فصلنامه رهیافت پیشگیری از جرم، دوره ۳، شماره ۱، بهار ۱۳۹۹
صفحه ۱۴۵ تا ۱۷۲
Prevention Approach Quarterly
Vol. 3 No. 1, Spring 2020

مقاله مروری

راهبردهای نوین پیشگیری از وقوع تروریسم سایبری

عاطفه عباسی کلیمانی[۱]، ملیکا محبوبی[۲]، فاطمه نوری[۳]

تاریخ دریافت: ۱۳۹۹/۰۱/۰۹ تاریخ پذیرش: ۱۳۹۹/۰۲/۲۹

چکیده

زمینه و هدف: به موازات نفوذ گسترده فضای مجازی در هر دو سطح کلان (حاکمیتی) و خرد (شهروندان)، تأمین امنیت آن نیز در کانون توجه قرار گرفته است. هر چند همه فعالیت‌های بزهکارانه در فضای مجازی از جهات موضوع، انگیزه بزهکار، اهمیت و آثار رفتار ارتکابی یکسان نیستند اما از این جهت که تمام رفتارهای بزهکارانه به نوعی امنیت را در این فضا خدشه‌دار می‌سازند با رفتارهای بزهکارانه در فضای حقیقی اشتراک دارند. بنابراین پژوهش حاضر با هدف بررسی و تحلیل راهبردهای نوین پیشگیری از جرائم سایبری انجام شد.

روش: پژوهش حاضر از نظر هدف کاربردی و از نظر روش تحقیق توصیفی - تحلیلی است. داده‌های پژوهش به شیوهٔ استقرایی - قیاسی و ضمن بهره‌گیری از منابع کتابخانه‌ای به بررسی انواع سیاست‌های پیشگیرانهٔ کیفری و غیر کیفری در عرصهٔ حقوق داخلی و بین‌المللی پرداخته است.

یافته‌ها: باید در نظر داشت که جرائم در فضای سایبر، در بستری متفاوت و با کیفیت خاصی ارتکاب می‌یابند بنابراین هر اقدام پیشگیرانه‌ای اعم از پیشگیری اجتماعی، وضعی و کیفری باید متناسب با این فضا تدارک دیده شود. بر این اساس و با عنایت به ویژگی‌های خاص جرائم سایبری، رویکرد رویارویی با این جرائم، نیازمند اتخاذ تدابیر پیشگیرانه خاص و در قالب پیشگیری اجتماعی است.

نتایج: از جمله اقدامات پیشگیری اجتماعی از وقوع جرائم سایبری می‌توان به برنامه‌های خانواده‌مدار، تدابیر آموزشی - سایبری، بالابردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، مشارکت و اجماع‌گری، ارتقای پاسخگویی و شفافیت، فرهنگ‌سازی و تولید رسانه‌ای اشاره کرد.

واژگان کلیدی: سایبر تروریسم، جرائم سایبری، پیشگیری از تروریسم سایبری، فضای سایبر، حقوق بین‌الملل کیفری.

۱. استادیار گروه حقوق، دانشگاه امام صادق (ع)، پردیس خواهران. تهران. ایران. (نویسنده مسئول). رایانامه: atefehabbasi@ius.ac.ir
۲. کارشناسی حقوق دانشگاه امام صادق (ع)، پردیس خواهران. تهران. ایران. رایانامه: melikamahboubi@yahoo.com
۳. کارشناسی حقوق دانشگاه امام صادق (ع)، پردیس خواهران. تهران. ایران. رایانامه: fatemhnoori@yahoo.com

مقدمه

یکی از موضوعاتی که زندگی بشر را با تحولات گسترده‌ای مواجه کرده، رایانه و فضای سایبر است. رایانه و بهره‌گیری از اینترنت از جمله روش‌های مورد استفاده افراد جهت انتقال اطلاعات در فضای مجازی است و تبادل اطلاعات موجود در سامانه‌های رایانه‌ای تاحدی توانسته زندگی بشر را دستخوش تغییراتی قرار دهد به گونه‌ای که با وجود حصول دستاوردهای مفید که در نتیجه رشد و گسترش فضای سایبر بوده، مشکلاتی را نیز به ارمغان آورده است. وقوع جرم علیه فناوری اطلاعات در فضای مجازی که با نام جرائم سایبری شناخته می‌شود، محدوده بزرگی از جرائم را شامل می‌شود که امنیت ملی کشورها را تهدید می‌کند. از سوی دیگر استفاده روزافزون اشخاص از فضای مجازی در امور مختلف ارتباطات تجاری، اقتصادی، فرهنگی، علمی، سیاسی، هنری و مانند آن، اتخاذ تدابیر خاص متناسب با این فضا را در زمینه پیشگیری و مقابله با وقوع این جرائم می‌طلبد. پیشگیری در مفهوم موسع، طیف وسیعی از اقدامات کیفری و غیر کیفری (اجتماعی و وضعی) را شامل می‌شود که مجموعه‌ای از تدابیر فردی و جمعی برای خنثی کردن عوامل ترکیبی وقوع جرم توسط مجرمان در آینده است. انواع کیفر و رسالت‌های آن نظیر ارعاب و عبرت‌آموزی، بازپروری مجرمان، جایگزین‌های کیفر که در نظام قضایی اعمال می‌شوند، در مفهوم موسع پیشگیری از جرائم قرار می‌گیرند. پیشگیری در مفهوم مضیق خود، اقدامات پیشگیرانه غیر کیفری را شامل می‌شود. پیشگیری غیر کیفری عبارت است از اقدام مناسب غیر کیفری که قبل از وقوع پدیده مجرمانه از طریق کاهش یا حذف و خنثی‌سازی علل جرم‌زا و نامناسب نشان دادن موقعیت‌های ارتکاب، درصدد جلوگیری از رخ دادن بزه است و در رایج‌ترین طبقه‌بندی بر دو قسم پیشگیری اجتماعی (جامعه‌مدار و رشدمدار) و پیشگیری وضعی تقسیم می‌شود. نقطه اشتراک تمام روش‌های پیشگیری از جرم توجه به وضعیتی است که عمل مجرمانه در آن شکل می‌گیرد. کانون توجه، تغییر سازوکارها و مدیریت پیرامون

دوره ۳، شماره ۱، بهار ۱۳۹۹/2020 Vol. 3, No. 1, Spring

ارتکاب جرم است، به نحوی که بزهکار معقول و محاسبه‌گر از دست یازیدن به عمل مجرمانه منصرف شود و یا توان غلبه بر شرایط محیطی را نداشته باشد اما در بحث پیشگیری از وقوع جرم در فضای سایبر باید ویژگی‌های انحصاری این جرائم را در نظر داشت. سرعت، کثرت، سهولت ارتکاب، ارزان بودن و هزینه کم ورود، بی‌مرز بودن و مشخص نبودن قلمرو جغرافیایی، ناشناختگی، خودکار بودن و تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبر و مانند آن در جرائم دیجیتال، موجب ظهور گونه‌ای متمایز از جرائم شده است. ویژگی‌های یادشده، سهولت سازماندهی و تهاجم از راه دور مجرمان سایبری از یک‌سو و وابستگی روزافزون ساختارهای اقتصادی، صنعتی، خدماتی، امنیتی و سیاسی به فضای سایبر از سوی دیگر، جامعه بشری را با تهدیدهای جدیدی مواجه ساخته است. از تلاقی اعمال تروریستی و فضای سایبر گونه‌ای نوپا از اعمال تروریستی با عنوان تروریسم سایبری پا به عرصه وجود نهاده است. تروریسم سایبری، با وجود نوظهور بودن به مراتب خطرناک‌تر از تروریسم سنتی و کلاسیک است و تهدیدات آن برای امنیت ملی دولت‌ها و کشورها به خطری بالقوه تبدیل شده است. بحث پیشگیری از جرم در فضای رایانه‌ای از آن رو اهمیت مضاعف می‌یابد که تهدیدها علیه امنیت ملی در این فضا با امکانات پیچیده‌ای همانند فناوری اطلاعات یا فناوری هسته‌ای صورت می‌گیرد که در مقایسه با تهدیدات گذشته، از تنوع بیشتری برخوردار است. تهاجمات سازمان یافته سایبر می‌تواند تمام زیرساخت‌های اجتماعی را در بر گرفته و حتی امنیت و حاکمیت ملی را هدف قرار دهند. از سوی دیگر پنهان بودن و جهانی بودن این دسته از جرائم، امکان شناسایی، مهار و کنترل آنها را دشوار می‌سازد. بر این اساس به نظر می‌رسد اقدامات پیشگیرانه غیر کیفری و به خصوص پیشگیری اجتماعی می‌تواند مؤثرترین راه برای پیشگیری و مقابله با این تهدیدات نوین بشمار رود. بدیهی است که پیشگیری به مراتب آسان‌تر از درمان بوده و هزینه‌های آن نیز کمتر از هزینه‌های درمان است و همچنین پیشگیری در سلامت فردی و اجتماعی نقش سازنده‌تری را ایفاء می‌کند و در این میان، پیشگیری اجتماعی دربردارنده دو

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

حیطه فردمدار و جامعه‌مدار است. منظور از پیشگیری اجتماعی مجموعه اقداماتی است که در پی حذف یا خنثی‌کردن آن دسته از عواملی است که در تکوین جرم مؤثر هستند. این نوع پیشگیری بر مبنای علت‌شناسی جرائم استوار است و با دخالت در محیط‌های اجتماعی مانع از شکل‌گیری رفتارهای بزهکارانه و خنثی‌سازی عوامل جرم‌زا می‌شود و با ایجاد تغییرات و اصلاحات در محیط اجتماعی به دنبال جلوگیری از وقوع جرم است. به همین دلیل درصدد است با بهره جستن از تدابیری در زمینه بالا بردن سطح آموزش، تربیت و یا روش‌هایی همچون تشویق و تنبیه، کاهش یا از بین بردن فقر، اشتغال‌زایی، فرهنگ‌سازی و حمایت از افراد ویژه، آنها را با قواعد اجتماعی همنوا سازد و با نهادینه‌کردن فرهنگ استفاده صحیح از فضای سایبر و بالابردن سطح سواد رسانه‌ای، از وقوع جرائم سایبر پیشگیری کند. آنگاه که عوامل جرم‌زا ناشی از مراحل مختلف رشد کودک و نوجوان است آن را پیشگیری فردمدار (رشدمدار) می نامند و زمانی که عوامل جرم‌زا ناشی از محیط‌های پیرامون انسان مدنظر باشد از آن به پیشگیری جامعه‌مدار یاد می‌شود. بدین ترتیب هر دو قسم پیشگیری اجتماعی با استفاده از تدابیر و اقدامات کنشی «غیر کیفری» به دنبال شخصیت‌سازی، مردم‌آمیزی و جامعه‌پذیری افراد است. مسلم است که بهره‌برداری صحیح و سودمند از این فضا مستلزم رعایت هنجارهایی است که تخطی از آنها می‌تواند باعث آسیب‌هایی شود و برخی از آنها حتی مستوجب جرم‌انگاری و مجازات شوند. با این‌حال، چنانچه به کاربران آموزش‌های صحیح داده نشود، هرگونه مقابله با هنجارشکنی‌های سایبری برای برقراری موازین اخلاقی سایبری، می‌تواند با ایرادات جدی حقوقی و اخلاقی مواجه شود. به همین جهت رویکرد این نوع پیشگیری، تقویت روابط اجتماعی، افزایش سطح کنترل غیر رسمی و در نتیجه بازدارندگی بالقوه و بالفعل از ارتکاب جرم است. اجتماع و فرهنگ، نقش بی‌بدیلی در رویکردهای پیشگیرانه غیر کیفری دارند. آموزش و فرهنگ به عنوان بستر حرکت جوامع و الگوهایی که انعکاس‌دهنده ارزش‌ها، سنت‌ها و هنجارهای پایدار جامعه هستند، در مباحث امنیت در فضای سایبری باید مدنظر باشد. با این تفاسیر ضرورت

دوره ۳، شماره ۱، بهار ۱۳۹۹/2020 Vol. 3, No. 1, Spring

پیش‌بینی و اتخاذ سیاست‌ها و قواعد جدید متناسب با تحول سریع فناوری در دیگر علوم و علم حقوق، یک امر غیر قابل انکار و الزامی است. به همین منظور در پژوهش حاضر ضمن بررسی اقدامات پیشگیرانه کیفری و غیر کیفری در نظام حقوقی ایران، به بررسی این امر در عرصه بین‌المللی نیز پرداخته شده است. در این راستا به بررسی اقسام برنامه‌های پیشگیرانه اجتماعی برای جلوگیری از این جرائم در حوزه ملی و اسناد بین‌المللی و منطقه‌ای در حوزه فراملی اشاره شده است.

پیشینه: میرعباسی و کورکی‌نژاد قرایی (۱۳۹۷) در پژوهش خود با عنوان «قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در مادۀ ۵۱ منشور سازمان ملل متحد» نوشته‌اند که تروریسم با پیدایش جوامع انسانی آغاز شده و در بستر پیشرفت جوامع با سرعت فزاینده‌ای خود را دگرگون کرده است. از نوین‌ترین گونه‌های تروریسم که امروزه توجه بسیاری از اندیشمندان را به خود جلب کرده، باید به تروریسم سایبری اشاره کرد. این پدیده به‌دلیل بستر بی‌همتای ارتکاب آن یعنی فضای سایبر، دچار ابهامات بیشتری می‌شود که، سنگ بنای بررسی سایر جنبه‌های آن، بررسی قابلیت تحقق این پدیده در عالم واقع است. در این مقاله تلاش شده است تا وجود چنین پدیده‌ای را اثبات و در نهایت ارتباط آن با مادۀ ۵۱ منشور سازمان ملل متحد بررسی شود، زیرا صدق عنوان حملۀ مسلحانه بر اقدامات سایبری خود چالش بزرگ دیگری در خصوص این اقدامات است که پیامدهای بسیاری را ممکن است به‌همراه داشته باشد. احمری، کحلکی و رحیم پور اصفهانی (۱۳۹۵) در پژوهش خود با عنوان «تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن» نوشته‌اند که تروریسم سایبری از مصادیق مدرن تهدیدهای تروریستی است که به سبب استفاده از فناوری‌های نوین و رایانه‌ای فضای مجازی در آن، توسط بازیگرانی در عرصه بین‌الملل استفاده می‌شود و از دانش فناورانۀ بالایی برخوردار هستند. از آنجایی که معمای امنیت بزرگ‌ترین مسئله بشری بوده و تهدیدهای امنیتی تروریسم نوین سایبری آن‌گونه که سازه‌انگاران معتقدند از رهگذر برساخت‌های امنیتی و هویتی باید نگریسته شود، این

پژوهش، امنیت سایبری را مبتنی بر ساختارهای هویتی و امنیتی ارزیابی کرد که به شکل‌گیری نظام‌های حقوقی در عرصه داخلی و بین‌المللی انجامیده است؛ پژوهش یادشده، از رهگذر مطالعه‌ای بین رشته‌ای و مبتنی بر نگاهی سازه‌انگارانه، پدیده سایبر تروریسم را بررسی کرده و به این پرسش مهم پاسخ داده است که چگونه چارچوب‌های ذهنی بازیگران در عرصه بین‌المللی بر ایجاد تهدیدهای سایبری مؤثر خواهد بود. موسوی، حیدری و قنبری (۱۳۹۲) در پژوهش خود با عنوان «تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن» نوشته‌اند که امروزه گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و از این جهت درک واقع‌بینانه از تهدیدات امنیتی در گرو توجه به عوامل نرم‌افزاری است که در واقع حلقه واسط بین محیط امنیتی کشورها و سخت‌افزارها قرار دارند و بدین جهت برداشت‌ها از مفهوم امنیت ملی در این فضا به چالش کشیده شده است. تروریسم سایبری با هدف نابودسازی ساختارهای اساسی یک کشور از جمله این تهدیدات (علیه امنیت ملی) است. این جرم از جمله مهم‌ترین جرائم فراملی در فضای مجازی می باشد. نوع پیشگیری، مقابله و مبارزه با این جرم، با نوع اقدامات کنترلی در سایر جرائم به کلی متفاوت است. در جرم تروریسم سایبری، جرم فاقد محل وقوع است. این جرم فرامرزی بوده و تهدیدی مستقیم علیه منافع و امنیت ملی کشور است. در این زمینه لازم است تدابیر تقنینی، قضایی و اجرایی ویژه‌ای در سطح ملی و بین‌المللی در نظر گرفته شود.

دوره ۳، شماره ۱، بهار ۱۳۹۹/2020 Vol. 3, No. 1, Spring

ادبیات پژوهش

اقدامات پیشگیرانه کیفری از وقوع تروریسم سایبری در نظام حقوقی ایران: پیشگیری از وقوع تروریسم سایبری به منظور حمایت از بزه‌دیدگان آن است و به منظور ممانعت از هرگونه ایراد خسارت بیشتر به زیرساخت‌های اطلاعاتی کشور، لزوم اتخاذ تدابیر پیشگیرانه احساس می‌شود اما در میان بیشتر نظام‌های حقوقی جهان، به جرم‌انگاری تروریسم سایبری،

صریح و اختصاصی پرداخته نشده است. بررسی منابع قانونی در حقوق ایران نشان می‌دهد که در خصوص پیشگیری از این بزه در مقررات کیفری، مقرره خاصی وجود ندارد بلکه با استناد به برخی قوانین عام همچون قانون جرائم رایانه‌ای و قانون مجازات اسلامی می‌توان به مواضع پیشگیرانه حقوق کیفری ایران در زمینه پیشگیری از این بزه و حمایت از بزه-دیدگان آن اشاره کرد. بنابراین قانون کیفری ایران فاقد جرم‌انگاری مستقل درباره تروریسم و جرائم آن است و در واقع، سیاست جنایی ایران مبتنی بر سیاست مصداقی است یعنی می‌توان از موضوعاتی که با مفهوم تروریسم منطبق است مانند محاربه، آن را تشخیص داد (قدیر و کاظمی فروشانی، ۱۳۹۸، ص ۲۳۷). در ادامه به اقدامات پیشگیرانه کیفری در نظام حقوقی ایران اشاره می‌شود:

الف- قانون جرائم رایانه‌ای مصوب ۱۳۸۸: در خصوص مواد قانونی کیفری، در رابطه با پیشگیری از وقوع تروریسم سایبری و برای حمایت از بزه دیدگان آن، می‌توان به موادی از این قانون اشاره کرد که شباهت خاصی به جرم‌انگاری تروریسم سایبری دارد. ماده ۱۱ این قانون مقرر می‌دارد: «هر کس به قصد به خطر انداختن امنیت، آسایش و امنیت عمومی اعمال یادشده در مواد ۸، ۹ و ۱۰ این قانون را علیه سیستم‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می‌روند از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود به حبس از سه تا ده سال محکوم خواهد شد». مقرره یادشده دو دسته از بزهکاران یعنی اشخاص حقیقی و حقوقی را خطاب قرارداده است که با تعیین کیفر در انتهای ماده به بازدارندگی مرتکبان افعال مندرج در ماده ۱۱ اشاره کرده است. بزهدیدگان مورد حمایت در این مقرره، سامانه‌های رایانه‌ای و مخابراتی هستند که برای ارائه خدمات ضروری عمومی به کار می‌روند. با توجه به اینکه در تروریسم سایبری به تأسیسات عمومی حمله می‌شود، اقدام شایسته‌ای توسط قانونگذار به شمار می‌رود. در این راستا قانونگذار با تعیین مجازات، به ارعاب بزهکاران بالقوه که قصد ارتکاب اعمال مندرج در این ماده را دارند و همچنین تکرار بزه توسط بزهکاران بالفعل

اقدام کرده است. قانون جرائم رایانه‌ای در مبحث دوم از این قانون به موضوع تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی پرداخته است که با جرم‌انگاری اعمال غیر مجاز از قبیل حذف یا تخریب یا مختل یا غیرقابل پردازش کردن داده‌های رایانه‌ای و مخابراتی، دو گونه مجازات را برای مرتکب این افعال در نظر گرفته است: یکی حبس از شش ماه تا دو سال و دیگری، جزای نقدی از ده تا چهل میلیون ریال یا هر دو مجازات که گام مفیدی برای برحذر داشتن افرادی است که با توسل به چنین اعمالی به زیرساخت‌های اطلاعاتی کشور، به منظور دستیابی به اهداف مختلف استفاده می‌کنند. یکی دیگر از جلوه‌های پیشگیری واکنشی از جانب قانونگذار کیفری، به منظور پیشگیری و مقابله با جرائمی از قبیل تروریسم سایبری، ماده دیگری از همین قانون است که به طور غیر حصری و مصداقی به افعال غیر مجازی اشاره کرده است که منجر به توقف یا اختلال عملیات سامانه‌های رایانه‌ای یا مخابراتی می‌شود. دسته‌ای دیگر از اعمال غیر مجازی که به طور معمول توسط تروریست‌های سایبری به منظور تخریب یا اختلال در داده‌ها و سامانه‌های رایانه‌ای و مخابراتی استفاده می‌شود، افعالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌هاست که بدین وسیله، منجر به ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی می‌شود. قانونگذار در این سه ماده به صورت کامل و غیر حصری به شایع‌ترین اعمال ارتکابی که علیه تأسیسات حیاتی کشور انجام می‌شود پرداخته است که اقدام شایسته‌ای در خصوص جرم‌انگاری افعال مرتبط با تروریسم سایبری به شمار می‌رود. همچنین قوانینی که به طور مستقیم به بیان مجازات اشخاصی که تأسیسات حیاتی کشور، اعم از رایانه‌ای و مخابراتی تعرّض می‌کنند، اشاره دارند، در لابه لای موادی دیگر از قانون جرائم رایانه‌ای، دسته‌ای از افعال جرم‌انگاری شده وجود دارد که برای ارتکاب تروریسم سایبری در اولویت قرار دارند. نمونه‌ای از افعال یادشده، جاسوسی رایانه‌ای، شنود و دسترسی غیر مجاز است که نفوذگران تروریستی از بدافزارهای گوناگونی برای دستیابی به اطلاعات محرمانه و حیاتی از آن‌ها استفاده می‌کنند. عناصر این جرم در حقیقت هر نوع

Vol. 3, No. 1, Spring 2020 دوره ۳، شماره ۱، بهار ۱۳۹۹

پردازش، مشاهده، شنود، دریافت یا ذخیره غیر قانونی اطلاعات در حال انتقالی است که مجرم، مجاز به دریافت یا شنود آن نیست، آن جا که داده غیر عمومی و خصوصی است، اگر غیر تجاری باشد مشمول ماده ۳ قانون مجازات جرائم رایانه‌ای می‌شود اما اگر تجاری باشد مشمول ماده ۵۸ قانون تجارت الکترونیکی است. اما اگر عمومی و جزء اطلاعات سرّی باشد، مشمول ماده ۴ قانون مجازات جرائم رایانه‌ای است. ماده ۳ فروعِ مختلف شنود و دریافت غیر مجاز، اعم از شنود داده‌های خصوصی، تجاری، عمومی سرّی و مربوط به امنیت ملی را شامل می‌شود. اما مواد خاصی چون ماده ۵۸ قانون تجارت الکترونیکی و ماده ۴ قانون مجازات جرائم رایانه‌ای موارد تجاری و مربوط به امنیت ملی را تخصیص می‌دهند (قدیر و کاظمی فروشانی، ۱۳۹۸، ص ۲۳۹-۲۴۰).

ب- قانون تجارت الکترونیکی مصوب ۱۳۸۲: با توجه به این که داده‌های رایانه‌ای و مخابراتی، اصلی‌ترین آماج جرم برای تروریست‌های سایبری محسوب می‌شود، لزوم حمایت از آن در برابر افعال غیر مجاز که به تمامیت و محرمانه بودن آن‌ها تعرض می‌کند ضروری است. فصل دوم از مبحث سوم این قانون، مجازات اشخاصی را بیان می‌کند که شرایط داده‌های مورد حمایت در مواد ۵۸ و ۵۹ این قانون را نقض می‌کنند و برای مرتکب کیفر یک تا سه سال حبس را تعیین کرده است. در جای دیگر از این قانون به نهادهای مسئول و دفاتر خدمات صدور گواهی الکترونیکی اشاره می‌کند. در این صورت برای مرتکب، حداکثر کیفر تعیین شده در ماده ۷۱ مقرر شده است. همچنین قانون تجارت الکترونیکی نیز با بی‌مبالاتی و بی‌احتیاطی دفاتر خدمات صدور گواهی (که مسئول حفظ داده پیام‌های شخصی نیز هستند) برخورد می‌کند. ماده ۶۴ قانون تجارت الکترونیکی بر اصل ممنوعیت دسترسی غیر مجاز تأکید کرده و با ناقضان این اصل، برخورد شدیدی کرده است. ماده ۷۵ این قانون، مجازات شدیدتری نسبت به ماده ۲ قانون مجازات جرائم رایانه‌ای تعیین کرده است. به موجب این ماده: «متخلفان از ماده ۶۴ این قانون به حبس از شش ماه تا دو سال و نیم و جزای نقدی معادل ۵۰ میلیون ریال محکوم خواهند شد».

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

ج- قانون مجازات نیروهای مسلح مصوب ۱۳۸۲: امنیت اطلاعاتی یک کشور، زمانی حفظ خواهد شد که ماموران ذی ربط با جدیت تمام در برابر حملات اطلاعاتی بایستند و هشیارانه و بدون کمترین اشتباهی از اطلاعات سرنوشت‌ساز کشور حراست کنند. از این روست که قانونگذاران به دلیل اهمیت حیاتی این موضوع، برخورد قاطعانه‌ای با کمترین کوتاهی در انجام وظائف در آن دارند. قانونگذار در ماده ۵۰۶ قانون مجازات اسلامی، ماموران آموزش‌دیده دولتی را که مسئول امور حفاظتی و اطلاعات طبقه‌بندی شده، هستند و به دلیل بی‌مبالاتی و رعایت نکردن اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند، به یک تا شش ماه حبس محکوم می‌کند. این قانون نیز در راستای جرم‌انگاری افعال غیر مجاز اقسام اعمال رایانه‌ای نظامیان را جرم‌انگاری کرده است که با توجه به مجازات‌های تعیین شده، بازدارندگی خاصی را برای این دسته از افراد تخصیص داده است. از جمله جرائم رایانه‌ای مورد اشاره در این قانون که افعال تشکیل دهنده تروریسم سایبری محسوب می‌شود و تروریست‌های سایبری از این طریق به فلج کردن زیرساخت‌های کشور اقدام می‌کنند، عبارت‌اند از: تخریب اطلاعات یا نرم‌افزارهای رایانه‌ای، تخریب سامانه‌های رایانه‌ای، سرقت یا معدوم کردن حامل‌های اطلاعاتی رایانه‌ای که قانونگذار حسب مورد، مرتکب را به مجازات‌های مقرر در این قانون محکوم می‌کند. با توجه به اینکه نیروهای نظامی و امنیتی به دلیل موقعیت شغلی در موقعیت‌های حساس و ویژه قرار دارند تدوین ضمانت اجراهای قوی به منظور ارعاب کارکنان سازمان‌های امنیتی حیاتی است. در این قانون به جرم‌انگاری دسته‌ای از افعال غیر قانونی نظیر تحریب اطلاعات اشاره شده است که رکن اصلی افعال تشکیل‌دهنده تروریسم سایبری به شمار می‌رود. حملات خودی که از شایع‌ترین حملات سایبری محسوب می‌شود، بیشتر توسط کارکنانِ ناراضی ارتکاب می‌یابد و نیروهای مسلح نیز از این امر مستثنا نیستند. به همین دلیل مفاد ماده ۱۳۱ قانون مجازات نیروهای مسلح می‌تواند در زمینه پیشگیری کیفری از تروریسم سایبری مؤثر واقع شود.

دوره ۳، شماره ۱، بهار ۱۳۹۹/2020 Vol. 3, No. 1, Spring

اقدامات پیشگیرانه کیفری در عرصهٔ بین‌المللی: در سال‌های ۱۹۹۰، ۱۹۹۵ و ۲۰۰۲ مجمع عمومی سازمان ملل متحد و شورای اقتصادی اجتماعی سازمان ملل متحد، سه رهنمود درباره پیشگیری از جرم بدین شرح تصویب کرده‌اند: «رهنمود همکاری و کمک‌های فنی درباره پیشگیری از جرائم شهری» که به قطعنامه ۱۹۹۵/۹ شورای اقتصادی و اجتماعی پیوست شده است، رهنمودهای سازمان ملل متحد برای پیشگیری از بزهکاری نوجوانان طی قطعنامه ۱۱۲/ ۴۵ سال ۱۹۹۰ مجمع عمومی و در نهایت رهنمود پیشگیری از جرم که به قطعنامه ۲۰۰۲/۱۳ شورای اقتصادی اجتماعی پیوست شده است.» این اسناد حاصل دیدگاه‌های مشترک کشورهای عضو سازمان ملل است که می‌توان محتوای آن‌ها را ناظر بر اصول و خطوط کلی و بین‌المللی پیشگیری از جرم دانست. بنابراین این سه سند، اسناد پایه و استاندارد و بین‌المللی هستند که با هدف پیشگیری از جرم تدوین شده‌اند. اما از دیدگاه تخصصیِ ناظر بر جرائم سایبری باید توجه داشت که رهنمود همکاری کمک‌های فنی در خصوص پیشگیری از جرائم شهری توجه خود را به برنامه‌های بومی و محلی برای پیشگیری در مناطق شهری معطوف ساخته است، از این رو این سند معیارهای لازم برای مواجهه با جرائم سایبری را ندارد. در حالت استاندارد، معیار اصلی برای پیشگیری از جرائم سایبری، توجه به فراملی بودن این قبیل جرائم است که به دنبال آن همکاری‌های بین‌المللی، اتخاذ سیاست‌های حقوقی مناسب و تدابیر امنیتی متناسب با این خصیصه لازم می‌آید. در رهنمودهای سازمان ملل برای پیشگیری از بزهکاری نوجوانان، اشاره‌ای به جرائم سایبری، جرائم رایانه‌ای و به طور کلی نقش فناوری‌های اطلاعاتی و ارتباطی در ارتکاب جرم نشده است اما این سند از دو جهت قابل بررسی است:

اول اینکه برخی ارکان، اداره یا نهادهای سازمان ملل را به صراحت مسئول رصد کردن بزهکاری و بزه‌دیدگی نوجوانان کرده است، امری که دولت‌های عضو سازمان ملل در سطح ملی مسئولیت آن را برعهده دارند (مواد ۶۶ و ۶۵ رهنمود). به همین ترتیب نهادها یا سازمان‌های ملی، منطقه‌ای و بین‌المللی مسئول انجام پژوهش‌های علمی و پیمایش‌هایی با

هدف پیشگیری از بزهکاری نوجوانان شده‌اند (مواد ۶۲ و ۶۳ و ۶۴ رهنمود) که هر دو مسئله می‌تواند درباره جرائم سایبری مصداق داشته باشد. دوم اینکه این سند از نظر جرم‌شناختی، نظرات را به صورت مستقل به نوجوانان معطوف می‌سازد. درباره رهنمود پیشگیری از جرم، یازدهمین کنگره پنج ساله سازمان ملل، اعلامیه بانکوک با عنوان «اقدام‌های جمعی و واکنش‌ها: ائتلاف‌های راهبردی در پیشگیری از جرم و عدالت کیفری» را صادر کرده است که در بند ۱۰ آن بیان می‌کند یکی از مبانی قطعی برای پیشگیری از جرم در سطح فراملی، رهنمود سال ۲۰۰۲ سازمان ملل متحد است. به دنبال آن دوازدهمین کنگره پنج ساله نیز چارچوب‌ها، اصول، ساختار و رویکردهای این سند را تصدیق کرده و به اجرایی کردن رهنمودهای سازمان ملل در پیشگیری از جرم می‌پردازد. بنابراین این سند بیش از دیگر اسناد، مبنایی برای دریافت اصول و خطوط کلی و بین‌المللی پیشگیری از جرائم سایبری در نظر گرفت (مقیمی، ۱۳۹۵، ص ۳۳-۳۴).

اقدامات پیشگیرانه غیر کیفری در نظام حقوقی ایران: پیشگیری غیر کیفری «کنشی»، تدابیر و شیوه‌های مختلفی است که برای پیشگیری از جرم و بزهکاری در بیرون از نظام کیفری به کار می‌روند. پیشگیری کنشی شامل آن دسته تدابیر و اقدامات غیر کیفری است که به پیش از ارتکاب جرم از طریق مداخله در اوضاع و احوال پیش جنایی و فرآیند شکل گیری شخصیت افراد به دنبال جلوگیری از وقوع بزهکاری است. رایج‌ترین طبقه‌بندی پیشگیری غیر کیفری عبارت‌اند از: ۱-پیشگیری اجتماعی ۲-پیشگیری وضعی (صبح دل، ۱۳۹۶، ۹۴) همیشه آنچه در مبارزه علیه یک پدیده ناخواسته موثرتر است، اقدام در از بین بردن علل و عوامل به وجود آورنده آن است که با رفع آنها معلول نیز خود به خود منتفی می‌شود. درباره پدیده بزهکاری نیز همین موضوع صادق است، بنابراین در ادامه به بررسی پیشگیری اجتماعی پرداخته خواهد شد.

پیشگیری اجتماعی از تروریسم سایبری: پیشگیری اجتماعی شامل آن دسته از تدابیر و اقداماتی است که با مداخه در فرآیند رشد افراد، بهبود شرایط زندگی آنها و سالم‌سازی

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

محیط اجتماعی و محیط طبیعی به دنبال حذف یا کاهش علل جرم‌زا و در نتیجه پیشگیری از بزهکاری است (نیازپور، ۱۳۸۲، ص ۱۳۸). پیشگیری اجتماعی، علل و عوامل اجتماعی مؤثر بر ظهور بزه را مدنظر داشته و با توجه به عوامل اقتصادی، سیاسی، فرهنگی و اجتماعی و تأمین حقوق اجتماعی، سیاسی و اقتصادی و مانند آن، سعی در کاهش یا ریشه کن کردن جرم دارد. پیشگیری اجتماعی به دنبال از بین بردن انگیزه‌های مجرمانه و منحرفانه است. به عبارت دیگر، پیشگیری اجتماعی بر مبنای علت‌شناسی جرم استوار است که نظر بر حذف یا خنثی کردن عواملی دارد که در تکوین جرم موثرند و با دخالت در محیط‌های اجتماعی مانع از شکل‌گیری انگیزه‌های بزهکارانه و خنثی‌سازی عوامل جرم‌زا می‌شود. عمده راهکارهای پیشگیری اجتماعی عبارت‌اند از: بسیج اجتماعی شهروندان که بدون تردید در بالابردن سطح کنترل، نظم و حمایت اجتماعی تأثیر فوق‌العاده‌ای دارد که با مدیریت و تدبیر مناسب قابل دسترسی است. توجه به نهادهای اجتماعی نظیر خانواده، مدرسه، محیط کار یا بازار که معمولاً در طی یک دوره زمانی اثر می‌گذارند. پیشگیری اجتماعی با استفاده از محیط‌های دور و نزدیک نسبت به افراد به دنبال تأثیر بر فرآیند شکل گیری شخصیت آنان است (شیرازی، ۱۳۸۴، ص ۱۹).

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

روش

پژوهش حاضر از نظر هدف کاربردی و از نظر روش پژوهش توصیفی - تحلیلی است. داده‌های پژوهش به شیوهٔ استقرایی - قیاسی و ضمن بهره‌گیری از منابع کتابخانه‌ای به بررسی انواع سیاست‌های پیشگیرانهٔ کیفری و غیر کیفری در عرصهٔ حقوق داخلی و بین‌المللی پرداخته است.

یافته‌ها

پیشگیری اجتماعی رشدمدار از جرائم سایبری: پیشگیری اجتماعی رشدمدار که به آن پیشگیری زودهنگام «زودرس» نیز گفته می‌شود در تلاش است تا با اتخاذ تدابیر مناسب و

به کارگیری به هنگام اقدامات حمایتی از پایداری رفتارها و گرایش‌های مجرمانه در افرادی که در سنین پایین و دوران کودکی دچار ناسازگاری، کجروی و بزهکاری زودرس شده‌اند، جلوگیری کند. (نیازپور، ۱۳۸۳، ص ۱۲) امروزه نسل کودک و نوجوان به نسبت گذشته با فضای سایبری انس بهتری گرفته است و به موازات آن از خطرات این فضا همچون فعالیت‌های علیه امنیت کشور مانند تبلیغ علیه نظام و مذهب رسمی کشور و ایجاد اختلافات و تنفرات قومی در امان نیستند. از این رو باید آن‌ها را از خطرات و آسیب‌های فراوان این فضا آگاه کرد. در این زمینه پیشگیری رشدمدار تنها گونه پیشگیری است که به طور تخصصی در پی ممانعت از منحرف شدن کودکان و نوجوانان است (بهره‌مند و داودی، ۱۳۹۷، ص ۳۳). پیشگیری رشدمدار، به مجموعه تدابیری اشاره دارد که با خنثی‌سازی عوامل اجتماعی جرم‌زا و منحرفانه در سنین رشد و دوران تکامل شخصیتی کودکان به اجرا در می‌آید. با توجه به اینکه بیشترین طرفداران محیط سایبر، جوانان و نوجوانان هستند، بیشترین آمار بزهکاری و بزه‌دیدگی را نسبت به سایر اقشار جامعه به خود اختصاص می‌دهند. بنابراین با استفاده از رهیافت‌های پیشگیری رشدمدار می‌توان با مداخله در مراحل اولیه شکل‌گیری شخصیت کودکان و سنین رشد آنها با استفاده از تدابیر محدود و کنترل‌کنندهٔ دسترسی به فضای مجازی توسط والدین، رسانه‌های جمعی، مدرسه و تدابیر الزام‌آور قانونی، به طور فزاینده‌ای از بزهکاری یا بزه‌دیدگی آن‌ها در آینده جلوگیری کرد (قدیر و کاظمی کاشانی، ۱۳۹۸، ص ۲۴۵). پیشگیری رشدمدار به دنبال بهبود پایدار توانایی اجتماعی اطفالی است که خطر گرایش آن‌ها به بزهکاری و بزه‌دیدگی زیاد است. این نوع پیشگیری بر این اندیشه مبتنی است که رفتار و آداب اکتسابی دوران رشد، یعنی از تولد تا بزرگسالی، زمینه‌ساز ارتکاب اعمال مجرمانه و منحرفانه می‌شود. از این رو مداخلات و اقدامات معمول باید مانع عوامل خطری که صغار در معرض آن هستند، بشوند. در این راستا قدرت شناخت و تمیز کودکان و نوجوانان تقویت شده و مهارت‌های زندگی اجتماعی به آنان آموزش داده می‌شود تا بتوانند به هنگام مواجهه با معضلات به ویژه طیف گسترده جرائم علیه امنیت کشور، از خود

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

واکنشی منطقی نشان دهند. پیشگیری رشدمدار انواعی دارد که برای جلوگیری از کجروی، بزهکاری، و بزه‌دیدگی برنامه‌هایی پیش‌بینی کرده است (بهره‌مند و داودی، ۱۳۹۷، ص ۳۳) برای نمونه‌ای از تلاش‌های صورت گرفته به منظور پیشگیری از بروز انحرافات سایبری، می‌توان به برگزاری دوره‌های آموزشی رایانه در مدارس فنی حرفه‌ای و اماکن فرهنگی کشور اشاره کرد که از سنین پایین کودکی برای کودکان و نوجوانان اعمال می‌شود. به طور کلی روند شکل‌گیری جرم تابع سه عامل است. این سه عامل که به مثلث جرم مشهور هستند عبارت‌اند از: انگیزه مجرمانه که نقش اولیه را در پیدایش بزه ایفا می‌کند، مقدمه‌ای برای پیدایش قصد مجرمانه است که به دنبال انگیزه در فرد بزهکار به وجود می‌آید. عامل دوم، فرصت‌های ارتکاب جرم و عامل سوم، وسایل و ابزار ارتکاب است. پیشگیری اجتماعی از طریق روش‌هایی چون بالابردن ارزش‌ها و تقویت نهادهای اجتماعی، مانند خانواده و مدرسه، از بین بردن انگیزه‌های مجرمانه از طریق اصلاحات فردی و اجتماعی، مانند نارسایی‌های ذهنی و جسمی اقدام می‌کند. در زمینه موضوعات مورد بحث، این نوع پیشگیری در زمینه علت‌یابی و جلوگیری از به وجود آمدن ریشه‌های تروریسم در جامعه تاثیر بسزایی دارد (قدیر و کاظمی کاشانی، ۱۳۹۶، ص ۲۴۵). انواع برنامه‌های پیشگیری رشدمدار عبارت‌اند از:

الف- مداخله در فرآیند تحصیل و تدابیر خانواده‌محور: یکی از مهمترین اقدامات پیشگیرانه، لزوم توجه کنشگران اجتماعی به نقش و جایگاه خانواده است. خانواده به عنوان نخستین نهاد پرورشی فرد، نقش تعیین کننده‌ای در این تمایلات ایفا می‌کند به گونه‌ای که می‌توان گفت کلیه حالات و رفتارهای کودک اعم از بهنجار و نابهنجار، به محیط داخلی و تربیت خانوادگی بستگی دارد. برنامه‌های پیشگیری مبتنی بر خانواده، عوامل خطر بزهکاری و انحرافات آینده کودک را که با خانواده همخوانی دارد، هدف قرار می‌دهد. یافته‌های ناشی از مداخلات خانواده در پیشگیری از رفتارهای منحرفانه از طریق بهبود رشد فکری، عاطفی و آموزشی طرح‌ریزی شده‌اند. از جمله مسائل زیربنایی این برنامه‌ها، نحوه آموزش کودک و

Vol. 3, No. 1, Spring 2020 دوره ۳، شماره ۱، بهار ۱۳۹۹

جوان در انتخاب عاقلانه گزینه‌ها، نحوه انجام فعالیت‌های آنلاین تحت کنترل دیگران، واکنش به پیام‌های تبلیغاتی و تصاویر نامناسبی است که امنیت ملی را هدف قرار می‌دهند، است (بهره مند، داودی، ۱۳۹۷، ص ۳۴).

پیشگیری اجتماع‌مدار از تروریسم سایبری: زمانی که عوامل جرم‌زا ناشی از محیط‌های پیرامون انسان مدنظر باشد از آن به پیشگیری اجتماع‌مدار یاد می‌شود (شیرازی، ۱۳۸۴، ص ۱۹)؛ پیشگیری اجتماعی جامعه‌مدار که از پیشینه‌ای طولانی برخوردار است، در برگیرنده اقدام‌های اجتماعی، فرهنگی و پیشگیرنده‌ای است که نسبت به محیطهایی که فرد در آنها زندگی می‌کند، اعمال می‌شوند. این پیشگیری در تلاش است تا با اتخاذ تدابیر و اقدامات مناسب برای از بین بردن یا کاهش عوامل جرم‌زا بر محیط اثر گذارد. بدین ترتیب، این پیشگیری از یک سو با شناسایی عوامل محیطی تأثیرگذار بر بزهکاری و از سویی دیگر با اعمال اقدامات مرتبط با ساختارها و نهادهای اجتماعی به دنبال اجتماعی کردن افراد است (صبح دل، ۱۳۹۶، ص ۹۶). پیشگیری اجتماع‌مدار از جرائم امنیتی - سایبری به معنای اتخاذ تدابیر همگانی و عمومی برای ایجاد بستری است که این جرائم ارتکاب نیابند یا میزان آن کاهش یابد. این روش در پی از بین بردن یا کاهش عوامل جرم‌زا بر محیط اجتماعی و عمومی اثر گذارد و به دنبال مداخله در محیط اجتماعی عمومی مانند فرهنگی، اقتصادی، سیاسی است که درمورد همه مشترک است. این مدل به دنبال تعیین عوامل بزهکاری — بزه‌دیدگی و سازماندهی برنامه‌هایی به منظور مقابله با آن و تغییر شرایط اجتماعی - اقتصادی نامناسبی است که فرد در آن زندگی می‌کند و منشا رفتارهای ضداجتماعی وی می‌شود. باید این نکته را در نظر داشت که در پیشگیری اجتماع‌مدار از جرائم امنیتی - سایبری بار اصلی پیشگیری اجتماعی بر دوش دولت است که باید هم در راستای اصلاح ساختار خویش و آگاهانیدن کارمندان و شهروندان از جرائم امنیتی - سایبری و عواقب آن دست به ارائه برنامه و پیشنهاد بزند (بهره‌مند و داودی، ۱۳۹۷، ص ۳۶) در این روش، در محیط مداخله می‌شود تا جرم‌زایی و مجرم‌پروری کاهش یابد. این

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

محیط‌ها می‌تواند خانواده (ارتباط با والدین، محیط تشنج، گسست خانواده، تأثیر رفتار والدین، تأثیرات روابط عاطفی و مانند آن) یا مسکن باشد که خود دو بخش اصلی دارد: محیط انتخابی (خانواده شخص، شغل، تفریح، ارتباط جمعی، گروه‌های سازمان یافته، باندهای گروهی) و تحمیلی (محل تحصیل، سربازی، اردوها، زندان‌ها و مانند آن) (دانش، ۱۳۹۳، ص ۲۹۵-۳۲۸) در پیشگیری اجتماعی، ابتدا عوامل جرم‌زا شناسایی می‌شوند، آنگاه اقداماتی برای خنثی کردن یا کنار زدن آثار آن عوامل صورت می‌گیرد. انواع پیشگیری اجتماع‌مدار عبارت‌اند از:

الف-نهادینه کردن فرهنگ استفاده صحیح از فضای سایبری: یکی از تدابیر پیشگیرانه جامعه‌مدار جهت جلوگیری از بروز تبعات نامطلوب یک ابداع جدید، نهادینه کردن کاربری مشروع و صحیح از آن است. در این راستا فضای مجازی به عنوان دستاورد بشری همواره آثاری اعم از مثبت و منفی در جامعه به وجود آورده است که بدنبال آن سیاست‌گذاران جنایی کشورها به ارائه تدابیر لازم برای تبدیل استفاده‌های نامشروع از این فضا به کاربردهای مفید و مطابق با اهداف اساسی و ابتدایی این نوآوری، پرداخته‌اند. تبیین فرهنگ استفاده صحیح از فضای سایبر و ترویج و نهادینه کردن این فرهنگ در جامعه از اقدامات اساسی قلمداد می‌شود که باید با تمسک به ابزارهای اطلاع‌رسانی آن را عملی کرد. منظور از استفاده صحیح و مناسب از فضای سایبری صرف اشاره به تدابیر و اقدامات حفاظتی برای در امان ماندن از مخاطرات فضای سایبر نیست. در حقیقت تدابیر یادشده، ابزاری برای پیشگیری از بزه‌دیدگی و منفعل واقع شدن در مواجهه با جرائم سایبری است. در حالی که نهادینه کردن فرهنگ استفاده صحیح از این فضا، به معنای نهادینه کردن افکار و عقاید مثبت و مشروع نسبت به این فضا در جامعه است که در نتیجه منجر به ظهور استفاده مفید و مؤثر از این فضا می‌شود. به عبارت دیگر باید با استفاده از ابزارهای تبلیغاتی و آموزشی، ماهیت فضای سایبری را به گونه‌ای توصیف کرد که جامعه دنیای مجازی را به عنوان ابزاری جهت کمک به بشریت در راستای فعالیت‌های روزمره خود شناخته و همواره به

Vol. 3, No. 1, Spring 2020 دوره ۳، شماره ۱، بهار ۱۳۹۹

دنبال این باشد که از فضای سایبر برای تسهیل و تسریع در امور خود استفاده کند (اسلامی، ۱۳۹۴، ص ۹۳-۹۴). بسیاری از جرائم علیه امنیت در فضای سایبر را می‌توان با فرهنگ‌سازی چه در بعد داخلی و چه در بعد بین‌المللی خنثی کرد. در بعد داخلی تقویت فرهنگ قانون‌مداری، ایجاد اعتماد به ظرفیت‌های خود در افراد جامعه، حمایت از ارزش‌های اجتماعی و فرهنگ پذیرش برنامه‌های پیشگیری، زمینه پیشگیری از این دسته جرائم را فراهم می‌کند. چنانچه مردم بدانند که برنامه‌های پیشگیری به بهبود فضای زندگی و کاهش بزه‌دیدگی منجر می‌شود، بیشتر در برنامه‌های پیشگیری مشارکت خواهند کرد. در بعد بین‌المللی با لحاظ فرامرزی بودن جرائم امنیتی- سایبری، پیشگیری و فرهنگ‌سازی نیز باید چهره جهانی به خود بگیرد. دلیل این امر هم آن است که فضای سایبر و ارزش‌ها و هنجارهای آن جهانی است و در نتیجه باید یک فرهنگ مطلوب و صحیح جهانی بر فضای سایبر حاکم شود. بر همین اساس طبق قطعنامه ۵۸/۱۹۹ مجمع عمومی سازمان ملل، امنیت سایبری در گرو یک فرهنگ جهانی شناخته شده است (بهره‌مند و داودی، ۱۳۹۷، ص ۴۳).

ب- بزه‌دیده‌زدایی و تدوین قوانین به روز و کارآمد: بزه‌دیده سایبری شخصی است که به علت بی‌احتیاطی و ناآگاهی از تدابیر حفاظتی در برخی مواقع خود عامل اصلی ارتکاب یک جرم سایبری است. جرم‌انگاری و تعیین واکنش‌های تأدیبی و کیفری متناسب با جرائم سایبری نه تنها مجرمان و محکومان را با اعمال و اقدامات ترهیبی و ترذیلی از ارتکاب مجدد این جرائم باز می‌دارد، بلکه صرف جرم قلمداد شدن یک اقدام و پیش‌بینی واکنش متناسب در مقابل آن، خود می‌تواند عاملی مؤثر در منصرف کردن افراد مستعد به ارتکاب جرم باشد. در تدوین نوع قوانین همواره باید به این نکته توجه داشت که مطابق نظریه الگوی اقتصادی جرم، مجرمان بالقوه بسته به نتایجِ براورد هزینه و نفع، فعالیت‌های مشروع یا نامشروع را مرتکب می‌شوند. در رابطه با جرائم سایبری نیز، نظر به اینکه منافع حاصل از این جرائم به تناسب گستردگی این فضا و گمنام بودن مجرمان سایبری زیاد است، باید در مقابل آن سیاست قانونگذاری متناسب ایجاد شود تا بتوان با بالا بردن هزینه ارتکاب جرم به

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

عنوان عاملی بازدارنده در مقابل مجرمان بالقوه این جرائم قرار گرفت (اسلامی، ۱۳۹۴، ص ۹۷-۹۵).

ج- اطلاع‌رسانی عمومی و رفع مشکلات اقتصادی: هرچند کوشش‌ها برای دستیابی به آمار جرائم مرتبط با رایانه به دلیل نبود سازوکارهای گزارش‌دهی و ثبت سوابق دشوار است اما تهیه آمار و ارقام جرائم سایبری ارتکابی، تعیین نوع جرائم پرتکرار، شیوه و نحوه ارتکاب این جرائم و در اختیار عموم قراردادن این اطلاعات با حفظ حریم خصوصی اشخاص از ابزارهای دیگری است که می‌توان جهت آگاه‌سازی جامعه از تهدیدات این فضا استفاده کرد. رسانه‌های جمعی مانند روزنامه‌ها، نشریات، صداوسیما و اینترنت و ماهواره از جمله ابزارهایی هستند که می‌توان از آن‌ها برای اطلاع‌رسانی عمومی استفاده کرد. براساس بند ۲ اصل ۳ قانون اساسی، بالابردن سطح آگاهی‌های عمومی در همه زمینه‌ها با استفاده صحیح از مطبوعات و رسانه‌های گروهی و وسایل دیگر، از وظایف اساسی جمهوری اسلامی ایران است. حق اطلاع‌رسانی و کسب اطلاع، پیش‌تر در اسناد بین‌المللی که ایران به آن‌ها ملحق شده است نیز به عنوان حقوق بشر پذیرفته شده است. از جمله ماده ۱۹ اعلامیه جهانی حقوق بشر که مقرر می‌دارد: «هر کس حق آزادی عقیده و بیان دارد و حق مزبور شامل آن است که از داشتن عقاید خود بیم و اضطرابی نداشته باشد و درکسب اطلاعات و افکار و در اخذ و انتشار آن با تمام وسایل ممکن و بدون ملاحظات مرزی، آزاد باشد.» اطلاع‌رسانی می‌تواند از طریق رسانه‌های سنتی مانند رادیو و تلویزیون در کنار اینترنت و اعلامیه‌های خدمات عمومی یا ویدئوها برای دادن اطلاعات کلی راجع به مسائل مربوط به جرم، اطلاعات مربوط به خدمات یا تغییرات جدید راهبردها و پیشرفت طرح‌ها انجام شود. به علت پیچیدگی، گستردگی و پنهان بودن فضای سایبر امکان ارتکاب انواع جرائم امنیتی - سایبری وجود دارد؛ از این رو تدارک برنامه‌ای جامع برای اطلاع‌گیری در این فضا لازم است. اطلاع‌گیری عمومی به این نحو که شماره یا مشخصات دیگر را به مردم ارائه دهند، خود سبب احساس ناامنی مجرمان جرائم امنیتی - سایبری از اطرافیان یا کسانی که با آن‌ها

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

ارتباط برقرار می‌کنند، می‌شود و نقش بسزایی در پیشگیری از جرائم سایبری دارد (بهره‌مند و داودی، ۱۳۹۷، ص ۳۹-۴۰).

به طور کلی، پیشگیری اجتماعی با ایجاد تغییرات و اصلاحات در فرد و جامعه به دنبال جلوگیری از ارتکاب جرم است. به دیگر سخن، پیشگیری اجتماعی بر کاهش یا از بین بردن عوامل فردی و محیطی جرم‌زا تمرکز می‌کند. هدف از پیشگیری اجتماعی تأثیرگذاری بر فرآیند شکل‌گیری و تکامل نظام شخصیتی افراد است. بدین سان، پیشگیری اجتماعی در برگیرنده اقداماتی است، خواه مستقیم یا غیرمستقیم، که هدفشان تأثیرگذاری بر شخصیت افراد است تا از شکل‌گیری انگیزه‌های مجرمانه در آنها جلوگیری کند (گسن، ۱۳۷۷، ص ۶۱). در پیشگیری اجتماعی تلاش می‌شود که با انجام برنامه‌های اجتماعی، فرهنگی، اقتصادی، رفاهی و نظایر آنها و درمان نارسائی‌های اجتماعی و بالا بردن ارزش‌های اجتماعی و اخلاقی شرایط یک منطقه و نیز وضعیت مجرمان بالقوه اعتلا یافته و این روند باعث کاهش میزان جرم می‌شود. (صبح دل، ۱۳۹۶، ص ۹۷).

پیشگیری وضعی از جرائم سایبری: یکی از راهکارهای مهم برای پیشگیری از بزه‌دیدگی ناشی از تروریسم سایبری، پیشگیری وضعی است. پیشگیری وضعی مبتنی بر تغییر وضعیت‌های پیش از جرم است که به تجربه با تحدید فرصت‌های ارتکاب جرم و یا مشکل‌تر کردن تحقق این فرصت‌ها برای مجرمان بالقوه سعی دارد شرایط را به‌گونه‌ای ایجاد کند که پاسخ شخص به آن موقعیت ارتکاب رفتار مجرمانه نباشد یا دست‌کم چنین پاسخ‌هایی تقلیل یابند. (معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضائیه، ۱۳۸۳، ص ۱۱) پیشگیری وضعی از جرم را به عنوان اقدامات قابل سنجش و ارزیابی مقابله با جرم می‌دانند. این اقدامات، معطوف به اشکال خاصی از جرم بوده و از طریق اعمال مدیریت یا مداخله، در محیط بی‌واسطه به شیوه‌های پایدار و نظام‌مند، منجر به کاهش فرصت‌های جرم و افزایش خطرات جرم می‌شود که همواره مدنظر تعداد زیادی از مجرمان بوده است. این پیشگیری به وسیله دستکاری و تغییر موقعیت و محیط در فرآیند وقوع جرم، به کاهش

دوره ۳، شماره ۱، بهار ۱۳۹۹/2020 Vol. 3, No. 1, Spring

فرصت‌های ارتکاب جرم کمک می‌کند (قدیر و کاظمی فروشانی، ۱۳۹۸، ۲۴۶). به طور کلی پیشگیری وضعی از جرم بر این فرض استوار است که انسانی متعارف در همه زمینه‌ها بطور منطقی و حساب شده عمل کرده و از خطرات شدید دوری می‌کند؛ یعنی درصورتی تن به خطر می‌دهد که منافع حاصل از آن عمل ارزشمند باشند. بنابراین اگر به هر شکل بتوان خطرپذیری جرم را افزایش داد یا جاذبه و منفعت حاصل از آن را کاهش داده یا از بین برد، مجرمان بالقوه از ارتکاب جرم منصرف می‌شوند. در پیشگیری وضعی هرچند به مجرم توجه می‌شود اما رویکردی بزه‌دیده‌محور دارد. در این میان یکی از ویژگی‌های فضای مجازی دسترسی آزاد به مکان‌های عمومی سایبری مانند اینترنت یا شبکه‌های اجتماعی است به گونه‌ای که اشخاص در سراسر دنیا با سهولت به این مکان‌ها دسترسی داشته و با حضور در آن با یکدیگر ارتباط برقرار می‌کنند و همین امر فضای سایبر را در معرض تهاجم بزهکاران قرار می‌دهد. بنابراین یکی از کلیدی‌ترین سازوکارهای پیشگیرانه، جاذبه‌زدایی از جرم است. پیشگیری وضعی در جرائم سایبری از اهمیت ویژه‌ای برخوردار است زیرا این قبیل جرائم مقید به وسیله هستند. به عبارت دیگر بدون استفاده از رایانه و فضای سایبر، ارتکاب این جرائم محال است. در نتیجه با اِعمال تدابیر لازم بر وسیله، می‌توان ارتکاب این جرائم را به نحو چشمگیری کاهش داد (مقیمی، ۱۳۹۵، ص ۱۲۲). در بند دوم و سوم اصل ۲۶ «رهنمود پیشگیری از جرم» سازمان ملل متحد سال ۲۰۰۲، بهره‌گیری از تدابیر پیشگیری وضعی که به قابلیت و بدنه محیط اجتماعی لطمه وارد نکند و دسترسی آزاد به مکان‌های عمومی را محدود نکند، تاکید شده است. در ارتباط با بند یک لازم به توضیح است که از نظر فنی و تخصصی، ممکن است با کاربرد تدابیر پیشگیری وضعی در فضای سایبری، شاهد برخی اختلالات همچون کاهش سرعت شبکه، بسته شدن اشتباهی برخی سایت‌ها و وبلاگ‌ها، محدودیت‌های بی‌جهت برای ورود به برخی فضاها، اعمال محدودیت در دسترسی به شبکه‌های بین‌المللی و مانند آن بود. بند ۲ این رهنمود نیز با تفویض تصمیم‌گیری به سازمان‌ها، نهادها یا اشخاصی که صلاحیت قانونی چنین امری را دارند یا بر

Vol. 3, No. 1, Spring 2020 دوره ۳، شماره ۱، بهار ۱۳۹۹

روند و نحوه اجرای این گونه تدابیر نظارت مستقیم دارند، قابل اجراست. در نگاهی کلی، با مرور اسناد سازمان ملل متحد می‌توان دریافت که تدابیر پیشگیرانه وضعی دارای نظم و طبقه‌بندی خاصی نیستند. این امر چند علت دارد که مهمترین آن‌ها عبارت‌اند از: اول آن که، تدابیر پیشگیری وضعی در یک یا چند سند مشخص و محدود ذکر نشده‌اند، بلکه این نوع تدابیر در طیفی گسترده از اسناد این سازمان وجود دارند. دوم، بسیاری از تدابیر پیشگیری وضعی با گذر زمان و طی سالیان مختلف ارائه شده‌اند. برای مثال؛ مسائل عام پیشگیری وضعی از جرم سایبری در چند سند ارائه شده‌اند که محوری‌ترین و شاخص‌ترین آن‌ها عبارت‌اند از: توصیه‌نامه ۱۲۰۵ سال ۲۰۰۸ و توصیه‌نامه ۱۲۰۶ سال ۲۰۰۸ (مقیمی، ۱۳۹۵، ص ۱۲۲-۱۲۳).

اقدامات پیشگیرانه غیر کیفری در اسناد بین‌المللی و منطقه‌ای

الف. توصیه‌نامه‌های بین‌المللی سیاست جنایی: یکی از اقدامات سازمان ملل به منظور نشر و توسعه آگاهی‌های مربوط به امنیت رایانه است. سازمان ملل متحد در سال ۱۹۹۴ در انتشارات خود به امنیت سامانه‌های رایانه‌ای پرداخته و امنیت این سامانه‌ها را در امنیت سامانه‌های پردازش داده‌های الکترونیکی در سازمان بیان می‌کند؛ با این توضیح که امنیت سامانه‌های پردازش داده‌های الکترونیکی در سازمان از هفت مؤلفه اساسی تشکیل شده است که شامل امنیت اداری و سازمانی، امنیت کارکنان، امنیت فیزیکی، امنیت مخابرات الکترونیکی، امنیت سخت‌افزاری و نرم‌افزاری، امنیت عملیاتی و برنامه‌ریزی است (قدیر و کاظمی فروشانی، ۱۳۹۸، ص ۲۵۹).

ب. دستورالعمل و توصیه‌نامه‌های سازمان همکاری و توسعه اقتصادی: کمیته تخصصی این سازمان در سال ۱۹۸۹ اقداماتی را به منظور اتخاذ سیاستی مشترک برای مقابله با جرائم اینترنتی و هماهنگی قوانین کیفری، همچنین حمایت از حقوق فردی و جریان فراملی داده‌های شخصی شروع کرد. در ژوئیه سال ۲۰۰۲ این سازمان، سند جامع «خط و

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

مشی‌هایی برای امنیت سامانه‌های اطلاعاتی و شبکه‌ای؛ به سوی فرهنگ امنیتی» را منتشر کرد. درباره ایمن‌سازی سامانه‌های اطلاعاتی، این سازمان شالوده‌ای را پی‌ریزی کرده است که براساس آن، کشورها و بخش‌های خصوصی، به صورت انفرادی یا هماهنگ با یکدیگر، خواهند توانست چارچوبی برای امنیت سامانه‌های اطلاعاتی به وجود آورند، این چارچوب شامل قوانین، ضوابط رفتاری، تدابیر فنی، تجربیات مدیران و کاربران، آموزش و اگاه ساختن مردم می‌شود.

ج. هشتمین نشست سازمان ملل متحد درباره پیشگیری از جرم و اصلاح مجرمان: این قطعنامه، نتیجه تلاش سیزدهمین نشست پیشگیری از جرم و اصلاح مجرمان، درباره جرائم رایانه‌ای بود که در سال ۱۹۹۸ در مجمع عمومی سازمان ملل متحد پذیرفته شد. مجمع عمومی در این قطعنامه از کشورهای عضو خواسته است که به منظور مبارزه با جرائم رایانه‌ای، مواردی از این قبیل را در دستور کار خود قرار دهند: به روزکردن قوانین و دادرسی‌های کیفری ملّی، تقویت و ایجاد سازوکارهای پیشگیرانه و امنیتی برای هرگونه استفاده از رایانه با در نظر گرفتن حریم خصوصی کاربران و آزادی‌های مشروع افراد، افزایش آگاهی عمومی و توجه قانونگذاران و مردم نسبت به جرائم رایانه‌ای و توسل به اقدامات پیشگیرانه، آموزش به دست اندرکاران قوه قضاییه در زمینه فرآیندهای کیفری مربوط به جرائم رایانه‌ای و اقتصادی، مطالعه و همکاری با سازمان‌های ذینفع در زمینه اخلاق استفاده از رایانه و اقدام به تدوین مواد درسی و آموزشی به منظور ارتقای سطح آگاهی جامعه و همچنین اتخاذ سیاست‌های مربوط به بزه‌دیدگان جرائم رایانه‌ای، بر اساس اعلامیه اصول بنیادین عدالت برای بزه‌دیدگان و قربانیان سوء استفاده از قدرت تلاش کنند.

Vol. 3, No. 1, Spring 2020 دوره ۳، شماره ۱، بهار ۱۳۹۹

بحث و نتیجه‌گیری

توسعه فناوری اطلاعات، تمام ابعاد زندگی اجتماعی را در برگرفته و افزایش استفاده از اینترنت در سطح جهان، چالش‌هایی را در زمینه مدیریت و قانونمندسازی ایجاد کرده است.

با وجود تلاش‌های صورت‌گرفته در حوزه حقوق و جرائم، فضای سایبر همچنان محیطی کنترل نشده و بی‌قانون توصیف می‌شود که برای همگان قابل دسترس است. جهانی و بدون مرز بودن این فضا و امکان انجام انواع جرائم با توسل به تبادل اطلاعات، تهدیدات و چالش‌هایی را در مقوله امنیت ملی ایجاد کرده است. این امر اندیشمندان حوزه حقوق را وادار به تأمل و تصمیم‌گیری کرده تا سیاست‌های ویژه‌ای را در ابعاد مختلف کنترل، مدیریت و پیشگیری تدوین کنند. بررسی مواد و منابع قانونی در حقوق ایران نشان می‌دهد که در خصوص پیشگیری از تروریسم سایبری در مقررات کیفری، مقرره خاصی وجود ندارد، بلکه با استناد به برخی قوانین عام همچون قانون جرائم رایانه‌ای، قانون مجازات اسلامی و سایر قوانین متفرقه می‌توان به مواضع پیشگیرانه حقوق کیفری ایران در زمینه پیشگیری از این بزه اشاره کرد. همچنین با نگاهی به اسناد بین‌المللی درباره جرائم سایبری و تروریستی و انواع قطعنامه‌های سازمان‌های بین‌المللی و منطقه‌ای که سازمان ملل متحد در رأس آنها قرار دارد، می‌توان به این نتیجه رسید که در سطح فراملی نیز، اقدامات کافی و شایسته‌ای به منظور پیشگیری از تروریسم سایبری صورت نپذیرفته است. در واقع، برای پیشگیری از تهدیدهای ناشی از ناهنجاری‌های برآمده از فضای سایبری، اسناد متعددی تاکنون به تصویب رسیده است اما با وجود تنوع این اسناد در نظام‌های ملی و بین‌المللی، متأسفانه هیچ یک از آنها موجب تحقق وضعیتی مطلوب را در مواجهه با تهدیدها فراهم نکرده است. باید در نظر داشت که جرائم در فضای سایبر، در بستری متفاوت و با کیفیت خاصی ارتکاب می‌یابند بنابراین هر اقدام پیشگیرانه‌ای اعم از پیشگیری اجتماعی، وضعی و کیفری باید متناسب با این فضا تدارک دیده شود. پیشگیری در مفهوم موسع خود، گستره وسیعی از اقدامات کیفری و غیر کیفری را دربر می‌گیرد که شامل مجموعه‌ای از تدابیر برای خنثی کردن عوامل وقوع جرم توسط مجرم است. در مقابل آن، مفهوم مضیق پیشگیری یا به عبارت دیگر، پیشگیری غیر کیفری (اجتماعی و وضعی) است که در نظر دارد امکان وقوع جرائم را از راه غیر ممکن ساختن یا دشوار کردن وقوع آن با مدیریت

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

مناسب نسبت به فرصت‌ها و عوامل عینی جرم‌زا تحدید کند. به این ترتیب پیشگیری غیر کیفری با منظور خاص و انحصاری، از نظام کیفری که نظر به بعد از وقوع جرم دارد، با وجود هدف مشترک، فاصله زیادی دارد و همین طور این نوع پیشگیری با مدیریت رفاه اجتماعی که نظر بر بهبود زندگی اجتماعی دارد نیز متفاوت است و نسبت به آنها به جهت سودمندی و اثربخشی در اولویت قرار می‌گیرد. بر این اساس و با عنایت به ویژگی‌های خاص جرائم سایبری، رویکرد رویارویی با این جرائم، نیازمند اتخاذ تدابیر پیشگیرانه خاص و در قالب پیشگیری اجتماعی است. آنچه که می‌تواند در مبارزه علیه یک پدیده ناخواسته موثر واقع شود، اقدام در از بین بردن علل و عوامل سازنده آن پدیده است که با رفع آنها، معلول نیز خود به خود منتفی می‌شود. درباره پدیده بزهکاری نیز همین موضوع صادق است، پیشگیری اجتماعی بر مبنای علت‌شناسی جرم استوار است که نظر بر حذف یا خنثی کردن عواملی دارد که در تکوین جرم موثر هستند و با دخالت در محیط‌های اجتماعی مانع از شکل‌گیری انگیزه‌های بزهکارانه و خنثی‌سازی عوامل جرم‌زا می‌شود. بر این اساس، پیشگیری اجتماعی، در مقایسه با پیشگیری وضعی و کیفری، مؤثرتر به نظر می‌رسد. پیشگیری وضعی که مبتنی بر تغییر وضعیت‌های پیش از جرم است، سعی دارد با مشکل‌تر کردن تحقق فرصت‌های ارتکاب جرم، شرایط را به گونه‌ای ایجاد کند که پاسخ شخص به آن فرصت، ارتکاب رفتار مجرمانه نباشد تا از این طریق امکان تحقق جرم را کاهش دهد. اما امروزه با تحول و گسترش سریع فناوری سایبری، پیشگیری وضعی چندان کارآمد به نظر نمی‌رسد؛ چون با تأکید بر عواملی همچون رمزنگاری و فیلترینگ و مانند آن تنها هزینه ارتکاب جرائم را افزایش می‌دهد بدون آنکه مانع وقوع این دسته از بزه شود. اجرای تدابیر پیشگیرانه وضعی، همانند بسیاری از سایر تدابیر پیشگیرانه، ممکن است محدودیت‌هایی ایجاد کند و در نهایت سبب جابجایی سیبل مجرمانه می‌شود و هدف از پیشگیری را تأمین نمی‌کند. از سوی دیگر خصلت جهانی بودن و پنهان بودن این جرائم، تأثیر پیشگیری کیفری را کاهش می‌دهد؛ چون پس از وقوع جرم با بهره‌گیری از تدابیر و اقدامات نظام

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

عدالت کیفری برای کاهش نرخ جرم مداخله می‌کند. از سوی دیگر، هدف از اجرای کیفر و تحمیل مجازات‌ها و اقدامات تأمینی و تربیتی، پیشگیری عام و خاص از تکرار جرم است که با وجود تحول و تجدد و دستیابی به فناوری در کنترل جرائم حتی نسبت به مجرمانی که سابقه ارتکاب جرم داشته‌اند، توفیق چندانی حاصل نشده است. هرچند که مقابله کیفری در خصوص این جرائم اجتناب‌ناپذیر است اما با توجه به واکنشی بودن این اقدام و اتخاذ آن پس از ارتکاب جرم نمی‌توان آثار سوء این جرائم را خنثی کرد. علت آن است که ارتکاب هر جرم، آثار زیانباری را برای مجرم و جامعه در بر داشته و لطمات زیادی را هم بر اشخاص مجرم و هم بر اعضای جامعه وارد می‌کند و مجازات هرچند که بر فرض بتواند مجرم را متنبه سازد و عبرت دیگران را در پی داشته باشد، ولی به هیچ وجه نمی‌تواند پیامدهای زیانبار آن را جبران کند و فرصت‌ها و حرمت‌های از دست رفته را باز یابد و مجرم و جامعه را به جایگاه قبل از وقوع جرم باز گرداند. پس بدون آنکه منتظر وقوع بزه یا تحمیل هزینه کیفر بر کسی باشیم باید به طریق دیگری درصدد حفاظت و صیانت از جامعه و افراد آن در مقابل بزهکار و پدیده بزهکاری برآمد و به عبارت دیگر، اقداماتی را مورد تحقیق قرار داد که به جای واکنش به این جرائم، از وقوع آنها پیشگیری کند و آن اقدام همان پیشگیری غیر کیفری و به عبارت دقیق‌تر پیشگیری قبل از ارتکاب جرم است. بر این مبنا، پیشگیری اجتماعی می‌تواند اثرگذاری بیشتری داشته باشد. از جمله اقدامات پیشگیرانه اجتماعی می‌توان به برنامه‌های خانواده‌مدار، تدابیر آموزشی - سایبری، بالابردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، مشارکت و اجماع‌گری، ارتقای پاسخگویی و شفافیت، فرهنگ‌سازی و تولید رسانه‌ای اشاره کرد.

پیشنهادها: از پیشنهادهایی که می‌تواند به نوعی در راستای پیشگیری از جرائم و جلوگیری از تکرار جرم ارزیابی و تعریف شود، بحث اعمال مجازات‌های جایگزین و تعقیب اهداف واقعی کیفرها است که همان اصلاح، تربیت و بازسازی مجرمان است. بهره‌گیری از جایگزین‌های مناسب مانند جریمه نقدی، کار عام المنفعه و منع اقامت در محل معین به

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

جای زندان و گزینه‌هایی چون تعهد درمانی و اجتماع درمانی، ایجاد محدودیت در صدور قرارهای بازداشت موقت، اقدام به صدور قرارهای قبولی کفالت و وثیقه، تشویق و ترغیب قضات و استفاده از نهادهای تاثیرگذاری چون تعلیق مجازات، آزادی مشروط، تخفیف مجازات، تقسیط جزای نقدی، پیشنهاد عفو به مناسبت‌های مختلف، درخواست عفو موردی و ایجاد تاسیسات ارزشمندی چون آزادی به شرط سپردن ضمانت، تعلیق مراقبتی و تشکیل ستادهای خصوصی و مردمی و سازمان‌های مردم‌نهاد برای پرداخت دیات و جرائم نقدی، مراقبت پس از خروج زندانیان و ایجاد زمینه برای پذیرش زندانیان پس از تحمل محکومیت و آزادی از جمله اقداماتی است که بعد از وقوع جرم می‌تواند نخست: از آثار زیانبار آن بر مجرم، خانواده و اجتماع بکاهد و دوم: با کاستن از جمعیت کیفری زندان‌ها، امکان تحقق اهداف اصلاحی و تربیتی مجازات‌ها را فراهم کند. در واقع با اعمال این تدابیر می‌توان مانع جلوگیری از تکرار جرم و بازسازی شخصیت مجرم و اصلاح آنان شد..

دوره ۳، شماره ۱، بهار ۱۳۹۹ Vol. 3, No. 1, Spring 2020

منابع

احمری، حسین؛ کحلکی، غلامرضا و رحیم پور اصفهانی، حامد. (۱۳۹۵). تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن. *پژوهش‌های روابط بین الملل*، ۶(۱۹)، صص ۳۰۵-۳۳۳.

اسلامی، ابراهیم. (۱۳۹۴). *مقابله با جرائم سایبری و حمایت از بزه‌دیدگان در حقوق بین‌الملل*. رساله برای دریافت درجه دکتری رشته حقوق گرایش حقوق بین‌الملل. دانشگاه شهید بهشتی. تهران.

بهره‌مند، حمید و داودی، ذوالفقار. (۱۳۹۷). پیشگیری اجتماعی از جرائم امنیتی – سایبری. *مطالعات حقوق کیفری و جرم‌شناسی دانشگاه تهران*. (۱)، صص ۲۷-۴۶.

دانش، تاج زمان. (۱۳۹۳). *مجرم کیست؟ جرم شناسی چیست؟* چاپ دوازدهم. تهران: انتشارات کیهان.

شیرازی، غلامرضا. (۱۳۸۴). *نقش پلیس محلی در پیشگیری از جرم*. پایان‌نامه دوره کارشناسی ارشد. دانشگاه آزاد اسلامی واحد دامغان.

صبح‌دل، محمد. (۱۳۹۶). جایگاه حقوقی قوه قضاییه در پیشگیری اجتماعی. *فصلنامه علمی - حقوقی قانون‌یار*. ۴(۴)، صص ۹۳-۱۰۸.

قدیر، محسن و کاظمی فروشانی، حسین. (۱۳۹۶). بررسی تطبیقی حقوق کیفری ایران با اسناد بین‌المللی در زمینه مقابله و پیشگیری از وقوع تروریسم سایبری. *مجله حقوقی بین‌المللی*، (۶۰)، صص ۲۳۷-۲۶۷.

معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه. (۱۳۸۳). *مجموعه مقالات قوه قضاییه و پیشگیری از وقوع جرم*. تهران: مرکز مطبوعات و انتشارات.

مقیمی، مهدی. (۱۳۹۵). *سیاست‌ها و تدابیر سازمان ملل متحد برای پیشگیری از جرم سایبری*، رساله برای دریافت درجه دکتری رشته حقوق گرایش حقوق بین‌الملل. دانشگاه شهید بهشتی. تهران.

موسوی، محمدرضا؛ حیدری، خدیجه و قنبری، سیدعلی. (۱۳۹۲). تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن. *فصلنامه علمی مطالعات بین المللی پلیس*، ۴(۱۴)، صص ۱۲۳-۱۴۵.

میرعباسی، سید باقر و کورکی‌نژاد قرایی، مجید. (۱۳۹۷). قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در مادهٔ ۵۱ منشور سازمان ملل متحد. *فصلنامه مطالعات حقوق عمومی دانشگاه تهران*، ۴۸(۲)، صص ۲۶۱-۲۸۰.