضرر و زیان‌های مادی و معنوی و منافع ممکن‌الحصول ناشی از جرم را مطالبه نماید و در صورت وقوع زیان معنوی که شامل صدمات روحی، هتک حیثیت ، اعتبار شخصی ، خانوادگی و اجتماعی هست، دادگاه علاوه بر صدور حکم به جبران خسارت مالی می‌تواند متهم را از طریق الزام به عذرخواهی و درج حکم در جراید و امثال آن محکوم نماید.

همچنین قانونگذار گذشته از قواعد عمومی دادرسی کیفری و تضمین حقوق بزه‌دیدگان، حمایت از بزه‌دیدگان ناشی از جرایم رایانه‌ای را در بخش دهم از قانون آیین‌دادرسی کیفری مصوب ۱۳۹۲ اجرایی ۱۳۹۴ تحت عنوان آیین دادرسی جرایم رایانه‌ای مورد تاکید قانونگذار قرار گرفته است.

مواد ۶۶۴ و ۶۶۵ قانون آیین‌دادرسی کیفری جدید به صلاحیت دادگاه‌های ایران در رسیدگی به جرایم‌سایبری با توجه به اصول صلاحیت حمایتی، شخصی، سرزمینی و جهانی پرداخته است که بزه‌دیدگان مصرح در بندهای الف، ب ، پ ، ت ماده ۶۶۴ می‌توانند به دادگاه‌های ایران جهت رسیدگی به جرایم وقوع پیوسته مراجعه نمایند. همچنین، اقدام حمایتی دیگر این قانون را می‌توان حفظ داده‌های رایانه‌ای یا سامانه‌های رایانه‌ای و مخابراتی دانست که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد که این حمایت از حمایت‌های تبعی از بزه‌دیدگان مطرح می‌باشد و برای تحقیق و دادرسی ، لازم و ضروری است از سوی مقام قضایی دستور حفاظت یا توقیف و تفتیش آنها صادر شود و چنانچه ضابطان قضایی، کارکنان دولت و یا اشخاصی که وظیفه حفاظت داده‌ها بر آنها سپرده شده خودداری یا آنها را افشا نماید مطابق مواد ۶۶۹ و ۶۷۰ و ۶۷۱ مستوجب مجازات خواهد بود این امر مبین آن است که مقنن در حفظ حقوق بزه‌دیده سایبری از حیث جمع آوری و نگهداری ادله جرم و شناسایی مجرمین اهمیت بسزایی قائل است.

بنابراین می‌توان اذعان داشت، حمایت تقنینی از بزه‌دیدگان نقش موثری در کاهش آسیب‌های جرایم و نیز جرایم رایانه‌ای خواهد داشت. البته حمایت از بزه‌دیدگان در پیشگیری وضعی نیز متجلی می‌شود. زیرا، پیشگیری وضعی با حمایت از آماجهای جرم و بزه‌دیدگان بالقوه و در معرض خطر و با به کارگیری تدابیر و ابزارهای فنی، پیشگیری از بزه‌دیدگی افراد یا آماجها را در برابر بزهکاران دنبال می‌کند و طبیعتا این امر، کاهش بزهکاری را هم به دنبال خواهد داشت.

۴-۲. توجه به راهبردهای بین‌المللی پیشگیری از جرایم سایبری

برآمد بررسی روش‌های پیشگیری از جرایم سایبری و چالش‌های پیش‌روی آن حاکی از آن است که، پیشگیری از جرایم رایانه‌ای باتوجه به ویژگی این جرایم و مرتکبان آن از جمله: فرامرزی بودن، گستردگی خسارت، سهولت ارتکاب و کم سن بودن مرتکبان ضرورتی دوچندان می‌یابد. از آنجایی که این جرایم همواره رو به گسترش‌های توقف‌ناپذیری بوده و قوانین داخلی بعضا نمی‌تواند آنچنان که شایسته است تمامی زوایای این جرایم را پوشش دهد، لازم و ضروری است که در مسیر تقنین و اجرا از رهنمودهای نهادهای بین‌المللی از جمله سازمان ملل متحد، در جهت ارتقای هرچه بیشتر حقوق جرایم سایبری و پیشگیری از آن، بهره برد.

در بخشی از رهنمودهای عملی پیشگیری از جرم سازمان ملل متحد (۲۰۰۲) آمده است: «کشورهای عضو باید به منظور اطلاعات و تجربیاتی که کارآمدی آنها به اثبات رسیده است یک شبکه‌ی بین‌المللی، منطقه‌ای و ملی پیشگیری از جرم ایجاد نمایند.» (جوان جعفری، ۱۳۹۱) بی‌شک ایجاد این شبکه را می‌توان گامی موثر و کارآمد، در جهتِ توسعه‌ی اقدامات پیشگیرانه در پرتو برنامه‌ها و اسناد بین‌المللی، تبادل اطلاعات در زمینه‌ی شیوه‌های پیشگیری و بهره‌مندی از تجربیات سایر کشورها، ایجاد بستر مناسب برای بهره‌مندی از تخصص کارشناسان فنی و پیشگیری‌های علمی روزآمد و نیز استقرار امنیت پایدار با تمسک به راهبردهای موثر پیشگیری در جرایم حساس با ویژگی فراملی، دانست.

یکی دیگر از رهنمودهای عملی پیشگیری از جرم که توجه به آن ضروری است، اجرای راهبردهای جلوگیری از بزه‌دیدگی مجدد است. امکان وقوع بزه‌دیدگی مجدد و حتی مکرر برای جرایم رایانه‌ای نسبت به جرایم حقیقی به دلیل گمنامی مجرمان، وجود قربانیان با سنین پایین و با آسیب‌پذیری بالا، سهولت ارتکاب جرم بیشتر است. استفاده از شیوه‌هایی مانند اعلام گزارش در مورد جرایم در حال وقوع در شبکه‌های مجازی مانند هرزه‌نگاری به منظور مسدود ساختن دسترسی این افراد از طریق سرورهای اصلی، ایجاد فیلترینگ و نیز مخفی‌کننده‌های هویت، می‌تواند در جلوگیری از بزه‌دیدگی مجدد نقش موثری داشته باشد. (رایجیان و همکاران، ۱۳۹۳، ۲۰۲-۲۰۱)

از آنجایی که جرایم سازمان‌یافته در بسیاری از موارد به صورت سایبری، کنترل، هدایت و به وقوع می‌پیوندد، در راهبردهای پیشگیری از جرم از حکومت‌های ملی خواسته شده است تا شرایطی را که می‌تواند به جرایم سازمان‌یافته کمک کرده و موجب رشدآن شود مورد توجه قرار دهند. جرایم سازمان‌یافته در شرایطی پیشرفت می‌کند که قانون‌گرایی ضعیف است، حکومت ناکاراست، فساد دولتی زیاد است و سیستم‌های کنترل کننده سهل انگارند به گونه‌ای که اموال، کسب و کار و نهادهای مالی در معرض سوء استفاده و بهره‌کشی قرار می‌گیرند. از همین‌رو، رهنمودهای سازمان ملل، راهکارهایی را طراحی کرده است که دولت‌ها می‌توانند برای کاهش چنین فرصت‌هایی از آنها استفاده کنند. برنامه‌ریزی برای آموزش مردم، پیشگیری از عضوگیری مجدد یا بهبود مقررات و تقویت کنترل‌های قانونی و اداری می‌تواند در این زمینه مفید باشد. (جوان جعفری، همان، ۱۷۱-۱۶۹) بنابراین توجه به رهنمودهای بین‌المللی می‌تواند نقش بسزایی در کاهش آسیب‌های ناشی از جرایم سایبری و نیز پیشگیری از این جرایم داشته باشد.

۴-۳. بهره‌مندی از نهادهای غیردولتی

به دلیل پیچیدگی و تخصصی بودن جرایم رایانه‌ای و در همان حال سهولت ارتکاب این جرایم، پیشگیری هرچه کارآمدتر از این جرایم در گرو مشارکت مسئولانه و همراه شدن نهادهای غیردولتی با دولت در فرآیند پیشگیری از جرم است. بهره‌مندی از دانش شرکت‌های خصوصی که در مسیر واردات تجهیزات رایانه‌ای اعم از سخت‌افزارها و نرم‌افزارهای کاربردی و مراقبتی مشغول فعالیت هستند و همچنین شرکت‌های دانش‌بینان که اقدامات کارآ و خدمات آموزشی نوین در جهت مقابله با آسیب‌های ناشی از جرایم رایانه‌ای ارائه می‌دهند می‌تواند نقشموثری در پیشگیری از این جرایم داشته باشد.

بدین‌ترتیب، دولت می‌تواند با بهره‌مندی از ظرفیت‌های بخش خصوصی در راستای اهداف خود در زمینه‌ی مقابله با جرایم سایبری پیشرفت چشمگیری در همگام‌سازی دانش مقابله با این جرایم در عرصه‌ی بین‌المللی داشته باشد. در همین راستا، ماده ۹ رهنمودهای پیشگیری از جرم سازمان ملل متحد می‌گوید: در برنامه‌های پیشگیری باتوجه به تنوع علل ایجاد جرم، مشارکت تمامی افراد و نهادهایی که در این زمینه فعالیت و مهارت دارند امری اجتناب ناپذیر است. (جوان جعفری، ۱۳۹۱، ۲۷۵-۲۷۳)

همچنین در این سند آمده است: مشارکت فعال گروه‌ها و سایر بخش‌های جامعه‌مدنی یکی از ارکان اساسی پیشگیری موثر از بزهکاری محسوب می‌گرددو انجمن‌ها باید در تعریف اولویت‌های پیشگیری، اجرای برنامه‌ها و ارزیابی از فعالیت‌ها، نقش کلیدی را ایفا نماید. همچنین دولت‌ها موظف‌اند اقدامات لازم را جهت حمایت و ترغیب این مشارکت‌کنندگان مبذول دارند. (همان، ۲۸۳-۲۷۷)

بنابراین یکی دیگر از راهبردهای مقابله با چالش‌های پیشگیری از جرایم سایبری استفاده از ظرفیت‌ها نهادها و گروه‌های غیردولتی است. با این اقدام ضمن اینکه بارسنگینی از دوش دولت در جهت دسترسی به شیوه‌ها و دانشِ لازمِ پیشگیری از جرایم سایبری برداشته می‌شود، امر پیشگیری با دقت و سازمان نظامندتر به وقوع می‌پیوندد.

۴-۴. توجه به اقشار آسیب‌پذیر

یکی دیگر از جرایم رایانه‌ای که هشداری جدی برای جوامع امروزی است روبه‌رو شدن با دسته‌ی بزرگی از مجرمان نوجوان و جوان است که گاه به سن مسئولیت کیفری نرسیده‌اند. به همین دلیل در کنار تقسیم بندی مرتکبان به مجرمان یقه‌سفید و یقه‌آبی توسط ساترلند، از دسته جدیدی از بزهکاران نوجوان جرایم رایانه‌ای با عنوان «مجرمان شلوار کوتاه» نام برده‌اند. از سویی دیگر، مطابق با آمار بین‌المللی نیز اکثر کاربران اینترنت را جوانان و نوجوانان تشکیل می‌دهند. (رایجیان و همکار، ۱۳۹۳،۲۱۰)

به همین‌جهت، از میان همه‌ی گروه‌های سنی جوان‌ترها به ویژه آنهایی که ساعت‌ها جلوی رایانه به سر می‌برند بیشتر آسیب‌پذیرند؛ زیرا جوان‌ها و نوجوانان خودشان را در این محیط‌ها بیشتر فاش می‌کنند. (Oslon,2005,3)

از سویی دیگر فارغ از اینکه زنان بیشتر بزه‌دیده می‌شوند یا مردان، جنسیت می‌تواند عاملی باشد که احتمال بزه‌دیدگی افراد نسبت به برخی از جرایم را بالا ببرد. در میان جرایم سایبری جرایم ویژه‌ای وجود دارد که در آن بزه‌دیده‌ی آنان فقط زنان و کودکان است. از همین‌رو، ماده ۴۱ رهنمودهای سازمان ملل متحد مقرر داشته است: راهبردهای پیشگیری از جرم در صورت لزوم باید به تفاوت‌های نیاز زن و مرد توجه داشته باشد، همچنین به نیازهای خاص طبقه‌ی آسیب‌پذیر توجه ویژه مبذول کنند. (جوان جعفری، همان، ۲۸۱-۲۷۳)

نتیجه و پیشنهادها

در عصر نوین شاید هیچ جرمی به‌مانند جرایم سایبری را نتوان سراغ داشت که بزهکاران آن بدین شکل معادلات شناسایی را برای مامورین تحقیق پیچیده ساخته باشند. بستر سایبر به‌واسطه ویژگی‌های خاص خود، در وهله نخست شناساییِ بزهکار و در مرتبه‌ی بعدی، کشف بزه را دشوار ساخته است.علاوه بر ویژگی‌هایی که فضای سایبر به بزهکاری مترتب داشته، ابزارهای سنتیِ تحقیقاتی نیز در مواجهه با این جرایم به شدت ناکارآمد و فاقد اثربخشیِ لازم می‌باشند از همین‌جهت است که ضرورت پیشگیری از این جرایم مورد توجه قرار گرفته است.

در پیشگیری از جرایم سایبری، عوامل متعددی دارای نقش هستند که هر کدام به نوبه خود دارای اهمیت و موثر در پیشگیری می‌باشند؛ لذا در جهت مقابله با ارتکاب بزه در محیط سایبر تنها نباید به یک شیوه و راه کنترلی، توجه و تاکید داشت و باید تمامی جوانب و زوایای پنهان در نظر گرفته شود و با بکارگیری روش‌های ترکیبی مقابله با جرایم مذکور، به کاهش هر چه بیشتر آن کمک کرد.

بنابراین، ماحصل یافته‌های ما در این پژوهش برای پاسخگویی به سوالات این پژوهش عبارت است از:

۱. نظام حقوقی ایران در قبال جرایم سایبری بر مبنای دو رویکرد سیاست‌های کیفری و سیاست‌های پیشگیرانه و حمایتی، عمل می‌کند. سیاست تقنینی ایران، از دهه‌ی ۷۰ تا کنون اقدام به واکنش‌های کیفری در جهت مقابله با جرایم سایبری نموده و قانون جرایم رایانه‌ای از اهم این قوانین است. در این قانون هرچند به صورت ناکافی و در پاره‌ای از موارد ناهمگن، جنبه‌های ماهوی حقوق کیفری فناوری اطلاعات و ارتباطات را مورد توجه قرار داده و اقدام به جرم‌انگاری جرایم علیه محرمانگی داده‌ها، صحت و تمامیت داده‌ها، اموال و عفت عمومی نموده است. اما بی‌شک، گسترش روزافزون این جرایم با لحاظ ویژگی‌های خاص آن، ضرورت سیاست‌های قضایی و پیشگیرانه رو دو چندان کرده است. از همین جهت، قوه‌ی قضاییه با مددجویی از نهادهای دولتی و غیردولتی اقداماتی را هرچند توام با موانع جدی در جهت مقابله با جرایم سایبری مبذول داشته است.

۲. طیف گسترده خصایص فناوری رایانه‌ای و متغیر بودن آن، امکان مقابله‌ی همه جانبه، فراگیر و کارآمدِ سیاست‌های کیفری را ناممکن ساخته است. بنابراین، بهره‌مندی از راهبردهای پیشگیری وضعی در مقابله با جرایم سایبری امری بایسته است. از همین جهت با بازشناسی عوامل جرم‌شناختی جرایم سایبری، افزایش موانع ارتکاب جرم، کاهش عوامل محرک، نظارت، کنترل دستیابی به اهداف و نیز بهره‌جویی از ظرفیت‌های ICT، به عنوان ابزارهای پیشگیری وضعی در جهت مقابله با جرایم سایبری نقش بسزایی را ایفا می‌کنند.

۳. باتوجه به تغییرات اساسی که فضای در تمامی ابعاد زندگی اجتماعی افراد ایجاد کرده است، و نیز باتوجه به کاستی‌های پیشگیری وضعی که توان پاسخگویی به تمام زوایای مقابله با جرایم سایبری را ندارد، تمسک به پیشگیری اجتماعی نیز امری لازم است. پیشگیری اجتماعی بر اساس مداخلات و تاثیراتی که بر فرایند شکل‌گیری شخصیت فرد یا محیط‌های پیرامون او صورت می‌گیرد به "پیش گیری جامعه مدار" و "پیشگیری رشد مدار" تقسیم می‌شود. همچنین شایسته است از آموزش همگانی و فرهنگ‌سازی و نیز کدهای رفتاری و منشور اخلاقی به عنوان ابزارهای پیشگیری اجتماعی در جهت مقابله با جرایم سایبری بهره‌مند شویم.

پیشنهادها

در نهایت، یافته اصلی پژوهش این است که پیشگیری از جرایم سایبری، تنها با پیشگیری وضعی راه به جایی نمی‌برد. زیرا ممکن است، با به‌کارگیری برخی از تدابیر و روش‌های پیشگیری وضعی در فضای سایبر شاهد برخی از اختلالات همچون کاهش سرعت شبکه، اعمال محدودیت در دسترسی و نیز نقض حق آزادی فردی شود. لذا بایستی با کمک شناسایی انواع راه‌های پیشگیری که از علوم مختلف حاصل می‌گردد، به صورت همه جانبه و در سطح ملی و بین المللی به مقابله با جرایم سایبری به عنوان یکی از جلوه‌های بزهکاری نوین همت گماشته شود. برهمین اساس، موارد ذیل پیشنهاد می‌شود:

۱. اتخاذ تدابیر انواع راه‌های پیشگری، منطبق با شرایط حاکم و نیز رهنمودها و سندهای بین‌المللی پذیرفته شده‌ی مقابله با جرایم سایبری.

۲. بهره‌مندی از ظرفیت‌های نهادرسانه و نیز مراکز امداد و آگاهی رایانه‌ای در جهت آموزش شیوه‌های نوین جرایم سایبری و راهکارهای مقابله با آن، به شهروندان و کنش‌گران فضای سایبر به ویژه کودکان و نوجوانان.

۳. دادن آموزش‌های فنی و تخصصی به دادرسان، ماموران و عوامل مسیول در زمینه‌ی پیشگیری، تحقیقات، تعقیب و احقاق حق در جرایم سایبری.

۴. در جهت کارآمدی برنامه‌ها و سیاست‌های قضاییِ پیشگیرانه توجه به فراهم ساختن زیرساخت‌های لازم و نیز همکاری با نهادهای متخصص و فنی در سطح داخلی و بین‌المللی امری ضروری است.

۵. اتخاذ سیاست‌های کیفری کارآمد و نیز به روزرسانی قوانین با بهره‌مندی از رهنمودهای بین‌المللی و تجربه‌ی کشورهای پیشرفته.

منابع

«فارسی

کتاب»

[۱]ابراهیمی،شهرام، (۱۳۹۰)، **جرم‌شناسی پیشگیری**، جلد ۱، چاپ اول، تهران: میزان.

[۲]پورصادق،ناصر، کشتکار، مهران، (۱۳۹۵)، **محیط‌شناسی در مدیریت استراتژیک**، چاپ اول، تهران: آذرین مهر.

[۳]جوان جعفری، عبدالرضا، (۱۳۹۱)، **رهنمودهای عملی پیشگیری از جرم**، تهران: میزان.

[۴]خالقی پوستچی، علی، (۱۳۸۸)، **پیشگیری از جرایم سایبری با بهره گیری از فناوری اطلاعات و ارتباطات**، مقاله‌های همایش ملیِ علمی کاربردی پیشگیری از جرم (قوۀ قضاییه، مشهد)، تهران: میزان.

[۵]داتن، ویلیام (۱۳۸۴)، **دگرگونی‌های اجتماعی در جامعه اطلاعاتی**، ترجمه محمد توکل و همکاران، چاپ اول، تهران: کمیسیون ملی یونسکو.

[۶]سازمان ملل،(۱۳۷۶)، **نشریه بین‌المللی سیاست جنایی**، شماره های ۴۳ و ۴۴ سال ۱۹۹۴ ، ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور.

[۷]گروه کار اقتصادی اروپا (۱۳۸۴)، **گزارش فناوری اطلاعات و ارتباطات در اروپا سال ۲۰۰۲** ، ترجمه ناصر زحمت کش و حسین مطلب پور، چاپ اول، تهران: دبیرخانه شورای عالی اطلاع رسانی.

[۸]لطیفیان، سعید، (۱۳۸۳)، **استراتژی و روش‌های برنامه‌ریزی استراتژیک**، تهران: انتشارات وزارت امور خارجه.

« مقاله »

[۹]آشوری، محمد، خدادادی، ابوالقاسم، (۱۳۹۰)، **حقوق بنیادین بزه‌دیده در فرایند دادرسی کیفری**، آموزه‌های حقوق کیفری، شماره ۲، صص ۳۶-۳.

[۱۰]احمدی ناطور، زهرا، آقا بابایی، حسین، (۱۳۹۵)، **جرایم علیه حریم خصوصی داده‌ها در فضای سایبری ایران و آلمان**، رسانه و فرهنگ پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال ششم، شماره ۱، صص ۲۳-۱.

[۱۱]اسلامی، ابراهیم، (۱۳۹۵)، **جایگاه حمایت ازبزه‌دیدگان جرایم سایبری درمقررات کیفری حقوق داخلی وحقوق بین الملل**، پژوهشنامه حقوق اسلامی، سال۱۷، شماره۱، صص ۱۸۲-۱۵۷.

[۱۲]اکرمی، سام، اکرمی، سعیده، (۱۳۹۵)، **پیشگیری غیر کیفری در جرایم اینترنتی**، : کنفرانس ملی چارسوی علوم انسانی، دوره ۲، صص ۱۰-۱.

[۱۳]ایار، علی و همکاران، (۱۳۹۳)، **بررسی عوامل اجتماعی موثر بر جرم (مطالعه موردی زندان دره شهر)**، امنیت اجتماعی، شماره ۴۰ ، صص ۶۰-۳۹.

[۱۴]بابایی، محمدعلی، نجیبیان، علی، (۱۳۹۰)، **چالش‌های پیشگیری وضعی از جرم**، مجله حقوقی دادگستری، شماره ۷۵، صص ۱۷۲-۱۴۷.

[۱۵]بهره‌مند، حمید، همکاران، (۱۳۹۳)، **راهبردهای وضعی پیشگیری از جرایم سایبری**، آموزه‌های حقوق کیفری، دانشگاه علوم اسلامی رضوی، شماره‌ی ۷، صص ۲۰۹-۱۴۷.

[۱۶]حاجی‌تبار فیروز جائی، حسن، (۱۳۹۰)، **دلایل توجیهی حمایت افتراقی از بزه‌دیدگان آسیب‌پذیر در پرتو آموزه‌های علوم جنایی (با نگاهی به قوانین موضوعه ایران)**، دانشنامه حقوق و سیاست، شماره ۱۶، صص ۲۸-۱۱.

[۱۷]حسینی، سیدمحمد، مصطفی پور، مسعود، (۱۳۹۶)، **«جرم شناسی عصب»؛ رویکردی نوین در تحلیل جرایم خشونت آمیز اطفال و نوجوانان (با تاکید بر منحنی سن- جرم)**، حقوق کیفری، شماره ۱۹، صص ۱۹۶-۱۶۵.

[۱۸]خانعلی پور، سکینه، آقابابایی، حسین، (۱۳۸۹)، **مدیریت جرمشناختی خطر جرم از منظر فناوری اطلاعات و ارتباطات**، دانش انتظامی، شماره دوم، صص ۲۵۲-۲۲۱.

[۱۹]خلفی، ابوذر، (۱۳۹۵)، **پیشگیری از جرایم سایبری با محوریت جرم‌یابی**، کارآگاه، شماره ۳۴، صص ۳۸-۲۳.

[۲۰]رایجیان، مهرداد و همکاران، (۱۳۹۳)، **پیشگیری از جرایم رایانه‌ای از رهیافت‌های نظری تا رهیافت‌های جهانی در پرتو رهنمود پیشگیری از جرم سازمان ملل متحد**،مطالعات راهبردی جهانی شدن، شماره ۱۳، صص ۲۱۶-۱۸۹.

[۲۱]رضوی فرد، بهزاد، موسوی، سیدنعمت الله،(۱۳۹۵)، **مسئولیت کیفری در فضای سایبر در حقوق ایران**، پژوهش حقوق کیفری، شماره ۱۶، صص ۴۵-۲۹.

[۲۲]ساریخانی، عادل، سلطانی بهلولی، مریم، (۱۳۹۵)، **نقش قوه‌ی مجریه در پیشگیری از جرم**، مجله حقوقی دادگستری، شماره‌ی ۹۴، صص ۱۵۳-۱۴۱.

[۲۳]شاه محمدی، غلامرضا، تاهو، منصور، (۱۳۹۳)، **بررسی شیوه های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات**، فصلنامه‌ی پژوهش‌های اطلاعاتی و جنایی، سال نهم، شماره‌ی سوم، صص۱۱۹-۹۹.

[۲۴] **راهبردهایی برای پیشگیری وضعی از آسیبهای فضای مجازی**، مطالعات راهبردی ناجا، شماره۱، (۱۳۹۵)،صص ۱۴۴-۱۰۱.

[۲۵]شاهبندر زاده، حمید، یوسفی ده بیدی، شهلا، (۱۳۹۱)، **تعیین درجه اهمیت جرایم رایانه ای از دیدگاه صاحب نظران انتظامی استان بوشهر**، فصلنامه نظم و امنیت انتظامی، سال پنجم شماره اول (پیاپی ۱۷)، صص ۱۵۵-۱۳۷.

[۲۶]صبحدل، محمد، (۱۳۹۶)، **جایگاه حقوقی قوه قضاییه در پیشگیری اجتماعی**، قانون یار، شماره۴، صص ۱۰۸-۹۳.

[۲۷]صفاری، علی، (۱۳۸۰)، **مبانی نظری پیشگیری وضعی از وقوع جرم**، مجلهٔ تحقیقات حقوقی، شماره ۳۳ و ۳۴، صص ۳۲۲-۲۶۷.

[۲۸]قهرمانی افشار، نیوشا و همکاران، (۱۳۹۵)، **پیشگیری رشدمدار؛ بررسی فقهی و حقوقی(ایران و انگلستان)**، فقه و مبانی حقوق اسلامی، شماره‌ی ۲، صص ۹۰-۶۷.

[۲۹]کلارک، رونالد، (۱۳۸۷)، **نظریه پیشگیری جرم از طریق طراحی محیطی**، ترجمه محمدحسن جعفریان، مطالعات مدیریت انتظامی،شماره ۳، صص ۳۵۶-۳۴۴.

[۳۰]کوچی، سعید، داودی، ابراهیم، (۱۳۹۴)، **نقش آموزش کارکنان در پیشگیری از جرایم فضای مجازی (مطالعه موردی کارکنان فرماندهی انتظامی تهران بزرگ)**، فصلنامه پژوهش‌های حفاظتی امنیتی دانشگاه جامع امام حسین(علیه السلام)، سال سوم، شماره ۱۳،صص ۸۹-۶۹.

[۳۱]لعل علیزاده، محسن، (۱۳۹۶)، **بررسی تطبیقی حقوق بزه دیدگان در مراحل تعقیب و تحقیق در قانون آیین دادرسی کیفری ۱۳۹۲ با دیوان کیفری بین المللی**، پژوهش حقوق کیفری، شماره ۱۹، صص ۱۲۶-۹۵.

[۳۲]محسنی، فرید، (۱۳۹۳)، **دستاوردهای نظری و عملی جرم شناسی رشد مدار**، دیدگاه‌های حقوق قضایی، شماره۶۶، صص ۱۶۸-۱۴۵.

[۳۳]محمدی جورکویه، علی، مصطفی پور، مسعود، (۱۳۹۴)، **رویکردی جرم شناختی اسلامی بر قلمرو تأثیر عوامل زیستی بر رفتار مجرمانه**،فصلنامه‌ی دیدگاه‌های حقوق قضایی، شماره ۷۰، صص ۱۵۱-۱۲۷.

[۳۴]مغازه ئی، محمد امین و همکاران، (۱۳۹۳)، **بررسی نقش پلیس در پیشگیری وضعی از جرم با نگاهی بر CPTEDوICT**، دانشنامه مرکزی، شماره‌ی۳، صص ۷۸-۵۵.

[۳۵]منفرد، محبوبه، جلالی فراهانی، امیرحسین، (۱۳۹۱)، کدهای رفتاری و پیشگیری از بزهکاری، پژوهشنامه حقوق کیفری، شماره۲، صص ۱۳۴-۱۰۵.

[۳۶]نبوی، محمدهادی، (۱۳۹۱)، **علل و عوامل روانی جرم از منظر قرآن کریم**،مهندسی فرهنگی، ۶۹-۷۰، صص ۲۴-۱۰.

[۳۷]نوغانی دخت بهمنی، محسن، میرمحمدتبار، سیداحمد، (۱۳۹۴)، **بررسی عوامل اقتصادی مؤثر بر جرم (فراتحلیلی از تحقیقات انجام شده در ایران)**، پژوهش‌های راهبردی امنیت و نظم اجتماعی، شماره ۳، صص ۱۰۲-۸۵.

[۳۸]نیازپور، امیرحسین، (۱۳۹۳)، **اساسی‌سازی حقوق پیشگیری از جرم در ایران**، پژوهش حقوق کیفری، شماره ۶، صص ۱۱۱-۹۱.

[۳۹]ورایی، اکبر و همکاران، (۱۳۹۵)، **بررسی عوامل اجتماعی مؤثر بر تکرار جرم (مطالعه موردی: شهر کرمانشاه)**، فصلنامه علمی-پژوهشی علوم اجتماعی دانشگاه آزاد اسلامی واحد شوشتر، شماره ۳، صص ۲۸-۱.

« منابع انگلیسی »

[۴۰] Graves, Kimberly (2010), CEH: **Certified Ethical Hacker Study Guide**, Indiana: Wiley Publishing, Inc.

[۴۱] International Centre for the Prevention of Crime, **International Report on Crime Prevention and Community Safety: Trends and Perspectives, 2010** (Montreal, 2010); Beccaria Project (www.beccaria.de).

[۴۲] Mcfarlane, L,& Bocij, P, (2003), **Cyber stalking Defi ning the invasion of cyberspace,** Forensic Update, no. 72.

[۴۳] Oslon,K, robin, cpcu, crisi, (2005), **ARM and ARP, identiy theft: a person risk management approach**, cpcu journal, vol 58, no10.

[۴۴] Seigfried, Kathryn C & Lovely, Richard W, Rogers, Marcus K , (2008), **Self-Reported Online Child Pornography Behavior: A Psychological Analysis**, International Journal of Cyber Criminology, Vol 2 (1): 286–297.

[۴۵] Welsh , B . C . , & Farrington , D . P. (2006) . **Surveillance for crime prevention in public space : Results and policy choices in Britania and America** ,Criminology and Public Policy , Volume3, Issue3 , pp497-526.

[۴۶] Wolak, J., Finkhelhor, D., and Mitchell, K. (2009). **Trends in Arrests of Online Predators**, Durham, NH: Crimes against Children Research Center, University ofNewHampshireScholars'Repository,https://scholars.unh.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1051&context=ccrc