فصلنامه بین المللی قانون یار
License Number: ۷۸۸٦٤ Article Cod: ۲۰۲۰S۳D۱۲SH۱M ISSN-P: ۲٥۳۸-۳۷۰۱

پیشگیری از جرایم سایبری و محدودیت های حاکم بر آن

(تاریخ دریافت ۱۳۹۸/۰۵/۲۵، تاریخ تصویب ۱۳۹۸/۱۲/۱۵)

دکتر سید عباس جزایری [۱]
استادیار دانشگاه آزاد شهرکرد
دکتر میثم نعمت اللهی
استادیار دانشگاه آزاد شهرکرد
دکتر امین امیریان فارسانی
دکتری حقوق کیفری و جرم شناسی

چکیده

امروز با پا گذاشتن در هزاره سوم میلادی فناوری های نوین اطلاعات و ارتباطات به نحوه شگفت آوری وارد ساختار زندگی انسانها شده است که تجلی آن فضای تبادل اطلاعات (فضای سایبر) است .بی تردید به موازات گسترش فعالیت ها و ارتباطات در فضای سایبر ، بخشی از بزهکاران نیز فعالیت های مجرمانه خود را به فضای سایبر منتقل کرده اند یا از رهگذر چنین فضایی مرتکب جرم یا جرائمی می شوند.از این رو با توجه به افزایش آمار جرایم و استفاده از شیوه های نوین در ارتکاب جرایم سایبری و عدم کارایی واکنش های کیفری ،ضرورت بکارگیری اقدامات پیشگیرانه در قالب تدابیر فنی که با تغییر شرایط محیطی در صدد است از ارتکاب جرم فرد مصمم به انجام جرم ، جلوگیری کند ،در دهه های اخیر در بسیاری از کشورهای دنیا مورد توجه قرار گرفته است . البته باید متذکر شویم ،تدابیرپیشگیرانه با محدودیت های فراوانی مواجه است ، از یک طرف می توان تدابیرپیشگیرانه را به تمام زمینه ها گسترش داده واز سوی دیگر در مقابل به کار گیری این روش مرتکبین جرایم سایبر قرار دارند که می خواهند این تدابیر را خنثی کنند بعضاً هم موفق به این کار می شوند.

واژگان کلیدی: پیشگیری، جرایم سایبری، چالش ، محدودیت، اینترنت

[۱] نویسنده مسئول

بخش اول: کلیات

امروزه هیچ حوزه‌ای از تأثیر و مداخله رایانه مصون نیست و شاید گزافه نباشد که در جهان حاضر، هرکسی کار با رایانه را نیاموخته باشد، یک بیسواد نوین است. حال صحبت ما این است که چگونه و از طریق چه راههای می توان از اینگونه جرایم پیشگیری کرد وجلو انرا گرفت چون درصورت ارتکاب ان اثرات جبران ناپذیری برای مفعولین این جرم به همراه داردکه از جمله رفتن آبروی این اشخاص ودر خیلی از موارد بردن مال انها را در پی داردکه در این مقاله سعی شده راهکارهایی برای پیشگیری وپیش بینی وقوع این جرایم مطرح گردد تا بتوان از وقع آنها واثرات جبران ناپذیری که آنها دارن جلوگیری کرد چون به نظر میرسد کسانی که اقدام به ارتکاب این جرایم میکنند اشخاصی هستند که اطلاع کامل از اینترنت وکامپیوتر دارند واین جرایم هیچگاه نمیتوان با سهو وخطا اتفاق افتد. جرایم رایانه ای جرمی است وارداتی که با ورود کامپیوتر در استفاده از اینترنت در سطح گسترده در کشور رواج پیدا کرده است ورود اینترنت به کشور از سال ۱۳۷۰و آغاز شد ودر سال ۱۳۷۲ به تکامل رسد امادراین چند سال نبود قاونی مدون باعث گردید که بسیاری از مجرمین رایانه ای از زیر مجازات فرار کنند وبه جرایم خود ادامه دهند واستناد انها نیز به اصل برائت واصل قانونی بودن جرم ومجازات بود که استناد درستی هم بودبا تصویب قانون جرایم رایانه‌ای (۱۳۸۸)، مفاهیم وجرایم تازه‌ای در حقوق کیفری ایران خلق شد که هریک نیازمند بررسی‌های دقیق وکارشناسانه می‌باشدوقتی در خصوص فناوری بحث می‌شود، نمی‌توان رایانه را نادیده گرفت. رایانه هم خود بزرگ ترین فناوری عصر حاضر است و هم سایر فناوری‌های نوین یا به وسیله آن و یا بر بستر آن شکل می‌گیرند البته فناوری‌ها در کنار مزایای خود می‌توانند بسترساز سوءاستفاده‌هایی نیز باشند. به خصوص اگر این فناوری، رایانه باشد، دامنه خطرهای آن افزایش می‌یابد. حقوق کیفری نوین، امروزه با جرایم و مجرمان رایانه‌ای باشد، دامنه خطرهای آن افزایش می‌یابد. حقوق کیفری نوین، امروزه با جرایم و مجرمان رایانه‌ای طرف است. ماهیت و ویژگی این دسته از جرایم به نحوی اساسی با جرایم سنتی تفاوت دارد. امروزه، مجرمان رایانه‌ای در مکان‌هایی به غیر از نقاطی‌که آثار و نتایج اعمال آنها ظاهر می‌شود، قرار دارند. در

صورتی‌که کارایی قوانین جزایی موجود و متداول، منحصر به قلمرو خاصی است و به دلیل آنکه اجزای عنصر مادی کاملاً یا بعضاً تغییر یافته و برخی عناوین مجرمانه تازه هم به وجود آمده است، نمی‌توان مجرمان را با قوانین قبلی محاکمه کرد. امنیت، یکی از مهمترین خواسته های مردم و تامین آن از اصلی ترین وظایف دولت است.ارتکاب جرایم ، یکی از مظاهر بارز ایجاد ناامنی در جامعه است که مبارزه با آن و از آن مهمتر، پیشگیری از وقوع جرایم ، از اصلی ترین وظایف دولت ها تلقی می شود.در گذشته و متاثر از عقاید نظریه پردازان مکتب تحققی،مجرمین دارای ویژگی های روانی و جسمانی خاصی فرض می شدند که آنان را از بقیه مردم متمایز می ساخت. این گروه از انسان ها همانند بمب های ساعتی فرض می شدند که هر لحظه امکان انفجار آنان وجود داشت.در این مدل، تنها راه پیشگیری و کاهش ارتکاب جرم، مجازات، درمان و بازپروی بود تا از طریق آن، در عوامل انگیزشی مجرمین تغییری ایجاد گردد.با منسوخ شدن نظریه کنترل رفتار به وسیله ویژگی های شخصیتی ثابت در روانشناسی،مفهوم تمایلات مجرمانه در روانشناسی طرفدارانش را از دست داد.کم کم روانشناسانی چون اسکینر، بر این امر گرایش پیدا کردند که رفتار را می توان با مداخله در محیط، کنترل کرد.این تحول در روان شناسی ، جرم شناسی را نیز متاثر از خود کرد.به مرور عقاید جرمشناسان پیرو نظریه کنترل اجتماعی، طرفداران خود را از دست داد جرم شناسان از انتخاب عقلانی مجرم و سنجش سود و زیان ارتکاب جرم توسط مجرم سخن راندند.با محاسبه گر قلمداد کردن مجرمین، برنامه های پیشگیری از جرم نیز بر بالا بردن ریسک و سلب فرصت های ارتکاب جرم متمرکز گشت.پیشگیری وضعی نیز از همین تفکر ناشی شده است.

بخش دوم: چالش های مربوط به قلمرو پیشگیری وضعی

بند اول: ملاحظات حقوق بشری

حقوق بشر، مجموعه امتیازاتی است که افراد به ما هو انسان و نه به دلیل ویژگی یا موقعیت خاص دارند و این حقوق لازمه ی ذات انسان است. برخورداری از این حقوق بنیادین لازمه ی کرامت ذاتی انسان است و نقض آن به معنی نقض آزادی های بنیادین و در نهایت به معنای چشم پوشی از کرامت ذاتی بشر است. در نتیجه دولت ها موظف به رعایت این حقوق می

باشند و این حقوق فارغ از توافق دولت ها، به آنها تحمیل می گردد. لذا باید قواعد و هنجارهای حقوق بشر در زمره ی قواعد آمره ی بین المللی و هنجارهای بنیادین بین المللی تلقی نمود. پیشگیری وضعی از جرم گاه در تعارض با برخی از ارزش های حقوق بشری قرار می گیرد که به بررسی آن خواهیم پرداخت.

بند دوم: نقض حریم خصوصی و آزادی های مدنی

حریم خصوصی و آزادی های مدنی ، یکی از مهمترین حقوق فردی است که چه در اسناد بین المللی و چه در قوانین داخلی بر ضرورت حفظ و احترام به آن ، تاکید شده است. هرچند تعریف دقیقی از آن در این منابع ارایه نشده است؛ دشواری تعریف حریم خصوصی و تعیین چارچوب ماهوی و شکلی آن، موجب ارایه تعاریف و برداشت های مختلفی از این مفهوم از سوی صاحب نظران شده است.برخی برای تعریف و تبیین حریم خصوصی به وسیله متوسل شده اند و برخی دیگر به هدف.به این معنا که حریم خصوصی به عنوان یک وسیله کنترل تلقی می شود که افراد نسبت به قلمروی زندگی خصوصی خود دارند؛ یا اینکه هدف حریم خصوصی، حمایت از شخصیت و کرامت انسان می باشد. از هر زاویه ای که به این مفهوم نگریسته شود، حق بر حریم خصوصی یک اصل است که باید خدشه ناپذیر تلقی شود.اصلی که نوشته ها و آثار معنوی ، افکار و احساسات شخص را محافظت کرده و حق داشتن یک چاچوب بدون دخالت را به افراد بشر اعطا می گند تا اظهارات، گفته ها، و اعمال آنها در این چارچوب مشخص مصون از تعارض بماند و مورد حمایت قانون واقع شود.(Eoghan ,۲۰۰۱,p۲۵) اهمیت حریم خصوصی و آزادی های مدنی به اندازه ای است که در مواد ۱۲،۱۷ و ۱۸ میثاق بین المللی حقوق مدنی و سیاسی ، به آن تاکید شده است.اما برخی از اشکال پیشگیری وضعی بدون تردید محدودیت هایی را برای این حقوق اساسی، ایجاد می کند.آزادی های فردی از طریق تحدید فضاهای عمومی و پایش رفتار شهروندان از طریق کار گذاشتن دوربین های مدار بسته در مکان هایی چون پارک ها، خیابان ها ، کوچه ها و حتی در فضاهای کوچکی چون داخل یک آسانسور، به شدت مورد تعرض قرار می گیرد.توجه به این نکته نیز ضروری است که حریم خصوصی افراد در محیط های مجازی نیز از گزند تهدیدات

پیشگیری وضعی، در امان نیست.به عنوان مثال ، یکی از ابزارهای پیشگیری وضعی در جرایم سایبری استفاده از تدابیر نظارتی است.این تدابیر ، ابزارها و برنامه هایی است که بر روی سیستم ها، نصب می شوند و به وسیله آن کلیه فعالیت های شبکه ای اشخاص ، حتی ضرباتی که بر روی صفحه کلیدشان می زنند و یا نقاطی را که به وسیله ماوس بر روی آن کلیک کرده اند، را ضبط می کنند.(جلالی فراهانی، امیر حسین، ۱۳۸۴:۱۴۴)در پیشگیری وضعی، این روش ها، ابزار های بسیار موثری برای کشف جرایم سایبری است، اما تردیدی نیست که با اعمال چنین شیوه ای ، حریم خصوصی افراد در فضای مجازی، به شدت مخدوش خواهد شد.

بخش سوم: یشگیری وضعی از جرائم رایانه‌ای در ایران

با توجه به توضیحاتی که داده شد،تا حدودی ماهیت پیشگیری از جرائم رایانه‌ای و مشکلات و محدودیت‌های ناشی از آن روشن شد.به نظر می‌رسد اجرای این نوع پیشگیری در کشور ما نیز با همان دو نوع محدودیتی که مورد بررسی قرار گرفت مواجه باشد،چرا که از یک طرف،کشور ما از لحاظ فناوری اطلاعات و ارتباطات نوین به سطحی نرسیده که رأسا اقدام به تولید ابزارهای پیشگیرانه نماید و از این لحاظ به خارج از کشور وابسته است و تا به حال نیز،متحمل هزینه‌های گزافی هم شده است.از طرف دیگر،به دلیل شفاف نبودن مقررات موجود ،نحوه به کارگیری این ابزارها نیز مشخص نمی‌باشد.به گونه‌ای که مشاهده می‌شود هریک از ارائه‌دهندگان خدمات شبکه‌ای به نحو متفاوتی از آن ها استفاده می‌کنند،در حالی که دسترسی به بعضی از سایت‌های غیرمجاز از طریق بعضی از ارائه‌دهندگان خدمات به سهولت امکان‌پذیر است،بعضی دیگر به نحوی حساسیت سیستم‌های خود را بالا برده‌اند که حتی سایت‌های علمی و پژوهشی معتبر یا سایت‌های نهادهای رسمی کشورمان را نیز پالایش می‌کنند(دربیگی، ۱۳۸۰،ص۱۵) البته باید خاطرنشان ساخت که هم‌اکنون در کشور ما حرکت رو به رشدی جهت سامان بخشیدن اقدامات پیشگیرانه وضعی از جرائم رایانه‌ای در حال انجام است.به عنوان مثال،شورای عالی امنیت ملی به مدد متخصصان و کارشناسان ذی‌ربط،شورای عالی امنیت فضای تبادل اطلاعات کشوررا تشکیل داده است و به بررسی راهکارهای مقابله وضعی با این طیف از جرائم که در ابعاد خرد و کلان ارتکاب می‌یابند می‌پردازد.همچنین،از

سوی شورای عالی انقلاب فرهنگی نیز دستورالعمل‌هایی برای نحوهء ارائه خدمات به ارائه‌دهندگان خدمات شبکه‌ای ابلاغ شده است.

بخش چهارم: محدودیت‌های پیشگیری وضعی از جرائم رایانه‌ای

همان طور که اشاره شد، پیشگیری وضعی در فضای تبادل اطلاعات با محدودیت‌های بسیاری مواجه است که البته بخشی از آن ها نسبت به فضای فیزیکی هم صادق هستند.به طور کلی،این محدودیت‌ها را می‌توان در دو بخش مورد بررسی قرار داد.

بند اول: محدودیت‌های فنی

به نظر می‌رسد بزرگ‌ترین مشکلی که در زمینه پیشگیری وضعی از جرائم رایانه‌ای وجود دارد،توسعه و ارتقای فناوری،آن هم به صورت ثانیه‌شمار می‌باشد که البته بر هیچ‌کس پوشیده نیست که بخشی از این رشد و توسعه را مجرمان رایانه‌ای به عهده دارند.به کرات مشاهده می‌شود، چند روز از اجرای یک طرح فنی پیشگیرانهء وضعی نمی‌گذرد که راه‌های خنثی‌کننده آن در فضای تبادل اطلاعات در اختیار همگان قرار می‌گیرد و عملا پیشگیری وضعی مزبور کان لم یکن می‌شود. دومین محدودیت فنی که پیشگیری وضعی از جرائم رایانه‌ای با آن مواجه است،وجود ابزارها و فناوری‌هایی در فضای تبادل اطلاعات می‌بشد که این امکان را در اختیار اشخاص قرار می‌دهد که در نهایت با ناشناس ماندن و پنهان کردن محتوای فعالیت‌های خود،به بهره‌برداری از این فضا بپردازند. به عنوان مثال، محیط هایی وجود دارند که به اشخاص این امکان را می‌دهند که به صورت زنده با یکدیگر ملاقات می‌کنند و یا اطمینان از ورود اشخاص بیگانه جلوگیری کنند.بدون تردید، چنین فضاهایی برای ارتکاب اعمال مجرمانه بسیار جذاب می‌باشند و عملا می‌توان گفت با توجه به محدودیت‌های فنی و قانونی‌ای که وجود دارد،تعقیب و پیگرد فعالیت‌های مجرمانه در این فضاها با چالش‌های بسیاری مواجه است.البته این موضوع سوای از یک سری قابلیت‌ها می‌باشد که با استفاده از آنها می‌توان ماهیت بهره‌برداری خود را به گونه‌ای مشروع جلوه داد و عملا تمهیدات پیشگیرانه وضعی را دور زد یا از فناوری رمزنگاری‌استفاده و عملا محتوای فعالیت‌های خود را پنهان کرد.

بند دوم: محدودیت‌های قانونی

مهم‌ترین مشکل قانونی که پیشگیری وضعی از جرائم رایانه‌ای با آن مواجه است،بحث به خطر افتادن حریم خصوصی افراد در فضای تبادل اطلاعات است.حریم خصوصی‌یا آنچه از آن به عنوان«حق تنها ماندن»یاد می‌شود، با ظهور فناوری‌های نوینی چون تبادل الکترونیک اطلاعات،حریم خصوصی افراد در معرض تعرضات بیشتری قرار گرفت،به همین دلیل ایالات متحده با تصویب قوانینی نظیر قانون حمایت از حریم خصوصی ارتباطات الکترونیک‌صراحتا به حمایت از آن پرداخت و دولت را در تدوین تدابیر پیشگیرانه وضعی،بخصوص شنود ارتباطات الکترونیک،با محدودیت‌های بسیاری مواجه کرد. البته باید توجه داشت که لزوم پرداختن به حریم خصوصی به حوزهء بین الملل نیز کشیده شده است و از آن جمله می‌توان به قطعنامه‌های اتحادیه اروپا در لزوم رعایت حریم خصوصی افراد اشاره کرد. البته باید خاطرنشان کرد که وزارت دادگستری ایالات متحده جهت تبیین مفاهیم مذکور، در سال ۱۹۹۴ کتابچه‌ای راهنما با عنوان«تفتیش و توقیف کامپیوترها و تحصیل ادله الکترونیک در تحقیقات جنائی»منتشر کرده .نیز آن را مطابق شرایط جدید اصلاح و روزآمد کرده است. بدون تردید،حریم خصوصی یکی از ارکان اصلی پابرجا ماندن فضای تبادل اطلاعات محسوب می‌شود و اگر ذره‌ای در حمایت از آن تردید شود، به شدت در میزان بهره‌برداری از آن تأثیر نامطلوب خواهد داشت و خسارات هنگفتی به بار خواهد آمد.نمونه بارزی که می‌توان ذکر کرد،انجام عملیات بانکی از طریق شبکه‌های اطلاع‌رسانی است که حریم خصوصی در آنها از جایگاه حساسی برخوردار است و اگر خدشه‌ای به این اصل مهم در فضای ق۱۹۹۷ راجع به پردازش داده‌های شخصی و حمایت از حریم خصوصی در حوزهء ارتباطات مخابراتی و دستورالعمل ۵۸/ECپارلمان شورای اروپا به تاریخ ۱۲ ژولای ۲۰۰۲ راجع به پردازش داده‌های شخصی و حمایت از حریم خصوصی در حوزه ارتباطات الکترونیک اشاره کرد. اما مشکل بزرگ حقوقی دیگری که پیشگیری وضعی با آن مواجه است، اصل آزادی جریان اطلاعات‌و حق بهره‌برداری مشروع اشخاص از اطلاعات است.همان طور که گفته شد،پیشگیری وضعی،خصوصا در فضای تبادل اطلاعات یک پیشگیری فنی و غیرارادی محسوب می‌شود و

چنانچه به خوبی طرح‌ریزی و اجرا نشود،ممکن است علاوه بر اطلاعات غیرقانونی،از دسترسی به اطلاعات قانونی و مشروع نیز جلوگیری کند و به این ترتیب، متصدیان اجرایی این نوع پیشگیری با تخلف زیر پاگذاشتن این اصل مواجه شوند.این مشکل از این جهت نیز خودنمایی می‌کند که شبکه‌های اطلاع‌رسانی رایانه‌ای بعضا برای اینکه در معرض این‌گونه اتهامات قرار نگیرند،به طور کلی از انجام وظایف قانونی خود جهت اجرای اقدامات پیشگیرانه وضعی نیز سرباز می‌زنند و در اینجاست که لزوم وضع مقرراتی شفاف و راهگشا به خوبی احساس می‌شود. البته باید خاطرنشان کرد که اخیرا این دو معضل بزرگ حقوقی در بحث خودتقنینی شبکه‌های اطلاع‌رسانی رایانه‌ای به طور خاص مورد توجه قرار گرفته است.چرا که به موجب اختیارات قانونی که به متصدیان شبکه‌ها اعطا شده است،آن ها می‌توانند از لحاظ مدیریتی و فنی اقداماتی انجام دهند که خواسته یا ناخواسته به این دو موضوع مهم حقوقی لطمه وارد نشود.بنابراین، هدایت صحیح قانونی شبکه‌ها به وضع تدابیر مناسبی که این‌گونه چالش‌ها را برنینگیزند،از اهمیت خاصی برخوردار است. بنابراین،همان طور که ملاحظه می‌شود،از آنجا که تدابیر پیشگیرانه وضعی به طور مستقیم یا غیر مستقیم(مانند تدابیر خودتقنینی‌شبکه‌های اطلاع‌رسانی رایانه‌ای که به موجب قانون اتخاذ می‌کنندبه دولت‌ها مربوط می‌شود و این احتمال وجود دارد که آنها با مستمسک قرار دادن مبارزه با جرائم و تعقیب و پیگرد مجرمان به حریم خصوصی افراد تعرض کنند،باید با وضع قوانین جامع و کارآمد،اعمال اختیار و صلاحدید آن ها را محدود به مصرحات قانونی کرد و مستلزم سیر تشریفات قانونی دانست.

بخش پنجم: پیشگیری اجتماعی از جرایم رایانه ای

درخصوص پیشگیری از وقوع جرایم وانحراف ها ،تابه حال، به ویژه طی سه دهه اخیر، الگوها ی بسیاری براساس معیارهای گوناگون مورد آزمون قرارگرفته اند که هر یک با نواقص وکاستی هایی همراهند. امایکی ازآن ها باعنوان پیشگیری اجتماعی ووضعی چندی است توجه جرم شناسان ومتخصصان پیشگیری را به خود جلب کرده، تا حدی که در خصوص عناوین مجرمانه بسیار مهمی نظیر فساد و جنایات سازمان یافته فراملی دراسنادبین المللی کاربرد آن هامقررشده است. دراین رابطه، گروهی ازجرم شناسان معتقدند برای این که یک جرم

براساس مبانی جرم شناختی، یعنی علت شناسی جرم،محقق گردد، بایدسه عنصر بایکدیگرجمع شوند که عبارت انداز: انگیزه ، فرصت و ابزار(عالی پور، حسن، ۱۳۹۰، ص۸۵) اما بسیاری ازافراد هستندکه انگیزه های مجرمانه ومنحرفانه بسیارومتنوعی درآن ها بیدار می شودکه برای عملی ساختن آن هامترصد دستیابی به دوعنصردیگر،یعنی فرصت وابزارمناسب هستند. چنان چه یکی ازاین دوعنصرفراهم نیاید،امکان تحقق انگیزه وجود نخواهد داشت. مجموعه اقدامات جلوگیری ازدستیابی مجرمان بالقوه به فرصت وابزار ارتکاب جرم تحت شمول تدابیر پیشگیرانه وضعی ازجرم قرارمی گیرند که به مجال دیگری موکول می گردند. اماوظیفه رفع انگیزه های مجرمانه ومنحرفانه به عهده کارکردهای پیشگیرانه ای است که ازآن ها به عنوان پیشگیری اجتماعی یاد می شود

بند اول: محدودیت‌های پیشگیری اجتماعی از جرائم رایانه‌ای

یکی از نکات بسیار مهمی که باید در خصوص تدابیر پیش‌گیرانه اجتماعی مورد توجه قرار داد، این است که به لحاظ اقدامات زیربنایی و اساسی که در دستور کار قرار می‌گیرد، نمی‌توان انتظار داشت همانند تدابیر پیش‌گیرانه وضعی یا ضمانت اجراهای کیفری و غیرکیفری، در کوتاه مدت نتایج محسوس و قابل مشاهده‌ای به دست آید. البته این مسأله هیچ‌گاه از دیدگاه جرم‌شناسان و متخصصان پیش‌گیری یک نقطه‌ضعف محسوب نمی‌شود؛ زیرا این تدابیر زیربنای فکری و شخصیتی بزه‌کاران و بزه‌دیدگان بالقوه را هدف قرار می‌دهند که در صورت تحقق اهداف پیش‌بینی شده، جامعه‌ای سالم و متعهد به رعایت هنجارها و ارزش‌های پذیرفته شده به‌وجود خواهد آمد. با این حال، بیشتر مسئولان اجرایی چنین دیدگاهی را ندارند. آن‌ها می‌خواهند در کوتاه مدت آثار مقابله با جرایم را مشاهده کنند و آن را در کارنامه خود به ثبت برسانند و به همین دلیل، حاضرند هزینه‌های بیشتری در راستای اتخاذ و اجرای انواع تدابیر پیشگیرانه وضعی و ضمانت اجراهای کیفری و غیرکیفری متحمل شوند؛ اما در کوتاه مدت نتایج مقطعی به‌دست آورند. از این‌رو متأسفانه به دلیل وجود چنین تفکری، چندان به سیاست‌های پیشگیرانه اجتماعی بها داده نمی‌شود.

بند دوم: محدودیت‌های ناشی از فضای سایبر

یکی از مبهم‌ترین موانع طبیعی یا به عبارت بهتر از اجزای جدایی‌ناپذیر فضای سایبر، امکان-پذیر بودن انجام تمامی فعالیت‌های رایانه‌ای و به‌خصوص شبکه‌ای در خلوت(Privacy) است. خلوت از آن جهت که باعث می‌شود شخص به سرعت بدون مشاهده کسی یا حتی بهتر از آن، بی‌آن‌که کسی اجازه داشته باشد به حریم او تعرض کند، مطابق میل خود عمل کند و این یک مانع برای تدابیر پیشگیرانه اجتماعی محسوب می‌شود. با قبول این‌که وظیفه یا به‌عبارت بهتر رسالت اصلی تدابیر اجتماعی، نهادینه کردن عدم توجه به انگیزه‌های مجرمانه و منحرفانه درونی است، اما نباید از یاد برد که محیط نیز بر غلیان یا فروکش کردن این انگیزه‌ها تأثیر قابل توجهی دارد. در دنیای فیزیکی، بسیاری افراد حتی در جایی که تدابیر پیشگیرانه وضعی وجود ندارد تا فرصت و ابزار ارتکاب جرم را سلب کنند، باز هم به دلیل این‌که در یک محیط بیگانه به سر می‌برند و انواع احتمال‌ها از ذهن آن‌ها عبور می‌کند، کمتر انگیزه‌های درونی آنان بیدار می‌شود.(جوان جعفری،۱۳۹۱، ص۴۶) در حالی‌که فضای سایبر این امکان را فراهم آورده که در خصوصی‌ترین و ایمن‌ترین مکان، زمینه‌های ارتکاب شدیدترین ناهنجاری‌ها فراهم گردد، که اگر کسی بتواند انگیزه‌های خود را سرکوب کند و در این فضای بیکران در میان انواع فرصت‌های مغتنم مجرمانه و منحرفانه لغزشی از او سر نزند، یکی از نمونه‌های بارز خود ساخته سرکوب کننده هوای نفس خواهد بود. همین مزیت، یعنی امکان ارتکاب در حریم امن در کنار ناشناس نگه‌داشتن هویت واقعی، باعث شده بسیاری از افراد در فضای سایبر و در دنیای فیزیکی دو چهره یا شخصیت متفاوت از خود بروز دهند. این افراد، به دلایل بسیار در دنیای خارج هیچ‌گاه تمایلات منحرفانه و مجرمانه خود را بروز نمی‌دهند و نزد همگان به عنوان یک چهره معتبر و واجد احترام شناخته می‌شوند. اما زمانی که در خلوت پای رایانه می‌نشینند و به فضای سایبر وارد می‌شوند، انواع تمایلات ناهنجار آن‌ها بیدار می‌شود. نمونه‌های بسیاری مشاهده شده که برای مثال شخصی مربی برجسته یک مدرسه بوده و در طول زندگی خود هیچ خطایی از او سر نزده، اما چون که توانسته در فضای سایبر با یک شخصیت متفاوت ظاهر شود و به زعم خود شخصیت واقعی خود را از دیگران بپوشاند، تمایلات آزارگری یا آزاربینی

جنسی او(Sado-Masochism) بیدار شده و تا آن‌جا پیش رفته که در دنیای فیزیکی منجر به مرگش شده است. همان‌طور که اشاره شد،کارکرد اصلی پیشگیری اجتماعی،تربیت و آموزش است.بنابراین،اگر این خط مشی نسبت به یک مجرم یا بزه دیده بالفعل یا بالقوه کارگر نباشد،باید به دنبال طرق دیگر پیشگیری رفت.اتفاقا در جرائم رایانه‌ای نمونه‌های این چنین بسیار است.زیرا همان طور که گفته شد،کسانی که با فضای تبادل اطلاعات در ارتباط اند،از بهره هوشی نسبتا بالایی برخوردارند و در حقیقت خود می‌دانند که چه می‌کنند و اگر قبح یا خطرپذیری عملی برایشان مسجل نشود،به راحتی از انجام آنچه منجر به بزهکاری یا بزه دیدگی می‌شود،سر باز نمی‌زنند.گروه کوچکی از مجرمان که از بهره هوشی بسیار بالایی برخوردارند و تعدادشان در سراسر جهان بسیار کم است،خطرناک‌ترین و زیانبارترین جرائم رایانه‌ای را مرتکب می‌شوند و مسلم است که اتخاذ تدابیر پیشگیرانه اجتماعی نسبت به چنین اشخاصی پاسخگو نمی‌باشد،یا حتی کارمند شرکتی که به قصد انتقام یا تحصیل نامشروع منافع مادی علیه شرکت خود مرتکب جرم رایانه‌ای می‌شود،ممکن است اتخاذ چنین تدابیری نسبت به وی ثمربخش نباشد. به نظر می‌رسد مهم‌ترین عاملی که پیشگیری اجتماعی از جرائم رایانه‌ای را با شکست مواجه می‌سازد،امکان ارتکاب این‌گونه جرائم در خلوت می‌باشد.مسلما تربیت وآموزش،برای تلقین شخص به خودداری از ارتکاب جرم و نقض نکردن هنجارهاست.اما باید دید این راهکار تا چه اندازه در جلوگیری از ارتکاب جرم در خلوت اشخاص مؤثر است.بسیار دیده شده شخصیت اشخاص در دنیای فیزیکی با فضای تبادل اطلاعات نمودهای کاملا متفاوتی داشته‌اند.

نتیجه گیری

جرایم رایانه ای یکی از پدیده های نوظهوری است که گرچه برخی از جرایم آن شباهت هایی با جرایم سنتی دارد، اما تفاوت هایی در روش و ماهیت و نوع جرم دارد که از لحاظ جرم شناسی و کیفرشناسی و حقوق کیفری پژوهش های نوی را می طلبد. جرایم رایانه ای به دلیل تأثیرات ناگواری که بر جامعه اطلاعاتی و کاربران دارد، برخورد جدی تری را از سوی دولتمردان سیاسی و قضایی می طلبد. نظارت و فیلتر کردن دقیق تر و جدی تری، چه برای

جلوگیری از آسیب های امنیتی و چه آسیب های فرهنگی را می طلبد. حقوق ایران در زمینه جرایم رایانه ای گرچه تلاش های مفیدی داشته، ولی همچنان نیاز به کار و پژوهش در زمینه ابعاد مختلف آن دارد. ضمن اینکه در عرصه قانونگذاری کاستی هایی نیز وجود دارد که امید است با تصویب قانون مجازات جرایم رایانه ای که سال هاست در فراموشخانه مجلس مورد بی مهری است، گامی در این راه برداشته شود متخصصان معتقدند جرم جاسوسی رایانه‌ای، با شدت و پیچیدگی بیشتری در سطح وسیع جهانی ادامه پیدا خواهد کرد). رفته رفته جاسوسی اینترنتی به عنوان ابزاری برای حصول برتری در رقابت بی‌پایان کشورها در زمینه‌های صنعتی، اقتصادی، نظامی‌و... تبدیل خواهد شد وکشورهای بیشتری وارد صحنه کارزار رایانه‌ای می‌شوند. این جنگی است که در آن نیازی به استفاده از پیاده نظام، هواپیما جنگنده و موشک نیست. کلید موفقیت در این جنگ اطلاعات است، عوامل جاسوسی رایانه‌ای و اینترنتی نقش پیاده نظام این جنگ پسامدرن را بازی می‌کنند. در حال حاضر با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت آموزش بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرایم رایانه‌ای به‌خصوص جاسوسی رایانه ای و اینترنتی، این آموزش‌ها باید در مقاطع مختلف زمانی تکرار و روزآمد شوند. اما واقعیت این است که مبارزه و کشف اینگونه جرایم کاری بس دشوار است، چرا که به واسطه ویژگی های فضای مجازی که ظرفیت سوء استفاده از آن را بالا می برد. ویژگی هایی؛ چون بدون مرز بودن فضای مجازی، کم هزینگی و پرثمری و پایین بودن احتمال دستگیری یا مجازات، امکان وارد آوردن خسارات بالا بدون آسیب جسمانی مجرم، آسان بودن تهیه و امکانات و عوامل مورد نیاز جرم، بازتاب جهانی موفقیت، به ویژه در ملات تروریستی و مکتوم ماندن شکست، امکان هماهنگی یکدیگر در جرایم سازمان یافته، امکان جذب حامی و همکار برای ارتکاب جرم از سراسر جهان بدون حضور فیزیکی، امکان جذب منابع مالی و پولشویی آسان تر و هرگونه انجام فعالیت های مالی الکترونیکی در جهت اهداف مجرمانه و... . با توجه به پیچیدگی جرایم رایانه ای، مطالعه و پژوهش بیشتر و نیز تصویب قوانین مورد نیاز در این زمینه بسیار ضروری است در این میان، از آنجا که پیشگیری وضعی حتی در دنیای فیزیکی نیز

ماهیتی فنی دارد، در حوزهٔ جرائم سایبر به طور خاص مورد توجه قرار گرفته است. البته باید گفت این اقدام با محدودیتهای فراوانی مواجه است که می‌توان آن را از ابعاد مختلف بررسی کرد. اما به طور کلی، در عمل سه عامل مانع تحقق اهداف پیشگیری وضعی از این جرائم می‌شوند که عبارت‌اند از: ۱. مجرمان سایبر، طیف خاصی از اشخاص را تشکیل می‌دهند. گروهی از آنها که از لحاظ تخصص و مهارت در سطح بالایی قرار دارند، واقعاً خطرناک هستند و متأسفانه تدابیر پیشگیرانه در برابر آنها یارای مقاومت ندارد. بنابراین، تنها انتظاری که می‌توان داشت این است که تلاش شود از ارتکاب جرم افراد نیمه‌حرفه‌ای یا آماتور جلوگیری گردد یا زمینهٔ بزه‌دیدگی افراد کاهش یابد. ۲. متأسفانه فضای سایبر با ویژگیهای منحصر به فرد خود، فی نفسه مانع تحقق اهداف پیشگیرانهٔ وضعی است. در این فضا انواع ابزارهای ارتکاب جرائم سایبر در اختیار همگان قرار دارد و هرکس می‌تواند به فراخور تخصص و مهارت خود از آنها استفاده نماید .انتقال سریع و بسیار سادهٔ اطلاعات و تجربیات حاصل از ارتکاب جرائم سایبر نیز می‌تواند مزید بر علت محسوب شود. ۳. از آنجا که این تدابیر صبغهٔ فنی دارند، چندان قابل اتکا نیستند، زیرا چندی نمی‌گذرد که ضعفها و نحوهٔ دور زدن آنها در فضای سایبر منتشر می‌شود؛ کما اینکه در کشورمان آنان که قصد خنثی کردن فیلترهای شبکه‌ای را دارند، در عمل با مشکلی مواجه نیستند. ماهیت فضای سایبر به گونه‌ای است که پیشگیری وضعی یکی از تدابیر ناگریز و لازم‌الاجرا محسوب می‌شود. حتی در دنیای فیزیکی نیز این سخن صادق است، زیرا تنها گزینه‌ای است که می‌تواند دو ضلع مثلث جرم، یعنی فرصت و ابزار ارتکاب جرم را هدف قرار دهد. بنابراین، باید یک راه حل بینابین اتخاذ شود که به موجب آن ضوابطی که تدوین می‌گردد، بر اساس قواعد و مقررات حقوقی و همچنین ملاحظات حاکم بر فضای سایبر باشند تا علاوه بر صیانت از امنیت ملی و نظم، سلامت یا اخلاق عمومی، به دیگر موازین حقوق بشر، یعنی آزادی بیان، جریان آزاد اطلاعات و حریم خصوصی نیز خدشه‌ای وارد نگردد. بی‌تردید مراجعه به تجارب دیگر کشورها با رعایت شرایط خاص کشورمان، چنانچه بر پایهٔ دیدگاههای واقع‌گرایانهٔ حقوقی ـ فنی باشد، می‌تواند نتایج مطلوبی را پدید آورد

پیشنهادات نویسندگان

۱- از آنجاکه پلیس به عنوان ضابط دادگستری وظیفه کشف جرایم را بر عهده دارد، در کنار آموزش قضات وسایر مقدمات قضایی، آموزش پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد.

۲- مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به عنوان راهکاری سریع وکم هزینه و در عین حال مؤثر. در این روش تمامی درگاه‌های سیستم‌های رایانه‌ای از قبیل درایو CD پورت‌های USB و... از طریق سرور (شبکه) بسته شده و به این ترتیب کاربر رایانه نمی‌تواند هیچ داده و اطلاعاتی را وارد رایانه کرده و یا از آن خارج کند. در این حالت کاربر تنها به داده‌های مجازی‌که از سوی مسؤولان و به منظور انجام وظیفه روی سیستم او قرار داده شده، دسترسی خواهد داشت.

منابع و مآخذ

قرآن کریم و بعد

۱.امام خمینی، سید روح‌الله. (۱۴۲۱ق) تحریرالوسیله، تهران: مؤسسه تنظیم و نشر آثار امام‌خمینی، چاپ و نشر عروج، چاپ اول.

۲.بابازاده، قاسم. \"پیرامون کنوانسیون اروپائی جرائم کامپیوتری\" خبرنامه انفورماتیک ، شورای عالی انفورماتیک شماره ۸۱ فروردین ۸۱، ص ۳۸.

۳.بازیگر – یدالله - کلاهبرداری ، اختلاس و ارتشاء درآرای دیوان عالی کشور (تهران)، نشر حقوقدان ، ۱۳۷۶ شمسی.

۴.باستانی، برومند، \"جرائم کامپیوتری و اینترنتی\"، چاپ بهنامی، سال ۱۳۸۳ ص ۲۷

۵.برومند باستانی«جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران،۱۳۸۳

۶.بهجت، محمدتقی. (۱۴۲۸ق) استفتائات، قم: دفتر معظم‌له، چاپ اول.

۷.پیمانی – دکتر ضیاء الدین : حقوق کیفری اختصاصی جرایم علیه امنیت و آسایش عمومی نشر میزان – چاپ سوم ، ۱۳۷۷

۸.تاریخچه اینترنت، تکنولوژی و اطلاعات ، شهریور ۸۵

۹.تاریخچه پیدایش اینترنت ، وب سایت مدرسه رشد... ۲۰۰۶

۱۰.جاویدنیا ، جواد جرایم تجارت الکترونیکی انتشارات خرسندی چاپ دوم ۱۳۸۸

۱۱.جعفری لنگرودی، محمد جعفر ، ترمینولوژی حقوق–انتشارات گنج دانش – ۱۳۸۳

۱۲.جعفری، محمدتقی. (۱۴۱۹ق) رسائل فقهی، تهران: مؤسسه منشورات کرامت، چاپ اول.

۱۳.حبیب زاده – محمد جعفر : ترجمه کلاهبرداری در حقوق تطبیقی مجلهٔ قضایی و حقوقی دادگستری – زمستان ۱۳۷۵

۱۴.دکتر ابراهیم حسن بیگی "حقوق و امنیت در فضای سایبر" موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران،۱۳۸۴

۱۵.زراعت – عباس : شرح قانون مجازات اسلامی – نشر فیض ، چاپ دوم : بی تا – جلد دوم

۱۶.زندی، محمدرضا، تحقیقات مقدماتی در جرائم سایبری، تهران، انتشارات جنگل، ۱۳۸۹، چاپ اول، ۵۰

۱۷.زیبر، ارلیش، جرایم رایانهای، ترجمه محمدعلی نوری و رضا نخجوانی و مصطفی بختیار وند و احمد رحیمی مقدم، تهران: نشرگنج دانش، چاپ نخست،۳ ۱۳۸

۱۸.سازمان ملل ، \"نشریه بین المللی سیاست جنائی\" ، ترجمه دبیرخانهٔ شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور، ۱۳۷۶، ص ۱۱۸.

۱۹.سلمان زاده، محمود، «جنگ اطلاعات و امنیت» خبرنامه انفورماتیک، سازمان برنامه و بودجه کشور، شمارهٔ ۸۰ آذرودی ۱۳۸۰، ص ۲۰.

۲۰.شاملو احمدی : محمد حسین ، فرهنگ اصطلاحات و عناوین جزایی ، نشر دادیار ۱۳۸۰

۲۱.شعیبی ، شهرام – مقایسه جرم کلاهبرداری سنتی و رایانه ای در حقوق ایران ماهنامهٔ شمارهٔ ۷۶ سال سیزدهم مهر و آبان ۱۳۸۸