■ فصلنامه‌ی مطالعات راهبردی جهانی شدن
سال پنجم/شماره‌ی سیزدهم/پاییز ۱۳۹۳(پیاپی ۱۶)
مرکز ملی مطالعات جهانی شدن

پیش گیری از جرایم رایانه‌ای
از رهیافت‌های نظری تا رهیافتِ جهانی در پرتو رهنمود پیش گیری از جرم سازمان ملل متحد

دکتر مهرداد رَایجیان اصلی[۱]
احسان سلیمی[۲]
علیرضا نوریان[۳]

تاریخ دریافت: ۹۳/۵/۲۸، تاریخ پذیرش: ۹۳/۹/۱

■ چکیده

امروزه، سیاستگذاران و مجریان قانون، به دلایل مختلف از جمله کاهش هزینه‌های تحقق عدالت جنایی، به اقدامات کنشی و پیش گیرانه، متمایل شده‌اند؛ اما پیش گیری از جرم، زمانی کارایی بهتری خواهد داشت که مبتنی بر مبانیِ سازگار با ویژگی‌های هر طبقه از جرم‌ها باشد. مسأله‌ی پیش گیری از جرایَم رایانه‌ای، به‌عنوان یکی از پدیده‌های نوظهور مجرمانه، با توجه به ویژگی‌های این جرایم و مرتکبان آن - از جمله فرامرزی بودن، گستردگی خسارت، سهولت ارتکاب و کم‌سن بودن مرتکبان - ضرورتی دوچندان می‌یابد. سازمان ملل متحد در سال ۲۰۰۲، سندی با عنوان «رهنمود پیش گیری از جرم» تصویب نموده که در آن به بیان چارچوب فعالیت‌ها، اصول بنیادی، روش‌ها

---

۱. استادیار دانشکده‌ی حقوق دانشگاه تربیت مدرّس(نویسنده مسئول)
.(e-mail: rayejianasli@modares.ac.ir)
۲. دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی دانشگاه تهران
.(ehsansalimi1367@yahoo.com)
۳. دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی دانشگاه علوم قضایی و خدمات اداری.

و دیگر اموری که کشـورها باید در پیش‌گیری از جرم رعایت کنند، پرداخته اسـت. مقاله‌ی حاضر، مسـأله‌ی پیش‌گیری از جرایم رایانـه‌ای را در دو محور اصلی بررسـی می‌کند، که عبارت‌اند: (۱) اتخاذپذیری رویکردهای پیش‌گیری مبتنی بر توسـعه‌ی اجتماعی و مبتنی بر موقعیت‌های جرم‌زا، که می‌توان آن را به‌عنوان «رهیافت‌های نظری» به این موضوع بررسـی کرد(۲) اصول راهبردی پیش‌گیری با محوریت سند رهنمود پیش‌گیری سازمان ملل متحد، که می‌توان آن را جلوه‌ای از یک «رهیافتِ جهانی» یا رهیافتی در بستر جهانی‌شدن درنظر گرفت، و تحلیل کرد.

کلید واژه‌ها: جرایم رایانه‌ای، رهنمود پیش‌گیری از جرم سـازمان ملل‌متحد، اصـول راهبـردی پیش‌گیری از جـرم، رهیافت‌های نظـری، رهیافت جهانی یا مبتنی بر جهانی‌شدن.

مقدمه

از زمـان ظهور مکتب تحققی، این دیدگاه کـه «نیازی به توجیه پیش‌گیری از جـرم وجود ندارد»، توسـعه یافت، تا آن‌جا که توسـل بـه پیش‌گیری و اعتبار آن، امـری بدیهی تلقی گردید (ابراهیمی،۱۳۹۱: ۲۷)؛ البته با وجودِ بدیهی‌بودن ضـرورت پیش‌گیری، بر مفهوم و قلمرو آن، اتفاق نظر وجود نداشـت. عده‌ای از جرم‌شناسـان، تنها اقدامات غیرقهرآمیز پیش از وقوع جرم را مشمول مفهوم پیش‌گیری از جرم می‌دانسـتند، که ارتباطَ مسـتقیم با جلوگیری از وقوع جرم داشته باشد. در مقابل، برخی پیش‌گیری را شامل اقدامات قهرآمیز هم می‌دانستند و معتقد بودند اقدام به مقابله با جرم و کلیه‌ی اقدامات پسینی نسبت به جرم نیز در قلمرو مفهوم پیش‌گیری اسـت؛ بنابراین، دستیابی و گزینش بهترین تعریف از مفهوم پیش‌گیری، نیازمند شناسـایی مبانـی نظری امکان پیش‌گیری از جرم بود. شاید بتوان برخی از این مبانی را شامل موارد ذیل دانست:

۱. شـخصیت فرد می‌تواند توسـط یک اقدام محیط بیرونی تغییر یابد ۲. رفتار افـراد بـه طور کلـی از قبل به صورت ژنتیکی تعیین شـده و جبری نیسـت ۳. آموزش بر شکل‌گیری شخصیت تأثیری تعیین‌کننده دارد.

بدیـن ترتیب و با لحاظ مبانـی پیش‌گیری از جرم، شـاید بهترین تعریف از

موضوع مزبور را موریس کوسن[1]، جرم‌شناس کانادایی ارائه داده است: مجموعه اقدامات و تدابیر غیر قهرآمیز که با هدف خاص مهار بزهکاری، کاهش احتمال جرم، کاهش وخامت جرم، پیرامون علل جرم اتخاذ می‌شود(Cusson، 2002: 28). سازمان ملل متحد در سال ۲۰۰۲، اقدام به تصویب «رهنمود پیش‌گیری از جرم»[2] نمود که به صورت اجمالی، عناصر لازم برای یک پیش‌گیری مؤثر و کارآمد را بیان می‌نماید. این امر از آن جهت حائز اهمیت است که طرح‌های پیش‌گیری، باید از همان ابتدا با رعایت موازین بین‌المللی و حقوق بشری، کنوانسیون‌ها و دیگر اسناد بین‌المللی و تکیه بر دانش روز پایه‌ریزی شوند.

ضرورت پیش‌گیری از جرم، نه تنها در مورد جرایم حقیقی، بلکه در مورد جرایم مجازی نیز احساس می‌شود؛ زیرا در سال‌های اخیر، پدیده‌ی رایانه، جرایم نوینی را تولید نموده و بر شیوه‌های ارتکاب جرایم سنتی نیز تأثیرات فراوانی داشته است؛ هم‌چنین، ناکامی نظام عدالت جنایی در توقف جرایم رایانه‌ای از یک سو و هزینه‌های گزاف اقدامات واکنشی نسبت به جرایم مزبور از سوی دیگر، ضرورت پیش‌گیری از این جرایم را توجیه می‌نماید. به طور کلی، هدف از اعمال اقدامات پیشگیرانه در محیط سایبر، عبارت است از محرمانه ماندن اطلاعات، احراز هویت فرستنده‌ی پیغام، سلامت داده‌ها در طی انتقال یا نگهداری، کنترل دسترسی یا امکان منع دسترسی افرادی که برای دسترسی به شبکه قابل اعتماد نیستند، در دسترس بودن تمام امکانات شبکه برای افراد مجاز و عدم امکان اختلال در دسترسی (ملزوماتی و یاری، ۱۳۸۴: ۱۵۱).

مقاله‌ی حاضر قصد دارد رویکردها و اصول راهبردی پیش‌گیری از جرایم رایانه‌ای را براساس دو دسته‌ی رهیافت‌ها تبیین کند. بدین‌سان، دو مسأله‌ی اصلی در این مقاله، بررسی و تحلیل خواهد شد: نخستین مسأله در چارچوب رهیافت‌های نظری این است که آیا رویکردهای اصلی پیش‌گیری از جرم (یعنی پیش‌گیری مبتنی بر توسعه‌ی اجتماعی و پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا) تا چه اندازه در زمینه‌ی جرایم رایانه‌ای، قابل اتخاذند؟ دومین مسأله‌ای که این مقاله در چارچوب یک رهیافت جهانی یا مبتنی بر جهانی‌شدن به

1. Maurice Cusson

2. The guidelines for the prevention of crime (council resolution 2002/13 annex)

آن می‌پـردازد، این اسـت که اصول راهبردی پیش‌گیـری از جرایم رایانه‌ای با محوریت سـند «رهنمود پیش‌گیری از جرم سازمان ملل متحد ۲۰۰۲» چیست؟ بـر این اسـاس، مقاله‌ی پیـش رو در قالبِ دو گفتار پیش‌گیـری از جرم، ارائه می‌شود. گفتار اول، رویکردهای پیش‌گیریِ از جرم را در دو محور پیش‌گیری اجتماعـی مبتنی بر توسـعه و پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا بررسـی می‌کنـد. گفتـار دوم نیز به اصـول راهبردی پیش‌گیری از جرایـم رایانه‌ای در هشت محور خواهد پرداخت.

گفتـار اول: اتخاذپذیـری رویکردهـای پیش‌گیری از جـرم در قبال جرایم رایانه‌ای

در بخشـی از رهنمـود عملـی پیش‌گیری از جرم، سـازمان ملـل متحد، به طور اجمالـی به رویکردهایی که دولت و جامعـه‌ی مدنی باید در جهت پیش‌گیری از بزهـکاری به کار برند، پرداخته شـده اسـت. از این رهگـذر به دو رویکردِ پیش‌گیـری مبتنی بر توسـعه‌ی اجتماعی و پیش‌گیری مبتنـی بر موقعیت‌های جرم‌زا اشاره شده است. در ادامه، در دو بند به این دو رویکرد خواهیم پرداخت.

بنـد اول: کارایی‌سـنجی پیش‌گیـری مبتنـی بـر توسـعه‌ی اجتماعـی در قبال جرایم رایانه‌ای

در خصوص رویکرد پیش‌گیری مبتنی بر توسـعه‌ی اجتماعی، در این سند آمده اسـت: دولت‌ها باید با عوامل ایجاد خطر بزهکاری و بزه‌دیدگی مقابله کنند و بدین منظور باید: الف) عوامل حمایتی در قلمرو بهداشـت، آموزش، مسـکن و شغل از طریق برنامه‌های عمومی تقویت شود. ب) از رفتارهایی که در راستای رفع مشکل حاشیه‌نشینی انجام می‌پذیرد، حمایت شود. ج) از شیوه‌ی حل‌وفصل مثبت اختلافات حمایت شـود. د) از راهبردهای آموزشی و حساس‌سازی مردم جهـت ایجاد فرهنگ قانون‌مداری و مدارا اسـتفاده بهینه شـود (جوان جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

برخی از رهنمودهای سـازمان ملل در خصوص پیش‌گیری مبتنی بر توسعه‌ی اجتماعی، به اقتضای ماهیت جرایم رایانه‌ای، سـالبه‌ی به انتفای موضوع اسـت. بـا وجود این، اغلب موارد مذکور را می‌تـوان به عنوان راهبردی برای مقابله با جرایم رایانه‌ای نیز به کار گرفت.

تأکید این سند بر تقویت عوامل حمایتی و استفاده‌ی بهینه از راهبردهای حساس‌سازی مردم و به ویژه اهمیت به آموزش برای پیش‌گیری از جرم، به خوبی قابل انطباق با جرایم رایانه‌ای است. حساس‌سازی مردم جهت ایجاد فرهنگ قانون‌مداری، مقوله‌ای مهم است که در رهنمود پیش‌گیری از جرم سازمان ملل به آن اشاره شده است. برای تحقق این منظور، باید با ارتقای فرهنگ استفاده‌ی صحیح از رایانه، تدبیری اندیشیده شود تا هریک از کاربران، ناظر رفتار دیگری باشند و در صورت ارتکاب تخلف آشکار توسط یک کاربر، دیگر کاربران او را از ادامه‌ی ارتکاب ناهنجاری بازدارند، و حضور او را در آن صفحه‌ی اینترنتی به حالت تعلیق درآورند؛ برای مثال، رعایت ادب و نزاکت در اتاق‌های گپ[1]، از مواردی است که در صورت عدم پای‌بندی به آن، دیگر کاربران شخصِ هنجارشکن را از ادامه‌ی حضور در آن اتاق محروم می‌کنند.

مقوله‌ی آموزش که در رهنمود عملی پیش‌گیری از جرم هم بر آن تأکید شده، امر مهم دیگری است که به اشکال گوناگون به پیش‌گیری از جرایم رایانه‌ای کمک می‌کند. با توجه به این‌که جرایم رایانه‌ای عمدتاً توسط نیروهای سازمان یافته و طراحی و نقشه‌ی قبلی و نیز توسط اشخاص رقیب یا اخراج شده از سازمان‌های مزبور صورت می‌گیرد (رضوی، ۱۳۸۶: ۱۲۴)، آموزش به اشخاص و شرکت‌هایی که احتمالاً در معرض جرایم رایانه‌ای هستند، برای مقابله با این جرایم بسیار سودمند است؛ علاوه بر این، آموزش‌های عمومی در رسانه‌های گروهی برای مقابله با ویروس‌ها و کرم‌های رایانه‌ای - در صورتی که سریعاً مقابله عمومی با این ویروس‌ها صورت گیرد - هزینه‌های پیش‌گیری از این جرایم به مراتب کاهش می‌یابد؛ هم‌چنین، آموزش تدابیری که به وسیله‌ی آن‌ها امنیت رایانه تامین می‌شود نیز امری ضروری است و بدین وسیله از بسیاری از جرایم که در ارتباط با محرمانگی داده‌ها است، جلوگیری به عمل می‌آید.

بند دوم: کارایی‌سنجی پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا در قبال جرایم رایانه‌ای

پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا، مذکور در رهنمود پیش‌گیری از جرم سازمان ملل را می‌توان تعبیر عامّی از پیش‌گیری وضعی دانست. توضیح

1. Chat Room

بیشتر این‌که آن‌چه که در پیش‌گیری وضعی مطرح می‌شود، این است که با جاذبه‌زدایی از سیبل جرم، بالابردن هزینه و کاهش احتمال نتیجه‌گیری از جرم، زمینه‌ی ارتکاب آن را از بین ببریم، یا تا حدّ قابل قبولی پایین آوریم (صفاری، ۱۳۸۰: ۲۹۲). آن‌چه که به عنوان پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا در رهنمود پیش‌گیری از جرم آمده، علاوه بر اتخاذ تدابیر پیش‌گیری وضعی به معنای خاص، شامل ارتقای شیوه‌های مراقبتی، نظارتی و راهبردهای پیش‌گیری از بزه‌دیدگی مجدد هم می‌شود. در این رهنمود آمده است: «دولت‌ها و نیز جامعه‌ی مدنی باید با تمرکز بر امور زیر، نسبت به تدوین برنامه‌های پیش‌گیری از موقعیت‌های جرم‌زا اقدام نمایند:

الف) ارتقای شیوه‌های مراقبتی- نظارتی مناسب به شرط این‌که به زندگی خصوصی افراد لطمه وارد ننماید. ب) اتخاذ تدابیر پیش‌گیری وضعی که به قابلیت و بدنه‌ی محیط اجتماعی لطمه وارد نکند، و دسترسی آزاد به مکان‌های عمومی را محدود ننماید. ج) اجرای راهبردهای پیش‌گیری از بزه‌دیدگی مجدد (جوان جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

در ادامه، ابتدا به برشماری شیوه‌های مراقبتی در جرایم رایانه‌ای می‌پردازیم و سپس بر شرطی که در رهنمود سازمان ملل برای ارتقای این شیوه‌های مراقبتی- نظارتی در نظر گرفته شده، یعنی مناسب بودن و این‌که به زندگی خصوصی افراد لطمه وارد ننماید، تأکید می‌کنیم.

۱. شیوه‌های مراقبتی– نظارتی بر فضای مجازی

در رهنمود پیش‌گیری از جرم سازمان ملل، مسئله‌ی نظارت برای پیش‌گیری از وقوع جرم، مسلّم فرض شدَه و بر ارتقای شیوه‌های نظارتی تأکید شده است. نظارت در محیط سایبر، هم‌چون نظارت در محیط مادّی از جمله راهکارهایی است که علاوه بر کشف سریع جرم، از ارتکاب آن نیز جلوگیری می‌کند.

تدابیر مراقبتی را می‌توان از دو طریق اعمال کرد؛ الف) به کار گرفتن تدابیر فیزیکی، آن‌طور که در سایر جرایم اعمال می‌شود. نصب دوربین‌های مداربسته در کافی‌نت‌ها و چیدمان صفحه‌ی نمایش رایانه‌ها به نحوی که در معرض دیدِ عموم باشد، از جمله موارد برای پیش‌گیری از ارتکاب جرم است. ب) روش

دیگر که با ویژگی‌های این محیط سازگاری بیشتری دارد، نظارت الکترونیکی است؛ در این شیوه با به کارگیری تجهیزات و برنامه‌های خاص، فعالیت‌های شبکه‌ای افراد زیر نظر قرار می‌گیرد (جلالی فراهانی، ۱۳۸۳: ۱۱۴). لازم به ذکر است در صورتی نظارت شبکه‌ای اثر بازدارنده خواهد داشت که کاربر «بداند» فعالیت‌های‌اش زیر نظارت قرار دارد؛ زیرا نظارت مخفی، فقط برای جمع‌آوری ادلّه علیه متهم به کار می‌رود و هیچ اثر پیشگیرانه‌ای ندارد (جلالی فراهانی، ۱۳۸۴: ۱۴۴)؛ بنابراین، به کارگیری ابزاری که زیر محافظت بودن شبکه و زیر نظارت بودن کاربر را اعلام کند، می‌تواند ابزارهای نظارتی را تکمیل نماید.

۱-۱ نظارت بر ورودی و خروجی داده‌ها

از جمله مواردی که در بحث نظارت باید بدان توجه نمود، کنترل ورودی‌ها و خروجی‌های داده است. در واقع باید از میزان داده‌های وارد شده، نوع و منشأ آن‌ها اطلاع و اطمینان حاصل نمود. خصوصاً در مواردی که به دلیل بالابودن هزینه، امکان به کارگیری کنترل‌های دولایه و تفکیک‌های تهیه‌ی مجوز، وجود نداشته باشد (خانعلی‌پور، ۱۳۹۰: ۱۴۰). یکی از گونه‌های کنترل، ورودی قراردادن رمز عبور در رایانه است (ابراهیمی، ۱۳۹۱: ۱۱۷) بسیاری از رایانه‌ها، اطلاعات مربوط به تلاش موفق یا ناموفق افراد در ورود به سامانه را ثبت می‌کنند (وایدنگ، ۱۳۷۹: ۹۳)

از دیگر راهکارها استفاده از شبکه‌های مجازی، کاوشگرهای الکترونیکی است. این کاوشگرها که از آن‌ها به پلیس مجازی نیز تعبیر می‌شود، وظیفه‌ی تشخیص هویت‌های مجازی، اعتبارسنجی امضاهای الکترونیک، کنترل دسترسی‌های مجاز به محتوای محرمانه‌ی داده‌ها و حتی تشخیص مصادیق محرمانه‌ی منتشرشده را به عهده دارند (خالقی پوستچی، ۱۳۸۸: ۴۶).

مجهز کردن شرکت‌ها و مراکزی که احتمالاً در معرض ارتکاب جرم‌اند به این رایانه‌های نظارتی و کنترل ورود، شیوه‌ی مناسبی برای پیش‌گیری از جرم است. بازرسی‌های اتوماتیک رایانه‌ای نیز باید به طور وسیع استفاده شوند؛ خصوصاً برای انجام بررسی‌های متوالی، بررسی‌های مربوط به معقول بودن ورودی‌ها، بازرسی‌های مربوط به حدود بالا و پایین و بازرسی‌های ویژه مربوط

بـه تصحیحات تعدیل‌کننده، باید از رایانه اسـتفاده نمود (زیبر، ۱۳۹۰: ۲۱۹). در کنترل‌های خروجی باید تمام داده‌هایی که منشـأ خود را ترک می‌کنند، مورد بررسی و نظارت کامل قرار گیرند. در این کنترل، علاوه بر این‌که باید تمامی راهکارهـای قانونـی خروج اطلاعات مدنظر قرار گیرد. لازم اسـت که احتمال نشت اطلاعات به خارج، به خصوص در ارتباطات راه دور و انتشار الکترونیکی، مـورد توجه واقع شـود. در ضمن، تمام داده‌های ذخیره شـده باید دارای علایم مشخص باشند به خصوص علایم حقّ نشر، شناسایی مخفی و شماره‌های سریالی که اصالت داده‌ها را به اثبات می‌رسانند (زیبر، ۳۲۲:۱۳۹۰).

علاوه بر شـیوه‌های مذکور، با پیدایش پدیده‌هایی چون پلیس سـایبری[1] که در ایران زیر عنوان پلیس فتا مشـغول انجام وظیفه اسـت، جلوه‌های دیگری از شـیوه‌های نظارتی به وجود آمده، که با الهام از نتایج مثبت پلیس گشـت پیاده به عنوان یک اقدام وضعی پیشگیرانه، به اجرا در آمده است (نجفی ابرندآبادی، ۱۳۷۸: ۱۳۸). پلیس را می‌توان مهم‌ترین عامل پیش‌گیری از جرم به شمار آورد (رضـوی، ۱۳۸۶: ۱۳۳) و حضور فیزیکی وی در مواردی که جرایم رایانه‌ای با ورود کاربران غیرمجاز به یک سایت رایانه‌ای صورت می‌پذیرد، نقش مؤثری در پیش‌گیـری از جرایم رایانه‌ای ایفا می‌کند (آیـکاو، ۱۳۸۳: ۱۶۹)؛ هم‌چنین این‌گونه مراقبت‌های پیش‌گیرانه از طریق گشـت‌زنی و تعقیب و مراقبت یک سوژه یا مظنون در محیط مجازی با استفاده از نرم‌افزارهای از پیش طراحی شده، میسر است (رضوی، ۱۳۸۶: ۱۷۳).

۱-۲ نظارت بر انتقال، پردازش و ذخیره داده‌ها

عـلاوه بر ایمنی و کنترل‌های ویژه‌ی ورودی در خصوص ایمنی انتقال داده‌ها، ضروری اسـت که تدابیر لازم را بـرای پیش‌گیری از جرایم علیه محرمانگی و اخلال در داده‌ها به کار بسـت. قسـمت عمده‌ای از امنیت، بـه ارتباطات داخل شـبکه مربوط می‌شـود، و بدین منظور هر طرفِ رابطه باید اطمینان داشته باشد کـه اطلاعـات دریافتی از طرف مقابل، به طور قطع از طرف وی ارسـال شـده و در بیـن راه نیـز تغییر داده نشـده اسـت؛ هم‌چنین هر دو طـرف باید مطمئن باشند در بین راه، اطلاعات را شخص دیگری نمی‌خواند (خانعلی‌پور و اجارگاه،

1. Cyber patrol

۱۳۹۰: ۱۲۹). چنان‌چه داده‌های حمل‌شونده توسط انتقال‌دهنده از اهمیت خاصی برخوردار باشند، باید با استفاده از روش‌های تضمین الکترونیکی یا با استفاده از رمزگذاری در مقابل تغییر داده، محافظت‌های لازم در زمان حمل‌ونقل داده، صورت گیرد.

شرکت‌هایی که به مبادله‌ی داده با دیگر بازرگانان یا دیگر بخش‌های خود نیاز دارند، باید همیشه ضرورت ایمنی انتقال داده را مدّنظر داشته باشند (زیبر، ۱۳۹۰: ۲۲۰). امروزه برای تأمین هرچه بیشتر امنیت انتقال داده‌ها از ناشناس‌کننده‌ها[1] و رمزنگارها[2] استفاده می‌شود. این دو اقدام با این‌که تا حدی با یکدیگر تفاوت دارند، اما یک هدف را دنبال می‌کنند. کارکرد اصلی‌شان این است که با پنهان‌کردن هویت یا محتوای اطلاعات افراد از بزه‌دیدگی جلوگیری می‌کنند (خانعلی پور و اجارگاه، ۱۳۹۰: ۱۲۹) ناشناس‌کننده‌ها، هویت افراد مبدأ و مقصدِ مبادله‌ی اطلاعات را پنهان می‌کنند و رمزنگارها، محتوای ارتباطات را نامفهوم می‌کنند. دلیل به‌کارگیری فرآیند رمزنگاری این است که از یک سو کلیه‌ی پیام‌هایی که در وب دریافت و ارسال می‌شود، به صورت متن ساده هستند و از سوی دیگر، ابزارهای بسیاری در این محیط برای شنود و دستیابی به ارتباطات افراد وجود دارد (جلالی فراهانی، ۱۳۸۳: ۱۱۵).

۱-۳ شرایط اعمال شیوه‌های مراقبتی- نظارتی

شیوه‌هایی که برشمرده شد، به عنوان بخشی از شیوه‌های مراقبتی- نظارتی در فضای مجازی به کار می‌رود. در رهنمود پیش‌گیری از جرم سازمان ملل، ضمن تأکید بر ارتقای شیوه‌های نظارتی به شرطِ مناسب بودنَ و این‌که به زندگی خصوصی افراد لطمه وارد ننماید، نیز تصریح شده است. در فضای مجازی، تمام فضاهای غیراشتراکی یا اشتراکیِ محدود که حاوی فایل‌های شخصی‌اند، حریم خصوصی اطلاعاتی فرد محسوب می‌شوند (یزدانی زنور، ۱۳۸۸: ۱۴۵). در واقع، تمام کاربران مجازی، حق تنها ماندن و گم‌نامی در فضای مجازی را مادام که مرتکب جرم نشده‌اند، دارا هستند.

با توجه به توضیح اجمالی که در خصوص شیوه‌های مراقبتی نظارتی بیان شد،

1. Anonymizers
2. Encryption

نمی‌توان تردید داشت که در موارد بسیاری این شیوه‌های نظارتی، خود موجب نقض غرض و خدشــه به حریــم خصوصی کاربران در فضــای مجازی خواهند شــد. در واقع، ابزارهای نظارتی که بازدارنده هم می‌توانند باشــند، تأثیرات سوءِ بســیاری بر فعالیت‌های شــبکه‌ای می‌گذارند. چنان‌چه ایــن حس در مردم بیدار شــود که به دلیل بی‌اعتمادی به آن‌ها، همواره تحت نظارت قرار دارند، این امر به شدت بر نحوه‌ی فعالیت آن‌ها تأثیر خواهد گذاشت.

اکنــون فعالیت‌هــای مختلف اقتصادی، اجتماعی، فرهنگی و سیاســی بســیار متنوعی در فضای مجازی جریان دارد که تمام آن به خاطر آزاد و عاری بودن این فضا از هرگونه محدودیت است؛ اما چنان‌چه کاربران شبکه‌ای احساس کنند فعالیت‌های آن‌ها تحت نظارت مســتمر زنده یا غیر زنده قرار دارد، بی‌تردید در نحــوه‌ی فعالیت خود تجدیدنظر خواهند کرد که این خود به معنای ناکام ماندن اهدافی است که از ظهور این فضا دنبال می‌شد (جلالی فراهانی، ۱۳۸۴: ۱۵۴).

بنابر آن‌چه که گفته شــد، متصدیان پیش‌گیری از جرایم رایانه‌ای و مسئولان نظارت بر محیط مجازی، بایســتی مطابق با رهنمود پیش‌گیری از جرم ســازمان ملــل متحد، علاوه بر ارتقای شــیوه‌های مراقبتی- نظارتی مناســب به امر خطیر حریــم خصوصی کاربران رایانه و فضاهای مجــازی، کاملاً توجه نموده و نباید موجبات نقض غرض را با تجاوز به حریم خصوصی افراد، فراهم نمایند.

۲. تدابیر پیش‌گیری وضعی و جرایم رایانه‌ای

در رهنمود پیش‌گیری از جرم ســازمان ملل متحد، بــر اتخاذ تدابیر پیش‌گیری وضعی که به قابلیت و بدنه‌ی محیط اجتماعی لطمه وارد نکند، و دسترسی آزاد به مکان‌های عمومی را محدود ننماید، تصریح شــده اســت. پیش‌گیری وضعی در جرایــم رایانــه‌ای از جایــگاه خاصی برخوردار اســت[۱]. یکــی از دلایلی که موجــب اهمیت این نوع پیش‌گیری برای جرایم رایانه‌ای شــده اســت، مقیّد به وســیله بودن این جرایم اســت. به عبارت دیگر، بدون استفاده از رایانه و فضای سایبر، ارتکاب این جرایم محال است. در نتیجه با اعمال محدودیت‌های لازم بر وسیله، می‌توان ارتکاب این جرایم را به نحو چشمگیری کاهش داد؛ بنابراین به

۱. برای مطالعه بیشتر در این زمینه ر.ک : جلالی فراهانی، امیرحسین، «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، مجله‌ی فقه و حقوق، سال دوم، پاییز ۱۳۸۴

کارگیری و پیاده‌سازی موارد پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا مذکور در رهنمود پیش‌گیری از جرم سازمان ملل، می‌تواند تا حد زیادی بر پیش‌گیری از این جرایم، مؤثر واقع شود.

آن‌چه امروزه در قالب نصب دیوار آتشین[1] و پالایه[2] در این شبکه‌ها انجام می‌شود، چیزی جز پیش‌گیری وضعی نمی‌باشد (جلالی فراهانی،۱۳۸۳: ۱۰۹). دیوار آتشین، ترکیبی از سخت‌افزار و نرم‌افزار است که یک شبکه را از لحاظ امنیتی به دو یا چند بخش تقسیم می‌کند (ویلیامز، ۱۳۹۱: ۲۸۲). به کارگیری این دیواره‌های دفاعی، بهترین راه برای کاهش هرزنامه‌ها[3] است (گاتن، ۱۳۸۴: ۷۱).

پالایه یا فیلترینگ، شیوه‌ی دیگری برای پیش‌گیری وضعی از جرایم رایانه‌ای است که به منظور کنترل و محدودکردن دسترسی به شبکه و برخی خدمات اعمال می‌شود (خانعلی‌پور واجارگاه، ۱۳۹۰: ۱۲۷). استفاده از پروکسی‌ها[4] را نیز باید روشِ دیگری برای پیش‌گیری وضعی از این جرایم دانست. از کاربردهای پروکسی می‌توان به بالا بردن امنیت در رایانه اشاره کرد. با استفاده از پروکسی، کاربران به جای این که مستقیم به اینترنت متصل شوند، همگی از طریق یک پروکسی به اینترنت وصل می‌گردند. از دیگر استفاده‌های پروکسی، مخفی بودن در اینترنت و از بین بردن آدرس IP است که در این حالت نیز می‌توان از نفوذ هکرها به سیستم جلوگیری کرد؛ هم‌چنین، شناسایی کاربران با استفاده از کوکی[5] را نیز می‌توان روش مناسبی از نوع پیش‌گیری وضعی دانست. روش کار کوکی‌ها به این طریق است که هنگامی‌که کاربر از طریق رایانه‌ی خود به یک وب‌سایت اینترنتی دسترسی می‌یابد، وب‌سایت مذکور فایلی با حجم کم، به نام کوکی ایجاد کرده و آن را بر روی رایانه کاربر ارسال و در شاخه‌ای به نام Temporary internet file ذخیره می‌نماید. یک کوکی‌حاوی اطلاعات مهمی مانند موضوع‌های مورد توجه کاربر، اطلاعات راجع به تماس

1. Fire wall
2. Filtering
3. Spam
4. Proxy
5. Cookie

نظیر زمان و تاریخ و دفعات اتصال و سوابق فعالیت‌های کاربر است که شامل فایل‌هایی که مورد دسترسی قرار گرفته یا خدماتی که استفاده کرده نیز می‌شود (الهی‌منش، ۱۳۹۱: ۲۰۵).

۲-۱ شرایط پیش‌گیری وضعی

تدوین و اجرای تدابیر پیشگیرانه، صرف‌نظر از اشکال مختلف آن، می‌بایست مقیّد به رعایت مبانی نظری، اصول علمی و به ویژه معیارها و محدوده های حقوقی باتوجه به نوع جرم، برنامه‌ها، روش و فنون مورد استفاده باشد (ابراهیمی، ۱۳۹۱: ۳۰). به بیان دیگر، هدف پیش‌گیری، نمی‌تواند کاربرد هر وسیله، فن یا اقدام و به‌ویژه کنارگذاری اصول عمومی حقوق را توجیه کرده، و بهانه‌ای برای توسل به مقررات فوق‌عادی و روش‌های خاص فراقانونی شود (نجفی ابرندآبادی، ۱۳۸۲: ۵۶۷). در رهنمود پیش‌گیری از جرم سازمان ملل متحد نیز به اتخاذ تدابیر پیش‌گیری وضعی که به قابلیت و بدنه‌ی محیط اجتماعی لطمه وارد نکند، و دسترسی آزاد به مکان‌های عمومی را محدود ننماید، تأکید شده است. در این رهنمود، دو شرط برای اعمال پیش‌گیری وضعی مقرر شده است که عبارت‌اند از:

۱. عدم ورود آسیب به قابلیت و بدنه‌ی محیط اجتماعی؛
۲. عدم محدودیت برای دسترسی آزاد به مکان‌های عمومی.

ممکن است با به کارگیری تدابیر و روش‌های پیش‌گیری وضعی در فضای مجازی، شاهد برخی اختلالات هم‌چون کاهش سرعت شبکه، بسته‌شدن اشتباهی برخی ازسایت‌ها و وبلاگ‌ها به جهت فیلترینگ، محدودیت‌های بی‌جهت برای ورود به برخی فضاها، اعمال محدودیت در دسترسی به شبکه‌های بین‌المللی و غیره باشیم. رعایت شرط اولِ رهنمود پیش‌گیری از جرم در خصوص پیش‌گیری وضعی از جرایم رایانه‌ای، در تقابل با همین تبعات منفی پیش‌گیری وضع شده است. با اعمال این شرط، متصدیان پیش‌گیری از جرایم رایانه‌ای، موظف می‌شوند که به گونه‌ای به امر پیش‌گیری وضعی اقدام نمایند که کمترین نابسامانی و اختلال در محیط مجازی رخ ندهد.

یکی از ویژگی‌های بی‌نظیر فضای مجازی، دسترسی آزاد به مکان‌های عمومی است، به‌گونه‌ای که اشخاص در سراسر دنیا با سهولت به این مکان‌ها دسترسی داشته و با حضور در آن‌جا با یک‌دیگر ارتباط برقرار می‌کنند. شبکه‌های

اجتماعی یکی از بزرگترین مکان‌های عمومی است؛ به طور مثال، فیس‌بوک با بیش از یک میلیارد کاربر، بزرگترین شبکه‌ی اجتماعی جهان است.[۱]

در رهنمود پیش‌گیری از جرم، به عنوان دومین شرط پیش‌گیری وضعی، بر عدم محدودیت برای دسترسی آزاد به مکان‌های عمومی تأکید شده است. نتیجه‌ی اعمال این رهنمود، چیزی جز اتخاذ رویکردی سنجیده و ملایم‌تر نسبت به ممنوعیت کاملِ شبکه‌های اجتماعی مجازی، مسئله‌ی فیلترینگ و افزایش دقت و هوشمندیَ سامانه‌های فیلترکننده برای اجتناب از اشتباه در فیلترینگ نیست؛ چه آن‌که فیلترینگ به دو جهت مانع دسترسی آزاد به مکان‌های عمومی است: اول، نگاه افراطی متصدیان فیلتر به ممنوعیت هر سایتی که مطالب آن با سلیقه فیلترکنندگانَ هم‌خوان نیست. آن‌چه که به گستره‌ی این محدودیت‌ها دامن می‌زند، گنجاندن طیف وسیعی از موضوعات مشکوک یا به اصطلاح خاکستری در فهرست‌های سیاه است (جلالی فراهانی، ۱۳۸۴: ۱۵۲)؛ دوم، کارکرد انطباقی، و نه هوشمندانه‌ی این ابزارهاست؛ زیرا اصطلاحات یا تصاویر مندرج در فهرست‌های سیاه، تنها در متون یا محتواهای غیرمجاز به کار نمی‌رود، و بسیار اتفاق می‌افتد که به لحاظ کاربرد آن‌ها در محتوای مجاز از دسترسی به آن‌ها جلوگیری می‌شود (جلالی فراهانی، ۱۳۸۴: ۱۵۲).

۳. اجرای راهبردهای پیش‌گیری از بزه‌دیدگی مجدد

در رهنمود پیش‌گیری از جرم سازمان ملل بر اجرایَ راهبردهای پیش‌گیری از بزه‌دیدگیِ مجدد، تأکید شده است. امکان وقوع بزه‌دیدگی مجدد و حتی مکرر برایَ جرایم رایانه‌ای نسبت به جرایم حقیقی به دلیل گم‌نامی مجرمان، وجود قربانیان با سنین پایین و با آسیب‌پذیری بالا، سهولت ارتکاب جرم و درهم‌تنیدگی ارتباط بزه‌دیده و بزه‌کار رایانه‌ای، بیشتر است.

استفاده از ناشناس‌کننده‌های هویتِ کاربرانِ محیطِ سایبر، یک راه حل مناسب برای پیش‌گیری از بزه‌دیدگی مجدد است. ناشناس‌کننده‌ها، هویت افراد در محیط سایبر را پنهان می‌کنند و از این طریق به آن‌ها امکان می‌دهند با ایجاد

۱. آقای زاکربرگ، خالق فیس‌بوک، اشاره می‌کند که «من رهبر سومین کشور پرجمعیت دنیا بعد از هند و چین هستم» و با عبور از مرز یک میلیارد کاربر حدود دوماه قبل می‌تواند این ادعا را داشته باشد که از این مرز و از این فضا عبور کرده است (روزنامه همشهری شنبه ۶/۱۲/۹۰).

حریم بیشتر به فعالیت شبکه‌ای بپردازند (جلالی فراهانی، ۱۳۸۴: ۱۴۵). این فرآیندها پیوندهای هویتی را قطع می‌نماید و تنها آن‌چه را که به طور تصادفی ایجاد شده، به عنوان هویت اشخاص ارائه می‌دهند و کاربران قادر خواهند بود در تعاملات شبکه‌ای خود از آن استفاده کنند (خانعلی پور واجارگاه، ۱۳۹۰: ۱۲۹). این اقدام به ویژه برای زنان و کودکان و یا به طور کلی اشخاصی که به هر دلیلی آسیب‌پذیرند، سودمند است (جلالی فراهانی، ۱۳۹۱: ۱۴۵)؛ زیرا آن‌ها را از هر نوع بزه‌دیدگی و به ویژه بزه‌دیدگی مجدد، مصون می‌دارد.

یکی دیگر از راهبردهای پیش‌گیری از بزه‌دیدگی مجدد، استفاده از برنامه‌های ویروس‌کش است. ویروس‌ها و کرم‌های رایانه‌ای، قابلیت زایش و تکثیر تصاعدی را دارا هستند و امکان بزه‌دیدگی مجدد به واسطه‌ی انتشار ویروس بسیار بالاست. با اجرای این برنامه‌ها، علاوه بر این‌که از شیوع و گسترده‌شدن بیشتر خسارت نسبت به شخص بزه‌دیده جلوگیری می‌شود، از بزه‌دیده‌شدن دیگران هم پیش‌گیری می‌شود.

استفاده از برنامه‌های فیلترینگ هم شیوه‌ی مناسبی برای جلوگیری از بزه‌دیدگی مجدد است؛ برای مثال، شخصی که به واسطه‌ی یک نامه‌ی الکترونیکی اعم از ناشناس یا شناخته شده، بزه‌دیده واقع می‌شود، با اعمال دستور فیلترینگ و عدم دریافت مجدد نامه‌ی الکترونیکی از آن ایمیل در پست الکترونیکی خود، می‌تواند از بزه‌دیدگی مجددِ خود، جلوگیری نماید.

گفتار دوم: اتخاذپذیری اصول راهبردی پیش‌گیری از جرم در قبال جرایم رایانه‌ای

به منظور تدابیر امنیتی پیشگیرانه، مطابق با رهنمود پیش‌گیری از جرم سازمان ملل، نظارت و رهبری دولت در پیش‌گیری از جرایم رایانه‌ای، همراه‌کردن نهادهای غیردولتی در فرآیند پیش‌گیری، ادغام پیش‌گیری با توسعه‌ی اجتماعی- سیاسی و اتکاء به برنامه‌های بلندمدت، تخصیص بودجه‌ی مناسب و ارزیابی مستمر برنامه‌ها، اتخاذ راهبردهای علمی و دانش میان‌رشته‌ای برای پیش‌گیری از جرایم رایانه‌ای، رعایت حقوق و آزادی‌های فردی در برنامه‌های پیش‌گیری، توجه به همکاری‌های بین‌المللی در خصوص برنامه‌های پیش‌گیری، توجه برنامه‌های پیش‌گیری به اقشار آسیب‌پذیر، کاملاً ضروری است. در ذیل،

بـه تفصیل دربـاره‌ی هر یک از اصـول راهبردی رهنمـود پیش‌گیری از جرم سازمان ملل مطابق با جرایم رایانه‌ای، پرداخته می‌شود.

بند اول: نظارت و رهبری دولت در پیش‌گیری از جرایم رایانه‌ای

مدیریت و نظارت مقتدرانه‌ی دولت بر محیط سایبر، گام نخست برای پیش‌گیری از جرایم رایانه‌ای است؛ علاوه بر این‌که هیچ نهاد یا سازمان بین‌المللی مشخصی بـر فضـای مجازی، حکومت و کنترل ندارد، قابلیت کنترل و نظارت بر آن نیز دشـوار است؛ زیرا محیط شبکه و سایبر، یک محیط عرضی است و نه طولی، و افراد مختلف که در گوشه و کنار دنیا با هم ارتباط دارند، به یک اندازه در این فضای مجازی، صاحب حق هسـتند؛ هم‌چنین نظارت بر این ارتباطات از جهت فنّی نیز دشوار است.

تمامـی سـطوح دولت، مسـئولیت دارند زمینـه‌ای را فراهم آورنـد که تمامی نهادهای دولتی و مدنی، از جمله بخش خصوصی، نقش خود را در پیش‌گیری از جرم ایفا کنند. ارکان دولت نه تنها در ایجاد این زمینه‌ها مسئول‌اند، بلکه وظیفه‌ی حفظ و پیشبرد این وظیفه را نیز بر عهده دارد (جوان جعفری، ۱۳۹۱: ۸۱).

مـاده‌ی ۷ رهنمود پیش‌گیری از جرم در خصوص نقش دولت در پیش‌گیری از جـرم اعـلام می‌دارد: توسـعه‌ی راهبردهـای کارآمد و انسـانی در خصوص پیش‌گیـری از جـرم، قبل از هر چیز مرهون مشـارکت فعال و مدیریت تمامی ارکان دولت در برنامه‌های پیش‌گیری اسـت. نقش دولت در مدیریت برنامه‌ها خلاصـه نمی‌شـود، بلکـه دولت در اجـرای پیاده‌سـازی و ارزیابـی برنامه‌های پیش‌گیری نیز نقش اساسی دارد (جوان جعفری،۱۳۹۱: ۲۸۶-۲۷۳).

بـا توجه به رهنمـود پیش‌گیری از جـرم، به طور مشـخص، نقش دولت در پیش‌گیری از جرایم رایانه‌ای را می‌توان شامل موارد ذیل دانست:

۱. استقرار نهاد مرکزی پیش‌گیری از جرم رایانه‌ای؛
۲. برنامه‌ریزی برای پیش‌گیری از جرایم رایانه‌ای با اهداف و اولویت‌بندی‌های مشخص؛
۳. تخصیص بودجه مناسب جهت پیش‌گیری از جرایم رایانه‌ای؛
۴. نظارت و ارزیابی مستمر برنامه‌های پیشگیری از جرایم رایانه‌ای.

بند دوم: همراه کردن نهادهای غیر دولتی در فرآیند پیش‌گیری

بـه دلیل پیچیدگـی و تخصصی بودن جرایم رایانه‌ای و در همان حال سـهولت ارتـکاب ایـن جرایم، پیش‌گیـری هرچه بهتـر از آن‌ها در گروی مشـارکت مسـئولانه و همراه‌شـدن نهادهای غیردولتی با دولـت در فرآیند پیش‌گیری از جرم اسـت. شـرکت‌های تولیدکننـده و واردکننده سـخت‌افزارهای رایانه‌ای، شـرکت‌های مخابراتـی، توزیع‌کننـدگان کلی و جزئی نرم‌افزار، شـرکت‌های دسترسـی به خدمـات اتحادیه‌ها و اصناف مرتبط، کافی‌نت‌ها، آموزشـگاه‌های رایانـه و کلیه‌ی افـراد و نهادهای مرتبط بـا فعالیت‌های رایانـه‌ای می‌توانند به طور مسـتقیم در امر پیش‌گیری از جرم مشـارکت کنند و دولت موظف است بـا برنامه‌ریـزی صحیح، همه‌ی ایـن نهادهـا را در فرآیند پیش‌گیـری به نحو مسـئولانه‌ای درگیر کند. ماده‌ی ۹ رهنمود پیش‌گیری از جرم سـازمان ملل در ایـن خصوص مقرر مـی‌دارد: در برنامه‌های پیش‌گیری، بـا توجه به تنوع علل ایجاد جرم، مشـارکت تمامی افـراد و نهادهایی کـه در زمینه‌ی پیش‌گیری از جرم، دارای مهارت و مسـئولیت هسـتند، امری اجتناب‌ناپذیر است، و به‌همین دلیـل برنامه‌های پیش‌گیری را نمی‌توان در یک وزارت‌خانه محدود سـاخت و وزارت‌خانه‌های مختلف، مقامات، نهادهای محلی، سـازمان‌های غیردولتی، تجار و شهروندان، همه و همه باید با همکاری یکدیگر، برنامه‌های پیش‌گیری را به اجرا درآورند (جوان‌جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

بنـد سـوم: ادغـام پیش‌گیـری بـا توسـعه‌ی اجتماعـی- سیاسـی و اتـکاء بـه برنامه‌های بلندمدت

برای پیش‌گیری مناسـب از جرایـم رایانه‌ای، باید انواع شـیوه‌های پیش‌گیری را بـه کار بسـت؛ زیرا جرایم رایانـه‌ای از ویژگی‌هایـی برخوردارند که اتخاذ تدابیـر پیشـگیرانه وضعـی را تا حـد زیادی خنثـی می‌کننـد (جلالی‌فراهانی، ۱۳۸۳: ۱۰۳). در کنـار پیش‌گیـری وضعی، اتخاذ انـواع دیگر پیش‌گیری که با برنامه‌های اجتماعی، فرهنگی، آموزشـی و اقتصادی ادغام می‌شوند، ضروری اسـت. یکی از این روش‌های شناخته‌شـده، پیش‌گیری اجتماعی اسـت. در این روش، پیش‌گیری از جرم در برنامه‌های اقتصادی و اجتماعی هم‌چون آموزش، اشـتغال، فقر و ... لحاظ می‌شـود. از طرفی، با توجه به این‌که طیف وسـیعی از مجرمان و بزه‌دیدگانِ جرایم رایانه‌ای را افراد خردسال و جوان تشکیل می‌دهند،

و این دو گروه مخاطبان اصلی پیش‌گیری اجتماعی محسوب می‌شوند، اتخاذ تدابیر پیش‌گیرانه‌ی بلندمدت می‌تواند مؤثر باشد (جلالی فراهانی، ۱۳۸۳: ۱۰۳). ماده‌ی ۸ رهنمود پیش‌گیری از جرم سازمان ملل در این باره مقرر می‌دارد: پیش‌گیری باید در تمامی برنامه‌های اجتماعی و اقتصادی مدنظر قرار گرفته و با آن‌ها ادغام شود. از جمله برنامه‌های اجتماعی و اقتصادی که پیش‌گیری باید در آن‌ها مدنظر واقع شود، می‌توان به برنامه‌های مربوط به اشتغال، آموزش، بهداشت، مسکن، برنامه‌ریزی شهری، فقر و مستضعفان شهری اشاره کرد. در این میان، برنامه‌هایی که گروه‌ها، خانواده‌ها، کودکان و جوانان در معرض خطر را هدف می‌گیرند، از بُعد پیش‌گیری بسیار حائز اهمیت‌اند (جوان جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

بند چهارم: تخصیص بودجه‌ی مناسب و ارزیابی مستمّر برنامه‌ها

هر کشوری در خصوص نحوه‌ی تخصیص بودجه برای برنامه‌های پیشگیرانه، رویه‌ی خاص خود را در پیش گرفته است. برخی بودجه را به مناطق هدف اختصاص می‌دهند و برخی بدون توجه به منطقه، مشکل خاصی را هدف می‌گیرند (جلالی فراهانی، ۱۳۹۱: ۹۳). در خصوص جرایم رایانه‌ای، پیش‌گیری هنگامی می‌تواند مؤثر باشد که بودجه و منابع کافی به طور خاص در اختیار نهادهای پیش‌گیری‌کننده از این نوع جرم قرار گیرد. نحوه‌ی هزینه‌شدن بودجه‌ها باید به شکل مناسبی طبق اولویت‌های مقابله با جرایم رایانه‌ای مشخص شود. تعیین دستوری و انعطاف‌ناپذیر نحوه‌ی مصرف بودجه، کارایی برنامه‌های پیش‌گیری را کاهش می‌دهد؛ بنابراین نحوه‌ی مصرف بودجه باید ضمن رعایت اولویت‌های مقابله با جرایم رایانه‌ای به شکل انعطاف‌پذیری دست متولیان و مجریان پیش‌گیری را باز بگذارد. ارزیابی مستمر برنامه‌ها و سنجش فاصله‌ی دستیابی به اهداف مشخص‌شده به مناسب‌ترشدن تخصیص بودجه، کمک می‌کند. در ماده‌ی ۱۰ رهنمود پیش‌گیری از جرم آمده است: برای حفظ ثبات در برنامه‌های پیش‌گیری، ضروری است که منابع، از جمله بودجه‌ی کافی برای زیرساخت‌ها و اقدامات موجود باشد؛ هم‌چنین مسئولان برنامه‌های پیش‌گیری باید در خصوص نحوه‌ی هزینه‌شدن بودجه‌های اختصاصی، چگونگی اجرا و ارزیابی برنامه‌ها و میزان دسترسی به اهداف برنامه، پاسخگو باشند (جوان‌جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

بند پنجم: اتخاذ راهبردهای علمی و میان‌رشته‌ای برای پیش‌گیری از جرایم رایانه‌ای

جرایم رایانه‌ای در فضا و بستری ارتکاب می‌یابند که امکان شناسایی و مقابله با آن‌ها بسیار دشوار است و از این لحاظ نسبت به نظایر فیزیکی‌شان از رقم سیاه بالاتری برخوردارند (جلالی فراهانی۱۳۸۳: ۱۱۸). رهنمود پیش‌گیری از جرم، تأکید می‌کند که برای شناخت وضعیت فعلی جرایم و راه حل‌های پیش‌گیری از آن‌ها، از دانش و اطلاعات مناسب استفاده شود (جوان‌جعفری،۱۳۹۱: ۱۲۴). برخلاف جرایم سنتی، علل و عوامل جرایم سایبری و طرق ارتکاب آن‌ها مختلف است؛ مثلاً جرم سرقت سنّتی به چند شیوه از قبیل کیف‌قاپی، سرقت مسلّحانه از بانک، سرقت ساده و... ارتکاب می‌یابد، و متناسب با این شیوه‌ها، قانونگذار اقدام به جرم‌انگاری انواع مختلف سرقت در قانون مجازات اسلامی نموده است؛ اما در جرایم رایانه‌ای، علاوه بر طرق مختلف ارتکاب یک جرم، گاهی با جرایم جدیدی روبرو می‌شویم که حتی شناخت مفهومیِ این جرایم برای حقوق‌دانان و قضات، دشوار می‌نمایاند. این امر، ناشی از سرعَت بالای پیشرفت فناوری و تکنولوژی اطلاعات و ارتباطات است.

شاید بتوان گفت به دلیل سرعت بالای این پیشرفت، قانون‌گذار همیشه یک گام عقب‌تر از فناوری است، و پس از قربانی‌شدن شهروندان بسیاری توسط مجرمان باهوش رایانه‌ای، به پیش‌گیری و یا جرم‌انگاری می‌پردازد (سلیمی، ۱۳۹۱: ۷)؛ از این‌رو، ضروری است که علوم مختلف را در شناسایی این جرایم و مرتکبان و بزه‌دیدگان آن به کار گیریم و با یک مبنای علمی دقیق، به مقابله با وقوع این جرایم بپردازیم.

ماده‌ی ۱۱ رهنمود پیش‌گیری از جرم، بر اتخاذ راهبردهای علمی و میان‌رشته‌ای برای پیش‌گیری از جرم تأکید دارد. این ماده مقرر می‌دارد: راهبردها، سیاست‌ها، برنامه‌ها و اقدامات پیش‌گیری از جرم قبل از هرچیز باید بر پایه‌ی تحقیقات علمی و دانش میان‌رشته‌ای در خصوص علل جرم و راهکارهای قطعی و احتمالی معضل جرم بنا شود (جوان‌جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

بند ششم: رعایت حقوق و آزادی‌های فردی در برنامه‌های پیش‌گیری

در قسمتی از رهنمود عملی پیش‌گیری از جرم سازمان ملل با عنوان

همکاری‌های بین‌المللی آمده است: دولت‌های عضو سازمان ملل در چارچوب همکاری بین‌المللی در زمینه‌ی پیش‌گیری از جرم، به رعایت اصول اسناد بین‌المللی مربوط به حقوق بشر و پیش‌گیری از جرم، دعوت شده‌اند. اسناد مذکور عبارت‌اند: کنوانسیون حقوق کودک، اعلامیه‌ی ریشه‌کن‌سازی خشونت علیه زنان، اصول راهبردی سازمان ملل برای پیش‌گیری از بزهکاری نوجوانان (اصول راهبردی ریاض) و..... (جوان‌جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

مهم‌ترین مشکل قانونی که پیش‌گیری وضعی- و شاید انواع پیش‌گیری - با آن مواجه است، بحث به خطر افتادن حریم خصوصی افراد در فضای تبادل اطلاعات است. حریم خصوصی یا آن‌چه از آن به عنوان حق تنها ماندن یاد می‌شود، برای اولین با توسط دو نویسنده‌ی مشهور به نام‌های ساموئل وارن و لوئیس براندیس، مطرح شد (جلالی‌فراهانی، ۱۳۸۴: ۱۱۳). در تعریف حریم خصوصی در فضای مجازی گفته‌اند: تمام فضاهای غیراشتراکی یا اشتراکی محدود که حاوی فایل‌های شخصی هستند، حریم خصوصی فرد در فضای سایبر محسوب می‌شوند و دسترسی غیرقانونی یا بدون رضایت صاحب آن، نقض این حریم محسوب خواهد شد (یزدانی زنور، ۱۳۸۸: ۱۴۵). کنوانسیون جرایم رایانه‌ای در ماده‌ی ۵۱ خود با عنوان شروط و تضمین‌ها، دولت‌های عضو را موظف کرده هنگام وضع قوانین و مقررات مطابق این کنوانسیون، حقوق و آزادی‌های فردیِ از جمله رعایت حریم خصوصی افراد را مطابق قوانین و مقررات بین‌المللی، دقیقاً رعایت کنند. در بخشی از این ماده آمده است: اعضا باید اطمینان دهند که .... حمایت شایسته‌ای از حقوق و آزادی‌های بشری به عمل می‌آورند که شامل حقوق برخاسته از تعهداتی است که آن‌ها در کنوانسیون شورای اروپا راجع به حمایت از حقوق و آزادی‌های اساسی بشر (۱۹۵۰). و سایر اسناد لازم‌الاجرای حقوق بشری پذیرفته‌اند (جلالی فراهانی، ۱۳۸۴: ۵۸).

در ماده‌ی ۲۱ رهنمود پیش‌گیری از جرم سازمان ملل بر رعایت قانون و آن دسته از حقوق بشر که در اسناد مختلف به رسمیت شناخته شده، تأکید شده است. به موجب این ماده: در تمام اجزای برنامه‌های پیش‌گیری از جرم، باید حاکمیت قانون و رعایت آن دسته از حقوق بشر که در اسناد بین‌المللی مختلف به رسمیت شناخته شده، در نظر گرفته شود. برنامه‌های پیش‌گیری باید بتواند به تقویت فرهنگ قانون‌گرایی در جامعه کمک کند (جوان‌جعفری، ۱۳۹۱: -۲۷۳

۲۸۶). بدیـن ترتیب، برنامه‌های پیش‌گیـری از جرایم رایانه‌ای باید به حقوق و آزادی‌های فردی احترام گذاشته و حریم خصوصی افراد را کاملاً رعایت کنند و موجبات نقض غرض را فراهم ننمایند.

بند هفتم: توجه به همکاری‌های بین‌المللی در خصوص برنامه‌های پیش‌گیری

در بخشـی از رهنمود عملی پیش‌گیری از جـرم زیر عنوان همکاری فنّی آمده اسـت: دولت‌های عضو و سازمان‌های بین‌المللی مسئول تامین بودجه‌ی مربوط، باید به منظور اجرایی کردن اصول ناظر بر تأمین امنیت گروهی و پیش‌گیری از جرم در سطح ملی و منطقه‌ای، زمینه‌ی همکاری مالی و فنی در خصوص تقویت ظرفیت‌ها، ساختارها و آموزش را با کشورهای در حال توسعه، گروه‌ها و سایر سـازمان‌های ذیربط فراهم کنند» (جوان‌جعفـری، ۱۳۹۱: ۲۸۶-۲۷۳). همکاری فنّـی در خصوص جرایـم رایانه‌ای، بیش از سـایر جرایم ضـرورت دارد؛ زیرا فضای سـایبر، فارغ از مرزهای جغرافیایی عمل می‌کند و محدود به چهارچوب خطوطی که دولت‌مردان در طراحی نقشـه‌های سیاسـی رسـم می‌کنند، نیست؛ هم‌چنین، این فضا از هیچ محدودیت مکانی تبعیت نمی‌کند. فضای مجازی یک گسـتره‌ی بدون مرز اسـت که نمی‌توان در برابر آن خطوط مقسّـم کشید یا با مرزهای طبیعی یا مصنوعی، آن را تکه‌تکه و جدا سـاخت (فضلی، ۱۳۸۹: ۶۶). این ویژگی باعث می‌شـود به تعداد یکایک کاربران اینترنت سرتاسـر جهان، مجرم بالقّوه وجود داشته باشد؛ زیرا هریک از آن‌ها توانایی امکان ارتکاب جرم را به همان اندازه که در کشـور خود دارد در کشـورهای دیگر نیز داراسـت؛ برای مثال می‌توان به این وقایع که جنبه‌ی فرامرزی بودن سـایبر را بهتر نشـان می‌دهد، اشاره کرد: یک ایمیل تهدیدآمیز دایر بر تهدید به بمب‌گذاری در یک فروشگاه مواد غذایی در لتونی دریافت شد. پس از بررسی‌های فراوان، مشخص شـد که مرتکب، سـاکن استونی است و با اسـتفاده از امکانات و فضای سایبر اقدامات خود را عملی می‌کرده اسـت. یا در قضیه‌ای دیگر، فردی ناشـناس از طریق ایمیل تهدیدآمیز، مقرّ ستاد پلیس نروژ را تهدید به بمب‌گذاری کرد. در پیگیری ماجرا، فرد مرتکب، شناسایی نشد، اما با استمداد پلیس نروژ از اینترپل، دولت کانادا دریافت که آن شخص در این کشور ثبت دامنه کرده و از خطوط آن کشـور بهره می‌برد. در حالی که اینترپل انتظار داشـت آن شـخص ساکن کانادا باشـد، پس از بررسی‌های فراوان مشخص شد که مرتکب ساکن نروژ و

در همان خیابان محل مقر ستاد پلیس نروژ بوده است (شیرزاد، ۱۳۸۸: ۳۰-۲۹).

ویژگی فرامرزی بودن جرایم سایبری، ضرورت همکاری بین‌المللی برای پیش‌گیری هرچه بهتر از جرایم رایانه‌ای را آشکار می‌کند. جرایم رایانه‌ای در همه‌ی کشورها وجود دارد، و حتی ممکن است به یک مسئله‌ی بین‌المللی یا فراملی تبدیل شود؛ بنابراین کشورها می‌توانند با همکاری مشترک، از تجارب یکدیگر بهره گیرند. کاربرد رایانه در بیشتر زمینه‌های زندگی و ظهور شبکه‌های بین‌المللی، داده‌های تحقیقاتی را که در آن‌ها میان مسائل داخلی و بین‌المللی تفکیک نشده، به بایگانی‌های گذشته منتقل کرده و آن‌ها را از اعتبار انداخته است (زیبر، ۱۳۹۰: ۷۴).

در کنار اسناد بین‌المللی هم‌چون کنوانسیون جرایم رایانه‌ای مصوب ۱۰۰۲، سازمان ملل نیز با انتشار متون و نشریات مختلف، در راستای پیش‌گیری از جرایم رایانه‌ای و مبارزه با آن‌ها، اقدامات بسزایی را انجام داده که از جمله‌ی این نشریات می‌توان به نشریه‌ی سیاست جناییِ سازمان ملل در زمینه‌ی جرایم رایانه‌ای اشاره کرد. اگرچه مطالب مندرج در این نشریه جنبه‌ی الزام‌آور به خود نمی‌گیرد، اما در هر حال، در راستای اتّخاذ سیاست‌های لازم برای زدودن این پدیده‌ی نوین بزه‌کاری، ایده‌های جدیدی به کشورها داده و مساعدت‌های شایسته‌ای به آن‌ها کرده است (رضوی، ۱۳۸۶: ۱۲۸)؛ البته باید گفت، برخی از این مصادیق، نظیر فحشای جهانی و قاچاق کودکان، از حدود یک‌صد سال پیش و قبل از تشکیل جامعه‌ی ملل و سازمان ملل متحد، مورد توجه دولت‌ها بوده، و حتی اسنادی هم به منظور مبارزه‌ی کیفری مؤثر با آن‌ها تدوین شده است. در رویکرد جدید به این حوزه، موانع و مقتضیات ناشی از بزه‌دیدگی کودکان در عصر جهانی‌شدن و جلوه‌های نوین این نوع بزه‌دیدگی، مورد توجه قرار گرفته است (زینالی، ۱۳۸۸: ۲۸۳). ارتباط مستقیمی بین بسیاری از جرایم رایانه‌ای و جرایم بین‌المللی وجود دارد. بسیاری از مجرمان، جرایم سازمان‌یافته‌ی بین‌المللی استفاده از ابزار رایانه و شبکه‌ی جهانی اینترنت، اقدام به جرائم سازمان‌یافته‌ای چون پول‌شویی، قاچاق انسان، و.....، می‌کنند و از تسهیلات فناوری اطلاعات و ارتباطات، برای ارتکاب جرایم سازمان‌یافته، بهره‌برداری می‌کنند (Keenan، 2006: 514).

در همین راستا، ماده‌ی ۳۱ رهنمود پیش‌گیری از جرم با تأکید بر توجه

بـه ارتباط میان جرایم محلی و جرایم سـازمان‌یافته‌ی بین‌المللی اشـعار می‌دارد: راهبردهـا و برنامه‌هـای ملّی پیش‌گیری از جرم برای تشـخیص و برنامه‌ریزی، درصـورت لـزوم باید بـه ارتباط میـان جرایم محلـی و جرایم سـازمان‌یافته‌ی بین‌المللی، توجه کند (جوان‌جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

بند هشتم: توجه برنامه‌های پیش‌گیری به اقشار آسیب‌پذیر

یکـی دیگر از ویژگی‌های جرایم رایانه‌ای که هشـداری جـدّی برای جوامع امروزی است، روبه‌رو شدن با دسته‌ی بزرگی از مجرمان نوجوان و جوان است، که گاه به سنّ مسئولیت کیفری نرسیده‌اند. به همین دلیل در کنار تقسیم بندی مرتکبان به مجرمان یقه‌سـفید و یقه‌آبی توسـط سـاترلند، از دسته‌ی جدیدی از بزهکاران نوجوان جرایم رایانه‌ای با عنوان «مجرمان شـلوارکوتاه» نام می‌برند. از سـوی دیگر، مطابق با آمار بین‌المللی نیز اکثر کاربران اینترنت را جوانان و نوجوانان تشکیل می‌دهند که نمودار زیر، موّید مطلب است.[۱]

بـه همیـن جهت، از میـان همه‌ی گروه‌های سـنی، جوان‌ترهـا، به‌ویژه آن‌ها که سـاعت‌ها جلوی رایانه به سـر می‌برند، بیشتر آسـیب‌پذیرند؛ زیرا جوان‌ها و نوجوانان، خودشان را در این محیط‌ها، بیشتر فاش می‌کنند (Olson، 2005: 3).

از سوی دیگر، فارغ از این‌که زنان بیشتر بزه‌دیده می‌شوند یا مردان، جنسیت می‌تواند عاملی باشـد که احتمال بزه‌دیدگی افراد نسـبت به برخی جرایم را بالا ببـرد (نجابتـی، ۱۳۷۹: ۳۵). در میان جرایم سـایبری، جرایم ویژه‌ای به چشـم می‌خـورد کـه بزه‌دیده‌ی آن تنها زنان و کودکان هسـتند. ایـن جرایم، عموماً داخل در آن‌چه که امروز از آن با عنوان صنعت مقاربت جنسـی یاد می‌شـود، قرار می‌گیرند. صنعت مقاربت جنسی از ماهیّت متخلّفانه‌ی محتوای هرزه‌نگاری زنـان و کودکان بهره می‌گیرد، و مواردی را که در گذشـته فقط در بازی‌های کثیـف و فرعی هرزه‌نگاری یافت می‌شـد، پذیرفتنی می‌سـازد (زینالی ۱۳۸۸: ۲۸۵). نگران‌کننده‌تریـن موضـوع در مـورد تمام این اطلاعات این اسـت که صنعت مقاربت جنسـی، نه تنها تجارت بزرگی محسـوب می‌شود، بلکه فروش

۱. توک، محمد، کاظم‌پور، ابراهیم، دگرگونی‌های اجتماعی در یک جامعه ی اطلاعاتی، ۱۳۸۴، تهران، انتشارات کمیسیون ملّی یونسکو.

محصولات آن، هرزه‌نگاری، خودفروشی و توریسم جنسی، اکثراً به زنان و کودکان مربوط می‌شود (زینالی ۱۳۸۸: ۲۸۵). ماده‌ی ۴۱ رهنمود پیش‌گیری از جرم در این خصوص مقرر می‌دارد: راهبردهای پیش‌گیری از جرم در صورت لزوم، باید به تفاوت نیازهای زن و مرد توجه داشته نموده و به نیازهای خاص طبقه‌ی آسیب‌پذیر، توجه ویژه مبذول کنند (جوان‌جعفری، ۱۳۹۱: ۲۸۶-۲۷۳).

■ نتیجه‌گیری

ضرورت پیش‌گیری از جرایم رایانه‌ای جهت خطر مضاعف این جرایم نسبت به جرایم سنتی، اهمیتی دوچندان دارد. برای پیش‌گیری همه‌جانبه از جرایم رایانه‌ای و به اقتضای بین‌المللی بودن، می‌بایست براساس رویکردها، اصول و مبانی یک سند پذیرفته‌شده‌ی بین‌المللی در زمینه‌ی پیش‌گیری از جرم اقدام نمود. بر این اساس، سند پیش‌گیری از جرم سازمان ملل متحد مصوب سال ۲۰۰۲، می‌تواند به منزله‌ی یک سند راهبردیِ پیشگیرانه از جرایم رایانه‌ای در دستور کار حقوق‌دانان و متصدیان مربوطه قرَار گیرد.

براساس رهنمود پیش‌گیری از جرم سازمان ملل متحد، دو رویکرد متفاوت برای پیش‌گیری از جرایم، یعنی رویکرد مبتنی بر توسعه‌ی اجتماعی و رویکرد مبتنی بر موقعیت‌های جرم‌زا و هشت اصل راهبردی پیش‌گیری از جرم وجود دارد. با ملاحظه‌ی این دو رویکرد و هشت اصل راهبردی مذکور و تطبیق این رویکردها و اصول با پیش‌گیری از جرایم رایانه‌ای، می‌توان به نتایج زیر دست یافت:

۱. تأکید این سند ارزشمند بر تقویت عوامل حمایتی و استفاده‌ی بهینه از راهبردهای حساس‌سازی مردم و به ویژه اهمیت آموزش برای پیش‌گیری از جرم، به خوبی قابلیتِ اِعمال و به کارگیری برای پیش‌گیری از جرایم رایانه‌ای را دارست.

۲. مقوله‌ی آموزش که در رهنمود عملی پیش‌گیری از جرم بر آن تأکید شده، است، امری است که به چند شکل به پیش‌گیری از جرایم رایانه‌ای کمک می‌کند.

۳. آن‌چه که به عنوان پیش‌گیری مبتنی بر موقعیت‌های جرم‌زا، در رهنمود پیش‌گیری از جرم سازمان ملل آمده، علاوه بر اتخاذ تدابیر پیش‌گیری وضعی به معنای خاص، شامل ارتقای شیوه‌های مراقبتی- نظارتی و راهبردهای پیش‌گیری از بزه‌دیدگی مجدّد هم می‌شود.

۴. در رهنمود پیش‌گیری از جرم، مسئله‌ی نظارت برای پیش‌گیری از وقوع جرم، مسلّم فرض شده و بر ارتقای شیوه‌های نظارتی، تأکید شده است. 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.

۵. متصدیان پیش‌گیری از جرایم سایبری و مسئولان نظارت بر محیط مجازی، باید مطابق با رهنمود پیش‌گیری از جرم، علاوه بر ارتقای شیوه‌های مراقبتی- نظارتیِ مناسب، به امر خطیر حریم خصوصی کاربران رایانه و فضاهای مجازی، کاملاً توجه نموده و نباید با تجاوز به حریم خصوصی افراد، موجبات نقض غرض را فراهم نمایند.

۶. ممکن است با به کارگیری تدابیر و روش‌های پیش‌گیری وضعی در فضای سایبر، شاهد برخی اختلالات هم‌چون کاهش سرعت شبکه، بسته‌شدن اشتباهی برخی از سایت‌ها و وبلاگ‌ها به جهت فیلترینگ، محدودیت‌های بی‌جهت برای ورود به برخی فضاهای مجازی، اعمال محدودیت در دسترسی به شبکه‌های بین‌المللی و... باشیم. رعایت شرط اول رهنمود پیش‌گیری از جرم، یعنی عدم ورود آسیب به قابلیت و بدنه‌ی محیط اجتماعی در تقابل با همین تبعات منفی پیش‌گیری وضع شده است.

۷. در رهنمود پیش‌گیری از جرم، به عنوان دومین شرط پیش‌گیری وضعی، بر عدم محدودیت برای دسترسی آزاد به مکان‌های عمومی تأکید شده است. نتیجه‌ی اعمال این رهنمود، چیزی جز اتخاذ رویکردی سنجیده و ملایم نسبت به ممنوعیت کامل شبکه‌های اجتماعی مجازی، مسئله‌ی فیلترینگ و افزایش دقت و هوشمندی سامانه‌های فیلترکننده برای اجتناب از اشتباه در فیلترینگ نمی‌باشد.

۸. در رهنمود پیش‌گیری از جرم سازمان ملل، بر اجرای راهبردهای پیش‌گیری از بزه‌دیدگی مجدد، تأکید شده است. امکان وقوع بزه‌دیدگی مجدد برای جرایم رایانه‌ای به‌دلیل گم‌نامی و بی‌چهرگی مجرمان، وجود قربانیان کم‌سن و آسیب‌پذیرتر، سهولت ارتکاب جرم و درهم‌تنیدگی ارتباط بزه‌دیده و بزهکار رایانه‌ای، بیشتر می‌نماید.

۹. در رهنمود پیش‌گیری از جرم سازمان ملل بر مدیریت و نظارت مقتدرانه‌ی

دولت بر محیط، تأکید شـده اسـت. با توجه به ویژگی‌های فضای سـایبر، باید مدیریت و نظارت دولت، نقش ویژه‌ای پیدا کند.

۱۰. مطابـق بـا رهنمود پیش‌گیری از جرم و به جهـت پیچیدگی و تخصّصی بودن جرایم رایانه‌ای و در همان حال سـهولت ارتکاب این جرایم، پیش‌گیری هرچـه بهتـر از آن‌ها در گروی مشـارکت مسـئولانه و همراه شـدن نهادهای غیردولتی با دولت، در فرآیند پیش‌گیری از جرم است.

۱۱. بـرای حفظ ثبـات در برنامه‌هـای پیش‌گیری، ضروری اسـت که منابع از جمله بودجه‌ی کافی برای زیرسـاخت‌ها و اقدامات، موجود باشـد؛ هم‌چنین مسـئولانِ برنامه‌های پیش‌گیری باید در خصوص نحوه‌ی هزینه‌شدن بودجه‌های اختصاصی، چگونگی اجرا و ارزیابی برنامه‌ها و میزان دسترسی به اهداف برنامه، پاسخگو باشند.

۱۲. ضـروری اسـت که علوم مختلف را در شناسـایی ایـن جرایم و مجرم و بزه‌دیده‌ی جرایم رایانه‌ای به کار گیریم و با یک مبنای علمی دقیق به مقابله با وقوع جرایم مزبور بپردازیم.

۱۳. برنامه‌های پیش‌گیری از جرایم رایانه‌ای می‌بایست به حقوق و آزادی‌های فردی احترام گذاشته و حریم خصوصی افراد را کاملاً رعایت کنند.

۱۴. همکاری فنی در خصوص جرایم رایانه‌ای بیش از سـایر جرایم ضرورت دارد؛ زیرا فضای سایبر و اینترنت، فارغ از مرزهای جغرافیایی عمل می‌کند.

۱۵. در جرایم سـایبری، بیش از جرایم سـنتی، با پدیده‌ی بزهکاری کودکان و نوجوانان و بزه‌دیده‌شـدن کودکان و زنان روبه‌رو هستیم؛ بنابراین لازم است برنامه‌های پیش‌گیری از جرایم رایانه‌ای و جلوگیری از وارد شـدن آسیب های ناشی از آن به این قشر آسیب‌پذیر توجه ویژه داشته باشند.

■ منابع

ابراهیمـی، شـهرام.(۱۳۹۱). جرم‌شناسـی پیش‌گیـری (چـاپ دوم). تهران: انتشارات میزان.

آلبرتس، دیوید و پاپ، دانیل.(۱۳۸۵).گزیده‌ای از عصر اطلاعات الزامات امنیت ملی در عصر اطلاعات (چاپ نخست) (ترجمه‌ی علی علی‌آبادی و رضا نخجوانی). تهران: پژوهشکده‌ی مطالعات راهبردی.

آیکاو، دیوید جی.(۱۳۸۳). راه‌های پیش‌گیری و مقابله با جرایم رایانه‌ای(چاپ اول)،(ترجمه‌ی: اکبر استرکی و محمدصادق روزبهانی و تورج ریحانی و راحله الیاسی). تهران: معاونت پژوهش دانشگاه علوم انتظامی.

جلالی‌فراهانی، امیرحسین.(۱۳۸۳). پیش‌گیری از جرایم رایانه‌ای.مجله‌ی حقوقی دادگستری. شماره‌ی ۴۷، ۱۲۰-۸۷

ـــــــــــــــــــــــــــ . (۱۳۸۴). پیش‌گیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر. مجله‌ی فقه و حقوق.۱۶۲- ۱۳۳.

ـــــــــــــــــــــــــــ.(۱۳۸۹).کنوانسیون جرایم سایبر و پروتکل الحاقی آن . تهران: انتشارات خرسندی.

جوان‌جعفری، عبدالرضا و سیدزاده‌ثانی، مهدی.(۱۳۹۱). رهنمودهای عملی پیش‌گیری از جرم (چاپ اول). معاونت پیش‌گیری از وقوع جرم قوه‌ی قضاییه. تهران: انتشارات میزان.

خالقی پوستچی، علی.(۱۳۸۸). پیش‌گیری از جرایم سایبری با بهره‌گیری از فناوری اطلاعات و ارتباطات. مقاله‌های همایش ملی علمی- کاربردی پیش‌گیری از جرم (قوه قضاییه، مشهد مقدس)(چاپ نخست). تهران: بنیاد حقوقی میزان.

گاتن، ویلیام.(۱۳۸۴). دگرگونی‌های اجتماعی در جامعه اطلاعاتی (چاپ نخست) (ترجمه‌ی محمد توکل و ابراهیم کاظمی‌پور) تهران:کمیسیون ملی یونسکو.

رضوی، محمد.(۱۳۸۶). جرایم سایبری و نقش پلیس در پیش‌گیری از این جرایم و کشف آن‌ها. فصل‌نامه‌ی دانش انتظامی. سال نهم. شماره‌ی اول.۱۴۰- ۱۲۰.

زینالی، امیرحمزه.(۱۳۸۸). حمایت کیفری از کودکان در برابر هرزه‌نگاری

از واکنش‌های جهانی تا پاسخ‌های نظام‌های کیفری ملی (چاپ نخست). حقوق فناوری اطلاعات و ارتباطات (مجموعه مقالات). گرامی‌داشت مرحوم دزیانی، گردآوری امیرحسین جلالی فراهانی. تهران: انتشارات روزنامه‌ی رسمی.

سلیمی، احسان. (۱۳۹۱). خطر مضاعف جرایم رایانه‌ای. مجموعه مقالات اولین کنگره‌ی فضای مجازی و آسیب‌های اجتماعی نوپدید. تهران.

شیرزاد، کامران. (۱۳۸۸).جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل (چاپ نخست). تهران: نشر بهینه.

صفاری، علی. مبانی نظری پیش‌گیری وضعی از جرم(۱۳۸۰). مجله‌ی تحقیقات حقوقی دانشگاه شهید بهشتی. شماره‌ی ۳۴-۳۳، ۳۲۲ - ۲۶۷.

فضلی، مهدی.(۱۳۸۹). مسؤلیت کیفری در فضای سایبر (چاپ نخست). تهران: انتشارات خرسندی.

ملزوماتی، الهام و یاری، علیرضا.(۱۳۸۴). امنیت مرکز خدمات اینترنت(چاپ نخست)(مجموعه مقالات همایش نقش مراکز داده در توسعه‌ی فناوری اطلاعات و ارتباطات). تهران: دبیرخانه‌ی شورای عالی اطلاع‌رسانی.

نجابتی، مهدی.(۱۳۷۹). نقش طراحی واحدهای مسکونی در پیش‌گیری از جرم. مجله‌ی امنیت. سال چهارم، شماره۱۵ و ۱۶.

نجفی ابرندآبادی، علی‌حسین.(۱۳۷۸).پیش‌گیری از بزهکاری و پلیس محلی. مجله‌ی تحقیقات حقوقی. شماره‌ی ۲۵ و ۲۶، ۱۵۰- ۱۲۹.

ـــــــــــــــــــــــــ .(۱۳۸۲). پیش‌گیری عادلانه از جرم(چاپ نخست). مجموعه مقالات در تجلیل استاد محمد آشوری. تهران: انتشارات سمت.

وایدنگ,۱۳۷۹ به نقل از رضوی، محمد.(۱۳۸۶). جرایم سایبری و نقش پلیس در پیش‌گیری از این جرایم و کشف آن‌ها. فصل‌نامه‌ی دانش انتظامی. سال نهم. شماره‌ی اول، ۱۴۰- ۱۲۰.

ویلیامز، ماتیو.(۱۳۹۱). بزهکاری مجازی، بزه، انحراف و مقررات‌گذاری

برخط (چاپ نخســت) (ترجمه‌ی امیرحســین جلالی‌فراهانی و محبوبه منفرد). تهران: نشر میزان.

الهی‌منش، محمدرضا و سدره‌نشــین، ابوالفضل.(۱۳۹۱). محشای قانون جرایم رایانه‌ای(چاپ اول). تهران: انتشارات مجد.

یزدانی زنور، هرمز.(۱۳۸۸). حریم خصوصی در فضای سایبر. (حقوق فناوری اطلاعات و ارتباطات؛ مجموعه مقالات). گرامیداشت مرحوم دزیانی.گردآوری امیرحسین جلالی‌فراهانی.

زیبــر، اولریش. (۱۳۹۰). جرایم یارانــه ای. (ترجمه‌ی محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی). تهران: گنج دانش

Cusson، Maurice, (2002).la criminology، parise، Hachette، coll، les fondamentaux.

Keenan، Patrick James, (2006), the New Deterrence: Crime and Policy in the Age of Globalization, Iowa Law Review، Vol. 91، p. 505. Available at SSRN: http://ssrn.com/abstract

Olson, k، robin، cpcu, cris, (2005) ، ARM and ARP، identity theft: a person risk management approach، cpcu journal، vol.58، no.10

The guidelines for the prevention of crime, (2002) ، council resolution