فصلنامه رهیافت پیشگیری/ دورهٔ دوم، شمارهٔ اول، بهار ۱۳۹۸
Prevention Approach Quarterly
Vol. 2, No.1, (Spring 2019)

تاریخ دریافت: ۱۳۹۸/۰۲/۰۲
تاریخ پذیرش: ۱۳۹۸/۰۴/۱۲

مقاله پژوهشی

موانع اثربخشی راهبردهای پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی

باقر شاملو[۱] و مهدی کاظمی جویباری[۲]

چکیده

زمینه و هدف: دغدغه جرم‌شناسان و سایر پژوهشگران علوم اجتماعی برای کاهش جرائم موجب شده است تا آنان پژوهش‌های تجربی متعددی برای شناسایی مشکلات و موانع اثربخشی ناکافی برنامه‌های پیشگیرانه یا اثربخشی پایین آنها انجام دهند. با توجه به ضرورت بکارگیری چنین رویکردی برای شناسایی و حل مشکلات موجود در این زمینه در نظام عدالت کیفری ایران، مسئله اصلی پژوهش حاضر، بررسی موانع اثربخشی راهبردهای پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی و ارائه راهکارهایی برای رفع آنها است.

روش: برای پاسخگویی به پرسش پژوهش، ضمن بررسی اسناد و قوانین موجود در این زمینه، از روش مصاحبه عمیق با ۲۰ نفر از کارشناسان و مجریان برنامه‌های پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی استفاده شد.

یافته‌ها و نتایج: یافته‌های پژوهش بیانگر چند نکته اساسی است: نخست آنکه همکاری ضعیف، انجام وظایف مشابه و مناسبات قدرت میان نهادها موجب شده است تا پیشگیری چند نهادی از جرائم علیه امنیت اخلاقی در فضای سایبر براساس اهداف مورد نظر عینیت نیابد. در این میان، مشارکت ضعیف میان بخش خصوصی و دولتی به همراه سهم ناچیز مردم و انجمن‌های مردم‌نهاد، از دیگر موانع اثربخشی مداخله‌های پیشگیرانه در این حوزه به شمار می‌روند. افزون بر این، بسیاری از طرح‌ها و برنامه‌های پیشگیری بدون ارزیابی اجرا می‌شوند و پس از اجرا نیز میزان اثربخشی آنها سنجیده نمی‌شود. همچنین استفاده بیش از اندازه از فیلترینگ و معرفی آن به عنوان یکی از راهکارهای درست برای پیشگیری از جرائم سایبری، نه تنها ممکن است موفقیت‌آمیز نباشد، بلکه پیامدهای ناخواسته‌ای نیز به بارخواهد آورد که اثربخشی این اقدامات را دچار تردید می کند.

کلیدواژه‌ها: جرائم علیه امنیت اخلاقی سایبری، برنامه‌های پیشگیرانه، پلیس سایبری، رویکرد چند نهادی، مشارکت.

❑ **استناد:** شاملو، باقر و کاظمی جویباری، مهدی (۱۳۹۸). موانع اثربخشی راهبردهای پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی. *فصلنامه رهیافت پیشگیری*، ۲(۱)، صص ۱۳-۳۶.

۱. دانشیار گروه حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی. تهران. (نویسنده مسئول). رایانامه: b-shamloo@sbu.ac.ir
۲. دکتری حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی. تهران. رایانامه: m.kazemi.j@gmail.com

مقدمه

فعالیت در فضای مجازی در حال حاضر یکی از برنامه‌های روزانه بیشتر انسان‌ها محسوب می‌شود، به گونه‌ای که بسیاری از تعاملات اجتماعی و مبادلات اقتصادی در بستر این فضا در حال شکل‌گیری و توسعه است. همراه با توسعه این فرایند، رفتارهای برخی انسان‌ها به این فعالیت‌ها آسیب زده و امنیت آنها را تهدید می‌کند. به طور خاص، جرائم علیه امنیت اخلاقی نظیر آزار و اذیت سایبری، قلدری سایبری، پورنوگرافی آنلاین و مانند آنها موجب می‌شود تا بسیاری از اشخاص دیگر نتوانند در این فضا فعالیت کنند. برای پرهیز از وقوع چنین رویدادهایی، نهادهای عدالت کیفری تلاش می‌کنند تا از طریق اجرای طرح‌ها و برنامه‌های پیشگیرانه متعدد امنیت کاربران اینترنتی را تأمین کنند. با وجود این، مسائلی نظیر تعداد روزافزون کاربران اینترنتی در دنیا، ساختار افقی و شبکه‌ای اینترنت، استفاده از فناوری‌های بسیار پیشرفته که روز به روز بر پیچیدگی آنها افزوده می‌شود، چالش جدی را برای نهادهای عدالت کیفری در تأمین امنیت اعضای اجتماع و حفاظت از آنان در فضای مجازی به وجود آورده است. همچنین، افزایش فرصت ارتکاب جرم، افزایش سرعت ارتباطات در زندگی روزمره، در دسترس پذیری اطلاعات و مانند آن، مشکلات مقامات عدالت کیفری را دو چندان ساخته است. این نهادها گاه به تنهایی و گاه با مشارکت نهادهای خصوصی تدابیر پیشگیرانه‌ای را به منظور محافظت از اشخاص ترتیب می‌دهند. به طور خاص، رویکردهای مشارکتی یکی از حوزه‌هایی است که تحت تأثیر این نگرش جدید به شدت توسعه یافته است. پیشگیری از جرائم سایبری علیه امنیت اخلاقی نیازمند رویکرد جامع در حوزه تدوین برنامه‌های پیشگیرانه است که با ارزیابی مداخله‌ها و اصلاح و توسعه آنها بر اساس پژوهش‌های تجربی به دست خواهد آمد. بر همین اساس، پژوهش حاضر درصدد است تا بر اساس پژوهش‌های تجربی موجود در این زمینه، موانع اثربخشی برنامه‌های پیشگیرانه در جرائم علیه امنیت اخلاقی در فضای مجازی را بررسی و راهکارهایی را برای رفع این موانع ارائه کند.

فناوری، زندگی نوین انسان‌ها را در اجتماع هدایت و به شیوه‌های مختلف، روابط اجتماعی، اقتصادی، سیاسی و مانند آن را شکل می‌دهد. در راستای این جریان، میزان استفاده از اینترنت در کشورهای جهان در مقایسه با گذشته به شدت افزایش یافته است. آمار اتحادیه بین‌المللی مخابرات نشان می‌دهد[1] که تا

1. International Telecommunications Union (ITU)

اکتبر ۲۰۱۷، میزان کاربران اینترنت در دنیا به بیش از ۸۳۰ میلیون نفر رسیده است. همچنین، بر اساس وب‌گاه آمار جهانی اینترنت[1] در سال ۲۰۱۸، حدود ۴۸/۷ درصد از کاربران اینترنت در کشورهای آسیایی بودند. همچنین، در ۱۰۴ کشور دنیا، بیش از ۸۰ درصد نوجوانان آنلاین بوده‌اند. در عصر فناوری اطلاعات و ارتباطات، اینترنت به آسانی در دسترس همگان قرار دارد. در این میان، هر چقدر که استفاده از اینترنت بیشتر شود و جامعه بیشتر به سمت تشکیل اجتماعات مجازی قدم بردارد، خطر آسیب‌پذیری به عنوان بعد منفی فضای مجازی بیشتر خواهد شد. گزارش‌ها و آمارهای ارائه‌شده از سوی مقامات عدالت کیفری ایران بیانگر افزایش روزمره جرائم سایبری به طور کلی است. برای نمونه، بر اساس آمار رئیس پلیس فتا از سال ۱۳۹۰ تا ۱۳۹۷، میزان جرائم سایبری حدود ۹۰۰ درصد افزایش داشته است. از طرفی، تعداد کاربران این فضا نیز به شدت افزایش یافته است؛ چنانکه به گفته وی، این تعداد از ۵ میلیون کاربر در سال ۱۳۹۲ به ۵۰ میلیون کاربر در سال ۱۳۹۷ افزایش یافته است[2].

فضای مجازی محیطی است که کنشگران متعددی دغدغه مدیریت آن را دارند. به همین دلیل، ممکن است در بازه‌های زمانی، نهادهای جدیدی برای مدیریت و مقابله با جرائم سایبری تشکیل یافته و نهادهای سابق منحل شوند یا در کنار نهادهای جدید به فعالیت خود ادامه دهند. یکی از پیامدهای ناخواسته وجود نهادهای متعدد در این حوزه، فقدان همکاری مشترک و اجرای رویکرد چند نهادی برای دستیابی به اهداف تعیین شده است. با وجود آنکه بسیاری از کشورها با جرم‌انگاری رفتارهای خلاف امنیت اخلاقی، تمهید سازوکارهای حمایت از بزه‌دیدگان و اجرای کیفرهای شدید تلاش کرده‌اند تا به هدف کاهش جرم در این فضا نزدیک شوند، ولی واقعیت‌های موجود خلاف اقدامات آن‌ها را نشان می‌دهد زیرا جرائم سایبری در حوزه امنیت اخلاقی نه تنها کاهش نیافتند، که افزایش قابل ملاحظه‌ای نیز داشتند. شدت و افزایش این جرائم در سال‌های اخیر، عملکرد کنونی مقامات عدالت کیفری را در کنترل این فضا به چالش کشیده است. برخی از این مقامات با این ادعا که جرائم سایبری نوظهورند، تدابیر مقطعی و ضربتی را برای کنترل آنها مناسب و مطلوب می‌دانند. این در حالی است که تاکنون اثربخشی این تدابیر در هیچ حوزه‌ای از عدالت کیفری ارزیابی نشده‌اند. ضرورت سیاستگذاری عقلایی

1. Internet World Statistics

2. http://www.hamshahrionline.ir/news/418840

در حوزه فضای مجازی دولت‌ها را بر آن داشته است تا جدا از اقدامات کیفری، در حوزه پیشگیری از این جرائم سرمایه‌گذاری کنند. به همین جهت، سیاست‌ها و برنامه‌های پیشگیری از جرم یکی از محورهای مهم دخالت دولت، سازمان‌های غیردولتی و مانند آن در رابطه با کنترل جرائم سایبری بوده، به گونه‌ای که گاه مشارکت آنها در اجرای طرح‌های پیشگیری را به دنبال داشته است. به طور خاص، سیاست‌ها و برنامه‌های پیشگیرانه متعددی در حوزه جرائم علیه امنیت اخلاقی در فضای مجازی اجرا شده است. این برنامه‌ها در قالب برنامه‌های پیشگیری وضعی از جرم نظیر فیلترینگ یا تدابیر نظارتی پلیس و برنامه‌های پیشگیری اجتماعی از جرم نظیر تولید محتوا یا افزایش سواد سایبری، درصدد کاهش ارتکاب جرم در فضای مجازی هستند و در کشورهای مختلف در حال اجرا هستند. با وجود این اقدامات متعدد، هنوز نرخ این جرائم در حال افزایش است. نکته قابل تأمل برای تحقق پیشگیری اثربخش در این حوزه، شناخت چالش‌ها، موانع موجود در تدوین و اجرای برنامه‌های پیشگیرانه خواهد بود. در واقع، توسعه، اصلاح و یا حذف سیاست‌ها و برنامه‌های موجود ایجاب می‌کند تا آسیب‌های آن‌ها در مراحل مختلف شناسایی و راهکارهای آن ارائه شود. با توجه به ضرورت این موضوع و صرف هزینه‌های فراوان در این حوزه، پرسش اصلی پژوهش حاضر موانع اثربخشی راهبردهای پیشگیری از جرائم سایبری علیه امنیت اخلاقی است. همچنین، تلاش می‌شود با بررسی پژوهش‌های تطبیقی و کاوش در برنامه‌ها و سیاست‌های کنونی نظام عدالت کیفری ایران در این رابطه، راهکارهایی نیز برای رفع این موانع ارائه شود.

پیشینه: پژوهش‌های متعددی در حوزه جرائم سایبری و پیشگیری از جرائم سایبری انجام شده است. در یکی از نخستین پژوهش‌ها، جلالی فراهانی (۱۳۸۳) پیشگیری از جرائم سایبری را به طور کلی بررسی و مزایا و محدودیت‌های هر یک از گونه‌های پیشگیری را تبیین کرده است. در حوزه پیشگیری وضعی از جرائم سایبری، بهره‌مند، کوره‌پز و سلیمی در مقاله خود با عنوان «راهبردهای پیشگیری از جرائم سایبری»، راهبردهای وضعی کورنیش و کلارک را که می‌تواند در فضای سایبر استفاده شود، تشریح کردند. آلاشتی نیز در کتاب خود با عنوان «پیشگیری از جرائم وضعی در فضای مجازی: راهکارها و چالش‌ها» افزون بر شناسایی و تبیین این راهبردها، چالش‌های آنها در فضای مجازی را بررسی و مواردی همانند نقض حریم خصوصی، خلاءهای حقوقی و مانند آن را برشمرده‌اند. رایجیان اصلی و همکاران (۱۳۹۳) نیز در مقاله خود با عنوان «پیشگیری از جرائم رایانه‌ای؛ از رهیافت نظری تا رهیافت جهانی در پرتو رهنمود پیشگیری

از جرم سازمان ملل متحد» پیشگیری از جرائم سایبری را بر اساس رهنمودهای پیشگیری از جرم سازمان ملل متحد تجزیه و تحلیل و پیشنهاداتی را به منظور انطباق تدابیر پیشگیرانه با این رهنمودها ارائه کردند. جدای از این، راهبرد پیشگیرانه آموزشی آگاهی ساز که یکی از راهبردهای کنترل انحرافات سایبری است، در یک مقاله جداگانه توسط رضوی فرد و کوره‌پز تجزیه و تحلیل شده است. در حوزه پیشگیری اجتماعی از جرائم سایبری، بهره‌مند و داودی (۱۳۹۷) در مقاله‌ای با عنوان «پیشگیری اجتماعی از جرائم امنیتی ـ سایبری»، پس از برشماری مصادیق جرائم امنیتی سایبری، موضوعاتی را درخصوص سواد رسانه‌ای، کدهای رفتاری، اطلاع‌رسانی و حکمرانی خوب در این فضا مطرح کرده‌اند. علیزاده در رساله دکتری خود با عنوان «سیاست جنایی کارآمد جهت سالم‌سازی فضای سایبر از محتوای مجرمانه و کاربری آن» ضمن ارائه مفهوم‌شناسی کامل از جرائم سایبری، ارکان و کنشگران فضای سایبر، نظام‌های کارآمد سیاست جنایی ناظر بر ساماندهی فضای سایبر، تدابیر سالم‌سازی را به دو گونه تدابیر دولتی و مشارکتی تقسیم کردند و در هر یک از این گونه‌ها، تدابیر کنشی را از تدابیر واکنشی تفکیک کرده است. بر این اساس، هدف پژوهشگر در رساله شناسایی تمام تدابیری بود که می‌تواند برای سالم‌سازی فضای مجازی تأثیرگذار باشد. همچنین، مقیمی و داودی دهاقانی (۱۳۹۷) در پژوهشی با عنوان «موانع اساسی تحقق پیشگیری از جرائم سایبر»، این موانع را در مورد تمام جرائم سایبری بررسی و در قالب موانع اجتماعی، موانع ساختاری، علمی آموزشی، فرهنگی، مدیریتی، حقوقی – قضایی و فنی احصاء کردند. نصری و اعظمی نیز در پژوهش خود با عنوان «جرائم مرتبط با امنیت اخلاقی در فضای مجازی» اشاره کردند که مسئولیت‌پذیری دولت در سیاست‌گذاری این جرائم و استفاده از توان علمی کشور نقش اصلی در پیشگیری از این جرائم خواهد داشت.

در حوزه پژوهش‌های تطبیقی می‌توان ادعا کرد که پژوهشگران خارجی مدت‌هاست که پژوهش‌های گسترده‌ای را در این زمینه انجام داده‌اند و از زوایای گوناگون برنامه‌های پیشگیرانه ناظر بر جرائم سایبری را نقد کرده‌اند. بخش گسترده‌ای از این پژوهش‌ها به طور کلی به تبیین مصادیق جرائم علیه امنیت اخلاقی سایبری مانند قلدری سایبری، اذیت و آزار سایبری، پورنوگرافی آنلاین و مانند آن اختصاص یافته است. بخشی از این پژوهش‌ها نیز اقدامات پیشگیرانه را در این زمینه ارزیابی کرده‌اند. برای نمونه، لوی و لیتن (۲۰۱۳) در پژوهش خود با عنوان «مشارکت چند نهادی در کاهش جرائم سایبری» به طور

کلی اقدامات چند نهادی در بریتانیا را در این حوزه آسیب‌شناسی کرده و به مواردی نظیر عدم شفافیت اقدامات، همکاری ضعیف در تبادل اطلاعات اشاره کردند. هارکین و همکاران (۲۰۱۸) نیز در پژوهش خود با عنوان «چالش‌های افسران پلیس سایبری: یک تحلیل تجربی»، مشکلات افسران پلیس در رابطه با کشف جرائم سایبری را بررسی کردند. در حوزه سواد سایبری نیز کرتیجان و همکاران در پژوهش خود با عنوان «چارچوب مفهومی برای افزایش امنیت و آموزش سایبری در آفریقای جنوبی» برنامه‌هایی که در این رابطه در آفریقای جنوبی انجام شد را تحلیل و به راهکارهایی برای افزایش این آگاهی‌ها اشاره کردند. صرف نظر از پژوهش‌های خارجی، در مجموع می‌توان نتیجه گرفت که تاکنون پژوهش جامعی در رابطه با موانع پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی در نظام عدالت کیفری ایران انجام نشده است. پژوهش‌های پیشین یا به صورت کلی ناظر بر جرائم سایبری بودند و یا به صورت موردی برخی از جرائم سایبری را مورد نظر قرار داده‌اند. این در حالی است که پژوهش حاضر بر تبیین موانع پیشگیرانه ناظر بر جرائم علیه امنیت اخلاقی تمرکز دارد. همچنین، در پژوهش‌های پیشین بیشتر راهکارهای پیشگیری وضعی و اجتماعی تبیین شده است، ولی در این پژوهش هدف آن است که راهکارها با توجه به موانع شناسایی شده ارائه شود. از این منظر، با توجه به خلاء پژوهشی در این حوزه، کاوش در مورد موانع پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی، و ارائه راهکارها برای رفع آن بسیار ضروری است.

مبانی نظری: جرائم علیه امنیت اخلاقی در پژوهش حاضر با توجه به بررسی قانون مجازات اسلامی (و قانون جرائم رایانه‌ای) و هم‌سنجی عناوین مجرمانه در این حوزه با پژوهش‌های متعدد علمی و قوانین کشورهای دیگر، به سه قسمت کلی اذیت و آزار سایبری، پورنوگرافی آنلاین و سکستینگ[1] تقسیم شده است.

اذیت و آزار سایبری[2]: برخی معتقدند که اذیت و آزار سایبری عنوان عامی است که ناظر بر انواع رفتارهای تعدی‌جویانه علیه شخص در فضای سایبر است. از این رو، جرائمی مانند تعقیب همراه با تهدید سایبری، قلدری سایبری زیرمجموعه این جرم قرار می‌گیرند. با وجود این در پاره‌ای از پژوهش‌ها هر یک از این واژگان معادل یکدیگر نگریسته شده است و به دنبال آن، تفاوت معنایی بین آنها وجود ندارد. به همین

1. Sexting
2. Cyber Harassment

جهت، واژگانی مانند قلدری سایبری[1]، سوءاستفاده سایبری[2] و آزار همراه با تهدید سایبری[3] به جای هم به‌کار می‌رود و بنابراین توافق عمومی در مورد این تعاریف وجود ندارد (وینکلمن[4] و همکاران، ۲۰۱۵). در پژوهش حاضر، معنای اول مورد نظر خواهد بود و از این رو، در ادامه به بررسی جرائم زیرمجموعه اذیت و آزار سایبری پرداخته می‌شود.

آزار همراه با تهدید سایبری: آزار همراه با تهدید سنتی[5] ناظر بر مجموعه رفتارهایی است که برای شخص مزاحمت ایجاد می کند و یا وی را مورد اذیت و آزار قرار می‌دهد، به طوری که در نهایت موجب ترسیدن و ارعاب بزه‌دیده می‌شود. کالیفرنیا اولین ایالتی بود که در سال ۱۹۹۰به دنبال قتل یک بازیگر تلویزیون، آزار همراه با تهدید را به طور مستقل جرم‌انگاری کرد.

قلدری سایبری: در پژوهش‌های مربوط به جرائم سایبری، گاه قلدری سایبری هم معنا با اذیت و آزار سایبری و یا آزار همراه با تهدید سایبری شناخته شده و بنابراین این واژگان به جای یکدیگر به کار می‌روند. گاه نیز این واژه تنها ناظر به آزارگری یا تعرض سایبری علیه کودکان و نوجوانان (اشخاص زیر ۱۸ سال) در دوران تحصیلات آموزشی است. در واقع، گروهی از پژوهشگران معتقدند که جرم قلدری سایبری از نظر نوع بزه‌دیده متفاوت از جرم اذیت و آزار سایبری است، ولی از نظر محتوای رفتار تفاوتی با آن ندارد (ویک[6]، ۲۰۱۷). به نظر می‌رسد با توجه به اینکه در بیشتر پژوهش‌های موجود قلدری سایبری در این معنا به کار رفته، در پژوهش حاضر نیز این معنا از قلدری سایبری پذیرفته شده است. در تایید این موضوع می‌توان بیان داشت که بیشتر پژوهش‌های موجود در حوزه قلدری سایبری نیز در مورد کودکان و نوجوانان انجام شده است.

پورنوگرافی آنلاین: پورنوگرافی اصطلاحی مربوط به علم هنر است که برای طبقه‌بندی آثار هنری و تفکیک میان برخی تصاویر بی‌پرده جنسی از سایر تصاویر به کار می‌رود (لاورل، ۲۰۰۲، به نقل از حبیب‌زاده و

---

1. Cyber Bullying
2. Cyber Abuse
3. Cyber Stalking
4. Winkelman
5. Traditional Stalking
6. Wick

رحمانیان، ۱۳۹۰). بسیاری از پژوهشگران پورنوگرافی را نمایش یا توصیف تصاویر و وضعیت برهنه یا نیمه برهنه مرتبط با فعالیت‌های جنسی می‌دانند (ترائین[1]، ۲۰۰۶).

سکستینگ: اشخاص معمولاً در طی روابطه دوستانه، عاشقانه و مانند آن از طریق فضای سایبر نیز با یکدیگر ارتباط برقرار کرده و پیام‌ها، تصاویر یا ویدئوهایی را برای یکدیگر ارسال می کنند که ممکن است محتوای برخی از آنها حاوی موضوعات جنسی باشد. بنابراین سکستینگ عبارت از رفتاری است که در آن اشخاص طی یک ارتباط تصویری، ویدئوهای برهنه یا نیمه برهنه و یا پیام‌های دارای محتوای جنسی را از طریق تلفن همراه، اینترنت، شبکه‌های اجتماعی و سایر وسایل الکترونیکی برای طرف مقابل خود ارسال و یا دریافت می کنند (ان. جی او[2] و همکاران، ۲۰۱۷).

پیشگیری از جرم: در ادبیات جرم شناسی، پیشگیری در دو معنا پذیرفته شده است: بیشتر پیشگیری از جرم تنها شامل تدابیری با ماهیت پیشگیرانه است که پیش از ارتکاب جرم به صورت هدفمند نسبت به جرم صورت می گیرد که در واقع همان اقدامات کنشی در رابطه با جرم و معنای مضیق پیشگیری است. گاه مفهوم پیشگیری افزون بر تدابیر کنشی، تدابیر واکنشی و اقدامات پسینی نسبت به جرم را نیز در بر می‌گیرد. در این معنا، تعیین و اجرای کیفر با هدف جلوگیری از تکرار جرم، نیز یکی از گونه‌های پیشگیری به شمار می‌رود (ابراهیمی، ۱۳۹۶). برای نمونه، شرمن در پژوهش خود در مورد ارزیابی با استفاده از این مفهوم عام پیشگیری به بررسی مداخله‌های موجود در این حوزه پرداخته است. با توجه به اینکه جرم‌شناسان بیشتر مفهوم مضیق از پیشگیری را در پژوهش‌های خود به طور عام و خاص در حوزه جرائم علیه امنیت اخلاقی در فضای سایبر پذیرفته‌اند، در پژوهش حاضر نیز همین مفهوم مورد نظر خواهد بود.

فیلترینگ: ویژگی‌های فضای سایبر ایجاب می کند تا افزون بر اقداماتی نظیر پیشگیری از تولید محتوای مجرمانه (برای نمونه، کسب مجوز برای انتشار محتوا)، تدابیری به منظور جلوگیری از انتشار گسترده و در دسترس قرار دادن محتوای مجرمانه تولید شده، انجام شود. برای نمونه، در حوزه جرائم علیه امنیت اخلاقی، فعالیت‌های پورنوگرافی برخط اصولاً از بستر انتشار و توزیع محتواهای پورنوگرافی در فضای مجازی صورت می گیرند و یکی از راه‌های پیشگیری از وقوع چنین فعالیت‌هایی، جلوگیری از انتشار این

1. Træen
2. Ngo

محتواها از طریق فیلترینگ است. در نظام عدالت کیفری ایران، واژه فیلترینگ (پالایش) بر اساس بند ۱۲ ماده ۱ مصوبه جلسه شماره ۱۹ تاریخ ۱۳۸۵/۱۰/۳ کمیسیون تنظیم مقررات ارتباطات، بدین صورت تعریف شد: «فیلترینگ فرایندی است برای دسته‌بندی و یا حذف بسته‌ها و یا آدرس‌های ناخواسته و یا جلوگیری از دسترسی به سایت‌های اینترنتی غیرمجاز که بر اساس تصمیم مراجع ذی‌صلاح ممنوعیت آنها اعلام شده یا خواهد شد». نهاد یادشده در سال ۱۳۸۹ تعریف مضیق‌تری از فیلترینگ را ارائه داد که تنها به محتوا مربوط می‌شود و عبارت است از: «شناسایی محتواهای درج شده در فهرست سیاه محتوا و مسدودسازی استفاده و یا مبادله آن در شبکه‌های ارتباطی و فناوری اطلاعات». با وجود این، در قانون جرائم رایانه‌ای به عنوان یکی از مهم‌ترین قوانین مرتبط با این موضوع، تعریفی از این مفهوم ارائه نشده است.

اعمال تدابیر نظارتی مدیران (اشخاص مسئول): در حوزه جرائم سایبری چند نهاد به موجب قانون مشمول برخی تکالیف پیشگیرانه در راستای فیلترینگ هستند، به طوری که می‌توان آنها را در شمار مدیران مکان‌ها دانست. نخست، بر اساس ماده ۷۴۹ قانون مجازات اسلامی (ماده ۲۱ قانون جرائم رایانه‌ای) ارائه‌دهندگان خدمات دسترسی مکلف شده‌اند تا بر اساس فهرست و ضوابط فنی ارائه شده از سوی کارگروه تعیین مصادیق محتوای مجرمانه، محتوای مجرمانه را پالایش و فیلتر کنند. ارائه‌دهندگان خدمات دسترسی، سازمان یا شرکتی است که به عنوان واسطه میان کاربر و اینترنت عمل کرده و امکان اتصال به اینترنت را برای آنان فراهم می‌کند. آیین‌نامه نحوه ارائه خدمات اطلاع‌رسانی و اینترنت، این اشخاص را به عنوان شرکت‌ها و یا موسسات و مراکز ارائه کننده خدمات اطلاع‌رسانی و اینترنت تعریف کرده و حدود فعالیت‌ها و وظایف آن‌ها بر شمرده است. آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مصوب ۱۳۹۳ نیز در بند الف ماده ۱ ارائه‌دهندگان خدمات دسترسی را اشخاصی دانسته که امکان ارتباط کاربران را با شبکه‌های رایانه‌ای یا مخابراتی و ارتباطی داخلی یا بین المللی یا هر شبکه مستقل دیگر فراهم می‌آورند از قبیل تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه‌های رایانه‌ای یا مخابراتی.

پیشگیری اجتماعی از جرم: بر اساس آمارهای موجود سن ورود به اینترنت کاهش پیدا کرده و هر لحظه کاهش می‌یابد. با توجه به تغییر ماهیت ارتباط اجتماعی و وقوع برخی از تعاملات اجتماعی در فضای مجازی، نیاز به یک محیط امن برای کودکان در این دنیای جدید بیش از پیش احساس می‌شود. این

موضوع که هدف بخش گسترده‌ای از بزهکاران سایبری و به طور خاص قلدران سایبری یا پورنوگراف‌های برخط، کودک یا نوجوان محسوب می‌شوند، ضرورت این نوع پیشگیری را بیشتر نشان می‌دهد. بر این اساس، هدف پیشگیری رشدمدار دخالت در مرحله جامعه پذیری کودکان و نوجوانان در محیط عمومی و خصوصی آنها از طریق راهبردهای مختلف و تبدیل آنها به شهروندان مطیع قانون است. بنابراین، ویژگی اصلی این نوع پیشگیری مداخله زودرس و تأکید بر ابعاد تربیتی کودک در مراحل رشد و در واقع، جامعه پذیری وی است. به همین جهت، احیای مهارت‌های زندگی اجتماعی، آموزش و تغییر متغیرهای خطرناک کودک، کانون توجه در این نوع پیشگیری خواهد بود (بهره‌مند و داودی، ۱۳۹۷).

افزایش سواد سایبری: گستردگی روزافزون فضای سایبر و افزایش کاربران این فضا، مسئله آگاهی کاربران از قلمرو آن، چگونگی انجام تعاملات اجتماعی، تبادل پیام، عکس، حفظ امنیت، حفاظت از حریم خصوصی و مانند آن را آشکار می‌سازد. دست‌یابی به آگاهی‌های این چنینی در قالب مفهومی با عنوان سواد رسانه‌ای، سواد سایبری[1]، سواد دیجیتال، سواد کامپیوتری و یا سواد اینترنتی[2] قرار می‌گیرد. بر این اساس، شهروندان برای اینکه از حضور در این دنیای جدید لذت ببرند و در عین حال احساس امنیت نیز کنند، باید از سطحی از آگاهی‌های مرتبط با این فضا برخوردار باشند.

تدوین کدهای رفتاری[3]: تدوین کدهای رفتاری برای چگونگی تعامل و رفتار فضای سایبر سهم بسزایی در تقویت اخلاق و هنجارهای اجتماعی حاکم بر این فضا و به تبع آن ایجاد فرهنگ سایبری خواهد داشت و از این جهت ارتباط تنگاتنگی با پیشگیری اجتماعی از جرم دارد. این کدها به عنوان یکی از مهم‌ترین تدابیر پیشگیرانه اجتماعی شامل رهنمودهای رفتاری و ارزش‌های اخلاقی هستند که با برشماری فهرستی از باید و نبایدها به دنبال تقویت هنجارمندی و پرهیز از نقض قواعد در حوزه‌های حرفه‌ای و اجتماعی هستند (منفرد و جلالی فراهانی، ۱۳۹۱). بعد تخصصی و درون گروهی کدهای رفتاری این امکان را فراهم می‌کند که محتوای آنها فقط در رابطه با ارائه اهداف، ارزش‌های آن گروه یا نهاد باشد و هنجارهای آن گروه را در چارچوب اسناد و مقررات بالادستی پیش‌بینی کند.

تولید و رتبه‌بندی محتوا: سرویس‌های ارائه محتوا و مدیریت آنها یکی دیگر از سیاست‌های پیشگیری

---

1. Cyber Litracy/Internet Litracy
2. Dijital Litracy
3. Codes of Conducts

اجتماعی به شمار می‌رود که به دنبال ارائه محتواهای مطلوب و غیرمجرمانه است تا شهروندان به واسطه دریافت این محتواها، از جست و جوی محتواهای مجرمانه منصرف شده و اشتیاقی برای توجه به آن‌ها نداشته باشند. بر این اساس، کنشگران دولتی در کنار فیلترینگ محتوای مجرمانه، توجه ویژه‌ای به ارائه محتواهای مناسب برای کاربران در این فضا دارند. نمود این توجه را می‌توان در تأکید کشورها بر ارتقای فرهنگ ملی، ارزش‌های مذهبی، اجتماعی و تاریخی، زبان و مانند آنها مشاهده کرد. در نظام عدالت کیفری ایران، مسئولیت اصلی در حوزه تولید محتوا به کمیسیون عالی ارتقای تولید محتوای فضای مجازی کشور سپرده شده است تا از طریق سیاست‌گذاری، تصمیم‌گیری، ارائه پیشنهادات و همچنین اعمال نظارت و مدیریت بر سازمان‌های مرتبط با تولید محتوای فضای مجازی، سطح محتوای مطلوب را در جامعه افزایش دهد.

روش

پژوهش حاضر با توجه به ماهیت موضوع و اهداف مورد نظر، کیفی و از حیث روش، توصیفی تحلیلی است. در این پژوهش افزون بر استفاده از مقالات و پژوهش‌های علمی فارسی و غیر فارسی، برای دستیابی به پاسخ‌های پژوهشگران و اهداف پژوهش، از شیوه‌های زیر برای جمع آوری اطلاعات مورد نیاز کمک گرفته است:

نخست، مصاحبه‌های عمیق: ظرفیت مصاحبه‌های عمیق بررسی ابعاد مختلف موضوع را امکان‌پذیر می‌سازد. در این نوع مصاحبه، پژوهشگر با طرح سوالاتی کلی به مصاحبه‌شونده اجازه می‌دهد تا دیدگاه‌های خود را تشریح کنند. انتخاب مصاحبه‌شونده‌ها به صورت هدفمند انجام شد، بدین معنا که پژوهشگر با توجه به معیارهای خاص و مرتبط با موضوع اصلی پژوهش و در واقع از روی هدف، مصاحبه‌شوندگان را انتخاب کرد. نمونه‌گیری تا اشباع نظری ادامه یافت. بر این اساس، با ۲۰ نفر از کارشناسان اعم از اعضای انجمن‌های مردم‌نهاد (۹ نفر)، افسران پلیس (۵ نفر) و قضات (۶ نفر) مطلع در جرائم سایبری مصاحبه و کدبندی داده‌ها انجام شد. زیرمجموعه‌های هر مقوله انتخاب شدند. در نهایت، نتایج حاصل از مطالعات خارجی و داده‌های کدبندی شده در قالب یافته‌های پژوهش ارائه شد.

برای اعتباریابی یافته‌ها، از روش‌های تأیید همکاران پژوهشی، استفاده از چند مصاحبه‌گر، تحلیل مستمر یافته‌ها و بازبینی پرسش‌ها و موضوعات مصاحبه‌ها، خودبازبینی محققان در طی فرایند جمع آوری

و تحلیل داده‌ها، دقت و وسواس در انتخاب مصاحبه‌شونده‌ها و آگاهی از دانش آنها در زمینه پرسش‌های مصاحبه، طرح پرسش‌های مصاحبه‌ها بر اساس تعداد زیادی از مطالعات خارجی دارای ارتباط مستقیم با موضوع، ثبت و یادداشت‌برداری مصاحبه‌ها و کدگذاری مصاحبه‌ها توسط دو نفر از پژوهشگران استفاده شد.

دوم، بررسی اسناد، قوانین و مدارک، اسناد، گزارش‌ها، آمار و اخبار: فضای مجازی حوزه‌ای است که نهادهای مختلفی برای مدیریت آن در حال فعالیت هستند و اسناد بالادستی، قوانین، آیین‌نامه‌ها و بخشنامه‌های مختلفی به چشم می‌خورد. برای نمونه، شورای عالی فضای مجازی، مجلس شورای اسلامی، کمیسیون تنظیم مقررات و هیئت وزیران مقررات متعددی در این حوزه نظیر قانون جرائم رایانه‌ای، مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای، آیین‌نامه جمع‌آوری و استناد پذیری ادله الکترونیک و سند راهبردی نظام جامع فناوری اطلاعات جمهوری اسلامی ایران را تصویب کرده‌اند. شناسایی و بررسی مقررات موجود در این حوزه به تحلیل موانع راهبردهای پیشگیرانه در این حوزه کمک شایانی خواهد کرد. به همین جهت، تلاش شده است تا قوانین مرتبط با جرائم علیه امنیت اخلاقی در این زمینه بررسی شوند.

همچنین، کنشگران فضای مجازی روزانه اخبار و گزارش‌های متعددی در خصوص تدابیر پیشگیرانه در مورد کنترل این فضا ارائه داده و دستاوردهای آن را به اطلاع همگان می‌رسانند. از این حیث، بررسی اظهارنظرها و گزارش‌های این مقامات برای شناخت چگونگی عملکرد مداخله‌های پیشگیرانه و پیامدهای آن در این حوزه ضرورت دارد. بسیاری از مقامات عدالت کیفری آخرین آمارهای موجود را به رسانه‌ها اعلام می‌کنند که آگاهی از آنها در ارزیابی برنامه‌ها بسیار تأثیرگذار بوده است.

یافته‌ها

ضعف در تدوین و اجرای رویکرد چند نهادی: رویکردهای مشارکتی مبتنی بر این ایده هستند که هیچ نهاد واحدی نمی‌تواند مسئول حل موضوعات پیچیده‌ای همانند جرم باشد. به طور خاص، رویکرد چند نهادی در سال‌های اخیر و پس از طرح مدرنیزاسیون دولت، اهمیت بسیار زیادی پیدا کرده است (بری[1] و همکاران، ۲۰۱۱). در این زمینه، پیشگیری چند نهادی از جرم، مداخله‌های عدالت کیفری در حوزه نوجوانان و پیشگیری چند نهادی در مصرف مواد مخدر از جمله حوزه‌هایی هستند که به شدت تحت تأثیر

1. Berry

رویکرد چند نهادی دچار تحول شده‌اند. وجود اختلاف و همکاری سازنده ناکافی میان نهادها در مورد این موضوعات موجب شده است که فیلترینگ یا حذف فیلترینگ برخی شبکه‌ها نظیر تلگرام محور توجه سیاست گذاران قرار گیرد و پوشش رسانه‌ای گسترده نیز در مورد آن وجود داشته باشد. نتیجه این موضوع خود تأکید بسیار زیاد بر استفاده از فیلترینگ به عنوان یکی از مهم‌ترین برنامه‌های پیشگیرانه و به حاشیه رفتن برخی برنامه‌های پیشگیرانه در حوزه افزایش سواد سایبری است. در واقع، با توجه به اختلاف نهادها در این موضوع، فیلترینگ در صدر اظهارات برخی مقامات رسمی در حوزه اقدامات پیشگیرانه قرار می گیرد. مصاحبه شونده شماره ۱۹ بر فقدان تعامل میان دو نهاد در این حوزه اشاره می کند: «همکاری سازنده ناکافی یکی از مشکلات بین قوا و بین ارگان‌ها است. مثلاً با اینکه دو ارگان مهم در مدیریت فضای مجازی قوه قضاییه و ارتباطات هستند ولی تعامل مثبت و سازنده‌ای با هم ندارند».

مصاحبه شونده شماره ۱۱ به تعدد سیاست گذاری‌ها در این خصوص اشاره کرده است. «ما در حیطه فرهنگ سند رسمی زیاد داریم. چند تا سند بالادستی داریم. نقشه جامع آموزش و پرورش، نقشه جامع علمی کشور، سند راهبردی صنایع خلاق و نوآورانه. سند خیلی داریم. هم چشم‌انداز در آن هست هم راهبرد هم سیاست. ۱۱ بند هم در برنامه ششم توسعه توسط مقام معظم رهبری به عنوان سیاست‌های کلی نظام در فضای مجازی ابلاغ شده، ما سیاست‌های کلی فضای مجازی را داریم، اما آن دکترین و چتر فکری را نداریم. ما آنقدر سند بالادستی داریم که خودمان گیج شدیم. هی سند می‌نویسیم. ما دچار اغتشاش ساختاری هستیم. همه مون داریم همه کاری می کنیم، اما مثل تیمی هستیم که همه خوب بازی می کنند اما گل نمی‌زنند! هرکسی جای خود خوب بازی می کند (صدا و سیما و سازمان تبلیغات و آموزش و پرورش و مانند آنها)، اما نتیجه نمی گیریم». در مجموع، چالش های مختلف بین نهادهای پیشگیری کننده، موازی کاری نهادها و تعدد نهادهای سیاست گذار، شکل همکاری و نتایج آن را دچار روابط بسیار پیچیده‌ای می کند که گاه انسجام، همکاری مشترک و سازنده بین نهادها را در این حوزه ضعیف می‌سازد.

اتکای بیش از اندازه بر پلیس فتا در انجام سیاست‌ها و برنامه‌های پیشگیرانه: نتایج پژوهش‌های جرم‌شناسی بیانگر نوعی تعادل ناکافی میان تقاضای عمومی برای انجام وظایف پلیسی در فضای سایبری و سطح خدماتی است که پلیس در حقیقت می تواند ارائه کند. در واقع، انتظار عمومی بر این است که پلیس پیشگیری از جرائم سایبری را در جامعه دنبال کند. مصاحبه شونده شماره ۱۲ در رابطه

با حقوق بسیار پایین پلیس فتا و تخصص ناکافی آنها اظهار می‌دارد: «هرچند فتا باید پلیس تخصصی باشد، اما سیستم جذب فتا نخبه‌پرور نیست. تخصص و کیفیت در درجه اول اهمیت نیست. نیروهای کیفی فتا بسیار کم هستند. در واقع، این سیستم به دلایلی نخبه‌گریز هست. اولاً حقوق فتا بسیار پایین است. ثانیاً به دلیل برخی از محدودیت‌ها نخبه‌های کامپیوتر ترجیح می‌دهند در فتا نباشند». همچنین، مصاحبه شونده شماره ۲ در رابطه با انتظارات بیش از اندازه از پلیس فتا گفت: «وظیفه ذاتی پلیس کشف جرم و دستگیری مجرمین است. در هر حال، پلیس از بسیاری از ارگان‌های دیگر کوشش بیشتری در عرصه پیشگیری دارد. اما نهایتاً عدم موفقیت‌ها در این عرصه به نام پلیس نوشته می‌شود. همه می گویند پس پلیس داره چیکار میکنه که این همه جرم داریم؟ کسی از سایر نهادها بازخواست نمی کند. مثلاً کسی نمی گوید آیا وزارت ورزش و جوانان هیچ کار جدی‌ای در این زمینه می کند یا نه؟ چرا آموزش و پرورش یا وزارت علوم واحدهای درسی تعریف نمی کنند. چرا صدا و سیما کار جدی و مدون نمی کند؟ چرا سینما و یا وزارت فرهنگ و ارشاد فیلم آموزشی تولید نمی کند. متأسفانه کم کاری سایر نهادها به نام پلیس نوشته می‌شود. توقع زیاد داشتن از پلیس باعث شده که از سایر ارگان‌های ذی ربط سلب مسئولیت بشه. اگر پلیس در سایر کشورها در این حیطه موفق‌تر هست، به این دلیل است که قسمت زیادی از مسئولیت‌ها را سایر ارگان‌ها به درستی انجام می‌دهند».

سهم پایین رویکردهای مشارکتی در پیشگیری از جرائم علیه امنیت اخلاقی در فضای سایبر: با توجه به اینکه برنامه‌های پیشگیری از جرم در بسیاری موارد به صورت مشارکتی انجام می‌شود، در قسمت حاضر در ابتدا مداخله‌های پیشگیرانه با مشارکت بخش خصوصی ارزیابی و سپس، سهم انجمن‌های مردم نهاد در پیشگیری از این جرائم بررسی می‌شود.

مشارکت پایین بخش خصوصی و دولتی در پیشگیری از جرائم: در حال حاضر، یکی از مهمترین مشکلات مدیریت فضای مجازی، همکاری ضعیف و نامناسب میان نهادهای عدالت کیفری در این حوزه است. در حوزه فعالیت‌های سایبری، با توجه به اینکه بسیاری از این فعالیت‌ها توسط شرکت‌های خصوصی در فضای مجازی انجام می‌شود، این شرکت‌ها به عنوان بخش خصوصی یکی از سهامداران مهم در کنترل فضای مجازی خواهند بود. از این رو، پیوند بخش خصوصی و دولتی در اجرای برنامه‌های پیشگیرانه، از جمله موارد اجتناب ناپذیر در این حوزه محسوب می‌شود. برای حل این مشکلات، در برخی

کشورها کدهای رفتاری برای ارائه‌کنندگان خدمات اینترنتی، اپراتورهای موبایل و به طور کلی مالکان غیر دولتی شبکه‌های اینترنتی، وب‌سایت‌ها و شبکه‌های اجتماعی ارائه شده است. مصاحبه‌شونده شماره ۴ در این زمینه گفت: «تشکیل موسسات خصوصی شناسایی جرائم سایبری، مانند کارآگاه‌های خصوصی می‌تواند یک راهکار پیشگیرانه باشد. این موسسات می‌توانند وقت و انرژی بیشتری بگذارند. مهندسان و متخصصین حرفه‌ای دارند. مجهز به نرم‌افزارهای پولی گران قیمت برای شناسایی و ردیابی هستند که فتا اینها را ندارد. درنتیجه ضریب موفقیت شناسایی پرونده‌ها و متهمین را بالاتر می‌برد و از تراکم کار فتا هم کمتر می‌کند. ولی این اتفاقات تاکنون نیفتاده و از ظرفیت‌های آنها استفاده نشده است». بنابراین پیشنهاد می‌شود که مشارکت میان بخش خصوصی و دولتی تقویت و از ظرفیت‌های آنان برای پیشگیری از جرائم علیه امنیت اخلاقی در فضای مجازی استفاده شود. در این راستا، عواملی همچون تعیین اهداف به صورت شفاف، گسترش حوزه‌های همکاری، تعیین ارزش کار گروهی، شفافیت مالی در مورد منابع مالی همکاری و تبادل اطلاعات تأثیرگذار در موفقیت مشارکت بخش خصوصی و عمومی ضروری خواهند بود و از این رو، توجه به آن‌ها مهم شمرده می‌شود.

استفاده ناکافی از ظرفیت سازمان‌های مردم نهاد و مشارکت مردم در تدوین و اجرای سیاست‌های پیشگیرانه: انجمن‌ها یا سازمان‌های مردم نهاد سهم عمده‌ای در اداره جامعه و تدوین برنامه اقدام در دنیای نوین برعهده دارند. دولت‌ها دیگر نمی‌توانند آن‌ها را نادیده بگیرند؛ بلکه باید در جریان مدرنیته از توانایی آنها برای پیشرفت و پرکردن کاستی‌های قدرت خود بهره ببرند. آنان تا اندازه‌ای قدرت پیدا کرده‌اند که می‌توانند به عنوان همکار دولت در پروژه‌های پیشگیری از جرم شرکت کنند و یا اینکه خود عهده‌دار تدوین پروژه باشند و دولت از دستاوردهای آنان استفاده کنند. آنها حتی می‌توانند به حمایت از بزه‌دیدگان برخاسته و در دادگاه‌ها نیز حضور داشته باشند. به موازات این پیشرفت، حوزه پیشگیری از جرائم سایبری نیز به شدت مورد توجه انجمن‌های مردم نهاد متعددی در بسیاری از کشورهای دنیا بوده است. این سازمان‌ها در دولت‌های مختلف اقدامات متعددی را در حوزه نرم‌افزارهای نظارتی و افزایش سواد سایبری انجام داده‌اند. در این زمینه، مصاحبه‌شونده شماره ۱۵ به مقایسه انجمن و اقدامات آن پرداخته است: «درکشورهای اروپایی و آمریکا برای ارتقای سواد رسانه‌ای، این بخش خصوصی است که با کمک دولت این رسالت را به پیش می‌برد. در ایران هم حدود دو سال است که انجمن سواد رسانه‌ای ایران تشکیل

شد که دو همایش و چندین کتاب و دو پودمان (مهارت‌های سواد رسانه‌ای و تربیت مربی سواد رسانه‌ای که محتوای آن مورد تایید وزارت علوم قرار گرفته است) از دستاوردهای آن است. تفاهم نامه با دانشگاه علم و صنعت (برای آموزش مجازی) و دانشکده خبر (برای آموزش حضوری) نیز صورت گرفته است». برای نمونه، این انجمن در تالیف کتاب سواد سایبری با همکاری وزارت آموزش و پرورش و تعلیم مربیان مشارکت داشته است. مصاحبه شونده شماره ۱۶ به پیامدهای این همکاری اشاره کرده است: «ما به یک برنامه هماهنگ نیاز داریم. ما به همراه آموزش و پرورش کتاب سواد رسانه‌ای را تالیف کردیم، اما معلم پرورش یافته برای تدریس این کتاب وجود ندارد. اخباری داریم مبنی بر اینکه معلمی که درس فیزیک و شیمی رو تدریس می کنه، بدون دانش رسانه‌ای خاص میاد این درس رو تدریس می کنه! یا نمونه‌هایی داشتیم که معلم چون به محتوای کتاب آگاه نبوده سرفصل‌ها را تغییر داده و اصلاً چیز دیگری درس داده!»

عدم ارزیابی سیاست‌ها و برنامه‌های پیشگیرانه: در دانش جرم‌شناسی، رویکرد تجربه‌محور به معنای استفاده متعادل و با هدف از پژوهش‌های موجود و بهترین داده‌های در دسترس، برای سیاست‌گذاری و تصمیم‌گیری است. این رویکرد دربردارنده بازنگری انتقادی از ادبیات پژوهشی موجود برای تعیین میزان اعتبار ادله و اطلاعات و کارایی آن‌ها است. همچنین، سیاست‌ها و رویه‌های نوین نیز برای تعیین اثربخشی ارزیابی می‌شوند تا همواره سیاست‌های کارا و به روز تدوین شود. یکی از مهم‌ترین ویژگی‌های تجربه محوری، پویایی و قابلیت بازنگری این رویکرد است؛ زیرا مداخله‌ها به صورت مداوم ارزیابی، سنجش و بازنگری می‌شوند (میرز[1]، ۲۰۰۹). بنابراین، سیاست تجربه‌محور دربردارنده برنامه‌ها و رویه‌هایی است که اثربخشی آنان به وسیله ارزیابی‌ها و سایر شیوه‌های علمی اثبات شده است.

تسامح اجتماعی در برابر جرائم علیه امنیت اخلاقی سایبری: بر پایه نتایج پژوهش‌های علمی، در حوزه مقابله با جرائم علیه امنیت اخلاقی سایبری نوعی ضعف در تدوین و اجرای رویکرد پیشگیرانه اجتماعی وجود دارد که یکی از دلایل مهم آن تسامح اجتماعی در قبال آنهاست. این تسامح اجتماعی که به تساهل فرهنگی می‌انجامد، پیامدهای ناخواسته‌ای را نیز به دنبال خواهد داشت که ممکن است امنیت فرهنگی را متأثر کند (سوفیان[2]، ۲۰۱۸). بنابراین، اشخاص، مصرف‌کنندگان منفعل فضای مجازی هستند

1. Mears
2. Sofian

و حساسیت و دغدغه خاصی در مورد چگونگی انجام فعالیت‌های سایبری دیگران ندارند. به همین جهت، در قسمت پیش رو، ابتدا پایین بودن سطح سواد سایبری به طورکلی بررسی و سپس، این موضوع در بحث والدین و کودکان در قالب نظارت ناکافی والدین تحلیل می‌شود و در نهایت، یکی از پیامدهای تسامح اجتماعی که همان اولویت پایین رسیدگی به جرائم سایبری علیه امنیت اخلاقی است، تحلیل می‌شود.

پایین بودن سطح سواد سایبری: بر این اساس، افزایش آگاهی و امنیت سایبری شهروندان را ترغیب می‌کند تا با کسب مهارت در برابر تهدیدات سایبری مقاومت خود را افزایش دهند و یک ساختار ملی شبکه‌ای مقاوم ایجاد شود. به باور پژوهشگران رعایت برخی عوامل در هنگام افزایش آگاهی و آموزش سایبری ضروری است و آنها باید در قالب محتوا در دسترس اشخاص قرار گیرند:

- اهداف تعیین شده به صورت شفاف تعریف شوند؛
- یک گروه تخصصی تشکیل شود؛
- یک برنامه اجرایی برای دستیابی به اهداف تدوین شود؛
- کمپین ملی افزایش آگاهی و آموزش سایبری تشکیل شود؛
- مشارکت به عنوان یکی از اجزای برنامه اجرایی درنظر گرفته شود؛
- منابع برای اجرای برنامه اجرایی تعیین شود و در دسترس باشد؛
- فنون نظارتی باید از پیش تعیین و تعریف شده باشند (کورتجان[1]، ۲۰۱۴).

در همین راستا، مصاحبه شونده شماره ۸ به درستی به ضرورت تغییر و افزایش آگاهی‌های سایبری و تغییر سبک سیاست‌گذاری اشاره می‌کند. «هزینه صورت گرفته برای فیلترینگ را می‌توان صرف محتواسازی نمود. کاری که انجام نشده و برنامه‌ای هم برای انجام آن نیست. برای حل مسائل جدید از طریق روش‌های قدیم نمی‌توان استفاده کرد. زندگی در جهان معاصر زندگی است که سرعت آن مرتب در حال افزایش است و این سرعت تغییرات است و غیر قابل اجتناب است و باید روش زندگی را تغییر دهیم. این کاری است که سیاستگذاران باید انجام دهند». مصاحبه شونده شماره ۱۷ نیز به ضرورت حساس کردن مردم اشاره کرده است: «هیچگونه حساسیت پذیری نداریم. به عنوان نمونه، به راحتی تصویر یا فیلم خانمی را در فضای مجازی به اشتراک می‌گذاریم و کسی به مردم نمی‌گوید که این عمل به لحاظ اخلاقی،

1. Kortjan

انسانی و حتی شرعی اشکال دارد. اگر ما بتوانیم آستانه حساسیت پذیری مردم را پایین تر بیاوریم، خود رفتار جمعی ما هم به بزه‌دیده کمک می کند هم نرخ این جرائم را کمتر می کند و هم به پیشگیری کمک می کند. ما واقعیات رو به مردم نمی گوییم. مثلاً چه می‌شود اگر تلویزیون هفته‌ای یک بار درباره یکی از پرونده‌های سایبری صحبت کند». در مجموع، افزایش سواد سایبری جامعه به افزایش فرهنگ گزارش جرائم و خشونت‌های روانی و جنسی علیه اشخاص و به طور خاص کودکان و زنان منتهی خواهد شد.

نظارت ناکافی والدین: برخی انسان‌ها از نیاز برای حمایت از داده‌های شخصی و محرمانه خود ناآگاه هستند و به همین جهت بزه‌دیده جرائمی مانند هک و بهره‌برداری از اطلاعات شخصی افراد قرار می گیرند. به باور پژوهشگران، برخی از والدین از تهدیدهای آنلاین اطلاعی ندارند و نمی‌توانند به فرزندان خود درباره رفتارهای ایمن در فضای مجازی آموزش بدهند. بنابراین، فقدان دانش کافی مردم را تهدید می کند. در واقع، برخی والدین از اینکه فرزندانشان مدت‌ها پشت میز لپ تاپ یا کامپیوتر به سر می‌برند، بیش از آنکه پشت تلویزیون یا بیرون از منزل باشند، خوشحال می‌شوند. به همین جهت، آنان تسامح بیشتری در قبال نظارت و میزان استفاده از اینترنت به خرج می‌دهند. حتی بر اساس نتایج برخی پژوهش‌ها، آنها به ندرت در مورد فضای سایبر و روابط جنسی در این فضا با فرزندان صحبت می کنند (فلیمینگ[1]، ۲۰۰۶)؛ از این رو، امنیت فرزندان به نحو کافی توسط والدین تأمین نمی‌شود.

اولویت پایین‌تر جرائم علیه امنیت اخلاقی سایبری در مقایسه با جرائم مالی سایبری: در حوزه سواد رسانه‌ای، بازنمایی اجتماعی جرائم سایبری عموماً معطوف به جرائم سایبری مالی به دلایل مختلف شده است و به همین جهت، رسانه‌ها تمرکز چندانی بر ارائه آگاهی‌های مرتبط با حوزه حریم خصوصی اشخاص ندارند. در همین حوزه نیز رسانه‌ها بیش از آنکه هدف اطلاع‌رسانی و افزایش آگاهی در مورد چگونگی فعالیت و حمایت از حریم خصوصی و حفاظت از اطلاعات شخصی را مدنظر داشته باشند، بیشتر بر توصیف جرائم مرتبط با فضای مجازی پرداخته‌اند. به دنبال آن، بیشتر دیدگاه‌های غیرکارشناسی و توصیفی ارائه می‌شود. برای نمونه، با اینکه مزاحمت سایبری به گفته رئیس پلیس فتا، دومین جرم سایبری مشهور در کشور محسوب می‌شود، ولی تدابیر پیشگیری تناسب چندانی با آن ندارد. وقتی به محتوای توصیه‌های پیشگیرانه مقامات رسمی دقت شود، مشخص می‌شود که بیشتر ناظر بر جرائم

1. Fleming

سایبری مالی است. مصاحبه شونده شماره ۱۷ به نقش رسانه در این حوزه پرداخته است: «نقش خیلی پررنگی وجود دارد، اما عموماً آن چیزی در رسانه بیان می‌شود که همه مردم می‌دانند. مثلاً نمی‌بینیم که در موضوعی کارشناسی بیاورند و در کنار توضیح مسئله، راهکارهای لازم را بدون چارچوب از پیش تعیین شده سیاسی، فرهنگی، اجتماعی و مانند آن ارائه دهند. بایدها و نبایدهای رسانه‌ای باعث شده اعتماد مردم نسبت به رسانه سلب شود. هرگاه این رسانه با زبان خود مردم و بر اساس واقعیت زندگی مردم صحبت کند مورد توجه و پذیرش قرار می‌گیرد». به طور کلی، در نظام عدالت کیفری ایران، یافته‌های حاصل از مصاحبه‌ها بیانگر اهمیت پایین‌تر جرائم سایبری علیه امنیت اخلاقی در مقایسه با جرائم مالی سایبری است. بنابراین، بهتر است رسانه‌ها بیشتر به پیشگیری و آگاه‌سازی در مورد جرائم سایبری علیه امنیت اخلاقی از جمله سوء استفاده جنسی علیه کودکان و سایر گروه‌ها، راه‌های پیشگیری از آزارهای سایبری و مانند آن تمرکز کنند. همچنین، به اشخاص در مورد رفتارهای پرخطر و الگوهای رفتاری بزهکاران سایبری هشدارهای لازم داده شود. همچنین، نیاز است تا با تغییر فرهنگ سازمانی پلیس و قضات رسیدگی کننده به این جرائم، پرونده‌های مربوط به این جرائم نیز مهم شمرده شود.

تأکید بیش از اندازه بر سیاست‌های فاقد اثربخشی کافی: همانند نظام عدالت کیفری ایران، در بسیاری از کشورها نیز از فیلترینگ به عنوان راهکاری برای ممنوعیت دسترسی همگان به محتواهای مجرمانه استفاده می‌شود. ولی تفاوت در این است که در ایالات متحده و یا برخی دیگر از کشورها، فیلترینگ به صورت موضوعی انجام می‌شود، نه اینکه یک شبکه که هم دارای کاربردهای مثبت و هم منفی است، به طور کلی فیلتر شود (آکدنیز[1]، ۲۰۰۱). در نظام عدالت کیفری ایران نیز درباره برخی پایگاه‌های اینترنتی از فیلترینگ موضوعی استفاده می‌شود. همچنین، ممکن است در مورد برخی پایگاه‌های اینترنتی، محتوای مجرمانه به کلی حذف شود ولی مقامات عدالت کیفری گاه بر اساس معیارهای مدنظر خودشان، کل پایگاه اینترنتی یا شبکه اجتماعی همانند تلگرام، فیس‌بوک، وی‌چت، یوتیوب و مانند آن را فیلتر و دسترسی به آن را برای همگان مسدود می‌کنند. به دنبال این جریان، کاربران این شبکه‌ها و پایگاه‌های اینترنتی یا از استفاده از آنها خودداری می‌کنند و یا اینکه با استفاده از فیلترشکن (وی پی ان) به فعالیت خود در این شبکه‌ها و پایگاه‌های اینترنتی ادامه می‌دهند.

1. Akdeniz

بحث و نتیجه‌گیری

یکی از راهکارهای مهم در پیشگیری از جرائم سایبری علیه امنیت اخلاقی، تقویت رویکرد چند نهادی در این حوزه و پایبندی به مؤلفه‌ها و تلاش برای افزایش مشارکت و تعیین سهم و میزان مسئولیت‌پذیری هر نهاد است. ولی آنچه تاکنون نشان داده شده است، مجموعه‌ای ناهمگن و در نهایت ناکارا از پیشگیری چند نهادی در این حوزه بوده است. مسائلی نظیر سردرگمی در تعیین و اجرای اولویت‌های سیاست‌گذاری و یا به بیانی بهتر ابهام در اولویت‌گذاری، امکان اجرای رویکرد چند نهادی را با چالش مواجه می‌کند. موازی‌کاری نهادهای کنترل کننده جرائم و شفافیت ناکافی اقدامات نهادها در حوزه کنترل جرائم علیه امنیت اخلاقی سایبری نیز بر این چالش‌ها می‌افزاید. جدای از این، به باور برخی در نظام عدالت کیفری ایران رویکرد چند نهادی یعنی به رسمیت شناختن اهمیت مشارکت و نقش سایر نهادها در کنار پلیس و به باور برخی دیگر این موضوع تلاشی برای سلطه یک نهاد بر سایر نهادهاست، به طوری که آنها مادون آن نهاد قرار می‌گیرند. برای پرهیز از عدم اجرای برنامه‌های پیشگیرانه در فضای سایبر و تلاش برای تقویت رویکرد چند نهادی ضروری است تا وظایف نهادها به صورت مشخص از هم تفکیک، قالب همکاری آنها تعیین و چگونگی پاسخگویی آنها در صورت انجام ندادن وظایف‌شان به صراحت تشریح شود. تعیین ضمانت اجرا یکی از موضوعاتی است که پاسخگویی سازمان‌ها در برابر همدیگر را افزایش می‌دهد. جدای از مقوله همکاری‌های میان‌نهادی، رویکردهای مشارکتی در حال حاضر یکی از بهترین گزینه‌ها برای افزایش مسئولیت‌پذیری اجتماع و دولت در حل مشکلات اجتماعی است. به باور برخی محققان، احتساب دولت به عنوان نهاد انحصاری با توجه به افزایش روزافزون کنشگران غیردولتی که سهم عمده‌ای در تدوین زیرساخت‌های سایبری جامعه دارند، دیگر معنادار نخواهد بود.

فضای سایبر دنیایی است که در حال حاضر نمی‌توان از ورود به آن خودداری کرد. حتی کودکان بیشتر از بزرگسالان در این فضا دارای تجربه هستند. به همین جهت، رویکردهای مبتنی بر ممانعت از ورود به فضای سایبر، به صورت کوتاه مدت مفید هستند. آگاهی از این فرایند که خواه ناخواه جریان دارد، ایجاب می‌کند تا دولت با همکاری سایر کنشگران، چگونگی فعالیت و تعامل اجتماعی در این فضا را به شهروندان آموزش دهند. افزایش آگاهی و سواد سایبری به کاربران فضای سایبری کمک می‌کند تا رفتارها و روابط دوستانه خود را در این فضا سامان دهند. در این خصوص، آموزش و پرورش

سهم گسترده‌ای باید در تبیین فعالیت‌های اجتماعی کودکان در فضای مجازی داشته باشد، نه اینکه با اندیشه‌ای غیرمعقول تمام آنان را از ورود به فضای مجازی منع کند. در واقع، جرائمی همانند قلدری سایبری، پورنوگرافی و اذیت و آزار سایبری گاه آثاری به مراتب بیشتر از جرائم مالی در زندگی اجتماعی انسان‌ها می گذارد.

جدای از این، دستیابی به اهداف و سیاست‌های پیشگیرانه مستلزم استفاده از نتایج پژوهش‌های تجربی در فرایند سیاست گذاری، اجرای سیاست‌ها و ارزیابی آنهاست. ایده اصلی رویکرد تجربه‌محور، ابتنای تصمیم‌ها و برنامه‌ها بر پژوهش‌های تجربی است. در واقع، این سیاست با ارائه ادله تجربی میزان موفقیت یا شکست یک برنامه و سیاست را سنجیده و راه‌هایی را برای انتخاب سیاست مناسب، بهبود اثربخشی و کارایی سیاست‌ها پیشنهاد می‌دهد. در این زمینه، ارزیابی نیاز یکی از انواع ارزیابی است که در رویکرد تجربه محور اهمیت بسیار زیادی دارد. شناسایی یک نیاز می تواند به مثابه پنجره فرصتی نگریسته شود که از خلال آن سیاست گذاری‌هایی صورت گیرد که با توجه به شناخت موضوع و پیچیدگی‌های آن، بسته‌های سیاستی عقلایی را ارائه دهد.

پیشنهادها: با توجه به موضوعاتی که در پژوهش حاضر مطرح شد، خلاصه‌ای از راهکارهای موجود در پژوهش به شرح زیر ارائه می‌شود.

- شفافیت در مورد تعداد نهادهای سیاستگذار و ارتباط آنها در فرایند سیاستگذاری؛
- تعیین و تفکیک سهم و میزان منابع مالی برای انجام هر یک از وظایف نهادها؛
- الزام نهادها به همکاری با دیگر نهادها و تعیین ضمانت اجرا در صورت همکاری نکردن؛
- تعریف منافع مشترک در تدوین و اجرای برنامه‌ها و سیاست‌های مشترک؛
- کاهش تعارض‌های ساختاری در همکاری‌های مشترک؛
- افزایش تخصص و دانش سایبری در سازمان پلیس از طریق برگزاری دوره‌های آموزشی تخصصی سایبری به موازات پیچیدگی روزافزون جرائم سایبری؛
- افزایش میزان مشارکت بخش خصوصی در کنترل جرائم علیه امنیت اخلاقی در فضای سایبر؛
- افزایش ظرفیت سازمان‌های مردم‌نهاد در تدوین و اجرای برنامه‌های پیشگیرانه؛
- همکاری مراجع دولتی و دانشگاهی در ارزیابی برنامه‌های پیشگیرانه؛

- پرهیز از فیلترینگ کلی پایگاه‌های اینترنتی و شبکه‌های اجتماعی؛
- افزایش سطح سواد سایبری جامعه.

فهرست منابع

ابراهیمی، شهرام. (۱۳۹۶). جرم‌شناسی پیشگیری. چاپ چهارم. تهران: انتشارات میزان.

بهره‌مند، حمید و داودی، ذوالفقار. (۱۳۹۷). پیشگیری اجتماعی از جرائم امنیتی- سایبری. مطالعات حقوق کیفری و جرم شناسی، ۳(۴۸)، صص ۲۷-۴۶.

حبیب‌زاده، محمدجعفر و رحمانیان، حامد. (۱۳۹۰). هرزه‌نگاری در حقوق کیفری ایران، مجله حقوقی دادگستری، ۷۵(۷۶)، صص ۸۹-۱۲۱.

رایجیان اصلی، مهرداد؛ سلیمی، احسان؛ و نوریان، علیرضا. (۱۳۹۳). پیشگیری از جرائم رایانه‌ای؛ از رهیافت نظری تا رهیافت جهانی در پرتو رهنمود پیشگیری از جرم سازمان ملل متحد، فصلنامه مطالعات راهبردی جهانی شدن، ۵(۱۶)، صص ۱۸۹-۲۱۶.

مقیمی، مهدی و داودی‌دهاقانی، ابراهیم. (۱۳۹۷). موانع تحقق پیشگیری از جرائم سایبر. طرح پژوهشی. مرکز مطالعات معاونت اجتماعی و پیشگیری از جرم قوه قضائیه. تهران.

منفرد، محبوبه و جلالی فراهانی، امیرحسین. (۱۳۹۱). کدهای رفتاری و پیشگیری از بزهکاری، پژوهشنامه حقوق کیفری، ۳(۲)، صص ۱۱۰-۱۰۸.

Akdeniz, Y. (2001). Internet content regulation: UK government and the control of Internet content. Computer Law & Security Review, 17(5), pp 303-317.

Berry, G., Briggs, P., Erol, R., & Van Staden, L. (2011). The effectiveness of partnership working in a crime and disorder context. A rapid evidence assessment, 1. Berry, G., Briggs, P., Erol, R., & Van Staden, L.2 (2011). The effectiveness of partnership working in a crime and disorder context. A rapid evidence assessment, 1

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. Youth & Society, 38(2), pp 138-140.

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal, 52(1), 34.

Levi, M. , & Leighton Williams, M. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. Information Management & Computer Security, 21(5), pp 420-443.

Mears, D. P., & Bacon, S. (2009). Improving criminal justice through better decision making: Lessons from the medical system. Journal of Criminal Justice, 37(2), pp 143-144.

Ngo, F., Jaishankar, K., & Agustina, J. R. (2017). Sexting: Current Research Gaps and Legislative Issues. International Journal of Cyber Criminology, 11(2), pp 161-163.

Sofian, A., Pratama, B., & Talerico, C. (2018). Weighting Approaches on Online Sexual Abuse of Children: Cultural Prevention or Crime-Based Enforcement?. Udayana Journal of Law and

Culture, 2(2), 191-193.

Træen, B., Nilsen, T. S. R., & Stigum, H. (2006). Use of pornography in traditional media and on the Internet in Norway. Journal of Sex Research, 43(3), 246.

Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of Cyber Harassment and Perpetration among College Students in the United States: A Test of Routine Activities Theory. International Journal of Cyber Criminology, 11(1), pp 25-26.

Winkelman, S. B., Early, J. O., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring Cyber Harrassment among Women Who Use Social Media. Universal journal of public health, 3(5), pp 195-196.