مقاله علمی - پژوهشی

موانع اساسی تحقق پیشگیری از جرائم سایبر

ابراهیم داودی دهاقانی[1]

پژوهش‌نامه نظم و امنیت انتظامی، سال دوازدهم، شماره دوم (پیاپی چهل و ششم)، تابستان 1398

از صفحه 53 تا 82

تاریخ دریافت: 97/11/13
تاریخ پذیرش: 98/01/14

چکیده

مقدمه: فضای سایبر به دلیل قابلیت‌ها و ویژگی‌های شگفتی‌ساز خود زمینه‌های سهولت ارتکاب جرم، فرامرزی شدن جرائم، کم شدن سن مجرمان، گستردگی خسارت و کثرت بزه‌دیدگان را در کنار ایجاد گمنامی فراهم کرده است؛ در این وضعیت، شناسایی موانع پیشگیری از جرائم سایبر در به‌کارگیری راهبردهای اثربخش، برای کنترل قابلیت‌های یادشده مؤثر خواهد بود؛ بنابراین هدف اصلی پژوهش حاضر، شناسایی اساسی‌ترین موانع تحقق پیشگیری از جرائم سایبری است.

روش: پژوهش حاضر از منظر روش‌شناسی، با رویکرد کیفی انجام شده است. مشارکت‌کنندگان پژوهش شامل کلیه خبرگان و صاحب‌نظران حوزه پیشگیری از جرائم سایبری در قوه قضائیه و سایر سازمان‌ها هستند که با آن‌ها مصاحبه شد. نمونه‌گیری در این پژوهش به‌صورت هدفمند انجام و تا رسیدن به اشباع نظری ادامه پیدا کرد. داده‌های به‌دست‌آمده به روش «تحلیل مضمون» تحلیل شدند. برای اطمینان از اعتبار داده‌های پژوهش، از نظرات اساتید صاحب‌نظر در حوزه پژوهش استفاده شد، ضمن این‌که متن مصاحبه‌ها به همراه کدهای به‌دست‌آمده در اختیار تعدادی از صاحب‌نظران قرار گرفت و پس از تأیید آنان، تحلیل مصاحبه‌ها ادامه یافت.

یافته‌ها: بر اساس یافته‌های پژوهش، موانع اساسی تحقق پیشگیری از جرائم سایبر در هفت حوزه اصلی موانع اجتماعی، موانع ساختاری، موانع علمی- آموزشی، موانع فرهنگی، موانع مدیریتی، موانع حقوقی قضایی و موانع فنی قرار دارند. در این میان، بر اساس تعداد مانع قرار گرفته در هر حوزه، به ترتیب، موانع در حوزه مدیریتی شامل 27 مانع، موانع حقوقی و قضایی شامل 19 مانع، موانع فرهنگی شامل 18 مانع، موانع فنی شامل 13 مانع، موانع ساختاری شامل 9 مانع، موانع علمی- آموزشی شامل 3 مانع و موانع اجتماعی نیز شامل 3 مانع هستند.

نتیجه‌گیری: با توجه به یافته‌های پژوهش برای پیشگیری از جرائم فضای سایبر، در دو سطح می‌توان نسبت به حذف موانع اقدام کرد: نخست، با تدابیر راهبردی و بلندمدت از طریق برنامه‌ریزی، سیاست‌گذاری و تصمیم‌گیری در سطح کلان کشور اقدام به رفع ریشه‌ای موانع کرد تا جرائم این فضا کاهش یابد. دوم، به‌صورت مستقیم از طریق اقدامات ایجابی یا سلبی، تدابیر زودبازده را به‌صورت مستقل و متمرکز سامان‌دهی کرد تا بتوان از گسترش جرائم در فضای سایبر پیشگیری کرد.

کلیدواژه‌ها: جرائم سایبر، پیشگیری از جرائم سایبر، موانع مدیریتی، موانع حقوقی، موانع فرهنگی.

1- استادیار مدیریت پیشگیری از جرم دانشگاه علوم انتظامی امین، تهران، ایران. رایانامه: davoodi57@chmail.ir

مقدمه

توسعه فناوری‌های نوین هر روز ابعاد جدیدتری پیدا می‌کند و در حال در هم نوردیدن و حضور فعال در تمامی زمینه‌ها و حوزه‌های بشری است. همین گستردگی و توسعه فراگیر آن موجب شده تا بسیاری از ابعاد آن ناشناخته بوده و محل مناسبی بر ای مجرمان در اجرای عملیات مجرمانه آن‌ها باشد. فضای سایبر در کنار برخورداری از مزایا و آثار مثبت فراوان، منشأ تهدیدهایی جدی برای کلیه افراد، سازمان‌ها و کشورهای جهان از توسعه‌یافته و غیر توسعه‌یافته شده است (جلالی، 1391: 7). امروزه، فعالیت بزهکارانه عمومی، دیگر منحصر به دنیای حقیقی نیست. به‌موازات گسترش فعالیت‌ها و ارتباطات در فضای سایبر، بخشی از بزهکاران نیز فعالیت مجرمانه خود را به این فضا منتقل کرده‌اند یا از رهگذر چنین فضایی مرتکب جرم می‌شوند (پیکا،[1] 1390: 11). در محیط سایبر به اقتضای ویژگی‌های خاص و ازجمله سهولت ارتکاب جرم و فرمان‌رانی آزادی در این فضا، امکان رخ دادن پدیده نامطلوب مجرمانه بیشتر می‌شود؛ زیرا یکی از ویژگی‌های به‌واقع متمایز و درعین‌حال، ارزشمند فناوری اطلاعات و ارتباطات الکترونیکی نسبت به دیگر فناوری‌ها، مانند فناوری هسته‌ای، زیستی و ریز فناوری، حداقل در برهه کنونی این است که اکثر افراد با حداقل مهارت فنی می‌توانند از قابلیت‌های متنوع آن استفاده کنند (جلالی، 1389: 15). به دنبال این امر، ارتکاب جرم در محیط سایبر نیز بسیار راحت است. هرکس با داشتن یک رایانه که امکان اتصال به اینترنت را دارد و با اندک آشنایی به سواد رایانه‌ای می‌تواند مجرمی بالقوه باشد (فضلی، 1389:72).

همان‌گونه که سال‌هاست اغلب کشورها، سازمان‌های منطقه‌ای و بین‌المللی برای پیشگیری و مبارزه با جرائم ارتکابی در فضای سنتی، برنامه، راهبرد یا سیاست مشخصی دارند، بدیهی است برای مبارزه با جرم سایبری نیز سیاست‌گذاری متناسب با این فضا ضروری است. در سطح ملی، این امر مسئولیت مشترکی است که به اقدام هماهنگ مسئولان دولتی، نهادهای خصوصی و شهروندان احتیاج دارد؛ اما با توجه به بُعد بین‌المللی و ماهیت این جرم، مبارزه هدفمند با آن در سطح منطقه‌ای و بین‌المللی،

1- Pica

نیازمند همکاری و هماهنگی با سایر کشورهاست؛ اما مبارزه هدفمند و نظام‌مند با جرم سایبری در سطح بین‌المللی، در ابتدا نیازمند دستیابی به درکی مشترک از این جرم و راه‌های مبارزه با آن است. یک چارچوب بین‌المللی برای دستیابی به این گفتمان تنها با سیاست‌گذاری در این زمینه امکان‌پذیر می‌شود (مک‌کی،[1] 2013: 216).

میزان استفاده از اینترنت و شبکه‌های مجازی چنان رو به گسترش است که نسل کنونی را «نسل اینترنت» یا «نسل شبکه» نام نهاده‌اند. این نسل متولدین اواسط دهه 1990 میلادی به بعد هستند. بین استفاده نسل‌های مختلف از شبکه‌های اجتماعی و همچنین انگیزه‌های آن‌ها از پیوستن به فضای مجازی تفاوت‌های قابل‌توجهی وجود دارد (بارتولومو، شاپ-سولیوان، گلاسمن، کامپ دوش و سولیوان،[2] 2012: 455). در تمام کشورهایی که در خصوص سن کاربران اینترنت سنجش به عمل آمده است، جوانان 16 تا 24 ساله بیشترین استفاده از اینترنت را دارند (توکل و کاظم‌پور، 1384: 120). در مطالعاتی که در سال 2002 توسط گروهی از وکلای قربانیان برخط (آنلاین) با عنوان «تلاش برای توقف سوءاستفاده آنلاین» (هالدر و جیشنکر،[3] 2010: 106) صورت گرفت، 71 درصد قربانیان مزاحمت سایبری زن بودند و 59 درصد آنان در گذشته نوعی از روابط را با مزاحم تجربه کرده بودند (هاتون و هانتز،[4] 2003: 12).

این فضا به‌نوبه خود سهولت ارتکاب جرم، فرامرزی شدن جرائم، کم شدن سن مجرمان، گستردگی خسارت و کثرت بزه دیدگان را در کنار ایجاد فضای گمنامی ایجاد کرده است. در برخی موارد، حملات گسترده به رایانه‌ها و زیرساخت‌های دولتی و هک کردن سراچه‌ها (سایت‌ها) امنیت ملی کشورها را هدف قرار داده است. آسیب‌پذیری امنیت ملی کشور در برابر کارکرد سیاسی فضای مجازی نیز در اولویت نخست تهدیدات قرار گرفته است؛ بنابراین بیش از هر امر دیگری، ضرورت پیشگیری از جرائم سایبری اهمیت می‌یابد. در نگاه کلی، تدابیر پیشگیرانه در برابر جرائم و آسیب‌های سایبری را به صورت‌های گوناگون می‌توان دسته‌بندی کرد. تقسیم‌بندی‌های علمی و شناخته‌شده طی سالیان اخیر، تقسیم تدابیر به وضعی و اجتماعی است. با توجه به ویژگی‌های جرم

1- Mackey
2- Bartholomew, Schoppe-Sullivan, Glassman, Kamp Dush and Sullivan
3- Halder and Jaishankar
4- Hutton, and Haantz

سایبری، در کنار پیشگیری وضعی، بهره‌گیری از انواع دیگر پیشگیری که با برنامه‌های اجتماعی، فرهنگی، آموزشی و اقتصادی ادغام می‌شوند، ضروری است. به دلیل این‌که اغلب بزه‌کاران و بزه‌دیدگان جرائم سایبری، نوجوانان و جوانان هستند، بهره‌گیری از تدابیر پیشگیرانه بلندمدت می‌تواند مؤثرتر باشد (جلالی فراهانی، 1387: 103).

عوامل و طرق ارتکاب بسیاری از جرائم سایبری به‌طورمعمول، متفاوت از جرائم سنتی است. جرائم سایبری در فضا و بستری ارتکاب می‌یابند که امکان شناسایی و مقابله با آن‌ها بسیار دشوار است. گسترش اینترنت زمینه‌ای را به وجود آورد که طیف وسیعی از اطلاعات، بدون هیچ‌گونه محدودیتی و فراتر از مرزهای جغرافیایی در سراسر جهان منتشر می‌شود و به نحو چشمگیری به یک رسانه ارتباطی و اطلاعاتی تبدیل گردد. این امر موجب شد تا فرصت‌ها و فضای جدیدی برای ارتکاب جرم ایجاد شده و فعالیت‌های بزهکارانه نیز به این جامعه جدید انتقال یابد. با فراگیر شدن ابزارها و سرویس‌های جدید در حوزه فن‌آوری اطلاعات و ارتباطات مانند شبکه‌های اینترنتی، شبکه‌های خصوصی و سرویس‌های مختلف ارائه‌شده در آن، تلفن‌های همراه و انتشار پیام‌های الکترونیکی بر روی انواع حامل‌های دیجیتالی (فضای مجازی یا سایبری و غیره) و همچنین استقبال عمومی در استفاده از این فناوری‌ها و خدمات، این محیط را برای ارتکاب به امور مجرمانه و انواع کلاه‌برداری‌ها، بزهکاری‌ها و اعمال خلاف قانون بر روی متخلفان و متجاوزان به حقوق عمومی و خصوصی افراد در جوامع مختلف باز کرده است. رویارویی با جرائم سایبری نیازمند پیشگیری و اتخاذ تدابیر ویژه و خاصی است. پیشگیری واقعی از جرائم سایبری، نیازمند شناسایی مسائل، مشکلات، چالش‌ها، آسیب‌ها، کمبودها و به‌عبارت‌دیگر، موانع پیش روی این حوزه است تا بتوان با رفع آن‌ها، به‌طور مؤثر اقدامات و فعالیت‌های سیاست‌گذاری و اجرایی پیشگیری از جرم را عملیاتی کرد. این موانع درزمینه‌های مختلفی مانند نیروی انسانی، تأسیسات، کارکردها، قوانین و فناوری‌ها وجود دارد که هرکدام از آن‌ها می‌تواند در فرایند پیشگیری از جرائم متنوع سایبری اختلال ایجاد کند. شناسایی این موانع از اهمیت فراوانی برخوردار است؛ به‌طوری‌که به نظر می‌رسد حتی قبل از هرگونه برنامه‌ریزی پیشگیرانه باید به این موانع عنایت داشت؛ بنابراین مسئله پژوهش حاضر آن است که موانع پیش روی پیشگیری از جرائم سایبری کدام‌اند؟

پیشینه و مبانی نظری پژوهش

پیشینه پژوهش

در بررسی پژوهش‌های گذشته، پژوهش‌های زیر در حوزه پیشگیری از جرائم سایبری انجام شده بود که در ادامه به آن‌ها اشاره می‌شود.

بیات و قنبری برزیان (1397)، در پژوهشی با عنوان «تبیین ارتباط رسانه‌های ارتباط‌جمعی و فضای مجازی با هویت ملی در جوانان عرب‌زبان اهواز»، به بررسی میزان تأثیر رسانه‌های ارتباط‌جمعی بر هویت ملی و نیز چگونگی رابطه بین متغیرهای فوق در بین جوانان دانشجوی عرب‌زبان اهوازی در سال 1395 پرداخته‌اند. نتایج تحلیل همبستگی در پژوهش یادشده نشان داد که بین دیدن موسیقی تصویری، فیلم سینمایی و برنامه جنسی از ماهواره و استفاده از اینترنت، چت، ایمیل، وبلاگ، سایت‌های (سراچه‌های) خبری، علمی، اجتماعی و فرهنگی با هویت ملی رابطه معناداری وجود دارد، همچنین دانشجویانی که از رسانه‌های ارتباط‌جمعی و فضای مجازی بیشتر استفاده کرده‌اند دارای هویت قومی قوی‌تری هستند و به عبارتی، استفاده بیشتر از فضای مجازی و رسانه‌های جمعی سبب برجستگی هویت قومی در برابر هویت ملی شده است.

نجفی علمی و نقیب السادات (1393)، در پژوهش خود با عنوان «روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر جمهوری اسلامی ایران» به دنبال پاسخ به این پرسش بودند که میزان و نقش روند تحولات فضای سایبر بر تحول تهدیدهای ناشی از جرم در کشور چگونه بوده است؟ نتایج پژوهش ایشان نشان داد که قابلیت و ظرفیت سازگاری روند تحولی جرم، همگام و همسو با روند تحولات فضای سایبر، الگوی تهدیدهای جرم را در کشور از قابلیت و ظرفیت‌های پیچیده و نوینی برخوردار کرده است. به همین منظور دکترین مدیریت راهبردی، یکپارچه، شبکه‌ای و هوشمند در چارچوب یک مدل، به همراه راهکارها، ارائه شده است.

جان‌پرور و حیدری موصلو (1390)، در پژوهشی با عنوان «آسیب‌شناسی فضای سایبر بر امنیت اجتماعی» به این یافته‌ها رسیدند که فضای سایبر دارای ظرفیت‌های منفی بالایی برای تحت تأثیر قرار دادن و به چالش کشیدن امنیت اجتماعی است، به‌طوری‌که حضور و استفاده رو به گسترش افراد از این فضا زمینه سست شدن بنیان

خانواده به‌عنوان تکیه‌گاه و پایه اصلی هر جامعه، فاصله گرفتن افراد از یکدیگر، تجمل‌گرایی، فردگرایی، مدگرایی، بی‌اعتمادی نسبت به مسئولان، نشر اکاذیب و مانند آن را فراهم آورده است و سبب شده امنیت اجتماعی دچار چالش و مشکل شود. بر این اساس، ازآنجاکه رشد و تعالی هر جامعه‌ای نیازمند برقراری نظم و امنیت اجتماعی است توجه به این عرصه جدید و شناخت آسیب‌های ناشی از آن بر جامعه می‌تواند جایگاه برجسته‌ای در برقراری امنیت اجتماعی در جامعه داشته باشد.

شاه‌محمدی و تاهو (1393)، در مقاله‌ای با عنوان «بررسی شیوه‌های پیشگیری از جرائم سایبری؛ مبتنی بر فناوری اطلاعات» اشاره داشته‌اند که فضای مجازی باوجود مزایای فراوان، به دلیل ویژگی‌هایی مانند امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، موجب مهاجرت بسیاری از جرائم به آن شده است نتایج نشان می‌دهد که شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت مجازی و نظارت بر فضای سایبر، جمع‌آوری ادله الکترونیکی جرم و مستندسازی صحنه جرم در پیشگیری از جرائم سایبر تأثیر دارد.

جوان جعفری (1389)، در رساله دکتری خود با عنوان «جرائم سایبر و رویکرد افتراقی حقوق کیفری؛ (با نگاهی به قانون مجازات اسلامی بخش جرائم رایانه‌ای به ابعاد فناوری اطلاعات)»، به فرامرزی بودن و سهولت ارتکاب جرم و مجرم در فضای سایبر اشاره و اثربخشی و کارایی قوانین برای مقابله با جرائم دیجیتال را مستلزم نگاهی متفاوت به مقولاتی مانند تعریف جرم، ارکان جرم و مسئولیت‌های کیفری و... دانسته که در زمان تصویب قوانین باید موردتوجه قرار گیرد.

شاهبندرزاده و یوسفی دهبیدی (1391)، در مقاله‌ای با عنوان «تعیین درجه اهمیت جرائم رایانه‌ای از دیدگاه صاحب‌نظران انتظامی استان بوشهر» سعی کرده‌اند با بررسی متون و ادبیات گذشته، پنج نوع جرم اصلی مرتبط با رایانه شناسایی شود که از این پنج جرم اصلی (جرائم علیه عفت و اخلاق عمومی، علیه مقدسات اسلامی، علیه امنیت و آسایش عمومی، علیه مقامات و نهادهای دولتی و عمومی و سایر جرائم رایانه‌ای جرائم علیه امنیت و آسایش عمومی) درجه اهمیت و امتیاز بیشتری به خود اختصاص داده است.

جلالی‌فراهانی (1387)، در پژوهشی با عنوان «جنبه‌های حقوقی اقدامات کیفری

بین‌المللی مجریان قانون در قبال جرائم سایبری» آورده است که مبارزه با جرائم سایبری، مستلزم بازاندیشی در قواعد و سازوکارهای تدابیر کیفری و سازگار سازی آن‌ها با مختصات جدید بین‌المللی است در این میان، مجریان قانون به‌عنوان حافظان اصلی امنیت و منافع ملی که در خط مقدم مبارزه با جرائم سایبری حضور دارند، باید از آمادگی کامل برخوردار باشند؛ در غیر این صورت، اقدامات ولو در جهت امنیت و منافع ملی، مشروعیت نخواهد داشت و به بی‌اعتباری ملی در عرصه بین‌المللی سایبری منجر خواهد شد.

میرمحمد صادقی و شایگان (1386)، در مقاله‌ای با عنوان «راهکارهای مقابله با جرم کلاه‌برداری رایانه‌ای در حقوق کیفری ایران با تشریح مفهومی و قانونی این جرم» به ایجاد فرهنگ بهره‌گیری از رایانه و آگاه ساختن افراد و سازمان‌ها بر روی سامانه‌های رایانه‌ای و تدابیر امنیتی مانند حفاظت فیزیکی، حفاظت کارکنان، حفاظت اطلاعات در مقابله با کلاه‌برداری رایانه‌ای اشاره کرده که از اهمیت ویژه‌ای برخوردار است. نظر به جنبه فرامرزی بودن جرائم رایانه‌ای و محدود بودن اختیارات مراجع قانونی، بر لزوم همکاری‌های بین‌المللی تأکید شده است.

بررسی پژوهش‌های انجام شده نشان می‌دهد که تاکنون به‌صورت مستقیم تمام ابعاد موانع پیشگیری از جرائم سایبری، به‌ویژه موانع مدیریتی این حوزه مورد بررسی قرار نگرفته است و در هیچ‌کدام شناسایی موانع مسئله نبوده است. ضمن این‌که پژوهش‌ها و مطالعات موجود هرکدام به بخشی از جرائم سایبری پرداخته‌اند و نگاه کلان و راهبردی در این تحقیقات نیز کم‌رنگ است و پژوهش حاضر تلاش کرده است تا خلأ پژوهشی موجود را پرکند.

مبانی نظری پژوهش

به‌موازات تأثیر فزاینده فضای سایبر بر زندگی انسان، تأمین امنیت و پیشگیری از جرائم آن نیز در کانون توجه قرار دارد و به‌عنوان یکی از مهم‌ترین دغدغه‌های حاکمیت‌ها شناخته می‌شود؛ زیرا در حال حاضر، فضای سایبر به یکی از ضرورت‌های زندگی انسان تبدیل شده و ارتباط مداوم وی با این فضا، فرصت مناسبی را نیز برای بزه‌کاران احتمالی فراهم کرده است؛ بنابراین می‌توان بر آن بود که شرایط تحقق نظریه

«فعالیت روزانه»[1] در فضای سایبر فراهم شده است؛ زیرا به علت وابستگی بسیاری از فعالیت‌های انسان معاصر به این فضا و عدم ارتقاء امنیت دستگاه‌ها توسط کاربران آسیب‌پذیر، این فضا جذابیتی دوچندان برای ارتکاب جرم ایجاد کرده است. نظریه «فعالیت روزانه» در سال 1979 توسط لورنس کوهن و مارکوس فلسون[2] مطرح شد. بر اساس این نظریه جرم زمانی اتفاق می‌افتد که بزهکار هدفی مناسب را بیابد و موقعیت و فرصت ارتکاب بزه مهیا باشد؛ بنابراین در صورت نبود هر کدام از این شرایط، بزه واقع نخواهد گردید. فعالیت‌های روزانه این فرصت را برای بزهکاران فراهم می‌کنند تا هدف موردنظر خود را که فاقد تدابیر محافظتی کافی است، بیابند (کلارک،[3] 1992: 5).

گستره کلان خسارات ناشی از جرائم سایبری سبب شده است تا کنگره‌های پیشگیری از جرم و عدالت کیفری سازمان ملل متحد نیز به همکاری بین‌المللی برای پیشگیری از این جرائم تأکید فراوانی نمایند (سازمان ملل متحد،[4] 2013). کنگره سیزدهم سازمان ملل نیز همچون کنگره‌های پیشین دغدغه افزایش جرائم سایبری را داشته و به استفاده از ابزارهای «فاوا» برای تأمین امنیت این فضا تأکید نموده است. بند نهم اعلامیه این کنفرانس به نقش مثبت پیشرفت‌های اقتصادی، اجتماعی و فناوری‌ها برای تسهیل فرآیند پیشگیری از جرم اذعان نموده و بر یافتن تدابیری خاص برای تأمین محیط سایبری امن و مناسب تأکید کرده است (سازمان ملل متحد،[5] 2015: 6).

نظریه «پیشگیری موقعیت‌مدار» به‌عنوان یکی از نظریات پیشگیرانه کنشی، درنتیجه شکست تدابیر پیشگیرانه اجتماعی، در اواخر دهه 1970 و توسط وزارت کشور بریتانیا مطرح شد. این تدابیر درصدد کاهش بزه‌کاری از طریق دست‌کاری در فرصت‌های پیش جنایی هستند؛ بنابراین پیشگیری موقعیت‌مدار 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 موقعیت‌مدار درصدد کاهش انگیزه‌های ارتکاب بزه از طریق

1-Routine activity theory
2- Lawrence Cohen and Marcus Felson
3- Clarck
4- UN General Assembly
5- UNODC

تعالی جامعه و نهادهای آن نیست، بلکه تمرکز آن بر کاهش فرصت‌ها و موقعیت‌های ارتکاب بزه از طریق کاهش جذابیت است» (کلارک،[1] 1992: 4).

تدابیر موقعیت‌مدار 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 «بازار امنیت سایبری»[2]، یکی از پردرآمدترین صنایع روز به شمار می‌رود؛ لیکن یکی از انتقادات صحیحی که همواره به تدابیر موقعیت‌مدار وارد است، دخالت در حریم شخصی افراد و یا محدود ساختن استفاده آن‌ها از حقوق بنیادین است (بابایی و نجیبیان،1390: 162).

دیدگاه‌های مختلفی در خصوص فضای سایبر وجود دارد که در ادامه به دیدگاه‌های جامعه‌شناسانه اشاره می‌شود:

1. دیدگاه مدرن: در نظریه مدرن مطالعه فناوری بر شناخت گونه‌های فناوری و توصیف آن‌ها استوار بوده و تحلیل‌های مدرنیستی از فناوری‌ها عمدتاً مبتنی بر گونه‌شناسی و طبقه‌بندی است.

2. دیدگاه نمادین تفسیری: این رویکرد ساخت اجتماعی فناوری نامیده می‌شود. این نگاه در انتقاد به دیدگاه نظریه‌پردازان مدرنیست که معتقد به مدل‌های نوآوری خطی هستند، پدید آمده است. مبنای نمادین تفسیری‌ها، پرداختن به اثرات هنجارهای فرهنگی و روابط اجتماعی است. در این دیدگاه فناوری‌ها فقط به‌عنوان کاربردهای محض یافته‌های علمی محسوب نمی‌شوند، بلکه اساس و پایه سازه‌های ذهنی تلقی می‌شوند (هچ،[3] 1390: 59).

3. دیدگاه پست‌مدرن: نظریه‌پردازان پست‌مدرن در مقابل نمادین تفسیری‌ها بیشتر به اثرات فناوری بر جامعه متمرکز شده و فناوری‌های جدید را محملی برای دیدگاه خود قرار داده‌اند. آن‌ها فناوری‌های نوین را فناوری‌هایی با سه مشخصه احتمالی، مستمر و انتزاعی می‌دانند. پست‌مدرن، فناوری را منشأ تغییرات بنیادی در جامعه می‌داند (هچ، 1390: 59).

1- Clarke
2- Cyber Security Market
3- Hatch

4. دیدگاه توحیدی: این دیدگاه به دنبال پاسخ به این سؤال است که در دنیای مدرن امروز، باوجود تنوع ابزارها و فناوری‌های متنوع که سراسر زندگی بشر را فراگرفته، نقش دیدگاه توحیدی چگونه است. به بیان ساده‌تر، آیا می‌توان از هر فناوری در هر فرهنگی استفاده کر د؟ اصولی همچون تعالی انسان، توحیدی عدالت و ولایت الهی با روح فرهنگی که فناوری غرب مروج آن است منافات دارد. تجربه کشورهایی که در اثر سلطه فناوری مدرن تمامی ساختارهای فرهنگی خود را از دست داده‌اند، مانع از پذیرش هر فناوری بدون ملاحظه فرهنگی و انتخاب عالمانه است. (طاهرزاده، 1387: 15).

پیشگیری از جرائم: با توجه به رویکرد کلی مقابله با جرائم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارت‌اند از: اقدامات کیفری و غیر کیفری. درزمینه اقدامات کیفری سعی می‌شود از طریق جرم‌انگاری، هنجارشکنی‌ها و سوءاستفاده‌های جدید و یا تجدیدنظر در قوانین کیفری گذشته، ارعاب انگیزی مؤثری درباره مجرمان بالقوه یا مکرر صورت گیرد تا به‌این‌ترتیب، از ارتکاب جرم بازداشته شوند (نیازپور، 1383: 124). رویکرد دوم که در بستر جرم‌شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان‌شناسی، جامعه‌شناسی و مانند آن پدید آمده، اتخاذ تدابیر پیشگیرانه را در دستور کار خود قرار داده است. در این زمینه، تاکنون الگوهای مختلفی در عرصه جرم‌شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است. از مهم‌ترین و مؤثرترین این الگوها می‌توان به پیشگیری اجتماعی و پیشگیری وضعی از جرائم اشاره کرد. به‌طور خلاصه، در پیشگیری اجتماعی سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آن‌ها، به‌ویژه قشر جوان و نوجوان جامعه، همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم، نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب گردد؛ اما در پیشگیری وضعی، هدف سلب فرصت و ابزار ارتکاب جرم از مجرم با انگیزه است (نجفی ابرندآبادی، 1382: 1208). با اینکه اتخاذ تدابیر پیشگیرانه نسبت به اقدامات کیفری از محاسن بسیاری برخوردار است، نباید از یاد برد که در اینجا نیز باید اصول و هنجارها را رعایت کرد. سیاست‌های پیشگیری، به‌ویژه پیشگیری وضعی، برخلاف سیاست‌های کیفری، تمامی افراد جامعه را در برمی‌گیرند، زیرا پرواضح است که شناسایی مجرمان بالقوه امکان‌پذیر نیست. لذا این

اقدامات باید به نحوی اجرا شوند که افراد جامعه از حقوق اساسی‌شان محروم نگردند (نجفی ابرندآبادی، 1383: 559).

تدابیر پیشگیری وضعی از جرائم سایبر: دو نکته اساسی را می‌توان راجع به فضای سایبر برشمرد: 1) این فضا با امکاناتی که در اختیار مجرمان قرار می‌دهد، از یک‌سو ارتکاب جرائم را سهل‌تر می‌سازد و نسبت به دنیای فیزیکی خسارات بسیار بیشتری را وارد می‌کند و از سوی دیگر، به لحاظ فرامرزی بودن آن و امکان ارتکاب جرم بدون نیاز به حضور فیزیکی مجرمان، تعقیب و پیگرد و درنهایت، دستگیری آن‌ها با مشکلات بسیاری همراه شده است. به‌این‌ترتیب، پیشگیری از وقوع این جرائم بسیار باصرفه‌تر و کم‌هزینه‌تر از طی فرایند رسیدگی کیفری آن‌ها و تحمل خسارات بی‌شمار است. 2) همچنین نباید از خاطر دور داشت که هدف اصلی از ایجاد فضای سایبر، نزدیک شدن به آرمان‌های جامعه اطلاعاتی است. لذا مبارزه با سوءاستفاده‌های این فضا، به هر شکل که باشد، نباید در تحقق این هدف خدشه‌ای ایجاد کند. (جلالی فراهانی، 1384: 109).

برای ارتکاب یک جرم، سه عامل باید جمع شوند. مهم‌ترین آن‌ها که قاعده مثلث جرم را هم تشکیل می‌دهد، انگیزه مجرمانه است. انگیزه باعث بیدار شدن میل درونی در افراد و به‌تبع آن، قصد مجرمانه می‌شود. برای از بین بردن این عامل، ضروری است تدابیر پیشگیرانه اجتماعی اتخاذ گردد؛ اما اگر به هر دلیل مجرمان واجد انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت و ابزار ارتکاب جرم جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد؛ زیرا متصدیان امر هرچه بکوشند ابزارهای ارتکاب جرم را از سطح جامعه جمع‌آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آن‌ها دست یابند. هرچند درعین‌حال نباید اهمیت جمع‌آوری این ابزارها را در کاهش جرائم نادیده گرفت. به‌هرحال، آنچه در پیشگیری وضعی از جرائم اولویت دارد، حفظ آماج‌ها و بزه‌دیدگان از تعرض مجرمان است. (صفاری، 1380: 292). در این زمینه، شیوه‌های مختلفی از سوی جرم‌شناسان ارائه شده که از مهم‌ترین آن‌ها می‌توان به شیوه‌های دوازده‌گانه کلارک، جرم‌شناس انگلیسی، اشاره کرد که آن‌ها را در سه گروه چهارتایی قرار داده است (ابراهیمی، 1383: 18):

1. دشوار ساختن ارتکاب جرم از طریق: الف) حفاظت از آماج‌ها و قربانیان جرم؛ ب) کنترل و ایجاد محدودیت در دسترس به موقعیت‌های جرم‌زا؛ ج) منحرف کردن مجرمان؛ و د) برچیدن ابزار ارتکاب جرم.
2. افزایش خطرپذیری مجرمان از طریق: الف) مراقبت از ورودی‌ها و خروجی‌ها؛ ب) مراقبت رسمی؛ ج) مراقبت غیررسمی؛ و د) مراقبت طبیعی.
3. کاهش جاذبه از آماج‌ها و قربانیان جرم از طریق: الف) حذف آماج‌های جرم؛ ب) علامت‌گذاری اموال؛ ج) تقلیل فرصت‌های وسوسه‌انگیز؛ و د) وضع قواعد خاص.

رویکرد سهل‌گیرانه در کیفر گزینی: این رویکرد مبتنی بر این موضوع است که قاضی در قبال جرائمی که به‌اندازه جرائم فضای سنتی خطرناک نیستند و معمولاً از سوی عموم شهروندان سر می‌زند و گاهی به کمترین تلاش برای انجام دادن نیاز دارند و فراتر از همه این‌ها، کیفر گزینی در قبال این جرائم عموماً بر این محور استوار است که فضای سایبر، فرع بر فضای سنتی و فیزیکی است و نباید برای یک فضای جایگزین و فرعی، سختگیری روا داشت. بر این اساس، رویکرد سهل‌گیرانه در قالب دو شاخص بررسی می‌شود (توحیدی نافع و امیرلی، 1395: 121-123):

عمومیت‌گرایی: فضای سایبر فضای خلوت‌ها است و در این فضا به جهت محوریت اطلاعات، حریم خصوصی و محرمانگی داده و سامانه، اولین و مهم‌ترین اولویت است. همین ویژگی سبب شده تا عموم شهروندان در فضای سایبر، احساس نبودِ کنترل دولتی و کنترل‌های اجتماعی و فرهنگی داشته باشند و بستر ارتکاب جرم مانند سرقت و بارگذاری‌های غیرمجاز، نقض حقوق پدیدآورندگان و هرزه‌نگاری را فراهم ببینند. گرایش عمومی به ارتکاب جرائم سایبری به‌ویژه اگر همراه با محدودیت‌های متعدد قانونی باشد، نشان می‌دهد که شمار مرتکبان جرائم سایبری در مقایسه با شمار کاربران یک استثناء تلقی نمی‌شود؛ برای نمونه، انتشار محتوای مبتذل یا انتشار بدون مجوز متون علمی و دانشگاهی در شبکه‌های اجتماعی مجازی جرم به شمار می‌رود ولی بخش بزرگی از کاربران این شبکه‌ها از ارسال یا بارگذاری چنین محتویاتی ابا نمی‌کنند. هرچند یک روی این سکه، بالا بودن آمار سیاه بزه‌کاری است ولی روی دیگر آن، گرایش عمومی به ارتکاب دست‌کم بخشی از جرائم سایبری است و همین نکته نشان می‌دهد

که قاضی نمی‌تواند در تعیین کیفر برای جرائم سایبری رویکرد سخت‌گیرانه‌ای داشته باشد، وقتی چنین رویکردی نمی‌تواند اهداف حقوق کیفری را در این زمینه تأمین کند.

فرد محوری: فرد محوری یا فردگرایی همان متناسب ساختن کیفر با وضعیت مرتکب و شرایط حاکم بر ارتکاب جرم است. آنچه به‌تناسب قضایی جرم و کیفر اطلاق می‌شود، نسبت به جرائم سایبری، اقتضای رویکرد سهل‌گیرانه را دارد. تناسب جرم و کیفر، برای منظور کردن همه بایسته‌های پرونده در تعیین کیفر گفته می‌شود که گاه اصل فردی کردن کیفر نیز در برابر آن گفته می‌شود. محتوای پرونده گویای واقعیت‌های فردی، اجتماعی و محیطی آن است که سبب می‌شود تا قاضی بر اساس آن‌ها اقدام به تعیین کیفر نماید. گاه قانون‌گذار به‌طور موردی به لزوم رعایت نسبت مجازات با این واقعیت‌ها اشاره کرده است؛ برای نمونه، طبق تبصره ماده 64 ق.م.آ 1392، دادگاه در ضمن حکم، به سنخیت و تناسب مجازات مورد حکم با شرایط و کیفیات مقرر در این ماده تصریح می‌کند. تناسب عرضی[تناسب محتوایی را می‌توان به دو گونه عرضی و طولی دسته‌بندی کرد]، اشاره به رعایت تناسب بین جرائم مختلف با ضررهای مشابه یا مساوی است؛ به‌عنوان‌مثال، چنان‌چه میزان ضرر و خطر جرم سرقت به‌طورکلی با جرم کلاه‌برداری یا هر جرم دیگری مقایسه شود و ضرر و خطر آن‌ها مشابه یا مساوی فرض شود، در این صورت بایستی میزان حداقل و حداکثر کیفر تعیین‌شده برای چنین جرائمی در قانون، تفاوت زیادی با هم نداشته باشد. در غیر این صورت تناسب عرضی رعایت نشده و ممکن است برای یک جرم با ضرر و خطر اجتماعی کمتری، مجازاتی شدیدتر از جرمی با ضرر و خطر اجتماعی بیشتر تعیین و اجرا شود. تناسب طولی به‌طور خلاصه عبارت از ایجاد تناسب بین کیفر مربوط به درجات مختلف یک جرم خاص است. به‌بیان‌دیگر، چنانچه جرمی دارای درجات متعددی از لحاظ شدت و ضعف باشد بایستی مجازات مناسب با همان درجه معین شود، در غیر این صورت اصل تناسب رعایت نگردیده است (صفاری، 1391: 260).

روش‌شناسی

از منظر روش‌شناسی، این پژوهش بر اساس روش پژوهش کیفی انجام شد. روش تحلیل داده‌های بکار رفته روش «تحلیل مضمون» است. در این چارچوب، نخست داده‌های

موردنیاز پژوهش گردآوری و به‌طور یکجا به خواندن آن‌ها پرداخته شد تا به شناخت کلی از محتوای داده‌های به‌دست‌آمده دست یافته و سرانجام مضامین اولیه شناسایی شوند. مشارکت‌کنندگان پژوهش شامل کلیه خبرگان و صاحب‌نظران حوزه پیشگیری از جرائم سایبری بودند و تعداد آن در فرایند پژوهش بر اساس اصل اشباع نظری تعیین شد. در این پژوهش، 20 مصاحبه جمع‌آوری‌شده با استفاده از نرم‌افزار مکس کیودا[1] نسخه 2018، تحلیل شدند. بعد از تحلیل متن بیستم، موانع اصلی و فرعی در مصاحبه‌های قبلی تکرار می‌شد و پژوهشگر به اشباع رسید.

برای اطمینان از اعتبار داده‌ها، از نظرات اساتید صاحب‌نظر در حوزه پژوهش استفاده شد؛ به این منظور، متن حاصل از مصاحبه‌ها و کدگذاری‌های انجام شده در اختیار تعدادی از صاحب‌نظران قرار گرفت و پس از تأیید آنان، کار ادامه یافت. درنهایت، در فرایند جمع‌آوری مصاحبه‌های بعدی، بلافاصله داده‌ها مورد تحلیل قرار گرفتند تا مواردی که ناقص بودند با دریافت اطلاعات از مصاحبه جدید کامل شوند. برای حصول اطمینان از پایایی داده‌های پژوهش از روش‌های رائو و پری[2] (2003) شامل قابلیت بازیافتی، تأییدپذیری و قابلیت تکرارپذیری و هدایت دقیق جریان گردآوری داده‌ها، ایجاد فرایندهای ساخت‌مند برای اجرا و تفسیر مصاحبه‌های همگرا، استفاده از نظرات ارزشمند اساتید آشنا با این حوزه و متخصصان که در این حوزه خبره و مطلع بودند، کمک گرفته شد.

پس از انجام هر مصاحبه، مکتوب کردن آن‌ها در دستور کار قرار گرفت. در گام بعد به‌منظور انجام کدگذاری توصیفی، ابتدا متن مصاحبه به‌دقت مطالعه شد، سپس بخش‌های مربوط مشخص‌شده و یادداشت‌گذاری در کنار آن‌ها صورت گرفت و کدهای توصیفی تعریف شدند و این عمل برای هر مصاحبه تکرار و کدها بازنگری شدند. در گام بعد، برای کدگذاری تفسیری، اقدام به خوشه‌بندی کدهای توصیفی و تفسیر معنای خوشه‌ها با در نظر گرفتن سؤال پژوهش و حوزه مطالعاتی شد و این کار برای کل مجموعه داده‌ها انجام گرفت. در گام بعد، مضامین کلیدی برای مجموعه داده‌ها به‌عنوان یک کل، از طریق مدنظر قرار دادن مضامین تفسیری استنتاج شد و برای ارزیابی کیفیت

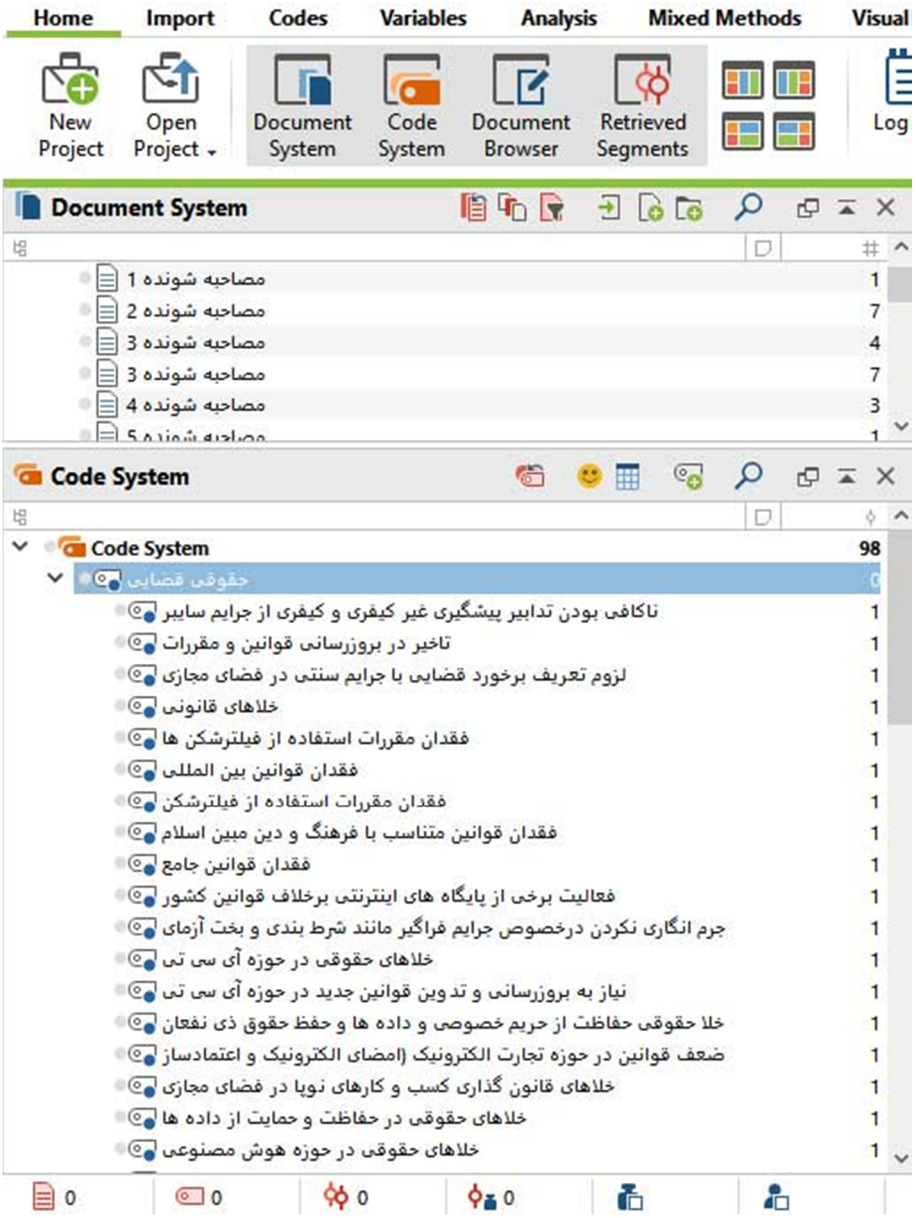
1 - MAXQDA
2- Rao & Perry

تحلیل مضمون انجام شده، بازخورد مصاحبه‌شوندگان (پاسخ‌دهندگان) دریافت شد که نشان از رضایت و تأیید نتایج تحقیق داشت.

در این پژوهش، یافته‌های حاصل از 20 مصاحبه پس از استخراج مضامین پایه، در قالب مضامین سازمان‌دهنده دسته‌بندی شدند. مصاحبه‌های اول، گاهی منجر به اضافه شدن چندین مضمون پایه و متعدد می‌شد اما با افزایش مصاحبه‌ها، این سیر، روند نزولی پیدا کرد تا جایی که از مصاحبه دهم به بعد هیچ مضمون پایه جدیدی شکل نگرفت؛ لذا تعداد نمونه‌ها کافی به نظر می‌رسید و کفایت نظری پژوهش مشخص شد.

یافته‌های پژوهش

مشارکت‌کنندگان: در پژوهش حاضر با اعضای شورای عالی فضای مجازی کشور، اعضاء کمیسیون قضایی مجلس، مسئولان قرارگاه پدافند سایبری سازمان پدافند غیرعامل کشور، رؤسا و مدیران پلیس فتا ناجا، حقوقدان و قضات دادگستری و اساتید دانشگاه‌های کشور، درمجموع، به تعداد 20 مشارکت‌کننده، مصاحبه شد. نمونه‌ای از کدگذاری داده‌ها در تصویر شماره (1) آمده است.

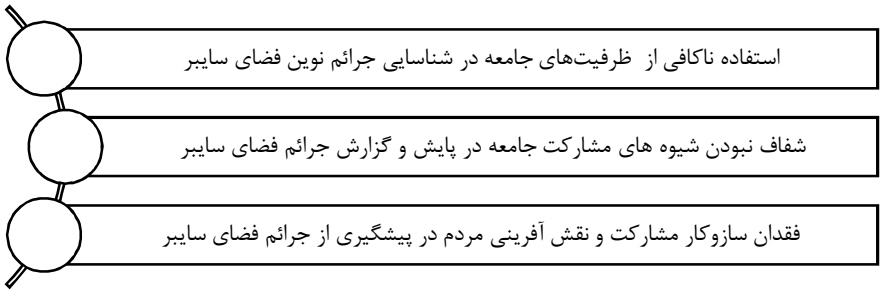


شکل 1: نمونه‌ای از کدگذاری مصاحبه‌ها در نرم‌افزار مکس کیودا

استخراج هفت مانع اساسی تحقق پیشگیری از جرائم سایبری: با توجه به یافته‌های به‌دست‌آمده از تحلیل مصاحبه‌ها، تعداد 92 مانع در قالب 7 مانع اساسی به

دست آمد که هر یک از موانع تحقق پیشگیری از جرائم سایبری به شرح ادامه هستند:

الف - موانع اجتماعی: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضمون سازمان‌دهنده موانع اجتماعی، 3 مانع به شرح زیر به‌دست آمد که عمدتاً مربوط به موانع مرتبط با جلب مشارکت مردم در پیشگیری از جرائم فضای سایبر است.



شکل 2: موانع اجتماعی تحقق پیشگیری از جرائم سایبری

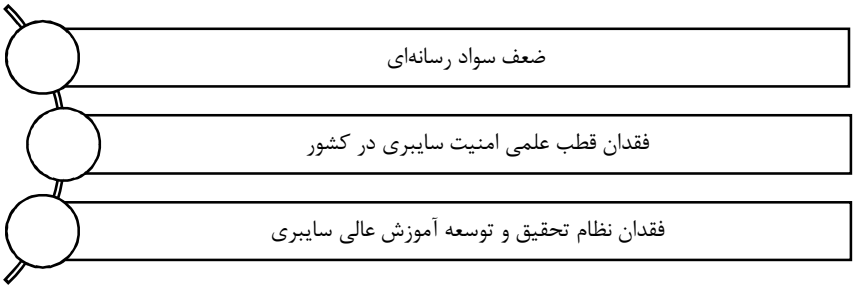
ب - موانع حقوقی- قضایی: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضمون سازمان‌دهنده موانع حقوقی- قضایی، به شرح زیر به‌دست آمد که بیشتر این موانع مربوط به خلأهای حقوقی در پیشگیری از جرائم فضای سایبر است.

شکل 3: موانع حقوقی- قضایی تحقق پیشگیری از جرائم سایبری

ج - موانع ساختاری: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضـمون سازمان‌دهنده موانع ساختاری، به شرح زیر به‌دست آمد.

شکل 4: موانع ساختاری تحقق پیشگیری از جرائم سایبری

د- موانع علمی- آموزشی: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضمون سازمان‌دهنده موانع ساختاری، به شرح زیر به‌دست آمد.

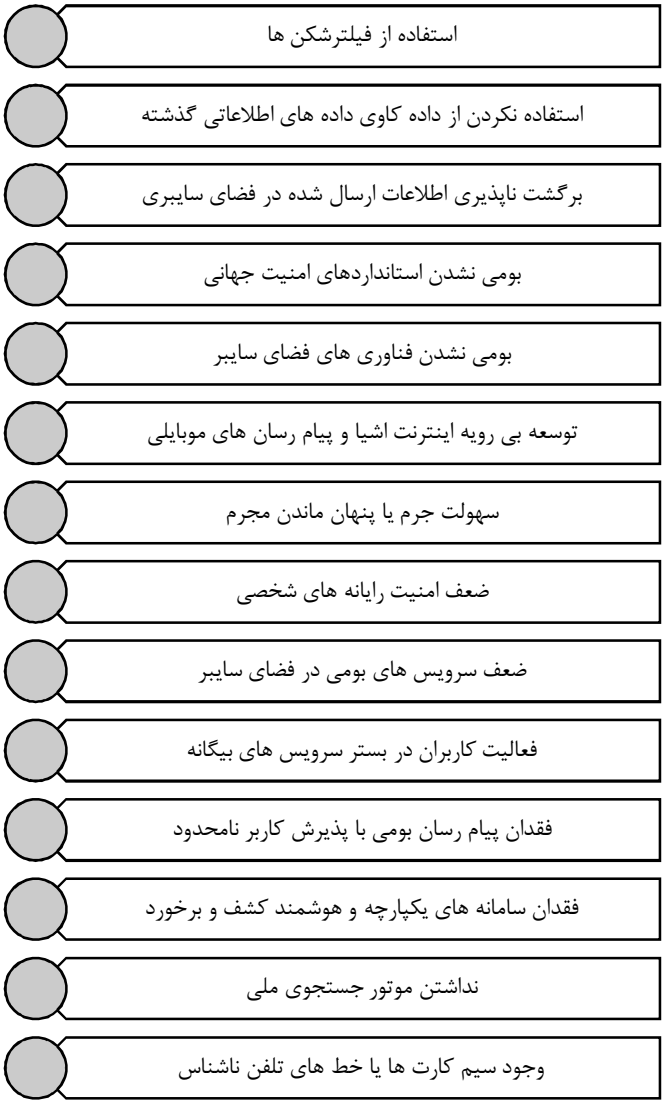


شکل 5: موانع علمی- آموزشی تحقق پیشگیری از جرائم سایبری

ه- موانع فرهنگی: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضمون سازمان‌دهنده موانع فرهنگی، به شرح زیر به‌دست آمد که بیشتر این موانع مربوط به ضعف آموزش و فرهنگ‌سازی در پیشگیری از جرائم فضای سایبر است.

شکل 6: موانع فرهنگی تحقق پیشگیری از جرائم سایبری

و- موانع فنی: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضمون سازمان‌دهنده موانع فنی، به شرح زیر به‌دست آمد که بیشتر این موانع مربوط به بومی نشدن فناوری‌های فضای سایبر است.



شکل 7: موانع فنی تحقق پیشگیری از جرائم سایبری

ز- موانع مدیریتی: پس از حذف و اصلاح و ادغام مضامین پایه مربوط به مضمون سازمان‌دهنده موانع فنی، به شرح زیر به‌دست آمد.

شکل 8: موانع مدیریتی تحقق پیشگیری از جرائم سایبری

بر اساس یافته‌های پژوهش، می‌توان چنین نتیجه گرفت که موانع اساسی تحقق پیشگیری از جرائم سایبر در هفت حوزه اصلی موانع اجتماعی، موانع ساختاری، موانع

علمی آموزشی، موانع فرهنگی، موانع مدیریتی، موانع حقوقی – قضایی و موانع فنی قرار دارند. در این میان، بر اساس تعداد مانع قرار گرفته در هر حوزه، به ترتیب موانع در حوزه مدیریتی شامل 27 مانع، موانع حقوقی و قضایی شامل 19 مانع، موانع فرهنگی شامل 18 مانع، موانع فنی شامل 13 مانع، موانع ساختاری شامل 9 مانع، موانع علمی آموزشی شامل 3 مانع و موانع اجتماعی نیز شامل 3 مانع به شرح جدول زیر هستند.

جدول 1: فراوانی موانع در هر حوزه به ترتیب بیشترین موانع

ردیف	مانع	تعداد	درصد فراوانی	درصد تجمعی
1	موانع مدیریتی	27	29/35	29/35
2	موانع حقوقی و قضایی	19	20/65	50/00
3	موانع فرهنگی	18	19/57	69/57
4	موانع فنی	13	14/13	83/70
5	موانع ساختاری	9	9/78	93/48
6	موانع علمی آموزشی	3	3/26	96/74
7	موانع اجتماعی	3	3/26	100
	جمع کل	92	100 درصد	

موانع مدیریتی و موانع حقوقی و قضایی به‌تنهایی 50 درصد و سایر موانع نیز که 5 مانع می‌شوند، 50 درصد موانع تحقق جرائم سایبری را شامل می‌شوند. این موضوع نشان‌گر آن است که برطرف شدن دو مانع اول در تحقق پیشگیری از جرائم سایبر بسیار تأثیرگذار خواهد بود.

نتیجه‌گیری

این پژوهش با هدف شناسایی موانع تحقق پیشگیری از جرائم سایبر انجام شد. روش گردآوری داده‌ها، استفاده از مصاحبه و روش تحلیل داده‌ها، تحلیل مضمون بود. ازاین‌رو، سؤال اصلی پژوهش به این شکل: «موانع تحقق پیشگیری از جرائم سایبر کدام‌اند؟» تدوین شد. از تحلیل مضمون متن 20 مصاحبه با افراد خبره، تعداد 92 مضمون پایه و 7 مضمون سازمان‌دهنده حاصل شده است که همگی بخشی از مضمون فراگیر موانع تحقق پیشگیری از جرائم سایبر هستند.

مطابق یافته‌های پژوهش، هفت مانع اساسی با تحلیل مضمون مصاحبه‌ها به‌دست

آمد. پس از بررسی و تحلیل موانع یادشده، نکته مهمی که باید مدنظر قرار گیرد این‌که برای پیشگیری از جرائم فضای سایبر، در دو سطح می‌توان نسبت به حذف این موانع اقدام کرد: اول اینکه، با تدابیر راهبردی و بلندمدت اقدام به رفع ریشه‌ای موانع به وجود آورنده جرائم سایبر اقدام نمود و در این صورت است که می‌توان انتظار داشت جرائم این فضا کاهش یابد اما این اقدامات نیازمند برنامه‌ریزی، سیاست‌گذاری و تصمیم‌گیری در سطح کلان کشور است؛ اما در سطح بعدی می‌توان به‌صورت مستقیم برای پیشگیری از جرائم سایبر در فضای سایبر گام برداشت و از طریق اقدامات ایجابی یا سلبی، تدابیر زودبازده را سامان‌دهی کرد تا بتوان از پیامدهای گسترش جرائم در فضای سایبر پیشگیری کرد.

تأکید زیاد مصاحبه‌شوندگان پژوهش حاضر بر موانع مدیریتی می‌تواند ناشی از گستردگی فضای سایبر و حجم رو به افزایش جرائم آن و درصد بالای جرائم با منشأ خارج از کشور باشد که باعث شده است امکان پیشگیری از بخش زیادی از این جرائم فراهم نشود و برای موفقیت بیشتر در ارتباط با این مهم، همت ملی و تلاش همه مسئولان و دستگاه‌ها را می‌طلبد. این در حالی است که روند رو به رشد تهدیدات این حوزه، سبب نگرانی همه کشورهای جهان شده است به‌طوری‌که در حال حاضر کمتر جرمی را می‌توان نام برد که رد پایی از آن در فضای مجازی یافت نشود. به‌عبارت‌دیگر، فضای مجازی از شکل غیرواقعی و ذهنی در حال خروج به شکل واقعی و کاملاً عینی است و بستری بسیار مستعد برای ارتکاب انواع جرائم و حوادث است. این تغییرات اهمیت حذف موانع مدیریتی در این حوزه را بیش‌ازپیش گوشزد می‌کند.

همچنین به‌موازات توسعه قوانین بین‌المللی، ضرورت دارد که قوانین داخلی به‌روز و پویایی در این حوزه وضع شود به‌نحوی‌که ضمن هماهنگی با قوانین بین‌المللی به‌سرعت خلأهای قانونی پیشگیری از جرائم سایبر را در سطح داخلی و خارجی مرتفع کند. مشارکت بیشتر در همکاری‌های فراملی، به اشتراک‌گذاری اطلاعات وقایع مجرمانه، یکپارچه‌سازی بانک‌های اطلاعات جرائم سایبری، ایجاد ساختارهای تخصصی مقابله و پیشگیری از جرائم سایبری، ایجاد مراکز پایش و رصد جرائم سایر و موضوعات مشابه، از مواردی است که می‌تواند موانع مدیریتی و حقوقی موجود را تعدیل سازد.

به موانع به‌دست‌آمده نمی‌توان فقط با نگاه امنیتی- انتظامی نگریست؛ زیرا بسیاری

از افراد جامعه با استفاده از کسب‌وکارهای نوین در این فضا مشغول فعالیت هستند و با توجه به شرایط کشور لازم است هرچه سریع‌تر به‌صورت ضابطه‌مند به‌عنوان یک فرصت به این فضا نگریسته شود و طی برنامه‌های مختلف کوتاه‌مدت و بلندمدت، هریک از موانع با انجام بررسی‌های کارشناسی مرتفع گردد. البته برخی از جرائم در فضای مجازی پیامدهای وسیعی در حوزه‌های امنیتی و انتظامی به دنبال دارند که لازم است به‌سرعت از طریق رفع موانع قانونی و مدیریتی از آن‌ها پیشگیری کرد. بااین‌وجود با توجه به نتایج به‌دست‌آمده از تحلیل مضمون و شناسایی موانع تحقق پیشگیری از جرائم در فضای سایبر پیشنهادهای کاربردی زیر ارائه می‌شود:

پیشنهادها

1ـ با توجه به این‌که موانع مدیریتی از فراوانی بیشتری در یافته‌های پژوهش برخوردار بود، بنابراین لازم است از طریق تعامل با شورای عالی فضای مجازی، تهیه الگوی ملی پیشگیری از جرائم سایبر به‌منظور تدوین راهبردهای پیشگیری از جرم در فضای سایبر با رویکرد پشتیبانی و حمایت از طرح‌های بومی پیگیری شود.

2ـ یکی از موانع مهم برای کاهش جرائم فضای سایبر رعایت نشدن مؤلفه‌های امنیت در دستگاه‌های اجرایی و سپردن مدیریت فضای سایبری کشور در دست بیگانگان است که لازم است از طریق قوه قضائیه ایجاد شبکه ملی اطلاعات و راه‌اندازی اینترنت ملی به‌صورت مستمر از نهادهای متولی پیگیری شود.

3ـ با توجه به در اولویت دوم قرار گرفتن موانع حقوقی و قضایی و قرار گرفتن عمده موانع این حوزه در مؤلفه قانون‌گذاری، پیشنهاد می‌شود برای رفع خلأهای قانونی و تسریع در به‌روزرسانی و تدوین قوانین جدید، با توجه به‌سرعت زیاد تغییرات در فضای سایبر، ساختار مناسب این موضع در قوه قضائیه ایجاد شود و به‌صورت مستمر قوانین موردنیاز را تدوین و تصویب آن را پیگیری کند.

4ـ با توجه به اینکه بر اساس یافته‌های پژوهش، ضعف آگاهی عمومی به‌عنوان یکی از تهدیدات فضای سایبری قلمداد می‌شود، پیشنهاد می‌شود به‌منظور فرهنگ‌سازی و کاهش ضعف فرهنگ استفاده از فضای سایبری، از طریق تعامل با وزارت آموزش‌وپرورش کارگاه‌های تربیت مربی برگزار و با استفاده از قضات با تجربه در

حوزه جرائم، مربیان پرورشی با آسیب‌ها و جرائم فضای سایبر آشنا شوند و در مدارس این موضوعات را به دانش‌آموزان آموزش دهند. همچنین تهیه برنامه‌ها و مستندهای تلویزیونی و سینمایی برای افزایش آگاهی و آموزش همگانی بسیار مؤثر خواهد بود.

منابع

- ابراهیمی، شهرام (1383). «پیشگیری از جرم». تهران: نشر میزان.
- بابایی، محمدعلی؛ نجیبیان، علی (1390). «چالش‌های پیشگیری وضعی از جرم». مجله حقوقی دادگستری، دوره هفتاد و پنجم، شماره هفتاد و پنجم، صص 172-147.
- بیات، بهرام؛ قنبری برزیان، علی (1397). «تبیین ارتباط رسانه‌های ارتباط‌جمعی و فضای مجازی با هویت ملی (موردمطالعه: جوانان عرب‌زبان اهواز)». پژوهش‌نامه نظم و امنیت انتظامی، دوره یازدهم، شماره سوم، صص 27-1.
- پیکا، ژرژ (1390). «جرم‌شناسی». (ترجمه علی حسین نجفی ابرندآبادی)، چاپ دوم. تهران: انتشارات میزان.
- توحیدی نافع، جلال؛ امیرلی، حسین (1395). «بایسته‌های کیفر گزینی در رویارویی با جرائم سایبری با تأکید بر رویه قضایی». مجموعه مقالات اولین همایش ملی رویارویی با جرائم سایبری؛ چالش‌ها و راهکارها. تهران.
- توکل، محمد؛ کاظم‌پور، ابراهیم (1384). «دگرگونی‌های اجتماعی در یک جامعه اطلاعاتی». تهران: انتشارات کمیسیون ملی یونسکو.
- جان‌پرور، محسن؛ حیدری موصلو، طهمورث (1390). «آسیب‌شناسی فضای سایبر بر امنیت اجتماعی». پژوهش‌نامه نظم و امنیت انتظامی، دوره چهارم، شماره سوم، صص 172-141.
- جلالی فراهانی، امیرحسین (1384). «پول‌شویی الکترونیکی». فصلنامه فقه حقوق، شماره چهارم، صص 132-109.
- جلالی فراهانی، امیرحسین (1387). «جنبه‌های حقوقی اقدامات کیفری بین‌المللی مجریان قانون در قبال جرائم سایبری». فصلنامه مطالعات پیشگیری از جرم، دوره سوم، شماره هشتم، صص 67-35.
- جلالی، علی‌اکبر (1389). «کنوانسیون جرائم سایبری و پروتکل الحاقی آن». (چاپ اول). تهران: انتشارات خرسندی.
- جلالی، علی‌اکبر (1391). «رفتارشناسی مجرمان در فضای سایبر». فصلنامه کارآگاه، دوره ششم، شماره بیست و یکم، صص 25-6.
- جوان جعفری، عبدالرضا (1389). «جرائم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرائم رایانه‌ای)»، دانش و توسعه، دوره هفدهم، شماره سی و چهارم، صص 191-169.

- شاهبندرزاده، حمید؛ یوسفی دهبیدی، شهلا (1391). «تعیین درجه اهمیت جرائم رایانه‌ای از دیدگاه صاحب‌نظران انتظامی استان بوشهر». فصلنامه نظم و امنیت انتظامی، سال پنجم، شماره اول، صص 155-138.
- شاه‌محمدی، غلامرضا؛ تاهو، منصور (1393). «بررسی شیوه‌های پیشگیری از جرائم سایبری؛ مبتنی بر فناوری اطلاعات». فصلنامه پژوهش‌های اطلاعاتی و جنایی، دور نهم، شماره سی و پنجم، صص 99-1.
- صفاری، علی (1380). «مبانی نظری پیشگیری وضعی». مجلس تحقیقات حقوقی، شماره سی و سوم و سی و چهارم، صص 322-267
- صفاری، علی (1391). «مقالاتی در جرم‌شناسی و کیفرشناسی». (چاپ اول)، تهران: انتشارات جنگل.
- طاهرزاده، اصغر (1387). «گزینش تکنولوژی از دریچه بینش توحیدی». اصفهان: لب المیزان.
- فضلی، مهدی (1389). «مسئولیت کیفری در فضای سایبر». (چاپ اول)، تهران: انتشارات خرسندی.
- میرمحمد صادقی، حسین؛ شایگان، محمد رسول (1386). «راهکارهای مقابله با جرم کلاه‌برداری رایانه‌ای در حقوق کیفری ایران». فصلنامه دیدگاه‌های حقوق قضایی. شماره چهل و دوم و چهل و سوم، صص 126-109.
- نجفی ابرندآبادی، علی حسین (1383). «پیشگیری عادلانه از جرم، علوم جنایی». مجموعه مقالات در تحلیل از استاد آشوری، تهران: انتشارات سمت.
- نجفی ابرندآبادی، علی حسین (1382). «تقریرات درس جرم‌شناسی (پیشگیری)». (تنظیم مهدی سیدزاده)، مجتمع آموزش عالی قم، دوره کارشناسی ارشد، نیمسال دوم 1382-1381.
- نجفی علمی، مرتضی؛ نقیب‌السادات، رضا (1393). «روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر جمهوری اسلامی ایران». پژوهش‌نامه نظم و امنیت انتظامی، دوره هفتم، شماره اول، صص 72-47.
- نیازپور، امیرحسین (1383). «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم». مجله حقوقی دادگستری، شماره چهل و پنجم، صص 159-124.
- هچ، ماری جو (1390). «تئوری سازمان، مدرن، نمادین تفسیری و پست‌مدرن». (ترجمه حسن دانایی‌فرد)، تهران: مؤسسه کتاب مهربان نشر.
- Bartholomew, Mitchell K., Sarah J. Schoppe-Sullivan, Michael Glassman, Claire M. Kamp Dush and Jason M. Sullivan (2012). “New Parent’s Facebook Use at

the Transition to Parenthood", Family Relations, 61(3), pp 455–469. doi: 10.1111/j.1741-3729.2012.00708.x

- Clarke, V. Ronald. (1992). "Situational Crime Prevention: Successful Case Studies", Second Edition. United States of America: Harrow and Heston.
- Halder, D. and K. Jaishankar (2010). "Cyber Crime and Victimization of Women: Laws, Rights, and Regulations", Hershey, PA, USA: LGL Global.
- Hutton, S. and S. Haantz (2003). "Cyber Stalking", Retrieved from http://www.nw3c.org.
- Jaishankar, K. (2011). "Cyber Criminology, Exploring Internet Crimesand Criminal Behavior", Boca Raton, CRC Press.
- Mackey, D., (2013). "Web security for network and system administrators", 2nd edition, Boston: Thomson-Course Technology.
- Rao. Sally & Perry. Chad (2003). "Convergent interviewing to build a theory in under-researched areas: principles and an example investigation of Internet usage in inter-firm relationships", Qualitative Marke Research: An International Journal, Volume6 Number4 2003 pp. 236-247
- UN General Assembly (2013). "Follow-up to the 12th United Nations Congress on Crime Prevention and Criminal Justice and preparations for the 13th United Nations Congress on Crime Prevention and Criminal Justice": resolution / adopted by the General Assembly.
- United Nations Office on Drugs and Crime (UNODC) (2015). "13th UN Congress on Crime Prevention and Criminal Justice, Doha, Doha Declaration on Integrating Crime Prevention and Criminal Justice", into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation, 12 –19.