کارکردها و دستاوردهای پیشگیرانه وضعی قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای

سیّد محمدجعفر رضوی اصل* ـ دکتر شهرداد دارابی**

چکیده:

اجرای تدابیر پیشگیرانه وضعی در پرتو افزایش خطر ارتکاب جرم می‌تواند به‌نحو مؤثری از وقوع جرایم رایانه‌ای پیشگیری نماید. مقید به‌وسیله بودن جرایم رایانه‌ای، سبب تأثیرگذاری مضاعف این مهم نسبت به دیگر اقسام پیشگیری در حوزه سایبر شده است؛ بر این اساس بررسی تدابیر پیشگیرانه وضعی با تأکید بر افزایش خطر ارتکاب جرم در نصّ مواد قانونی برای شناخت و تقویت آن از یک سو و برطرف‌سازی نقاط ضعف آن از سوی دیگر اهمیت بسزائی پیدا می‌کند. ازآنجاکه فناوری خصوصاً در حوزه رایانه و فضای مجازی به‌صورت روزآمد درحال دگردیسی می‌باشند، بنابراین هماهنگ‌سازی قواعد و اصول قانونی با چنین سرعت تغییری، نیازمند بررسی و برنامه‌ریزی‌های دقیق‌تر نسبت به سایر حوزه‌هاست. در این نوشتار به کارکردها و دستاوردهای پیشگیرانه وضعی قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای با امعان نظر به موارد افزایش‌دهنده خطرات ارتکاب جرایم رایانه‌ای پرداخته شده است.

کلیدواژه‌ها:

پیشگیری وضعی، جرایم رایانه‌ای، افزایش خطر ارتکاب جرم، دادرسی الکترونیکی، آیین دادرسی جرایم رایانه‌ای.

مجلهٔ پژوهشهای حقوقی (فصلنامه علمی - ترویجی)، شمارهٔ ۴۰، زمستان ۱۳۹۸
صفحهٔ ۳۶۹-۳۸۷، تاریخ وصول: ۱۳۹۵/۱۲/۰۸، تاریخ پذیرش: ۱۳۹۶/۰۵/۱۴

* کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد قم، ایران
Email: Abbasrazavi47@gmail.com

** استادیار دانشگاه آزاد اسلامی، واحد قم، ایران، نویسنده مسئول
Email: Shahrdad.darabi@yahoo.com

مقدمه

از اواخر دهه ۶۰ میلادی با اختراع اینترنت، ارتباطات بین جوامع تغییر کرد و سبب به‌وجود آمدن دنیای مجازی شد که درحالِ‌حاضر کمتر کسی دیده می‌شود که با آن در ارتباط نباشد. این استفاده روزافزون از این فضا و ویژگی‌های خاص آن (نامحدود بودن، پیچیدگی و تخصصی، دسترسی آسان و ...) سبب ایجاد پدیده مجرمانه در آن شده است، به‌عنوان مثال دسترسی آسان این اجازه را به افراد می‌دهد که به‌راحتی به داده‌ها دست یابند و همچنین به‌آسانی نیز می‌توانند آنها را دستکاری کنند. این ویژگی‌ها نه‌تنها بزهکاران را بر شیوه‌های جدید ارتکاب جرم توانمند ساخته است، بلکه افرادی را که پیشتر منحرف نبودند نیز به رفتارهای مجرمانه واداشته است. بدین‌ترتیب، بخشی از زندگی اجتماعی، فرهنگی، علمی و اقتصادی انسان‌های امروزی، در اینترنت و به‌طورکلی در دنیای سایبر در جریان است و طبیعی است که دولت‌ها به فکر تأمین امنیت و نیز حفظ حقوق و آزادی‌های مدنی مردم در این دنیا باشند.[۱]

ازاین‌رو مداخله سیستم عدالت کیفری برای مقابله با جرایم رایانه‌ای در فضای سایبر بیش‌ازپیش موردنیاز است. مداخله می‌تواند به دو شیوه کیفری یا غیرکیفری باشد. اقدامات کیفری که درواقع، پاسخ و واکنش به جرم اتفاق‌افتاده است، از طریق جرم‌انگاری شکستن هنجارها، سوءاستفاده‌های جدید از فناوری یا تجدیدنظر در قوانین کیفری گذشته به‌موقع اجرا گذاشته می‌شود که سبب ارعاب‌انگیزی مؤثری درباره مجرمان بالقوه یا مکرر می‌شود تا به این ترتیب از ارتکاب جرم توسط این افراد در آینده جلوگیری به‌عمل آید؛ اما اقدامات غیرکیفری که معمولاً قبل از وقوع جرم می‌باشند یا به دیگر سخن کُنشی هستند، غالباً از دستاوردهای علم جرم‌شناسی می‌باشند که مهم‌ترین آنها پیشگیری اجتماعی[۲] و پیشگیری وضعی[۳] است.

کارکردها و دستاوردهای پیشگیرانه وضعی قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای موضوع نوشتار حاضر است؛ مع‌الوصف ازآنجاکه تدابیر و اقدامات راهبرد پیشگیری وضعی متعدد است و طرح همه آنها در این مقاله نمی‌گنجد؛ لذا صرفاً تکنیک

---

۱. ژرژ پیکا، دیباچه بر *جرم‌شناسی، از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی*، ترجمه علی‌حسین نجفی ابرندآبادی (تهران: میزان، ۱۳۹۵)، ۱۰.

2. Social Prevention
3. Situational Prevention

افزایش خطر ارتکاب جرم در این نوشتار موردبررسی قرار گرفته است. این راهبرد با سلب فرصت و ابزار ارتکاب جرم از مجرم با انگیزه درجهت مقابله با جرایم عمل می‌نماید. در ایران از سال ۱۳۷۲ که به‌طور رسمی به اینترنت جهانی پیوست، نیاز به برقراری امنیت دراین‌زمینه سبب شد که قانون جرایم رایانه‌ای در سال ۱۳۸۸ برای تعیین مصادیق استفاده مجرمانه از سامانه‌های رایانه‌ای و مخابراتی به تصویب مجلس شورای اسلامی برسد. به‌تبع تصویب آن، قانونگذار، قانون دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای را برای اجرای آن قانون تحت بخش ۹ و ۱۰ قانون آیین دادرسی کیفری ۱۳۹۴ به‌تصویب رساند. از سویی دیگر باتوجه‌به بند ۵ اصل ۱۵۶ قانون اساسی و قانون پیشگیری از وقوع جرم که پیشگیری از جرم را مطرح نموده است، وظیفه قانونگذار ایجاد مواد قانونی متناسبی است که سبب جلوگیری از ارتکاب جرایم در حدود صلاحیت آن قانون شود.

می‌توان بیان داشت که امروزه توجه قانونگذار به مباحث پیشگیرانه در متون قانونی بیش‌ازپیش شده است، ازاین‌رو افزایش خطر ارتکاب جرم در مواد متعددی در دو قانون دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای به چشم می‌خورد که با ایجاد تغییرات در اوضاع‌واحوال خاصی که انسان متعارف ممکن است در آن مرتکب جرم شود باعث جلوگیری از وقوع جرم می‌شود. منظور از ایجاد تغییر، جاذبه‌زدایی از سیبل جرم، بالا بردن هزینه، سخت کردن ارتکاب جرم و در آخر خطرناک کردن آن است. برای شناخت این‌گونه تدابیر، می‌توان از تکنیک‌های خاص پیشگیری وضعی که توسط رونالد کلارک[4]، جرم‌شناس مطرح انگلیسی، بیان شده است، استفاده نمود و آن مواردی را که قابلیت اجرا در فضای مجازی دارد با موارد مصرّح در دو قانون مذکور تطبیق نمود. استفاده از این روش به شناخت موارد پیشگیری وضعی می‌انجامد و راهکارهای مناسب جهت برخورد با جرایم رایانه‌ای را در اختیار متولیان امر پیشگیری قرار می‌دهد. از طرف دیگر این روش سبب آشنایی با نقاط ضعف چنین تدابیری خواهد شد که امکان یافتن راه‌حل جهت تقویت سیستم دادرسی مجازی و پیشگیری علیه جرایم مرتبط با آن داده‌ها را آسان می‌نماید.

بر این ابتناء پرسش اصلی آن است که مهم‌ترین جنبه تأثیرپذیری قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای از کارکرد افزایش خطر ارتکاب جرم چیست؟

و پرسش‌های فرعی نیز بدین‌شرح است که:

4. Ronald Clarke

چالش اساسی ناشی از افزایش خطر ارتکاب جرم در قوانین مذکور کدام است؟

مؤثرترین راهبرد، جهت برون‌رفت از چالش‌های افزایش خطر ارتکاب جرم چیست؟

برای پاسخ به این پرسش‌ها با رعایت روش توصیفی ـ تحلیلی در بند اول تکنیک‌های پیشگیری وضعی از جرایم با رویکرد اجرا در محیط سایبری، در بند دوم کارکرد افزایش محافظت‌ها و مراقبت‌ها در قانون دادرسی الکترونیکی و قانون آیین دادرسی جرایم رایانه‌ای و در بند سوم کاهش گمنامی در قوانین مذکور تحلیل می‌شود.

۱- تکنیک‌های پیشگیری وضعی از جرایم با رویکرد اجرا در محیط سایبری

در اواسط دهه ۹۰ میلادی با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، اصطلاح فضای مجازی یا فضای سایبر[۵] برای نسل جدیدی از ارتباطات مبتنی‌بر اینترنت به‌کار برده شد. واژه سایبر در زبان فارسی به مجاز و مجازی ترجمه شده است و مترادف لغت انگلیسی "Virtual" است؛ اما باید بیان داشت، این ترجمه گویای دقیق این واژه نیست زیرا محیط سایبر، محیطی است حقیقی و واقعی، نه دروغین و فقط به شکل مادی و ملموس احساس‌شدنی نیست و این نکته کافی نیست که به آن مجاز و مجازی اطلاق شود.[۶] واژه سایبر به‌طور مصطلح به محیط‌هایی گفته می‌شود که اساس آن برمبنای صفر و یک کار می‌کنند. درواقع سایبر علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی و رایانه‌ای بوده است.

قبل از ارائه تعریفی از جرایم رایانه‌ای باید به این نکته توجه نمود که در قانون جرایم رایانه‌ای مصوب ۱۳۸۸[۷] و اکثر اسناد بین‌المللی درزمینهٔ جرایم سایبری، جرم رایانه‌ای و جرم سایبری را مترادف هم و در یک مفهوم شناسایی نموده‌اند، در این نوشتار به تبعیت از آنان این دو واژه را هم‌معنا در نظر گرفته و منظور از جرایم سایبری همان جرایم رایانه‌ای تلقی می‌شود.

---

۵. واژه «فضای سایبر» را نخستین بار در سال ۱۹۸۴ ویلیام گیبسون نویسنده داستان‌های علمی ـ تخیلی در کتابی با عنوان نورومنسر به‌کار برد.

۶. محمدرضا زندی، *تحقیقات مقدماتی در جرایم سایبری* (تهران: انتشارات جنگل، ۱۳۸۹)، ۳۸.

۷. در قانون جرایم رایانه‌ای ایران در قالب مواد ۱ الی ۲۵ جرایم سایبری را تحت عنوان جرایم رایانه‌ای در هفت فصل احصاء نموده است؛ بنابراین ازآنجاکه این تقسیم‌بندی در قوانین داخلی لحاظ نشده است، از عبارت جرایم سایبری به‌طور عام در مفهوم جرایم رایانه‌ای استفاده می‌شود.

درخصوص تعریف جرایم رایانه‌ای می‌توان بیان داشت که تعریف دقیق و روشنی از آن وجود ندارد. بعضی از نویسندگان آن را چنین تعریف نموده‌اند: «هر فعل یا ترک فعل مجرمانه‌ای که علیه رایانه یا موضوعات مرتبط با آن صورت گرفته یا به‌واسطه رایانه محقق گردد، جرم سایبری می‌باشد.»[۸] در تعریف دیگری بیان شده که جرایم سایبری فعالیت‌هایی هستند که در آنها رایانه‌ها، تلفن‌ها و به‌طورکلی امکانات تکنولوژیک برای اهداف نامشروعی چون کلاهبرداری، سرقت، خرابکاری الکترونیکی، تجاوز به حقوق مالکیت افراد، سوءاستفاده جنسی از زنان و کودکان و شکستن و وارد شدن به سیستم‌های کامپیوتری و شبکه‌ها مورداستفاده قرار می‌گیرد.[۹] اما می‌توان به‌طور مختصر جرایم سایبری را این‌گونه تعریف نمود که جرایم سایبری به جرایمی گفته می‌شوند که در محیط غیرفیزیکی علیه فناوری اطلاعات ارتکاب می‌یابند.

در شرایطی که فضای مجازی به بخش مهمی از زندگی روزمره اغلب مردم تبدیل شده، اهمیت جرایم سایبری بیش از گذشته احساس می‌شود. جرایم سایبری با سرعت فزاینده‌ای درحال افزایش هستند و بدون کنترل به‌عنوان فعالیت‌های به‌واسطه رایانه به‌صورت غیرقانونی و نامشروع ارتکاب می‌یابند، اغلب این جرایم می‌توانند از طریق شبکه‌های الکترونیکی جهانی هدایت شوند. از سال ۱۳۸۹ تا نیمه اول سال ۱۳۹۲، آمار جرایم سایبری در ایران به‌شدت افزایش یافته است.[۱۰] این موضوع سبب اهمیت شناخت هرچه بیشتر فضای سایبری و برنامه‌ریزی جهت مقابله و پیشگیری از نوع وضعی آن است، زیرا پیشگیری اجتماعی، درخصوص جرایم سازمان‌یافته و دولتی که غالب جرایم رایانه‌ای را تشکیل می‌دهند، بی‌اثر است. ازآنجاکه پرداختن به حوزه عمل پیشگیری وضعی از جرایم رایانه‌ای درمقابل سایر انواع پیشگیری، از حوصله این نوشتار خارج است، بررسی آن را به تحقیقی دیگر موکول خواهیم نمود.

---

۸. ماتیو ویلیامز، *بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری برخط*، ترجمه امیرحسین جلالی فراهانی و محبوبه منفرد (تهران: نشر میزان، ۱۳۹۱)، ۴۸.

9. David ..... ‘‘iiiiii ii gggddddsss:: eee ellllll ll ssss ff iiiiiiii i ,, ’’’’*Marquette University, Political Science Department: Crime Law & Social Change* 34 (2003): 279.

۱۰. پلیس فتا، *مجموعه مستندات آمار جرایم فضای سایبر* (تهران: انتشارات پلیس فتا، ۱۳۹۲)، ۹۰.

۱-۱- برهم زدن معادله جرم در فضای سایبری با افزایش خطر ارتکاب جرم

روشن است در پیشگیری وضعی به انصراف رسانیدن فرد مصمم به بزهکاری در اولویت قرار می‌گیرد؛ بر این ابتناء بررسی عامل‌های وضعی ـ فنی بزهکاری یعنی وضعیت‌های پیش‌جنایی و نیز عوامل خطر جرم موجود نزد بزهکار که زمینه تحقق و فرصت‌های ارتکاب جرم و تکرار جرم را آسان‌تر می‌کند از اهمیت بسزائی برخوردار است.[۱۱] کلارک و کرنیش[۱۲]، پنج راهبرد اصلی را برای پیشگیری وضعی از جرایم پیشنهاد کردند که هرکدام از آن راهبردها به پنج راهکار تقسیم می‌شوند که در مجموع بیست و پنج[۱۳] راهکار پیشگیری وضعی را تشکیل می‌دهند. پنج راهکار اصلی عبارتند از دشواری ارتکاب جرم، افزایش خطر جرم، کاهش منافع، کاهش تحریک‌پذیری و حذف بهانه‌ها.[۱۴] تمام راهکارهای مذکور قابلیت اجرا در محیط سایبری را ندارند، دلیل آن، اختصاص بعضی از تکنیک‌ها به محیط حقیقی و عدمِ‌قابلیت تحقق در فضای مجازی می‌باشد. ازاین‌رو امکان وجود در قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای را نیز نخواهند داشت. در این تحقیق تنها مورد دوم یعنی تکنیک افزایش خطر ارتکاب جرم در قوانین مذکور بررسی خواهد شد و موارد دیگر نیازمند بررسی جداگانه است. لازم به ذکر است بعضی از مواد قوانین مذکور دارای چند تکنیک پیشگیری وضعی به‌صورت هم‌زمان هستند که ممکن است در برخی موارد مشابهت‌هایی با یکدیگر داشته باشند.

ازجمله تکنیک‌های پیشگیری وضعی کلارک، برای منصرف کردن بزهکاران از ارتکاب جرم، افزایش خطرات ملموس ارتکاب جرم است. هرچقدر خطری که از ارتکاب جرم ناشی می‌شود، زیاد باشد، بزهکاران کمتری رغبت به ارتکاب جرم پیدا می‌کنند[۱۵]؛ دلیل آن، حسابگر

---

۱۱. علی‌حسین نجفی ابرندآبادی، *درآمدی بر سیاست جنایی مدیریتی خطرمدار، کیفرشناسی نو ـ جرم‌شناسی نو* (تهران: تازه‌های علوم جنایی، ۱۳۸۸)، ۷۳۰.

12. Derek Cornish

۱۳. اولین بار تکنیک‌های پیشگیری وضعی در سال ۱۹۹۳ میلادی توسط کلارک ارائه شد و شامل دوازده تکنیک برای پیشگیری از انواع جرایم خیابانی بود. بعد از آن در سال ۱۹۹۷ میلادی کلارک و هومل (Homel) دوازده تکنیک اولیه را اصلاح نمودند و با اضافه کردن دسته جدیدی تحت عنوان «سلب توجیه‌ها» آنها را به ۱۶ تکنیک رساندند. در ادامه، انتقاداتی به تکنیک‌های کلارک وارد شد که در رأس آنها ورتلی (Wortley) قرار داشت، انتقادها سبب شد، کلارک به همراه کرنیش در سال‌های بعدی، دسته پنجمی به تکنیک‌های پیشگیری تحت عنوان «کاهش تحریک بزهکاران» اضافه کنند که مجموعاً تکنیک‌ها به ۲۵ عدد افزایش یابد.

14. Rnnll ddrrrr eeeddd Dkkkkkkkkkkkkk OOttttt ttt ti,,,, iiiii ii ttt sssssdddddii milll lDiii ii:::: :AA yyyyyyyodlll ''' ssiii tieeeefffii tttt illll liii meeeeetttt i,,, '''*London, Crime Prevention Studies* 16 (2003): 43.

۱۵. غلامرضا محمدنسل، *کّلیات پیشگیری از جرم* (تهران: نشر میزان، ۱۳۹۳)، ۱۲۷.

بودن مجرم است. کلارک برای افزایش خطر جرم پیشنهاد نمود که با اعمال تدابیر نظارتی و اتخاذ رویکردهای مراقبتی خطرات ارتکاب جرم را افزایش داده و از این طریق از جرم پیشگیری به‌عمل آید.[۱۶] برای دستیابی به این هدف دو روش را می‌توان ارائه نمود که قابلیت اجرا در محیط‌های سایبری را داشته باشند. این دو روش عبارت‌اند از: ۱- افزایش محافظت‌ها و مراقبت‌ها؛ ۲- کاهش گمنامی و ناشناختگی.

۲- افزایش محافظت‌ها[۱۷] و مراقبت‌ها[۱۸] در فضای سایبری

راهکار افزایش محافظت‌ها و مراقبت‌ها دارای تفاوت‌هایی هستند که آنها را از یکدیگر متمایز می‌نماید، اما درعین‌حال ارتباط تنگاتنگی نیز از لحاظ نظری با یکدیگر دارند[۱۹] که سبب نزدیکی مباحث این دو راهکار شده است؛ بنابراین در این قسمت به‌صورت مشترک و ذیل یک عنوان از آنها سخن به‌عمل خواهد آمد. نظریه فرصت[۲۰] در پیشگیری وضعی بر این عقیده استوار بوده است که فقدان محافظ توانا یکی از عوامل افزایش خطر ارتکاب جرم است؛ بنابراین مؤثرترین راهکار مقابله با جرایم تقویت محافظت و مراقبت (محافظ توانا) از اهداف مناسب برای ایجاد مانع درمقابل بزهکاران بالقوه می‌باشد. قرار دادن محافظ حتی درصورتی‌که مجرم اقدام به شروع عملیات اجرای جرم نموده باشد، می‌تواند مجرم را از اتمام عمل بازدارد. برای اثرگذاری بهتر محافظها از وقوع جرایم باید اشخاص بدانند که فعالیت آنان زیر نظر و تحت مراقبت قرار دارد، درغیراین‌صورت نظارت مخفیانه، فقط برای جمع‌آوری ادلّه علیه متهم و شناسایی شرکا و معاونین جرم به‌کار می‌رود و نمی‌توان اثر پیشگیرانه بر آن مترتب ساخت.[۲۱] نحوه انتخاب محافظها نیز باید کارشناسی شده و برخورد با جرایم با مطالعه قبلی توسط کنشگران متولی صورت پذیرد، درغیراین‌صورت ممکن است اثرات پیشگیرانه نداشته باشد و حتی منجر به تبعات منفی مانند هتک حریم خصوصی افراد، تحدید حقوق بنیادین و غیره بشود. برای نمونه قرار دادن نگهبان شب برای محله‌ها، می‌تواند از وقوع

16. Clarke and Cornish, op.cit. 44.
17. Growth Guardianship
18. Ovservation

۱۹. پرداختن به تفاوت‌های مذکور از حوصله این نوشتار خارج است.

۲۰. The Opportunity Theories، برای مطالعه بیشتر دراین‌زمینه نک: شهرداد دارابی، *پیشگیری از جرم در مدل مردم‌سالار سیاست جنایی* (تهران: نشر میزان، ۱۳۹۵)، ۱۳۰ به بعد.

۲۱. امیرحسین جلالی فراهانی، «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، *مجله فقه و حقوق* ۲ (۱۳۸۴): ۱۴۴.

سرقت جلوگیری نماید اما در ساعات شلوغ صبح که رفت‌وآمد افراد محله زیاد می‌شود و به‌نوعی نظارت طبیعی افراد به‌وجود می‌آید دیگر گماردن نگهبان سودمند نخواهد بود بلکه ممکن است باعث ایجاد حس فضای امنیتی در افراد و عدم‌داشتن احساس تعلق به آن محیط شود.

مراقبت‌ها و محافظت‌ها در محیط سایبری، همانند محافظت در محیط حقیقی ازجمله راهکارهایی است که از وقوع جرایم پیشگیری می‌نماید، همچنین سبب کشف سریع جرم به‌دلیل افزایش کنترل‌ها می‌شود. ازآنجاکه در قانون دادرسی الکترونیکی تمهیدات امنیتی برای افزایش محافظت‌ها به‌طورکلی بیان شده، یافتن و بررسی راهکارهای عملی آن در محیط مجازی کاری بسیار مهم است. ازاین‌رو قبل از بررسی مواد مرتبط با بحث در قانون دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای ابتدا راهکارهای عملی افزایش محافظت‌ها در فضای مجازی موردبررسی قرار می‌گیرند.

در فضای مجازی به‌کارگیری عملی محافظت‌ها بسیار شایع است. استفاده فراگیر از نرم‌افزارهای ضدویروس‌ها[۲۲] مانند کاسپراسکای[۲۳] توسط کاربران، نمونه‌ای از استفاده محافظ‌ها در برابر حملات سایبری و درنتیجه آن پیشگیری از این جرایم است. راهکارهایی مانند استفاده از پراکسی‌ها و دیواره آتشین نیز به‌عنوان محافظ در برابر جرایم سایبری عمل می‌کنند. یک راهکار بسیار مناسب برای پیشگیری وضعی از جرایم سایبری با استفاده از محافظ‌ها این است که اقدام به جداسازی و تفکیک شبکه‌های داخلی از اینترنت و فضای خارج آن انجام شود.[۲۴] این موضوع ابعاد مختلفی دارد که بعضاً در محیط فیزیکی نمایان می‌شود و بعض دیگر خاص محیط مجازی است. برای نمونه در محیط فیزیکی می‌توان با مهروموم کردن جعبه رایانه‌ها[۲۵] در ادارات و شرکت‌ها از سخت‌افزارهای سیستم‌های رایانه‌ای به‌نحو مناسب محافظت نمود. در جریان آلوده شدن نیروگاه اتمی نطنز توسط ویروس استاکس‌نت در سال ۱۳۸۷، احتمال داده شده بود که با استفاده از تغییر محل ذخیره اطلاعات (هارد)[۲۶] یک یارانه قابل‌حمل (لپ‌تاپ)[۲۷]، این ویروس به سیستم‌های آن مرکز راه یافته باشد.

22. Antiviruses
23. Kaspersky
24. Nicole gggg g eeeeeeeediii ii aannnnooo,, "Uii gggii tttt illll l iii me Prevention Theory to iiiiii ii teeeccccciisssssss sffff fff rr mtt innnttttt mnssiiiiii i,, ""*Proceedings of the 2005 soft Wares Conference, Las Vegas NV* 7 (2005): 6.
25. Case
26. Hard
27. Laptop

این نمونه به‌خوبی نشان‌دهنده اهمیت قرار دادن محافظت‌ها در محیط فیزیکی برای افزایش خطر ارتکاب جرم است.

در ادامه باید بیان داشت، درصورت پلمب بودن قسمت سخت‌افزار رایانه‌ها دیگر امکان تعویض قطعات و یا دستکاری آنها بدون نظارت محافظت‌ها وجود ندارد. هکرها راحت‌تر می‌توانند به شبکه‌هایی که از طریق امواج الکترومغناطیسی که بدون محدوده مشخصی تا بُرد معین منتشر می‌شوند، نسبت به شبکه‌های متصل کابلی (سیمی)، نفوذ کنند و خود را به‌عنوان عضویی از شبکه معرفی نمانید و اقدام به عمل غیرمجاز در آن شبکه مانند شنود یا سرقت اطلاعات درحال عبور نمایند. استفاده از ارتباط شبکه کابلی در داخل مراکزی مانند ساختمان دادگاه‌ها که با چندین سیستم به یکدیگر مرتبط هستند به‌جای استفاده از شبکه بی‌سیم (وایرلس)[۲۸] یکی دیگر از راهکارهای فیزیکی برای تفکیک شبکه‌های داخلی می‌باشد که هرگونه نفوذ به آن به دلیل وجود سرور متمرکز (محافظ توانا) به‌سرعت قابل‌شناسایی است.

راهکارهای تفکیک شبکه در فضای مجازی نیازمند فناوری و تخصص بیشتری نسبت به راهکارهای فیزیکی جداکننده شبکه‌هاست. امروزه در ایران اقدام سازنده‌ای دراین‌خصوص صورت پذیرفته و همچنان نیز ادامه دارد. افتتاح فاز اول شبکه ملی اطلاعات[۲۹] که ابتدا با نام اینترنت ملی معرفی شده بود در نیمه اول سال ۱۳۹۵ ازجمله این اقدامات است. باتوجه‌به تبصره ۲ ماده ۴۶ قانون برنامه پنجم توسعه کشور شبکه ملی اطلاعات، شبکه‌ای مبتنی بر قرارداد اینترنت (IP) به همراه سوئیچ‌ها، مسیریاب‌ها و مراکز داده‌ای است به‌صورتی که درخواست‌های دسترسی داخلی و اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شود به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی امن داخلی در آن فراهم شود. این شبکه سبب کاهش میزان نفوذپذیری و افزایش امنیت رایانه‌های کاربران ایرانی خواهد شد. وجود سرورهای مجزّا در داخل ایران، به همراه

28. Wireless

۲۹. طرح شبکه ملی اطلاعات در دهه ۱۹۹۰ میلادی در کشورهای پیشرفته در صنعت فناوری رایانه‌ای همچون انگلستان، کره جنوبی و چین برنامه‌ریزی و شروع شده است. در کشور ما از اواخر سال ۱۳۸۴ این موضوع مطرح شد. مهم‌ترین دلیل پیاده‌سازی این شبکه کاهش وابستگی به شبکه جهانی اینترنت بود که واجد بسیاری از خلأهای امنیتی و فضاهای نفوذپذیر هست. برای این پروژه در سه سال گذشته بیش از ۲۰ هزار میلیارد تومان سرمایه‌گذاری شده است. دسترسی کاربران به کلیه سایت‌های داخل کشور با سرعت بالاتر و قیمت ارزان‌تر از شبکه جهانی از مزیت‌های اقتصادی این شبکه است. طرح شبکه ملی اطلاعات بر اساس قانون برنامه پنجم توسعه و مصوبه شورای عالی فضای مجازی تا پایان سال ۱۳۹۵ باید به‌طور کامل اجرا گردد.

نظارت‌های مسئولین امنیت سایبری، خطر ارتکاب جرایم سایبری را برای بزهکاران به‌شدت افزایش می‌دهد. افزایش خطر ارتکاب جرم توسط مراقبت‌ها و توسعه محافظت‌ها این پیام را به بزهکاران بالقوه سایبری می‌رساند که درصورت انجام جرم، مشاهده، تعقیب و درنهایت دستگیر و محاکمه خواهند شد. شبکه ملی اطلاعات، مزایای دیگری نیز دارد مانند آنکه هویت تمامی کاربران در آن آشکار است که مربوط به دیگر قسمت‌های تکنیک‌های پیشگیری می‌شود. اکنون مواد مرتبط با بحث افزایش محافظت‌ها در قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای بررسی می‌شود.

۲-۱- کارکرد افزایش محافظت‌ها در قانون دادرسی الکترونیکی

قانون دادرسی الکترونیکی در ماده ۶۵۸ مقرر داشته است که: «قوه قضائیه موظف است تمهیدات فنی و قانونی لازم را برای ... تأمین امنیت داده‌های شخصی آنان، در چهارچوب اقدامات این بخش فراهم آورد.» تمهیدات پیش‌بینی‌شده در ماده منجر به‌نوعی ایجاد محافظین توانا در برابر بزهکاران سایبری می‌شود تا امنیت داده‌ها که مهم‌ترین هدف بزهکاران سایبری است از این طریق تأمین شود. با استفاده از محافظ توانا خطر ارتکاب جرم سایبری تا حد زیادی افزایش خواهد یافت و از این طریق می‌توان منجر به پیشگیری وضعی از جرایم رایانه‌ای شد.

از طریق راهکارهای مختلفی می‌توان افزایش محافظت‌ها را در چهارچوب اقدامات فنی و قانونی برای حمایت از بزه‌دیدگان سایبری منظور داشت که در مبحث قبلی به آنها پرداخته شد؛ بنابراین در این ماده قانونگذار به‌طورکلی اقدامات فنی لازم را به‌کار برده است تا از این طریق دست متولیان امر برای به‌کارگیری تدابیر مناسب مبتنی‌بر فناوری به‌روز، باز باشد. این پیش‌بینی قانونگذار یک ایراد عمده تدابیر پیشگیری وضعی از جرایم رایانه‌ای را که به‌روزرسانی آنی و لحظه‌ای فناوری در فضای سایبر است، برطرف نموده که در جای خود نمونه‌ای از قانون‌نویسی نوین را به نمایش می‌گذارد؛ زیرا بسیار پیش آمده که برای به‌کار بستن یک ترفند پیشگیرانه وضعی در محیط سایبری هزینه‌های (اعم از مادی و معنوی) گزافی صورت گرفته، اما هکرها در عرض چند ساعت راهکار خنثی‌سازی آن را به‌دست آورده‌اند. از همین رو باز گذاشتن دست متولیان اجرایی سامانه‌ها برای به‌کار بستن تدابیر امنیتی شرایط را برای پیشگیری و مقابله با جرایم رایانه‌ای بسیار هموار می‌نماید.

از طرف دیگر، ایراد مهمی که می‌توان به این ماده وارد ساخت، این است که قانونگذار در ماده ۶۵۸ تنها قوه قضائیه را مسئول اجرای تدابیر فنی و قانونی نموده. درصورتی‌که قوای دیگر ازجمله قوه مجریه (دولت به مفهوم اخص) نقش تأثیرگذارتری در به‌کارگیری و اجراسازی تدابیر فنی ایفاء می‌نماید؛ زیرا زیرساخت‌های ارتباطی و اطلاعاتی همچون مخابرات غالباً در اختیار قوه مجریه قرار دارند که زمینه اجراسازی اقدامات وضعی ـ فنی همانند فیلترینگ در حوزه صلاحیت آنهاست. ازاین‌رو برای حل این مشکل پیشنهاد می‌شود که علاوه‌بر قوه قضائیه سایر قوای حاکمیتی در امر افزایش محافظت‌ها، مشارکت فعال‌تری داشته باشند که این امر می‌تواند با ایجاد کارگروه‌های فنی مشترک بین قوا محقق گردد.

البته این موضوع در ماده ۶۴۹ قانون دادرسی الکترونیکی آمده است که شورای متشکل از اعضای مختلف سه قوه به ریاست رئیس قوه قضائیه تشکیل شود تا اجراسازی تدابیر پیش‌بینی‌شده در آن قانون ازجمله تدابیر افزایش خطر ارتکاب جرم مانند افزایش محافظت‌ها با همکاری میان آنان صورت بپذیرد. ماده ۶۴۹ قانون دادرسی الکترونیکی مقرر داشته: «به‌منظور سیاستگذاری و تدوین راهبردهای ملی، برنامه‌ریزی میان‌مدت و بلندمدت و تدوین آیین‌نامه‌های لازم برای توسعه و ارتقای دادرسی الکترونیکی و نظارت بر حسن اجرای آنها، «شورای راهبری دادرسی الکترونیکی» که در این بخش به‌اختصار شورا نامیده می‌شود به ریاست رئیس قوه قضائیه و عضویت افراد زیر تشکیل می‌شود: ...» که تا حد بسیاری نقش هماهنگ‌کننده میان قوا را ایفاء می‌کند؛ اما ماده ۶۵۸ به‌طور انحصاری این موضوع را برعهده قوه قضائیه نهاده است که این امر، راه را برای شورای دادرسی الکترونیکی مشکل می‌سازد؛ بنابراین اصلاح ماده ۶۵۸ به صواب نزدیک‌تر است.

۲-۲- کارکرد افزایش محافظت‌ها در قانون آیین دادرسی جرایم رایانه‌ای

بدیهی است، یکی از مؤثرترین راهکارهای مقابله با جرایم، تقویت محافظت‌ها و مراقبت‌ها از اهداف مناسب برای ایجاد مانع درمقابل بزهکاران بالقوه می‌باشد. بدین‌سان رهیافت کیفری غیرموقعیت‌مدار با تکیه بر عامل‌های وضعی ـ فنی بزهکاری درصدد است، از آماج آسیب‌پذیر محافظت نماید.[۳۰]

۳۰. علی‌حسین نجفی ابرندآبادی، «پیشگیری عادلانه از جرم»، *علوم جنایی مجموعه مقالات در تجلیل از استاد دکتر محمد آشوری* (۱۳۹۵)، ۵۸۱.

افزایش محافظین توانا در قانون آیین دادرسی جرایم رایانه‌ای در ماده ۶۶۹ به چشم می‌خورد. ماده مذکور بیان داشته است: «هرگاه حفظ داده‌های رایانه‌ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام قضایی می‌تواند دستور حفاظت از آنها را برای اشخاصی که به‌نحوی تحت تصرف یا کنترل دارند، صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضایی می‌توانند دستور حفاظت را صادر کنند ... تبصره ۱– حفظ داده‌ها به‌منزله ارائه یا افشای آنها نیست و مستلزم رعایت مقررات مربوط است. تبصره ۲– مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و درصورت لزوم با دستور مقام قضایی قابل‌تمدید است.»

هرچند که ماده مذکور مربوط به حفاظت از داده‌ها مرتبط با دادرسی یا تحقیق است اما ممکن است داده‌های نیازمند حفاظت، یک موقعیت پیش‌جنایی نسبت به جرایم سایبری ایجاد نمایند. منظور از موقعیت‌های پیش‌جنایی گاهی به خصوصیات درونی یا ذاتی فرد یا به موضوع جرم بازمی‌گردد؛ گاهی به شرایطی که تلاقی بین مرتکب بالقوه و فرد یا سیبل جرم را تسهیل می‌کند نیز اطلاق می‌شود؛ گاهی هم در سطح کلان به بافت و شرایط فیزیکی و اجتماعی که ارتکاب فعل را عملی می‌سازد، برمی‌گردد.[۳۱] در بعضی مواقع موقعیت پیش‌جنایی می‌تواند بعد از وقوع جرمی ایجاد شود. گاهی انجام یک عمل خلاف مقدمه‌ساز و آماده‌کننده برای ارتکاب جرمی اصلی است. این سخن با پیشگیری ثانویه و مخصوصاً پیشگیری ثالث دارای قرابت است اما با کمی دقت می‌توان میان آنها قائل به تفاوت شد. عمل خلافی که از سوی شخص بزهکار برای ارتکاب جرم دیگر انجام می‌شود یک وضعیت پیش‌جنایی را نسبت به پیشگیری از جرم اصلی شکل می‌دهد. به‌عنوان نمونه شخصی اقدام به سرقت داده‌های یک شرکت تجاری می‌نماید که با استفاده از آن داده‌ها می‌تواند اقدامات مجرمانه دیگری را پی‌ریزی نماید، بنابراین اگر نسبت به داده‌های به‌سرقت‌رفته چه در فضای مجازی و چه در فضای حقیقی تدابیر پیشگیرانه وضعی تدارک دیده شود، حتی اگر این اقدامات بعد از وقوع سرقت داده‌ها باشد باز هم اثرات پیشگیرانه بر آن مترتب خواهد بود. به دیگر سخن محسوب نمودن این قبیل اقدامات به‌عنوان پیشگیری وضعی می‌تواند وقوع بسیاری از جرایم را دشوار و با خطر همراه سازد. اقدامات انجام‌شده به‌نوعی کنترل‌کننده ابزارهای ارتکاب جرایم آتی

۳۱. منون جندلی، *درآمدی بر پیشگیری از جرم (تعاریف، تاریخچه، رویکردها، دورنما)*، ترجمه و تحقیق شهرام ابراهیمی (تهران: نشر میزان، ۱۳۹۳)، ۸۶–۸۵.

هستند و نباید آن را یک اقدام کیفری محسوب نمود، هرچند که تعیین حدود تمایز بین آنها با دشواری همراه است؛ بنابراین محسوب نمودن این قبیل اقدامات در حوزه پیشگیری وضعی به نفع و صلاح جامعه خواهد بود. توجه به این سؤال، نفع جامعه را آشکار خواهد ساخت که اگر بزهکار سایبری به هر روشی به داده‌های مهم اشخاص دستیابی نماید راهکار پیشگیری‌کننده از جرم اصلی چه خواهد بود؟ در این حالت دیگر اقدامات پیشگیرانه اجتماعی به‌دلیل مواجهه با بزهکار مصمم نتیجه‌بخش نخواهد بود و هم اینکه جرم اصلی به وقوع نپیوسته است که بتوان اقدامات و ضمانت‌اجراهای کیفری را برای متوقف‌سازی بزهکار به اجرا گذاشت. ازاین‌رو بهترین راهکار مقابله با این موقعیت پیش‌جنایی خارج کردن ابزارهای ارتکاب جرم از کنترل بزهکار بالقوه است و این امر با تدابیر پیشگیرانه وضعی محقق می‌گردد؛ بنابراین سخن پیشگیری وضعی را می‌توان همانند پیشگیری ثالث در داخل فرایند کیفری انجام داد. از این لحاظ لزوم ایجاد تدابیر پیشگیری وضعی مانند افزایش محافظت‌ها را در فرایند دادرسی بااهمیت خواهد نمود. نحوه محافظت از داده‌ها نیز با استفاده از فناوری‌های نوین به‌راحتی امکان‌پذیر است. قرار دادن داده‌های حفاظت‌شده در شبکه‌های وایرلس میزان آسیب‌پذیری آنها را افزایش می‌دهد؛ بنابراین همان‌طور که در قسمت ابتدای مبحث افزایش محافظت‌ها و مراقبت‌ها، راهکارهای مناسب فضای مجازی ارائه شد، قابلیت اجرا برای ماده ۶۶۹ را دارا می‌باشند که از توضیح بیشتر اجتناب به‌عمل می‌آوریم.

۳- کاهش گمنامی و ناشناختگی[۳۲]

کاهش گمنامی و سهولت شناسایی مرتکبان اقدامات بزهکارانه، ازجمله تدابیری هستند که خطر دستگیری پس از ارتکاب جرم را افزایش داده و از این طریق موجب انصراف بزهکاران از انجام عملیات اجرایی جرم می‌گردند.[۳۳] گمنامی هویت کاربران در فضای مجازی ازجمله مزایا و ویژگی‌های شاخص آن است که موجب تحریک بزهکاران به وقوع جرم نیز می‌شود. ناشناختگی افراد اجرای تدابیر پیشگیرانه را با دشواری همراه می‌سازد، از طرف دیگر درصورت وقوع جرم، گزارش‌دهی آن را پایین می‌آورد و کشف جرایم را با دشواری همراه می‌سازد.[۳۴]

32. Anonymity Slake

۳۳. محمدنسل، پیشین، ۱۲۸.

۳۴. جرایم سایبری ازجمله جرایمی هستند که همانند جرایم آپارتمانی از آمار سیاه بالایی برخوردارند. یکی از دلایل آن گمنامی افراد اعم از بزه‌دیده و بزهکار در محیط‌های سایبری می‌باشد.

بنابراین لزوم به‌کارگیری تدابیر وضعی برای کاهش گمنامی هویت بزهکاران در فضای مجازی دارای اهمیت خواهد بود.

اولین راهکار برای روشن نمودن اشخاص استفاده‌کننده از رایانه، روش «تصدیق (تأیید) هویت دومرحله‌ای»[۳۵] است. تأیید هویت دومرحله‌ای فرایندی است که فقط هنگامی به کاربر اجازهٔ ورود می‌دهد که کد دریافت‌شده به‌وسیله سامانه‌های ارتباطی امن مانند پیام کوتاه یا ایمیل که مستقیم از سرور برای کاربر ارسال می‌شود را وارد سیستم مربوطه کند. درواقع، تأیید هویت دومرحله‌ای، لایه امنیتی مضاعفی را برای حساب کاربران آنلاین ایجاد می‌کند که دسترسی به آن برای دیگران تقریباً غیرممکن است. امروزه بیشتر خدمات آنلاین ارائه‌شده به‌وسیله شرکت‌های مختلف، از تأیید هویت دومرحله‌ای استفاده می‌کنند. برای نمونه در ثبت‌نام از طریق سایت سازمان سنجش و دریافت کد ثبت‌نام برای آزمون‌های مشترک در سطح کشور مانند آزمون‌های استخدامی از روش تأیید هویت دومرحله‌ای استفاده می‌شود.

پالایه نمودن ورودی‌های ناشناس[۳۶] که اغلب مورداستفاده هکرها و کراکرها واقع می‌شود، راهکار دیگری است که می‌توان برای کاهش ناشناختگی از محیط‌هایی که آماج مناسب در آنجا قرار دارد، به اجرا گذاشت. به‌عنوان نمونه غالباً هکرها برای نفوذ به سیستم یک فرد ابتدا سعی می‌کنند با ابزارهایی همچون «شبکه خصوصی مجازی»[۳۷] اقدام به ناشناس نمودن پروتکل اینترنتی (IP) خود کرده و سپس اقدام به عملیات خرابکارانه در داخل سیستم شخص میزبان بنمایند. گاهی نیز با جعل پروتکل اینترنتی دیگران و استفاده از هویت جعلی به اطلاعات غیرمجاز دسترسی پیدا می‌کنند که حتی درصورت کشف نفوذ، ردیابی مجرم را دشوار می‌سازد. استفاده از پالایه‌ها منجر می‌شود افرادی که با استفاده از پروتکل‌ها، هویت خود را ناشناخته کرده‌اند، اجازه دسترسی به شبکه را نداشته باشند و این موضوع تا زمانی که از پراکسی‌های صحیح وارد شوند، ادامه خواهد داشت؛ بنابراین با سد کردن مسیر اشخاص ناشناس، مجرمین بالقوه که با استفاده از این ویژگی عمل می‌کنند را برای ارتکاب جرم با دشواری و خطر بیشتری مواجه می‌کند و هرچقدر که موانع وضعی و فنی در کاهش گمنامی افراد در دنیای مجازی موفق‌تر عمل کنند، وقوع جرایم رایانه‌ای کمتر خواهد بود.

35. Tow Factor Authentication
36. Anonymity
37. VPN

۳-۱- کارکرد کاهش گمنامی در قانون آیین دادرسی جرایم رایانه‌ای

گمنامی که از ویژگی‌های بارز فضای سایبری است، عامل اصلی جرایم رایانه‌ای نیز می‌باشد. ازاین‌رو در قانون آیین دادرسی جرایم رایانه‌ای مواد قانونی به چشم می‌خورد که هویت کاربران را در استفاده از فضای مجازی آشکار می‌سازد. نمونه این سخن ماده ۶۶۷ قانون مذکور است که مقرر داشته: «ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند. تبصره ۱- داده ترافیک، هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره ۲- اطلاعات کاربر، هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورداستفاده و مدت زمان آن، هویت، نشانی جغرافیایی یا پستی یا قرارداد اینترنت (IP)، شماره تلفن و سایر مشخصات فردی را شامل می‌شود.» این قانون ارائه‌دهندگان خدمات دسترسی را مکلف نموده تا اطلاعات کاربران را ثبت و ذخیره نمایند. این امر یک راهکار بسیار مناسب برای شناسایی هویت افراد و زیر نظر گرفتن و قابل‌ردیابی بودن اعمال آنان در فضای مجازی است. اگر با وجود گمنامی در فضای سایبر، نیات مجرمانه به شخصی رسوخ نماید، با آگاهی از اینکه اعمال و هویتش به‌راحتی قابل‌پیگیری است، از ارتکاب جرم و گذر اندیشه به عمل مجرمانه منصرف می‌شود؛ زیرا با استفاده از تدابیر وضعی ـ فنی خطر ارتکاب جرم برای بزهکار بالقوه افزایش یافته است.

همچنین ماده ۶۶۸ قانون مذکور مقرر نموده است: «ارائه‌دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره‌شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند.» این ماده نیز منجر به کشف هویت کاربران خواهد شد که این راهکار به‌نوعی پیشگیری وضعی از جرایم رایانه‌ای خواهد بود.

ایراد مهمی که این مواد از لحاظ پیشگیری وضعی دارند[۳۸] این است که زمانی کشف هویت و اعمال کاربران اثر پیشگیرانه دارد که کاربران از این موضوع آگاهی داشته باشند.

---

۳۸. از لحاظ نحوه قانون‌نویسی و اصول دادرسی، ایرادی بر این مواد وارد نخواهد بود.

امروزه اشخاص اندکی وجود دارند که از وجود چنین ماده قانونی اطلاع کافی در اختیارشان باشد. فرض آگاهی داشتن افراد از قوانین جاری کشور نیز نمی‌تواند توجیه‌کننده این ایراد باشد، زیرا هدف از وضع این قاعده موضوع دیگری است که نمی‌تواند توجیه‌کننده اثرات پیشگیرانه تدابیر وضعی قرار گیرد. عدمِاطلاع کافی کاربران در فضای مجازی از وجود چنین موادی در قانون آیین دادرسی جرایم رایانه‌ای سبب شده است این مواد درحال‌حاضر اثر پیشگیرانه وضعی کمی داشته باشند و تنها درخصوص تعقیب، مجازات مجرمان و تحصیل دلیل بر ضد مجرمین دارای اثر باشند.

برای رفع این اشکال پیشنهاد می‌شود با استفاده از تبلیغات مستمر و منظم سطح آگاهی افراد جامعه به‌خصوص قشر جوان و نوجوان نسبت به وجود چنین تدابیری افزایش یابد تا افراد به‌واسطه گمنامی تشویق به ارتکاب جرایم رایانه‌ای نشوند. آموزش مباحث حقوقی مانند این دو ماده در مدارس می‌تواند آگاهی کاربران فضای مجازی را از وجود تدابیر فنی کنترل‌کننده اعمال و هویتشان افزایش دهد. همان‌طور که امروزه واحد درسی سواد رسانه‌ای برای دوره دبیرستان تدوین شده است.

۳-۲- کارکرد کاهش گمنامی در قانون دادرسی الکترونیکی

در قانون دادرسی الکترونیکی نیز ماده قانونی وجود دارد که منجر به کاهش گمنامی می‌شود. این ماده در ارتباط میان کاربران با محاکم قضایی موجب کشف هویت طرفین شده که این راهکار سبب خواهد شد اطلاعات و داده‌های تبادل‌شده در محیط سایبری با امنیت بیشتری به حرکت دربیایند و به‌نوعی پیشگیری وضعی از داده‌های مورداستفاده در فضای سایبری و نهادهای زیرمجموعه قوه قضائیه مانند محاکم شود. ماده ۶۵۶ قانون دادرسی الکترونیکی مقرر داشته: «به‌منظور حفظ صحّت و تمامیت، اعتبار و انکارناپذیری اطلاعات مبادله‌شده میان شهروندان و محاکم قضایی، قوه قضائیه موظف است تمهیدات امنیتی مطمئن برای ...، احراز هویت و احراز اصالت را فراهم آورد. تبصره ـ قوه قضائیه موظف است مرکز صدور گواهی ریشه برای امضای الکترونیکی را جهت ایجاد ارتباطات و مبادله اطلاعات امن راه‌اندازی نماید.» تمهیدات امنیتی مورداشاره در این ماده منجر به تقویت و آشکارسازی هویت کاربرانی خواهد شد که قصد ارتباط و ارسال داده‌ها به محاکم قضایی را دارند؛ بنابراین برای پیشگیری وضعی از داده‌های افراد و جلوگیری از بزه‌دیدگی آنان، در زمان استفاده از فناوری برای ارتباط با قوه قضائیه مشخص بودن هویت کاربران بسیار می‌تواند مؤثر واقع

شود. به‌دلیل آنکه اکثر داده‌ها در سیستم قضایی دارای منفعت اعم از مالی یا غیرمالی هستند، موجبات جذب بزهکاران بالقوه به آنان فراهم می‌شود و ازآنجاکه جرمی هنوز واقع نشده که بتوان از ضمانت‌اجراهای کیفری استفاده نمود بهترین راهکار استفاده از اقدامات وضعی ـ فنی است که همانند ماده ۶۵۶ با تمهیدات ایمنی مانند استفاده از سیستم تصدیق هویت دومرحله‌ای می‌توان هویت کاربران را مشخص نمود.

گواهی ریشه (SSL)[۳۹] یکی دیگر از راهکارهای کاشف هویت کاربران و امن‌کننده ارتباطات مجازی می‌باشد که در خود ماده ۶۵۶ پیش‌بینی شده است. منظور از گواهی ریشه اطمینان حاصل کردن از امنیت شبکه می‌باشد. برای نمونه هنگام ورود به یک سایت در کنار آدرس سایت در انواع مرورگرها یک علامت قفل نمایش داده می‌شود که با کلیک بر روی قفل ظاهرشده، اطلاعات گواهی صادرشده قابل‌مشاهده خواهد بود. اطلاعات مذکور شامل نام دامنه، نام کاربر، نشانی کاربر، شهر، کشور و تاریخ صدور گواهی ریشه می‌شود. درواقع با استفاده از گواهی ریشه صاحبان داده‌ها مشخص شده و دیگر گمنامی در کار نخواهد بود. امروزه گواهی ریشه یک استاندارد فنی بین‌المللی است که توسط میلیون‌ها کاربر و شرکت در فضای سایبری برای برقراری امنیت بیشتر انتقال اطلاعات استفاده می‌شود. ازاین‌رو استفاده از این راهکار در ماده ۶۵۶ قانون دادرسی الکترونیکی برای شناسایی هویت صاحبان گواهی امضاء پیش‌بینی شده است که اثر وضعی در پیشگیری از جرایم رایانه‌ای خواهد داشت.

نتیجه

مهم‌ترین چالشی که اجرای تکنیک افزایش خطر ارتکاب جرم را در قانون دادرسی الکترونیکی و آیین دادرسی جرایم رایانه‌ای با مشکل مواجه ساخته، به‌روز شدن و روزآمدی تکنولوژی به‌صورت آنی و لحظه‌ای است. پیشرفت‌های روزافزون فناوری در حوزه اطلاعات و ارتباطات و سهولت دسترسی و تهیه تجهیزات رایانه‌ای و اتصال به شبکه جهانی اینترنت از یک سو، سطح و نوع خدمات قابل‌ارائه در محیط سایبری را ارتقاء داده است.

از سوی دیگر، تعداد کاربران فضای مجازی چه در سطح جهانی و چه در سطح ملی، افزوده شده است و در هر روز مبادلات مالی بسیاری از طریق این شبکه جهانی انجام می‌شود. در همین راستا، هرچقدر راهکارهای ارتقای امنیت سیستم‌های رایانه‌ای و وب-سایت‌ها نیز پیشرفته‌تر شوند، درمقابل، راهکارهای ارتکاب جرم نیز از پیشرفت و پیچیدگی

39. Secure Socket Layer

بیشتری برخوردار خواهند شد؛ بنابراین راهکارهای مقابله‌کننده با جرایم رایانه‌ای با تأسی از تکنیک افزایش خطر ارتکاب جرم می‌بایست همواره موردبررسی و بازنگری قرار گیرند.

ازاین‌رو مؤثرترین راهبرد، جهت برون‌رفت از چالش‌های افزایش خطر ارتکاب جرم، لزوم توجه قانونگذار به مباحث پیشگیری در زمان تدوین مقررات مرتبط با حوزه سایبر است به‌طوری‌که جوابگوی روزآمدی فناوری باشد. این امر می‌تواند امکان به‌کار بستن تدابیر دشوارکننده را بیش‌ازپیش هموار سازد و این خود منجر به توسعه بهتر تکنولوژی و فناوری و همچنین افزایش امنیت به‌طور موازی با آن پیشرفت‌ها خواهد شد. امید است متولیان امر پیشگیری، با به‌کار بستن تدابیر ذکرشده در این نوشتار، زمینه افزایش امنیت را در حوزه فعالیت قوانین مذکور به‌دست آورند.

فهرست منابع

الف) منابع فارسی

ابراهیمی، شهرام. *جرم‌شناسی پیشگیری*. جلد اول. ویرایش دوم. تهران: نشر میزان، ۱۳۹۱.

الهی‌منش، محمدرضا، ابوالفضل سدره‌نشین. *محشای قانون جرایم رایانه‌ای*. ویرایش سوم. تهران: انتشارات مجد، ۱۳۹۱.

بهرمند، حمید، حسین محمد کوره‌پز و احسان سلیمی. «راهبردهای وضعی پیشگیری از جرایم سایبری». *مجله آموزه‌های حقوق کیفری دانشگاه علوم اسلامی رضوی* ۷ (۱۳۹۳): ۱۷۶-۱۴۷.

پلیس فتا. *مجموعه مستندات آمار جرایم فضای سایبر*. ویرایش اول. تهران: انتشارات پلیس فتا، ۱۳۹۲.

پیکا، ژرژ. دیباچه بر *جرم‌شناسی، از جرم‌شناسی حقیقی تا جرم‌شناسی مجازی*. ویرایش چهارم. ترجمه علی‌حسین نجفی ابرندآبادی. تهران: میزان، ۱۳۹۵.

جلالی فراهانی، امیرحسین. «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر». *مجله فقه و حقوق* ۲ (۱۳۸۴): ۱۶۳-۱۳۳.

جندلی، منون. *درآمدی بر پیشگیری از جرم (تعاریف، تاریخچه، رویکردها، دورنما)*. ویرایش اول. ترجمه و تحقیق شهرام ابراهیمی. تهران: نشر میزان، ۱۳۹۳.

دارابی، شهرداد. *پیشگیری از جرم در مدل مردم‌سالار سیاست جنایی*. ویرایش اول. تهران: نشر میزان، ۱۳۹۵.

رزنبام، دنیس، آرتور لوریسیو و روبرت داویس. «پیشگیری وضعی از جرم». ترجمه رضا پرویزی. *مجله حقوقی دادگستری* ۳۲ (۱۳۷۹): ۱۷۲-۱۴۷.

زندی، محمدرضا. *تحقیقات مقدماتی در جرایم سایبری*. ویرایش اول. تهران: انتشارات جنگل، ۱۳۸۹.

محمدنسل، غلامرضا. *کلیات پیشگیری از جرم*. ویرایش اول. تهران: نشر میزان، ۱۳۹۳.

نجفی ابرندآبادی، علی‌حسین. «پیشگیری عادلانه از جرم». *علوم جنایی مجموعه مقالات در تجلیل از استاد دکتر محمد آشوری* (۱۳۹۵): ۵۸۹-۵۷۰.

نجفی ابرندآبادی، علی‌حسین. درآمدی بر *سیاست جنایی مدیریتی خطرمدار، کیفرشناسی نو ـ جرم‌شناسی نو*. ویرایش اول. تهران: تازه‌های علوم جنایی، ۱۳۸۸.

ویلیامز، ماتیو. *بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری برخط*. ویرایش اول. ترجمه امیرحسین جلالی فراهانی و محبوبه منفرد. تهران: نشر میزان، ۱۳۹۱.

ب) منابع انگلیسی

Clarke, Ronald, Derek Cornish. "Opportunities, Precipitators and Criminal Decisions: A Reply to Worley's Critique of Situational Crime Prevention." *London, Crime Prevention Studies* 16 (2003): 20-60.

Lang Beebe, Nicole, Srinivasan Rao. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security." *Proceedings of the 2005 Soft Wares Conference, Las Vegas NV* 7 (2005): 1-18.

Speer, David. "Redefining Borders: The Challenges of Cybercrime." *Marquette University, Political Science Department: Crime Law & Social Change* 34 (2003): 259-273.