فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال دوازدهم
شمارهٔ اول، بهار ۱۳۹۶

چالش‌های رویاروی پیشگیری موقعیت مدار از جرائم سایبری فرامرزی[۱]

تاریخ دریافت: ۱۳۹۴/۱۲/۵ تاریخ پذیرش: ۱۳۹۵/۵/۱۰

از صفحهٔ ۹ تا ۳۲

زهرا فرهادی آلاشتی[۲]، عبدالرضا جوان جعفری بجنوردی[۳]

چکیده

با گسترش ابزارهای اطلاعاتی و ارتباطاتی، شمار فراوانی از افراد به فضای سایبر دسترسی یافته و گردش آزادانهٔ اطلاعات آسان شده است. لیکن، به‌موازات تسهیل ارتباطات فرامرزی سایبری، تأمین امنیت فضای برخط و پیشگیری از بزه‌دیدگی احتمالی کاربران اهمیتی دوچندان یافته و هرگونه خللی در این امر، منجر به خسارات کلان خواهد شد. ماهیت فرامرزی غالب جرائم سایبری سبب می‌شود که کاربست تدابیر پیشگیرانهٔ موقعیت مدار فرامرزی یا شناسایی موقعیت‌های پیش جنایی و پیشگیری فوری از آن‌ها، نیازمند همکاری کشورهای درگیر در قضیه باشد. لیکن؛ عدم تبعیت همگان از معیار قانونی هماهنگ (و نه یکسان)، قوانین متشتّت سایبری و شکاف‌های علمی و فنی موجود بین طرفین درگیر در قضیه، فرآیند پیشگیری را با چالش‌های اساسی مواجه می‌سازد. بنابراین، هرگونه موفقیت در این فرآیند، در گام نخست نیازمند آشنایی با خلأهای علمی و فنی رویاروی پیشگیری از این جرائم و سپس، تدوین راه بردهای علمی و عملی برای رفع آن‌ها است. در اثر پیشرو، به این نتیجه رسیده‌ایم که چالش‌های حقوقی و پلیسی به‌عنوان مهم‌ترین چالش‌های پیشگیری از جرائم فرامرزی به‌حساب می‌آیند. از همین رو، بر آن هستیم تا با استفاده از روش توصیفی- تحلیلی و با رجوع به اسناد منطقه‌ای و بین‌المللی، جایگاه فعلی جامعهٔ جهانی در زمینهٔ پیشگیری از جرائم سایبری فرامرزی و چالش‌های موجود را مورد ارزیابی قرار دهیم و سپس راهکارهای پیشنهادی برای غلبه بر آن‌ها را ارائه دهیم.

کلیدواژه‌ها: جرائم سایبری، فرامرزی، پیشگیری موقعیت مدار، چالش‌ها، پناهگاه امن داده، چالش‌های پلیسی.

استناد: فرهادی آلاشتی، زهرا و جوان جعفری بجنوردی، عبدالرضا (بهار ۱۳۹۶). چالش‌های رویاروی پیشگیری موقعیت مدار از جرائم سایبری فرامرزی. *فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی*. ۱۲(۴۵)، صص ۳۲-۹ .

---

۱. این مقاله مستخرج از پایان‌نامهٔ کارشناسی ارشد دانش‌آموخته تحت عنوان «چالش‌های رویاروی پیشگیری موقعیت مدار از جرائم سایبری» که در سال ۹۴ در دانشکدهٔ علوم اداری و اقتصادی دانشگاه فردوسی مشهد انجام شده است.

۲. کارشناس ارشد حقوق جزا و جرم‌شناسی دانشگاه فردوسی مشهد، z.farhadialashti@gmail.com

۳. دانشیار حقوق جزا و جرم‌شناسی دانشگاه فردوسی مشهد، نویسندهٔ مسئول: javan-j@um.ac.ir

مقدمه

سرعت بی حدّ و حصر نفوذ اینترنت به زندگی بشر سبب شده است که جوامع از حالت ارتباطات درون‌مرزی عبور کنند و فارغ از مرزها، با یکدیگر در ارتباط باشند. استفاده کاربران از خدماتی همچون بانکداری مجازی، خرید برخط و مواردی ازاین‌دست اگرچه که کیفیت زندگی آن‌ها را افزایش داده است، لیکن؛ بزهکاران نیز در این شاه‌راه‌های ارتباطی، در جستجوی آماج احتمالی خود هستند.

امروزه بزهکاران با استفاده از دستگاه‌های مرتبط به اینترنت، می‌توانند در سرتاسر کره خاکی آماج موردنظر خود را هزاران کیلومتر دورتر از کشور خود شناسایی کرده و آنان را هدف قرار دهند. از همین رو، غالب جرائم سایبری واجد خصیصهٔ فرامرزی[1] هستند. چراکه؛ عموماً مرتکب (یا مرتکبان) و بزه‌دیده (یا بزه‌دیدگان) متعلّق به کشورهای مختلف بوده یا در صورت تعلق به یک کشور، قسمتی از جرم در کشور ثالثی واقع شده است. بنابراین، تأمین امنیت این فضا، نیازمند همکاری‌های فرا منطقه‌ای بوده و سیاست جنایی هماهنگی را می‌طلبد.

یکی از علل عمدهٔ تأمین امنیت این فضا و پیشگیری از موقعیت‌های احتمالی پیش جنایی، خسارات کلانی است که از عدم پیشگیری از این موقعیت‌ها ناشی می‌شود و سرعت بالای انتقال اطلاعات در این فضا برشمار بزه‌دیدگان می‌افزاید و فرآیند پیشگیری را با چالش‌های بیشتری مواجه می‌سازد. همچنین، لازم به ذکر است که در جرائم سنتی فرامرزی «وجود مرزهای بین‌المللی و شیوه‌های کنترل متعارف مانند ایست و بازرسی و استفاده از ابزارهای الکترونیکی، ارتکاب بزه در ورای مرزها را با موانع جدی مواجه ساخته است» (جوان جعفری، ۱۳۸۹، ص ۱۷۸). درحالی‌که؛ مفهوم مادی مرز در جرائم سایبری صدق نکرده و یکی از ویژگی‌های مهم جرائم سایبری بدون مرز بودن[2] آن است و همین امر، پیشگیری را دشوارتر می‌کند.

در کنار چالش‌های یادشده که ناشی از ماهیت فضای سایبر می‌باشند، دسته‌ای دیگر از چالش‌ها نیز به علّت نوظهور بودن این جرائم ایجاد شده‌اند که مهم‌ترین آن‌ها کمبود قوانین مرتبط با پیشگیری از جرائم سایبری در بعد فرا منطقه‌ای است. به‌عبارت‌دیگر،

1.Transnational
2.Borderless

مداخله و مشارکت چندین کشور در فرآیند پیشگیری از جرم که هرکدام قوانین خاص خود را داشته و چه‌بسا وابسته به نظام‌های حقوقی متفاوتی نیز باشند، همکاری بین‌المللی برای پیشگیری از جرائم سایبری را با مشکلات متعددی مواجه می‌کند. به‌موازات این چالش، در برخی از موارد، نیروهای مسئول پیشگیری از بزه، سطح دانش یکسانی نداشته یا به فنّاوری‌های نوین پیشگیری از بزه دسترسی نداشته و نمی‌توانند درخواست‌های طرف مقابل برای پیشگیری از موقعیت‌های پیش جنایی را فراهم آورند. در این نوشتار بر آن هستیم در ابتدا به بررسی زوایای چالش‌های حقوقی و پلیسی یادشده بپردازیم و سپس پیشنهادها و راه‌حل‌های مناسب برای غلبه بر این چالش‌ها را معرفی کنیم.

اگرچه که تحقیقات بسیاری پیرامون چالش‌های فراروی پیشگیری موقعیت مدار از جرائم سنّتی صورت گرفته است. لیکن، بررسی انحصاری چالش‌های ناشی از پیشگیری موقعیت مدار از جرائم سایبری، بسیار کمتر مورد توجّه قرارگرفته و غالباً در کنار سایر چالش‌ها به آن‌ها اشاره شده است.

صبح خیز (۱۳۹۴) در مقالهٔ خود با عنوان «چالش‌های حقوقی جرائم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران»، قسمتی از مباحث خود را به چالش‌های موجود در نظام بین‌المللی برای مبارزه با جرائم سایبری اختصاص داده و بر این عقیده است که حقوق جزای سنتی نتوانسته هم سو با تحولات سریع جرائم سایبری، حرکت کند و در بسیاری از موارد، عناوین مجرمانهٔ جدیدی که تهدیدکنندهٔ امنیت بین‌المللی هستند، همچنان جرم‌انگاری نشده‌اند و قابل برخورد کیفری نمی‌باشند. نگارندگان اثر پیشرو نیز در قسمت نخست این نوشتار، بر آن هستند که با نگاهی آسیب شناسانه زوایای چالش‌های حقوقی موجود در جریان پیشگیری موقعیت مدار از جرائم سایبری فرامرزی را بررسی کنند و راه‌حل‌هایی را برای رفع این چالش ارائه دهند.

دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد در سال ۲۰۱۳ طرح پژوهشی را با عنوان «بررسی جامع جرائم سایبری» انجام داده است و با استفاده از مطالعات میدانی، به ارزیابی مانع و مشکلات موجود در میان ۶۹ کشور پرداخته و اذعان داشته است که در هر دو بعد داخلی و بین‌المللی موانع قانونی و اجرایی فراوانی برای مبارزه با جرائم سایبری وجود دارد. در این اثر، با استفاده از آمارهای پژوهش یادشده که جدیدترین و جامع‌ترین آمار موجود در این حیطه تا به امروز است، تأثیرات حرکت کُند جامعهٔ جهانی برای

زدودن این نواقص در فرآیند پیشگیری موقعیت مدار از جرائم سایبری را مورد ارزیابی قرار خواهیم داد. همچنین، مقیمی (۱۳۹۵) در قسمتی از رسالهٔ دکتری خود با عنوان «سیاست‌ها و تدابیر سازمان ملل متحد برای پیشگیری از جرم سایبری»به بررسی خط‌مشی‌ها و راهکارهای سازمان ملل متحد برای پیشگیری موقعیت مدار از این جرائم پرداخته‌اند. نویسنده در این اثر با دقّت فراوان، اسناد الزامی و ارشادی سازمان ملل متحد را که در طول زمان برای هماهنگ‌سازی قوانین و ارائه معیاری هماهنگ برای پیشگیری از جرائم سایبری موجود است را مورد بررسی و ارزیابی قرار داده‌اند. در قسمت نخست مقاله پیشرو نیز، چالش‌های ناشی از فقدان معیاری هماهنگ و نه واحد که ناشی از عدم تبعیت از دستورهای الزامی یا ارشادی سازمان ملل و سایر نهادهای منطقه‌ای و بین‌المللی است را ارزیابی خواهیم کرد.

علی‌رغم گذشت چند دهه از ورود فضای سایبر به زندگی بشر و استفاده روزافزون از آن، هنوز هم اجماعی بر ارائه تعریفی واحد از جرائمی که در این فضا ارتکاب می‌یابند، وجود ندارد و دکترین و نهادهای داخلی و بین‌المللی حقوقی، تعاریف متعدّدی از این جرائم ارائه می‌دهند. مروری اجمالی بر سیر تحول جرائم سایبری، درک ماهیت آن‌ها را آسان‌تر می‌کند.

از دههٔ ۶۰ تا اواخر دههٔ ۸۰ میلادی، نسل نخست جرائم سایبری[1] ظهور پیدا کردند. در این برهه، بزهکاران رایانه‌های کاربران را به‌عنوان سیبل و هدف بزه برمی‌گزیدند و از آن به‌عنوان ابزاری برای ارتکاب جرائم سنّتی همچون کلاهبرداری و سوءاستفاده‌های مالی استفاده می‌کردند. نسل دوم جرائم سایبری،[2] از دههٔ ۸۰ آغاز و تا اواخر دههٔ ۹۰ ادامه داشت. ویژگی غالب این نسل را می‌توان در رابط بودن بین جرائم نسل اوّل و سوم دانست. چراکه «پیش از آنکه به‌عنوان یک نسل از جرائم با ویژگی‌های خاص مورد توجه قرار گیرد، پل ارتباطی میان نسل اول و سوم بوده است. دلیل بارز آن‌هم عمر بسیار کوتاه این نسل است که به‌سرعت با ظهور نسل سوم منتفی شد» (جلالی فراهانی (الف)،۱۳۸۴، ص ۱۴۰). در این نسل، جرائم علیه داده‌ها و محتوا مورد توجّه قرار گرفت و بزهکاران غالباً به داده‌های موجود در رایانه‌ها نفوذ می‌کردند. از همین رو، در این دوره توجّه

1.First generation of cybercrimes
2.Second generation of cybercrimes

قانون‌گذاران داخلی و منطقه‌ای بـه مباحـث حمایـت از داده‌هـا جلـب شـد و صـیانت از *محرمانگی*،[1] *تمامیت*[2] و *دسترس‌پذیری*[3] *اطلاعات* مورد توجّه قرار گرفت.

نسل سوم جرائم سایبری،[4] در اواسط دهۀ ۹۰ شـکل گرفـت و بـا عنـاوینی همچـون جرائم سایبری، جرائم مجازی، جرائم محیط سایبری شناخته می‌شود. این نسل از جرائم به‌واسطۀ ظهور فناوری‌های ارتباطی که امکان ارتباط با همگان را فراهم می‌کردند، شکل گرفت. «این نسل از جرائم بدون وجود اینترنت قابل ارتکاب نمی‌باشند و به‌عبـارت‌دیگـر، اینترنت شرط لازم تحقق آن‌ها است» (برایانت‌ها[5]، ۲۰۱۴، ص ۳۲). از همین رو، در این دوران با جرائمی نوینی همچون هرزنامه‌ها و باتنت‌ها مواجه هستیم که ماهیتی متفاوت از جرائم نسل‌های پیشین دارند.

نهادهای منطقه‌ای و بین‌المللی نیز سـعی در ارائـه تعریفـی جـامع از جـرائم سـایبری کرده‌اند. به‌عنوان نمونه، سازمان همکاری و توسعه‌ی اقتصادی، جـرائم سـایبری را «هـر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پـردازش خودکـار و یـا انتقـال داده‌هـا» تعریف کرده است (زیبر،۱۳۹۰، ص ۱۸). از طرفـی دیگـر، کنوانسـیون جـرائم سـایبری شورای اروپا نیز، جرائم سایبری را تحت چهار گروه جـرائم علیـه محرمـانگی، تمامیـت و دسترس‌پذیری سیستم‌ها و داده‌های رایانه‌ای،[6] جرائم مرتبط با رایانه،[7] جرائم مـرتبط بـا محتوا[8] و جرائم مرتبط با نقض حق نشر و حقوق مـرتبط[9] تقسـیم کـرده اسـت. لـیکن، تعریفی مستقل از جرائم سایبری ارائه نداده و به تقسیم‌بندی مذکور اکتفا کرده است.

با توجّه به مباحث فوق می‌توان گفت که در یک مفهوم وسیع، جرائم سایبری آن دسته از جرائمی را در برمی‌گیرد که از دستگاه متصل به اینترنت به‌عنوان ابزار یا هدف ارتکـاب بزه استفاده می‌شود. زمانی رایانه هدف ارتکاب جرم خواهد بود که بزهکـار یـا بزهکـاران دستگاه کاربر موردنظر را آماج بزه خود قرار می‌دهد. انتشار بدافزارها، نفوذ به دسـتگاه یـا جاسوسی اطلاعات نمونه‌های بارز این حالت هستند. از طرف دیگر، هنگامی‌که بزهکـار از

1.Confidentiality
2.Integrity
3.Accessibility
4.Third generation of cybercrimes
5.Bryant
6.Offences against the confidentiality, integrity and availability of computer data and systems
7.Computer-related offences
8.Content-related offences
9.Offences related to infringements of copyright and related rights

رایانه به‌عنوان وسیله‌ای برای ارتکاب بزه استفاده کند، در این حالت رایانه به‌عنوان ابزار ارتکاب بزه خواهد بود.

به‌موازات نفوذ فضای سایبر به زندگی بشر و ضرورت استفاده از آن برای انسان معاصر، محافظت در مقابل جرائم روبرو رشد این فضا نیز اهمیتی دوچندان یافته و پیشگیری از بزهکاری جز اولویت‌های فعالیت امن و کم‌خطر در این فضا به شمار می‌رود. کاربست ابزارهای فناوری اطلاعات و ارتباطات در قالب تدابیر پیشگیرانهٔ موقعیت مدار می‌تواند از خسارات کلان سایبری پیشگیری کند و فضای نسبتاً امنی را برای کاربران شبکه ایجاد کند، چراکه؛ در این حالت مبارزه و پیشگیری از جرائم سایبری با ابزارهای خود بزهکاران صورت می‌گیرد. به‌عبارت‌دیگر، در این نوع از جرائم، هر دو طرف درگیر در قضیه (بزهکار و نظام عدالت کیفری) از فناوری واحدی برای نیل به مقصود خود استفاده می‌کنند و تنها تفاوت آن‌ها در روزآمدی و استفادهٔ حداکثری از فناوری‌های موجود است.

نظریهٔ پیشگیری موقعیت مدار به‌عنوان یکی از نظریات پیشگیرانهٔ کنشی، درنتیجهٔ شکست تدابیر پیشگیرانهٔ اجتماعی، در اواخر دههٔ ۱۹۷۰ و توسط وزارت کشور بریتانیا مطرح شد. این تدابیر درصدد کاهش بزهکاری از طریق دست‌کاری در فرصت‌های پیش جنایی هستند. بنابراین، پیشگیری موقعیت مدار درصدد شناخت شخصیت بزهکار و همچنین، علل اجتماعی، اقتصادی و فرهنگی بزه نیست، بلکه؛ سعی در دست‌کاری موقعیت‌های ارتکاب بزه و برهم زدن آن‌ها دارد. درنتیجه، با مداخله در عوامل محیطی و زمانی سعی در کاهش منافع احتمالی ارتکاب بزه برای بزهکاران دارد. کلارک بر این عقیده است که «پیشگیری موقعیت مدار درصدد کاهش انگیزه‌های ارتکاب بزه از طریق تعالی جامعه و نهادهای آن نیست، بلکه؛ تمرکز آن بر کاهش فرصت‌ها و موقعیت‌های ارتکاب بزه از طریق کاهش جذابیت است» (کلارک،[1] ۱۹۹۲، ص ۴).

امروزه، تدابیر موقعیت مدار با استفاده از روش‌های سلبی و ایجابی، سعی در محافظت از آماج احتمالی و افزایش هزینه‌های ارتکاب بزه برای بزهکاران سایبری دارند، تا جایی که *صنعت امنیت سایبری*[2]، یکی از پردرآمدترین صنایع روز به شمار می‌رود. لیکن، علی‌رغم افزایش آگاهی کاربران شبکه از تهدیدات سایبری و لزوم تجهیز فکری و فنی

1.Clarke
2.Cybercrime security industry

خود برای رویارویی با این تهدیدات، این جرائم همچنان رو به افـزایش بـوده و خسـارات خرد و کلانی را وارد می‌سازند.

همان‌گونه که در ابتدا نیز گفته شد، امـروزه درصـد فراوانـی از جـرائم سـایبری دارای ماهیت فرامرزی هستند. براساس بررسی‌های سازمان ملل متحد در سال ۲۰۱۳، از میان ۵۰ کشور از ۵ قارهٔ آمریکا، آفریقا، آسیا، اروپا و اقیانوسیه، میانگین ۳۰ تا ۷۰ درصـدی از جرائم سایبری فرامرزی گزارش شده است و بیش‌ترین این آمار متعلّق به قارهٔ اروپا بـوده است (دفتر مقابله با مواد مخدر و جرم سـازمان ملـل متحـد[1]، ۲۰۱۳، ص۱۸۳). درصـد بالای یادشده، اتخاذ تمهیدات برون‌مرزی برای پیشگیری موقعیت مدار از ایـن جـرائم را دشوار می‌کند و عرصه را برای جولان بیشتر بزهکاران بالقوّه فراهم می‌کند. از همـین رو، در این اثر برآنیم تا به بررسی برخـی از مهـم‌تـرین چـالش‌هـایی کـه همـواره رویـاروی پیشگیری از جرائم سایبری فرامرزی هستند، پرداخته و راهکارهای موردنیاز برای کاهش یا حذف این چالش‌ها ارائه شود.

روش‌شناسی تحقیق

روش پژوهش اثر پیشرو به شیوهٔ توصیفی _تحلیلی است و در بازهٔ زمانی یک‌ساله، سعی در بررسی عملی خلأهای موجود در عرصهٔ فاوا برای مبارزه با فرصت‌هـای پـیش جنـایی فرامرزی شده است. همچنین، تعامل با متخصصـان ایـن حـوزه، فرصـت خـوبی را بـرای شناسایی چالش‌های تأمین فضای سایبری امن و یافتن راهکارهای عملی برای پیشگیری از بزه‌یدگی فرامرزی کاربران این فضا در هر دو سطح خرد و کـلان فـراهم کـرده اسـت. چراکه، تهدیدات سایبری فرامرزی علاوه بر اینکه تهدیـدات بـالقوه‌ای بـرای تأسیسـات و زیربناهای اقتصادی، امنیتی، نظامی، بهداشتی و خدماتی یک کشور محسوب مـی‌شـوند، درعین‌حال، می‌توانند یکایک کاربران را هم تهدید کنند و آن‌ها را آماج خود قرار دهند.

داده‌های موردنیاز به روش کتابخانه‌ای و از طریق مطالعه و تحلیـل تحقیقـات نهادهـای معتبر منطقـه‌ای و بـین‌المللـی، کتـب، مقـالات، قطعنامـه‌هـای سـازمان ملـل متّحـد و پرونده‌های جدیدی که در اثر کاربست تدابیر پیشگیرانه در دادگاه‌های بین‌المللی مطـرح شده، گردآوری شده‌اند. یکی از مهم‌ترین منابع اثر پیشرو، استفاده از نتایج مطالعهٔ بررسی

1.Comprehensive Study on Cybercrime

آماری دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد با عنوان «بررسی جامع جرائم سایبری» است. داده‌های مذکور با هدف یافتن تصویری موشکافانه و واقع‌بینانه‌تری از چالش‌های چندگانه و بعضاً پیچیدهٔ عرصهٔ جرائم سایبری گردآوری شده است و تا به امروز از مهم‌ترین منابع آماری مورد استناد پژوهشگران این حوزه به شمار می‌رود.

یافته‌های تحقیق

براساس پژوهش‌های انجام‌شده، دو گروه از چالش‌ها، فرآیند پیشگیری موقعیت مدار را با مشکلات عمده مواجه می‌سازند که در این قسمت با استفاده از پرونده‌ها و آمار معتبر بین‌المللی و منطقه‌ای به ارزیابی آن‌ها در دو دستهٔ چالش‌های حقوقی و پلیسی پرداخته می‌شود.

الف) چالش‌های حقوقی

هرگونه شناسایی خلأهای امنیتی، فرصت‌های پیش جنایی و پیشگیری از رفتارهای پرخطر بزهکاران برون‌مرزی باید در چهارچوب اصل قانونی بودن پیشگیری از جرم صورت گیرد و در صورت فقدان قانون یا نقص آن نمی‌توان با استفاده از تدابیر پیشگیرانه آزادی‌های شخصی افراد را محدود کرد. از همین رو، هرگونه همکاری همه‌جانبه نیروهای پیشگیری از جرم کشورهای درگیر در قضیه نیازمند وجود قوانین در حوزه‌های مربوط است. در این قسمت به بررسی این چالش‌ها پرداخته می‌شود.

۱- وجود پناهگاه‌های امن داده‌ها[1]: مشکل اولیه در روند پیشگیری موقعیت مدار از جرائم فرامرزی، از آنجایی آغاز می‌شود که هرگونه پیشگیری از این جرائم، مستلزم وجود معیارهایی هماهنگ در قوانین طرفین درگیر برای همکاری است و این امر اختصاص به جرائم سایبری ندارد. از همین رو، کنوانسیون‌ها و رهنمودهای بسیاری همچون کنوانسیون سازمان ملل متحد برای مبارزه با جرائم سازمان‌یافتهٔ فرا ملّی یا کنوانسیون مبارزه با فساد این سازمان درصدد رفع این خلأ در مسیر مبارزه و کاهش جرائم فرامرزی هستند.

یکی از مهم‌ترین چالش‌های حقوقی در مسیر پیشگیری از جرائم فرامرزی، جرم‌انگاری عمل موردنظر در قوانین طرفین درگیر در قضیه است و در صورت عدم وجود چهارچوب

1.Safe havens of data

و خط‌مشی واحد، فرآیند پیشگیری با مشکلات بسیاری مواجه خواهد شد. لزوم جرم‌انگاری عمل مجرمانهٔ احتمالی، به *اصل مجرمیت متقابل*[1] بازمی‌گردد. به‌موجب این اصل، «فعل یا ترک فعل موردنظر باید در قوانین همهٔ طرفین موردنظر مجرمانه شناخته شده باشد» (کریر، هاکان، رابینسون و ویلمیزهارت[2]، ۲۰۱۰، ص ۸۹). بنابراین، چنانچه عمل مورد نظر در قوانین طرف مقابل جرم نباشد، نمی‌توان تقاضای همکاری برای پیشگیری از آن بزه احتمالی را کرد. این موضوع در جریان یازدهمین کنگرهٔ سازمان ملل متحد دربارهٔ پیشگیری از جرائم و بسط عدالت کیفری نیز مغفول نمانده و توجّه ویژه‌ای به آن شده است. در دورهٔ آموزشی فشرده‌ای که با عنوان «*تدابیری برای مبارزه با جرم‌های مرتبط با رایانه*»[3] در جریان این کنگره تشکیل شد، توجّه کشورها را به این موضوع جلب کرد که جرائم مرتبط با رایانه از خلأهای موجود در چهارچوب‌های حقوقی و ظرفیت‌های نظام عدالت کیفری بهره می‌برند و افزایش می‌یابند. از همین رو، کشورها را به به‌روزرسانی قوانین خود در همهٔ حیطه‌ها به‌خصوص درج ماهیت خاص جرائم سایبری و آن دسته از جرائم سنتی که از طریق فناوری‌ها ارتکاب می‌یابند، تشویق کرده است و برای جلوگیری از تشتّت قوانین و چالش‌های ناشی از آن، از کشورها خواسته است تا از کنوانسیون جرائم سایبری شورای اروپا الهام بگیرند (یازدهمین کنگرهٔ سازمان ملل متحد دربارهٔ پیشگیری از جرائم و بسط عدالت کیفری[4]، ۲۰۰۵، پاراگراف‌های ۵۲ و ۷۰).

عدم جرم‌انگاری اعمال ممنوعه، سبب شکل‌گیری مناطق امن برای بزهکاران شده و عموماً از چنین کشورهایی، با اصطلاحاتی همچون «*پناهگاه‌های امن داده‌ها*» یا «*پناهگاه‌های مجازی*» تعبیر می‌شود. پناهگاه‌های امن داده‌ها سبب می‌شوند که بزهکاران سایبری عملی را مرتکب شوند که در کشور آن‌ها جرم نبوده و هنوز به رسمیت شناخته نشده است. از همین رو، «آنان از خلأ موجود در قوانین کیفری خود سود می‌جویند و با مصونیت کامل به ارتکاب جرم می‌پردازند» (برنر و گودمن[5]، ۲۰۱۲، ص ۱۵). بنابراین، آن‌ها از این کشورها به‌عنوان «سکوی پرتابی برای حملاتشان یا مخزنی برای نگهداری داده‌های غیرقانونی خود استفاده خواهند کرد» (وست‌بای[6]، ۲۰۰۳، ص ۸۷). نمونهٔ بارز

1.Double /dual criminality
2.Cryer, Hakan, Robinson & Wilmshurst
3.Measures to Combat Computer-related Crime
4.Eleventh United Nations Congress on Crime Prevention and Criminal Justice
5.Brenner & Goodman
6.Westby

توجه جامعهٔ جهانی به این چالش را می‌توان در انتشار سریع *ویروس دوستت دارم*[1] یا *حشرهٔ عشق*[2] مشاهده کرد. این ویروس دستگاه‌های میلیون‌ها کاربر از نقاط مختلف دنیا را از طریق پیوست کردن فایل آلوده به نامه‌های الکترونیکی، مورد هدف قرارداد. این بدافزار از فیلیپین شروع به فعالیت کرد و همان روز در سرتاسر دنیا پخش شد. در آن زمان، هیچ قانونی در فیلیپین وجود نداشت که این عمل را جرم شمرده باشد و همین امر، هرگونه اقدامی علیه طراحان این ویروس را بسیار دشوار کرده بود (هالت[3]، ۲۰۱۵، ص ۱۴).

پناهگاه‌های امن داده در دو حالت تشکیل خواهند شد. حالت نخست زمانی است که کشورها به قوانین سنتی خود اکتفا می‌کنند و قوانین خاصی را برای جرائم سایبری وضع نمی‌کنند. نمونهٔ بارز چنین وضعیتی را می‌توان در بسیاری از کشورهای قارهٔ آفریقا مشاهده کرد. امروزه، این کشورها به مانعی جدی در فرآیند پیشگیری بین‌المللی از جرائم سایبری تبدیل شده‌اند. تأمین پهنای باند بالا[4] در سال‌های اخیر از یک‌سو و ضعف بنیادین قوانین آن‌ها از سوی دیگر، سبب شده است که شمار نفوذگران موجود در این قاره افزایش چشم‌گیری یافته و به مبدأ بسیاری از حملات سایبری تبدیل شود، به‌طوری‌که؛ «از میان ۵۷ کشور موجود در قارهٔ آفریقا، که تقریباً یک‌سوم کشورهای دنیا را تشکیل می‌دهند. صرفاً ۵ کشور کامرون، کنیا، موریس، آفریقای جنوبی و زامبیا دارای قوانین جرائم سایبری بوده» (خارونی[5]،۲۰۱۳، ص ۸) و ۵۲ کشور باقیمانده، فاقد قوانین جرائم سایبری هستند.

آنچه که امروزه به‌مراتب به چشم می‌خورد و کاربست تدابیر پیشگیرانه را دشوار می‌کند این است که برخی از کشورها، علیرغم در اختیار داشتن قوانین جرائم سایبری، موارد حائز اهمیت را پیش‌بینی نکرده‌اند یا در صورت جرم انگاری، به علت تفاوت اجزا عنصر مادی جرم موردنظر با طرفین دیگر، بزه احتمالی قابل پیشگیری نخواهد بود. بنابراین، مشکل ازآنجا ناشی می‌شود که قانون‌گذاران از معیارهایی هماهنگ برای به رسمیت شناختن جرم سایبری پیروی نمی‌کنند. «برخی از کشورها جرم سایبری، جرائم

1.I love you virus
2.Love bug
3.Holt
4.Broadband
5.Kharouni

با فناوری بالا، جرائم مرتبط با رایانه و جرائم فناوری اطلاعات را بجای یکدیگر به کار می‌برند و بین زمینه‌های حقوقی خاص هر یک از آن‌ها تفکیک قائل نمی‌شوند» (ساونا[1]، ۲۰۰۴، ص ۳۳) (قاجارقیونلو، ۱۳۹۱، ص۶۴۲)، درحالی‌که، برخی دیگر از کشورها صرفاً به مفهوم مضیق جرم سایبری پای بند هستند و مابقی موارد را در دسته‌بندی‌های خاص خود، به رسمیت می‌شناسند.

«امروزه، دیدگاه بین‌المللی بر این باور است که حقوق کیفری از صلاحیت دولت‌ها خارج شده است. برای پیشگیری از یک جرم فراملی مانند جرم سایبری، باید همهٔ کشورهایی که این جرم در حوزهٔ آن‌ها واقع می‌شود، آن رفتار را جرم تلقی کنند. هم‌اکنون ممکن است برخی از کشورها یک رفتار زیان‌بار سایبری را جرم تلقی کنند، امّا برخی دیگر خیر؛ این در حالی است که به‌واسطهٔ اینترنت و فناوری‌های سایبری، این رفتار زیان‌بار در محدودهٔ همهٔ این کشورها به وقوع می‌پیوندد. این امر هم در حوزهٔ حقوق کیفری و هم در امر پیشگیری کاربرد دارد. در حوزهٔ پیشگیری از جرم، آنچه در محور کار قرار دارد، رفتاری است که باید از آن پیشگیری کرد و تا توافق نسبی دربارهٔ ماهیت این رفتار صورت نگیرد، پیشگیری ناکارآمد خواهد ماند. احصاء این دست رفتارها و توصیف ویژگی‌های آن دربارهٔ فضای سایبر باید به‌صورت بین‌المللی صورت گیرد» (مقیمی، ۱۳۹۵، ص۵۶).

در *دعوای انجمن بلژیکی نویسندگان و شاعران علیه شرکت ارائه‌دهندهٔ خدمات اینترنتی اسکارلت*[2]، یکی از دلایلی که موجب نظر دیوان دادگستری اتحادیهٔ اروپا[3] مبنی بر رد درخواست انجمن برای پالایش ترافیک داده‌ها شد، عدم جرم انگاری عمل موردنظر انجمن در قوانین کشورهای متبوع کاربران بوده است. قضیه از این قرار بود که انجمن خواستار پالایش هرگونه بارگیری[4] آزاد و رایگان آثار اعضای خود بود. به‌موجب درخواست انجمن، شرکت اسکار لت می‌بایست تمامی آثار دارای مالکیت معنوی انجمن را از سوی هر یک از کاربرانی که خواهان بارگیری رایگان آن‌ها از طریق این شرکت بودند، پالایش کرده و اجازهٔ دسترسی ندهد. لیکن، قوانین حمایت از حقوق مالکیت معنوی در فضای

1.Savona
2.Scarlet Internet service provider
3.The European Court of Justice (ECJ)
4.Download

سایبر از سوی بسیاری از کشورها به رسمیت شناخته نشده و چنین عملی مجرمانه نیست. چنانچه شرکت اسکارلت می‌خواست از این عمل پیشگیری کند، بارگیری چنین آثاری می‌بایست در کشور متبوع کاربر نیز جرم بوده باشد، درحالی‌که؛ در بسیاری از کشورهای کاربران عضو شرکت اسکارلت این‌گونه نبوده و حتی آن دسته از کشورهایی که چنین قوانینی داشتند، شرایط و استثنائات متفاوتی را برشمرده‌اند، به‌گونه‌ای که در برخی از موارد بارگیری برخی از آثار عملی قانونی تلقی شده و منعی نداشته است.

به‌موجب نظر دادگاه، قوانین حمایت از حقوق مالکیت معنوی در فضای سایبر از کشوری به کشور دیگر متفاوت است و انجمن نمی‌تواند انتظار داشته باشد که شرکت ارائه‌دهندهٔ خدمات اینترنتی که در کشور او قرار ندارد و تحت نظام حقوقی کشور متبوع وی نیست، از مقررات آن‌ها تبعیت کند. بنابراین، اگرچه که در اینجا با جرم سایبری فرامرزی مواجه هستیم، امّا؛ به نظر دادگاه فقدان قوانین هماهنگ، مانع از پیشگیری از این جرائم می‌شود. به‌عبارت‌دیگر، نظر دادگاه را می‌توان این‌گونه تحلیل کرد که باید قانون مشابهی وجود داشته باشد و سپس کاربران ملزم به تبعیت از آن قانون باشند. از این‌رو، درصورتی‌که عملی در کشوری جرم شناخته نشده باشد، براساس اصل قانونی بودن جرائم و مجازات‌ها، جرمی احتمالی واقع نخواهد شد که خواستار پیشگیری موقعیت مدار احتمالی از آن فعل مجرمانه باشیم. همچنین، دادگاه با توجه به عدم جرم انگاری همهٔ موارد در قوانین طرفین درگیر بیان داشته است که شرکت اسکارلت نمی‌تواند موارد قانونی و غیرقانونی را تشخیص دهد و از جرائم احتمالی پیشگیری کند. به‌موجب قسمتی از این رأی: «پاسخ به این سؤال که انتقال ترافیک داده آثار دارای مالکیت معنوی عملی قانونی است یا خیر در یک نگاه کلی ممکن نخواهد بود. استثنائات قوانین آثار دارای حقوق مالکیت معنوی از کشوری به کشور دیگر متفاوت هستند. همچنین، در برخی از کشورها انتشار یا بارگیری برخی از آثار موجب مسئولیت نیست و موجب نقض حقوق نویسنده نیز نخواهد شد» (اسکارلت اکستندد علیه سابام[1]، ۲۰۱۱، پاراگراف ۵۲).

با توجّه به مباحث پیشین می‌توان دریافت که پناهگاه‌های امن داده سبب می‌شوند که نتوان از بزه‌دیدگی احتمالی شمار فراوانی از آماج احتمالی پیشگیری کرد. چراکه؛ هرگونه همکاری طرف یا طرف‌های مقابل منوط به رسمیت شناخته شدن اصل عمل

1.Court of Justice of the European Union

مورد نظر است و تا کشور مقصد، عملی را جرم نشناخته باشد، از هرگونه همکاری بـرای پیشگیری از آن سر باز خواهد زد. همین امر سبب شده است که بزهکـاران بـه محاسـبهٔ عقلانی روی آورده و کم‌خطرترین مسیر را به‌منظور کسب بیشترین منافع انتخاب کننـد. نمونهٔ بارز این امر را می‌توان در جرائم سازمان‌یافته سایبری کـه در زمـرهٔ جـرائم بسـیار دشوار برای پیشگیری است، مشاهده کرد. «این گروه از بزهکاران، معمولاً حملات خود را از کشور امن شروع کرده و از همان‌جا نیز هدایت می‌کنند. رهبری و هدایت فعالیت‌هـای مجرمانه از این کشورها، آنان را در مقابل هرگونه اقدام احتمالی نیروهای پلـیس مصـون می‌دارد و درنتیجه، بدون کمتری خطری به فعالیت‌های بزهکارانه خود ادامه می‌دهنـد» (رنسام و میسرا[1]، ۲۰۱۴، ص۳۳۳).

۲- قوانین شکلی: امروزه بر این امر اتفاق‌نظر وجود دارد که صرف وجود قوانین مـاهوی سایبری، راهگشای حل مشکلات پیشگیری، تعقیب و تحقیق از جرائم سایبری فرامرزی نخواهد بود. از همین رو، یکی از مهم‌تـرین مسـائل مطروحـه در سـیزدهمین کنفـرانس بین‌المللی پیشگیری از جرائم سایبری سازمان ملل که در سال ۲۰۱۵ برگزار شده است، نیز جلب‌توجه نهادهای تقنینی کشورها به چالش‌های همه‌جانبه‌ای است که مخصوصاً در حیطه‌ی قوانین شکلی وجود دارد. به‌موجب قسمتی از این گزارش: *هرگونـه پاسـخی بـه جرائم سایبری باید در همهٔ حیطه‌های تقنینی و سیاست‌هـای حـاکم بـر آن‌کـه شـامل جرم‌انگاری، دادرسی کیفری، صلاحیت مأموران اجرایی و قضایی برای تحقیقات سایبری، جرم‌شناسی دیجیتـال و شـواهد و مـدارک الکترونیکـی و مکـانیزم‌هـای همکـاری‌هـای بین‌المللی و پیشگیری از جرائم سایبری* باشـد (سـیزدهمین کنگـرهٔ پیشـگیری از جـرم عدالت کیفری سازمان ملل[2]، ۲۰۱۵، ص۲۹).

یکی از مشکلاتی که همواره برای پیشگیری از جرائم سایبری اعم از کنشی و واکنشی وجود دارد، قوانین مربوط به حیطهٔ صلاحیت می‌باشند؛ چراکه به سبب عدم صدق مفهوم مادی مکان در این فضا نسبت به جرائم سنتی، تطبیق قواعـد سـنتی صـلاحیت بـا ایـن جرائم بسیار دشوار است. این مشکل از آنجایی ناشی می‌شود که معیارهای تعیین مراجع صالح برای پیشگیری از بزه احتمالی مشخص نیست. به‌عنوان نمونـه، سـؤالاتی از قبیـل،

1.Ransome & Misra
2.Thirteenth United Nations Congress on Crime Prevention and Criminal Justice

پیشگیری از بزه احتمالی در صلاحیت کشوری است که میزبان (سرور) در آن قرار دارد؟ یا کشوری که نام دامنه در آن به ثبت رسیده است؟ یا کشورهایی که هر یک از بزهکاران احتمالی در آن قرار دارند؟ یا کشوری که رایانه‌ها و دستگاه‌ها از آنجا شروع به حمله کرده‌اند؟ همواره در مرحلهٔ پیشگیری موقعیت مدار از جرائم سایبری وجود دارند. درنتیجه، در بسیاری از موارد تعارض منفی صلاحیت‌ها و رفع آنان، منجر به وقوع بزه احتمالی خواهد شد. چراکه؛ اگرچه که می‌توان در نهایت با استفاده از معاهدات یا کنوانسیون‌هایی که طرفین به آن‌ها پیوسته‌اند، تعارض را رفع کرد، لیکن؛ بزه اتفاق افتاده است و پیشگیری از آن دیگر بی‌معنی خواهد بود و در نهایت، راه‌حل پذیرفته شده را می‌توان در آینده به‌منظور پیشگیری از فرصت‌های جنایی احتمالی به کاربست.

مشکلات مربوط به صلاحیت سبب می‌شوند که نتوان از بزه‌دیدگی شمار فراوانی از کاربران جلوگیری کرد. امروزه، یکی از راهکارهای مؤثری که به‌منظور کاهش این چالش برداشته می‌شود، معاهدات دو یا چندجانبه است. لیکن، علی‌رغم تأثیر مثبت این معاهدات بر پیشگیری از برخی از جرائم، باید یادآور شد که تعداد این معاهدات و طرفین آن اندک بوده و نمی‌توانند تأثیر چشمگیری در کاهش جرائم سایبری داشته باشند و چه‌بسا هنوز با نوعی عدم امکان وجود چنین معاهداتی در سطح گسترده مواجه باشیم.

همچنین، فقدان قوانین شکلی حوزهٔ همکاری‌های بخش‌های خصوصی و دولتی نیز منجر به عدم موفقیت پیشگیری موقعیت مدار از جرائم سایبری فرامرزی می‌شود. علی‌رغم آثار مثبت همکاری بخش‌های خصوصی و دولتی[1] در بعد داخلی و بین‌المللی موانع قانونی بسیاری برای تعامل گستردهٔ این نهادها وجود دارد. در بسیاری از موارد، رهگیری و پیشگیری از بزهکاری نیازمند همکاری تنگاتنگ بخش‌های خصوصی با دولتی است. فقدان شرایط و ضوابط قانونی همکاری، غالباً سبب عدم تمایل بخش‌های خصوصی به همکاری با بخش‌های دولتی می‌شود. چراکه؛ عدم تعیین محدودهٔ همکاری‌ها، شرایط صیانت از امنیت داده‌ها و مواردی از این قبیل مشخص نیست. از همین رو، جز در مواردی که توافقنامه‌ها یا قوانین خاص این حیطه وجود نداشته باشد، عموماً همکاری حاصل نمی‌شود و نتیجهٔ فقدان و کمبود قانون‌گذاری در این حیطه، افزایش انگیزهٔ بزهکاران برای ارتکاب بزه است.

1.Public and private sector cooperation

همچنین، لازم به ذکر است که یکی از عمده‌ترین دلایل عدم همکاری‌ها را می‌توان به علت انگیزه‌های اقتصادی شرکت‌ها دانست؛ چراکه در صورت همکاری، موظف به در اختیار گذاشتن اطلاعات کاربران می‌باشند و همین امر می‌تواند همواره دغدغهٔ نقض حریم خصوصی از جانب کاربران را به دنبال داشته باشد و شمار آنان کاهش یابد. علت نیز آن است که در برخی از موارد، علیرغم وجود قوانین حمایت از حریم خصوصی، تضمینی برای رعایت این قوانین وجود نداشته و به‌منظور پیشگیری حداکثری از بزه‌دیدگی حریم خصوصی برخط کاربران نقض می‌شود. نمونهٔ بارز این امر را می‌توان در اتهام وارده به شرکت‌های گوگل، فیس‌بوک، یوتیوب، اسکایپ، مایکروسافت، اپل و یاهو به علت همکاری با پروژه‌های رهگیری غیرقانونی اطلاعات دولت انگلستان دانست که پروندهٔ آن هم‌اکنون با نام *«دیده‌بان برادر بزرگ و دیگران علیه دولت انگلستان»*[1] در دادگاه اروپایی حقوق بشر در حال رسیدگی است و دولت انگلیس متّهم به نقض حریم خصوصی برخط کاربران است.

نمونهٔ واضح شکست تدابیر پیشگیرانه به علت فقدان قوانین لازم را می‌توان در عدم موفقیت تلاش‌های وزارت امنیت داخلی ایالات‌متحدهٔ آمریکا[2] برای غلبه بر حملات *خونریزی قلبی*[3] مشاهده کرد. بنا به اذعان مدیر مرکز امنیت سایبری و ارتباطات انسجام ملی وزارت کشور آمریکا[4] دولت فدرال این حملات را شناسایی کرده و آمادهٔ پاسخ سریعی برای پیشگیری از آسیب‌های کلانتر بوده است، لیکن، فقدان قوانین صریح و روزآمد در مورد تکالیف و وظایف شرکت‌های اینترنتی برای همکاری، منجر به تأخیر در واکنش به حملات و آلوده شدن هزاران وب‌سایت شده است.

تعامل بخش‌های خصوصی و دولتی منحصر به مرزهای یک کشور نبوده و در غالب موارد برای پیشگیری از جرائم سایبری فرامرزی، نیاز به همکاری بخش‌های خصوصی کشورهای مختلف نیز است. در این موارد، به سبب فقدان یا کمبود توافق‌نامه‌های بین‌المللی، پیشگیری دشوارتر می‌شود. چراکه؛ لازمهٔ رهگیری سریع بسیاری از رفتارهای مشکوک و همچنین پیشگیری از برخی از خطرات احتمالی شناسایی‌شده، در اختیار

1.Big Brother Watch and others against the United Kingdom
2.Department of Homeland Security
3.Heart bleed
4.National Cyber security and Communications Integration Center (NCCIC)

داشتن اطلاعات در حال انتقال کاربران این شرکت‌ها است. نمونهٔ بارز چنین چالشی را می‌توان در عدم موفقیت پیشگیری از هرزنامه‌ها[1] دانست. هرگونه پیشگیری از گسترش دامنهٔ خسارات انتشار هرزنامه‌ها، مستلزم همکاری شرکت‌های ارائه‌دهنده‌ی خدمات پست الکترونیکی، مخصوصاً شرکت‌های بین‌المللی است که در بسیاری از موارد به علّت عدم الزام قانونی ناشی از همکاری‌های بین‌المللی، از همکاری سرباز می‌زنند و نتیجهٔ این عدم همکاری، آلوده شدن شمار بسیاری از دستگاه‌ها به این بدافزارها است. این مشکل حتّی میان کشورهای قارهٔ اروپا که دستورالعمل نگهداری و ذخیرهٔ داده‌ها[2] را در اختیار دارند نیز مشاهده می‌شود و بسیاری از کشورها قوانین مربوط به گردآوری و ذخیره داده‌ها در آن‌ها متفاوت بوده و در بسیاری از موارد، ارائه‌دهندگان خدمات دسترسی مسئولیتی مبتنی بر ذخیره و یا ارائهٔ داده‌های مشکوک به نهادهای قانونی مسئول جرم داخلی و یا خارجی را ندارند.

ب) چالش‌های پلیسی

در کنار چالش‌های پیشین، دسته‌ای دیگر از چالش‌ها وجود دارند که مختص به نهادهای تعقیب‌کننده می‌باشند. از آن‌رو، نام این چالش‌ها را پلیسی نهاده‌ایم که غالباً مسئولیت اصلی پیشگیری از جرائم سایبری را نیروهای پلیس بر عهده دارند. البته لازم به ذکر است که چالش‌های پیشین نیز همواره فراروی نیروهای پلیس قرار داشتند، لیکن، چالش‌هایی که در ادامه راجع به آن‌ها صحبت می‌کنیم، مختص به نیروهای پلیس می‌باشند.

۱- شکاف تخصصی: یکی از چالش‌های مهم پیشگیری از جرائم سایبری فرامرزی، شکاف تخصصی است که بین طرف‌های مختلف درگیر وجود دارد. تدابیر پیشگیرانه در صورتی می‌توانند مؤثر واقع شوند که طرفین درگیر در قضیه قادر به پاسخگویی به درخواست‌های یکدیگر باشند و این امر در گام نخست، نیازمند روزآمد بودن سطح دانش هر یک از نیروهایی است که به‌نوعی در این فرآیند مشارکت دارند. چراکه؛ سلاحی که بزهکاران سایبری از آن‌ها استفاده می‌کنند، همان سلاح مورد استفادهٔ نهادهای مسئول پیشگیری از جرم است. بنابراین، غلبه یکی از آن‌ها بر دیگری منوط به دانش و تخصص بیشتر است. صرف توان علمی بالای یکی از طرف‌های درگیری نمی‌تواند منجر به موفقیت

1.Spams
2.Eu data retention directive 2006/24/ec

پیشگیری از بزهکاری سایبری شود و اهمال و کاستی هر یک از طرفین می‌تواند همگان را با خسارات سهمگین سایبری مواجه کند. این شکاف، امروزه میان کشورهای توسعه‌یافته و کشورهای کمتر توسعه‌یافته یا توسعه‌نیافته به‌وضوح قابل مشاهده است. به همان میزانی که کشورهای اخیر با ضعف قوانین خود، پناهگاه‌هایی امن به شمار می‌آیند، عدم آگاهی نیروهای پلیس سایبری آن‌ها نیز بزهکاران را در انتخاب این کشورها مصمم می‌سازد.

سازمان ملل متحد در تحقیق جامع خود با بررسی میان ۶۹ کشور دریافت که در کشورهای کمتر توسعه‌یافته به‌طور میانگین به ازای هر صدهزار نفر کاربر فضای سایبر، ۰/۲ نیروی پلیس متخصص مشغول به فعالیت هستند. درحالی‌که؛ این عدد برای کشورهای توسعه‌یافته ۲ تا ۵ برابر بیشتر است. همچنین، تعداد نیروهای پلیس متخصص سایبری تمام کشورها، کمتر از یک درصد نسبت به‌کل نیروهای پلیس است. حال، از میان این آمار، نیروهای پلیس حدود ۴۰ درصد از کشورها با سطح دانش فناوری اطلاعات پیشرفته، ۳۰ درصد در سطح متوسط، ۲۰ درصد با دانش ابتدایی و ۶ درصد آن‌ها هیچ‌گونه مهارتی در زمینهٔ فناوری اطلاعات و ارتباطات ندارند. در کنار مستندات فوق، آنچه که بسیار حائز اهمیت است و عدم توجه کشورها به پیشگیری از جرائم سایبری را نشان می‌دهد این است که صرفاً ۳ درصد از همین آموزش‌های اندک، به مباحث پیشگیری از بزه اختصاص دارد (دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد، ۲۰۱۳، ص ۱۵۴).

نیروهای پلیس برخی از کشورها با استخدام نفوذگران کلاه‌سفید، سعی در جبران این چالش دارند. این دسته از نفوذ گران، عموماً به‌عنوان مشاورین امنیتی[1] به استخدام نیروهای پلیس درمی‌آیند و ازآنجایی‌که عموماً با شیوه‌های نوین ارتکاب جرم آشنایی دارند و روش‌های نفوذ در شبکه‌های با لایهٔ امنیتی مختلف را می‌دانند، می‌توانند فرصت‌های مجرمانه را شناسایی و آن‌ها را خنثی کنند. آن‌ها با استفاده از تست نفوذ[2] «سعی در ورود به سیستم و یافتن نقاط ضعف آن‌ها و اتخاذ تدابیر امنیتی دارند» (سیمپسون، بکمن و کورلی[3]، ۲۰۱۳، ص ۲.) دولت فدرال ایالات‌متحدهٔ آمریکا یکی از

1.Security Analyzer
2.Penetration test
3.Simpson, Backman & Corley

پیشگامان این حیطه است کـه از سـالیان پـیش بـا اسـتخدام ایـن نفـوذگران سـعی در شناسایی تهدیدات پیشروی سیستم‌های رایانه کشورش کرد (جیکوبز[1]، ۲۰۱۰، ص۱۵۲). چالش‌های برشمرده شده سبب می‌شود که نیاز به وجود مرجعی بین‌المللی برای نظارت بر نهادهای مسئول پیشگیری از جـرائم سـایبری احسـاس شـود. چراکـه؛ اگـر کشـورها به‌صورت مستقل مبادرت به آموزش واحدهای فنی خـود کننـد و «همـاهنگی و تعامـل کارآمد و اثربخش میان تمامی دست‌اندرکاران این حـوزه بـه وجـود نیایـد و یـک مرکـز فرماندهی واحد برای آن‌ها پیش‌بینی نشود، بیش از همـه، کـاربران فنـاوری اطلاعـات و ارتباطات یا به عبارت بهتر، شهروندان سایبری لطمه خواهند دید» (جلالی فراهانی (ب)، ۱۳۸۸، ص۹۳). همچنین، به سبب عدم هماهنگی آموزش‌ها و مهارت‌های متخصصان با یکدیگر، هر یک از روش‌ها و شیوه‌های گوناگونی برای پاسخگویی به درخواست طرف یـا طرف‌های مقابل استفاده می‌کنند و قادر به تعامل مناسب با یکـدیگر نیسـتند و احتمـال عدم موفقیت در تأمین خواسته‌های طرف مقابل وجود خواهد داشت.

در سال‌هـای اخیـر، نهادهـای بـین‌المللـی و منطقـه‌ای مبـارزه بـا جـرائم سـایبری، فعالیت‌های بسیاری را به‌منظور ارتقای توان علمی و تخصصـی واحـدهای مربوطـه آغـاز کرده‌اند. به‌عنوان نمونه، مجمع عمومی پلیس بین‌الملل طی نشستی در سـال ۲۰۱۰، بـا تأسیس *انجمن جهانی نوآوری پلیس بین‌الملل*[2] موافقت کرد. این انجمن اخیراً در کشـور سنگاپور شروع به فعالیت کرده و *مرکز جرائم دیجیتالی*[3] را راه‌اندازی کرده است. یکـی از اهداف این مرکز، غلبه بر چالش یاد شده است و برای نیـل بـه ایـن منظـور، از اقـداماتی همچون «توسعهٔ راه‌حل‌های عملی برای همکاری بین نیروهـای پلـیس، آزمایشـگاه‌هـای تحقیقاتی جرائم سایبری، مجامع دانشگاهی و بخش‌هـای عمـومی و خصوصـی، ارتقـای آگاهی نیروهای پلیس کشورها از طریق انجام تحقیقات مختلف و در اختیار نهادن نتـایج آن در دسترس آن‌ها و همچنین، آموزش جدیدترین شیوه‌های پیشگیری از جرائم» بهره می‌برد (گیرنو- هیبلی[4]، ۲۰۱۳،ص۲۸۲). همچنین، *مرکز جرائم سـایبری اروپـا*[5] نیـز بـا پشتیبانی از آموزش و افزایش توانایی‌های اعضای خود، درصدد تسهیل پیشگیری از این جرائم است.

1.Jacobs
2.The INTERPOL Global Complex for Innovation (IGCI)
3.Digital Crime Center
4.Ghernaouti-Hélie
5.The European Cybercrime Centre (EC3)

۲- شکاف فنّاورانه: یکی دیگر از مشکلاتی که فراروی کاربست تدابیر پیشگیرانهٔ موقعیت مدار وجود دارد، شکاف فناورانه‌ای است که بین طرفین درگیر وجود دارد. تهیهٔ تجهیزات و امکانات سخت‌افزاری و نرم‌افزاری موردنیاز این نوع از پیشگیری، برای همهٔ کشورها میسّر نیست. کمبود منابع مالی در برخی از کشورها سبب می‌شود که نیروهای پلیس همهٔ تجهیزاتی که برای مبارزه با جرائم سایبری نیاز است را در اختیار نداشته باشند و نتوانند خود را با استانداردهای جهانی مبارزه با جرائم سایبری هماهنگ سازند (کاشتری[1]، ۲۰۱۰، ص۴۰).

فقدان تجهیزات موردنیاز پیشگیری از بزه سبب می‌شود که در بسیاری از موارد، موقعیت‌های خطر شناسایی نشوند و گمان رود که امنیت تأمین شده است و پس از بروز خسارات و گزارش بزه‌دیدگی ارتکاب جرم مسلّم شناخته شود. در اختیار داشتن ابزارهای بروز و پیشرفته مبارزه با جرائم سایبری از آن‌رو حائز اهمیت است که گاه برای پیشگیری از این جرائم ثانیه‌ها نیز ارزشمند هستند و هرگونه قصوری نتایج زیان باری را در پی خواهد داشت. چراکه؛ «بعضی از انواع داده‌های رایانه‌ای صرفاً برای مدت زمان کوتاهی قابل ذخیره شدن هستند و سپس پاک خواهند شد. در دیگر موارد، چنانچه شواهد، به‌سرعت جمع‌آوری نشوند احتمال ورود خسارات جانی یا مالی اساسی وجود خواهد داشت» (شورای اروپا[2]، ۲۰۰۱، ص۴۴).

رهنمود پیشگیری از جرم شورای اقتصادی و سیاسی سازمان ملل متحد، به‌منظور کاهش آثار سوء چنین مشکلاتی، مبحثی تحت عنوان همکاری فنی را پیش‌بینی کرده است و به مساعدت کشورهای پیشرفته برای ارتقای این‌گونه از همکاری‌ها تأکید کرده است. به‌موجب این مبحث: *«دولت‌های عضو و سازمان‌های بین‌المللی مسئول تأمین بودجهٔ مربوطه باید به‌منظور اجرایی کردن اصول ناظر بر تأمین امنیت گروهی و پیشگیری از جرم در سطح ملّی و منطقه‌ای، زمینهٔ همکاری مالی و فنی در خصوص تقویت ظرفیت‌ها، ساختارها و آموزش را با کشورهای با اقتصاد درحال‌توسعه، گروه‌ها و سایر سازمان‌های ذی‌ربط فراهم آورند»* (جوان جعفری و سیّد زاده ثانی،۱۳۹۱، ص۲۸۴).

1.Kshetri
2.Council of Europe

نتیجه‌گیری

سرعت بالای ورود جرائم سایبری به زندگی بشر، فرصت تعیین چهارچوب‌های لازم برای پیشگیری از مخاطرات احتمالی این فضا را سلب کرده است و به همین سبب، پیشگیری از جرائم سایبری، برخلاف بسیاری دیگر از جرائم فرامرزی با چالش‌های متعدّدی مواجه است. یکی از مهم‌ترین چالش‌های رویاروی نهادهای مسئول، فقدان معیار هماهنگ برای تسریع پیشگیری همه‌جانبه از این جرائم است. به سبب عدم الزام بسیاری از طرفین درگیری به بروزآوری و هماهنگ ساختن مصادیق جرائم سایبری، در بسیار از موارد امکان همکاری برای پیشگیری از بزه احتمالی وجود نخواهد داشت، چراکه طرف یا طرف‌های مقابل عمل احتمالی را مجرمانه ندانسته و درنتیجه، به پناهگاه‌های امن برای بزهکاران سایبری تبدیل می‌شوند.

همچنین، فقدان قوانین هماهنگ در حوزه‌هایی همچون صلاحیت بین‌المللی، همکاری بخش‌های خصوصی داخلی و خارجی با نهادهای مسئول پیشگیری از بزه و قوانین پیشگیری از بزه سبب شده است که امروزه پیشگیری از موقعیت‌های احتمالی بزه سایبری، به یکی از دشوارترین آرمان‌های عدالت کیفری تبدیل شود. بنابراین، می‌توان گفت، آنچه که در بعد تقنینی پیشگیری از بزهکاری سایبری را دشوار می‌نماید، عدم وجود خط‌مشی واحدی برای قانون‌گذاری سایبری است. کنوانسیون‌ها و رهنمودهای موجود به علّت عدم پیوستن شمار فراوانی از اعضای جامعهٔ جهانی نتوانستند به هدف نهایی خود دست یابند و چه‌بسا یکی از علل احتمالی این امر این باشد که کشورهایی که مبدأ حملات سایبری هستند و بزهکاران ازآنجا مبادرت به ارتکاب بزه می‌نمایند، به این دسته از اسناد نپیوسته‌اند. از طرف دیگر، حتی در صورت وجود قوانین کافی، در برخی از موارد شکاف علمی و فنی موجود بین اشخاص و نهادهای درگیر در فرآیند پیشگیری موقعیت مدار از بزه سایبری، در مقام عمل پیشگیری را به تعویق انداخته یا حتی غیرممکن می‌سازد. این شکاف میان کشورهای توسعه‌یافته و کشورهای درحال توسعه و توسعه‌نیافته به‌وضوح مشاهده می‌شود. چراکه؛ به علّت ضریب نفوذ بالای استفاده از شبکهٔ جهانی اینترنت در کشورهای دستهٔ نخست، تأمین امنیت این فضا بسیار مهم تلقی می‌شود و توانایی مالی و انسانی کافی به‌منظور تأمین امنیت این فضا وجود دارد. درحالی‌که، شمار فراوانی از کشورهای دستهٔ دوم از کمبودهای بسیاری رنج می‌برند و توانایی ارتقای امنیت کاربرانشان و پیشگیری از بزه احتمالی را نخواهند داشت. بنابراین،

زمانی که این دو گروه با یکدیگر مسئول پیشگیری از جرائم سایبری باشند، احتمال عدم موفقیت بسیار خواهد بود.

با ارزیابی شرایط موجود جامعهٔ جهانی، نیاز به وجود مرجعی بین‌المللی برای نظارت، راهنمایی و تدوین قواعد و مقررات الزام‌آور برای پیشگیری از جرائم سایبری احساس می‌شود. دستاوردهای ارزندهٔ کنگره‌های بین‌المللی پیشگیری از جرم و عدالت کیفری می‌تواند به‌عنوان پشتوانه‌ای موثّر برای این مرجع به‌حساب آید و حرکت جامعهٔ جهانی برای مبارزه با این جرائم را تسریع بخشد. همچنین، ایجاد واحدهای آموزشی پیشگیری از جرم، تخصیص بودجه به کشورهای کمتر توسعه‌یافته یا توسعه‌نیافته، ایجاد مراکز پاسخ سریع بین‌المللی که با مراکز داخلی در ارتباط هستند نیز از دیگر راهکارهای پیشگیری حداکثری از جرائم سایبری است.

منابع

منابع فارسی

- جوان جعفری، عبدالرضا؛ سیّد زاده ثانی، سیّد مهدی (۱۳۹۱). *رهنمودهای عملی پیشگیری از جرم*. تهران: میزان.

- جوان جعفری، عبدالرضا (اسفند ۱۳۸۹). جرائم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرائم رایانه‌ای). *مجلهٔ دانش و توسعه*. ۳۴، صص۱۹۳-۱۶۹. بازیابی از: http://fa.journals.sid.ir/ViewPaper.aspx?id=159235

- جلالی فراهانی، امیرحسین (الف)(پاییز ۱۳۸۴). پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر. فقه و حقوق. ۶(۲)، صص۱۶۳-۱۳۳. بازیابی از: magazines.iict.ac.ir/uploads/5_51_06.07.pdf

- جلالی فراهانی، امیرحسین (ب) (۱۳۸۸). نهادسازی برای پیشگیری از جرائم رایانه‌ای (با نگاهی به قانون جرائم رایانه‌ای)؛ رویکرد چند نهادی به پیشگیری از وقوع جرم. *مجموعه مقالات نخستین همایش ملی پیشگیری از جرم*. تهران: معاونت آموزشی ناجا، صص ۱۴۳-۹۳.

- زیبر، اولریش (۱۳۹۰). *جرائم رایانه‌ای* (محمدعلی نوری، رضا نخجوانی، مصطفی بختیارون و احمد رحیمی مقدم، مترجمان). تهران: گنج دانش.

- صبح خیز، رضا (پاییز ۱۳۹۴). چالش‌های حقوقی جرائم سایبری در نظام حقوق

بین‌الملل و نظام حقوقی ایران. فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی. (۱۰)۳۹، صص ۱۳۸-۱۱۷. بازیابی از: goo.gl/Up7mU

- قاجارقیونلو، سیامک (۱۳۹۱). *مقدمه حقوق سایبر* (درآمدی بر جامعه‌شناسی حقوق توسعه و پیش‌نیازهای قانون‌نویسی در فضای سایبر). تهران: میزان.

- مقیمی، مهدی (۱۳۹۵). *سیاست‌ها و تدابیر سازمان ملل متحد برای پیشگیری از جرم سایبری (رسالهٔ دکتری)*. دانشگاه شهید بهشتی. تهران.

منابع انگلیسی

- Jacobs, T. (2010). *Teen Cyber bullying Investigated: Where Do Your Rights End and Consequences Begin?* United States of America: Perfection Learning.

- Bryant, R. Bryant, S. (2014*). Policing Digital Crime*. England: Ashgate Publishing.

- Brenner, S., Goodman, M. (2002). Cybercrime: The Need to Harmonize National Penal and Procedural Laws. *International Society for the Reform of Criminal Law 16th Annual Conference Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice*, 16th Annual Conference Technology and Its Effects On Criminal Responsibility, Security,Criminal justice,PP 1-37.

- Cryer, R. Friman, H. Robinson, D. Wilmshurst, E(2010). *An Introduction to International Criminal Law and Procedure*. United States of America: Cambridge University Press. Retrieved from: *assets.cambridge.org/97805211/35818/frontmatter/9780521135818_frontmatter.pdf*

- Council of Europe. *Explanatory Report to the Convention on Cybercrime.* Budapest, 23.XI.2001. European Treaty Series - No. 185. Retrieved from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.

- Eleventh United Nations Congress on Crime Prevention and Criminal Justice (2005). *Workshop 6: Measures to Combat Computer-related Crime*. A/CONF.203/14. Retrieved from https://documents-dds-ny.un.org/doc/UNDOC/GEN/V05/822/59/PDF/V0582259.pdf? Open Element.

- General Assembly of United Nations, *Combating the criminal misuse of information technologies*. (A/56/574) 56/121. 23 January 2002. Retrieved from: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf.

- Holt, T. Bossler,A. Seigfried-Spellar.K (2015). *Cybercrime and Digital*

Forensics: An Introduction. United states of America: Routledge.
- Kharouni, L (2013). *Africa: A New Safe Harbor for Cybercriminals?*.Trend Micro Incorporated. Retrieved from :*www.trendmicro.nl/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf*
- Kshetri, N (2010). Chapter2. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspective*s, USA: springer.
- Savona, E (2004). chapter3. *Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research*. Springer.
- *Scarlet Extended SA v SABAM—Société belge des auteurs, compositeurs et éditeurs SCRL*.(2001). Court of Justice of the European Union (ECJ), Case C-70/10.
- Ghernaouti-Hélie, S (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace,* Switzerland: EPFL Press.
- Ransome, J. Misra, A. (2014).*Core Software Security: Security at the Source*, Auerbach Publications. Retrieved from: *https://books.google.com/books?id=MX5cAgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.*
- Westby, J. (2003). *International Guide to Combating Cybercrime*. United States of America: American Bar Association.
- Taylor, P.(1999). *Hackers: Crime and the Digital Sublime*. UK: Routledge. Retrieved from: *https://books.google.com/books?id=0w-Qze539QC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=f alse*
- Simpson, M. Backman, K. Corley, J. (2013). *Hands on Ethical Hacking And Network Defense*. United States of America: Cengage Learning.
- Sofaer, A. Goodman, S (2001). *Cyber Crime and Security: The Transnational Dimension*, United States of America: Hoover Institution. Retrieved from: *media.hoover.org/documents/0817999825_1.pdf*
- Thirteenth United Nations Congress on Crime Prevention and Criminal Justice (2015).*Strengthening crime prevention and criminal justice responses to evolving forms of crime, such as cybercrime and trafficking in cultural property, including lessons learned and international cooperation.* Doha, 12-19 April 2015, Workshop 3. (A/CONF.222/12). Retrieved from:*https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_e_V1500663.pdf*
- United Nations Office On Drugs and Crime Vienna (2013). *Comprehensive Study on Cybercrime.* Retrieved from: *https://www.unodc.org/documents/...EG.4.../CYBERCRIME_STUDY_210213.pdf.*
- V. Clarke, R (1992). *Situational Crime Prevention: Successful Case Studies* (Second Edition). United States of America: Harrow and Heston. Retrieved from: *www.popcenter.org/library/reading/PDFs/scp2_intro.pd1f.*