پژوهشهای سیاسی جهان اسلام، انجمن مطالعات جهان اسلام
فصلنامه علمی (مقاله علمی - پژوهشی) پژوهشهای سیاسی جهان اسلام، سال یازدهم، شماره چهارم، زمستان ۱۴۰۰، صص ۱۷۴ - ۱۵۱

DOI: ۱۰.۲۱۸۵۹/priw-۱۱۰۴۰۷

نقش سیاست جنایی مشارکتی در پیشگیری از جرایم سایبری در ایران

سید غنی نظری[۱]
سیامک جعفرزاده[۲]
رضا نیک خواه سرنقی[۳]

تاریخ دریافت: ۱۴۰۰/۰۵/۲۸ تاریخ پذیرش: ۱۴۰۰/۰۹/۰۶

انجمن مطالعات جهان اسلام
Islamic World Studies Association
جمعیة دراسات العالم الاسلامی
فصلنامه علمی -پژوهشی
پژوهشهای سیاسی جهان اسلام

[Downloaded from priw.ir on 2026-02-03]

[DOR: 20.1001.1.23222980.1400.11.4.7.1]

چکیده

مقاله حاضر با هدف بررسی نقش سیاست جنایی مشارکتی در پیشگیری از جرایم سایبری به نگارش درآمده‌است. این مقال، با استفاده از نظریه‌های مختلف و روش تحلیلی و اسنادی سعی در بررسی موشکافتاه این مهم نموده‌است. بر اساس یافته‌های این مقاله، تدابیر سیاست جنایی مشارکتی برای سالم سازی فضای سایبر، تدابیر متنوعی اعم از تدابیری با ماهیت فنی نظیر فناوری صدور مجوز و فناوری‌های راجع به تایید هویت اشخاص (به ویژه سن و جنسیت آن‌ها) و تدابیر مختلفی با ماهیت غیر فنی نظیر آموزش و ارتقاء سواد دیجیتالی قابل اعمال است. سیاست جنایی مشارکتی کارآمد مستلزم بکارگیری تمامی تدابیر ممکن و وزن دهی مناسب به این تدابیر نسبت به یکدیگر با کمک جامعه مدنی و سازمان‌های مردم نهاد است. از این رو سیاست جنایی مشارکتی ایران ظرفیت‌های قابل توجهی به ویژه در حوزه اقدامات پیشگیرانه اجتماعی و وضعی از سوی سازمان‌های مردم نهاد داراست، لیکن در حقوق ایران بیشتر بر تدابیر وضعی و البته فقط یک نوع از این تدابیر که مربوط به محدود کردن دسترسی (پالایش) است سرمایه گذاری و تاکید شده است ولی در راستای پیش گیری کنشی از جرایم سایبری، هیچ ابزاری به اندازه «آموزش» نمی‌تواند مؤثر واقع شود.

واژه‌های کلیدی: پیشگیری اجتماعی، پیشگیری وضعی، پیشگیری مشارکتی، جرایم سایبری.

۱. دانشجوی دکتری حقوق کیفری و جرم شناسی، دانشگاه ارومیه، ارومیه، ایران. snnazari743@gmail.com
۲. دانشیار گروه فقه و حقوق اسلامی، دانشگاه ارومیه، ارومیه، ایران(نویسنده مسئول). s.jafarzadeh@urmia.ac.ir
۳. استادیار گروه فقه و حقوق اسلامی، دانشگاه ارومیه، ارومیه، ایران. rnsj_nikkhah@yahoo.com

Copyright © 2010, SAIWS (Scientific Association of Islamic World Studies). This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International, which permits others to download this work, share it with others and Adapt the material for any purpose

مقدمه

فضای سایبری از جمله محیط‌های بدیع دست بشر است که روز به روز بر اهمیت آن افزوده می‌شود و جنبه‌های مختلف زندگی را تحت تأثیرات مثبت و منفی این فضا قرار خواهد گرفت؛ گزافه نخواهد بود اگر گفته شود امروز مناسبات و روابط اجتماعی اشخاص در دو شق مستقل جهان واقعی و فضای سایبری قابل تحلیل و بررسی است؛ تقریباً هر جنبه‌ای از ارتباطات اجتماعی متصور در جهان واقعی در فضای سایبری نیز قابلیت تحقق پیدا کرده است یا در آینده ای نزدیک تحقق خواهد داشت؛ ماهیت فضای سایبری با جهان واقعی به کلی متفاوت است و این تفاوت در ماهیت، تبعاً مفاهیم و چالش‌های جدیدی را در حوزه‌های مختلف ایجاد خواهد کرد؛ از جمله حوزه‌های مبتلابه و مورد چالش، حوزه علم حقوق است.

در فضای سایبر، برخلاف بسترهای ارتباطی قدیمی که در آن‌ها یک رابطه یک سویه برقرار بوده، با توجه به ویژگی‌های خاص این فضا؛ از جمله سهولت تولید و انتشار محتوا، گمنامی و نیز فرامرزی بودن آن، مخاطب به طور فعال در فرآیند ارتباط و تولید محتوا مشارکت داشته و به عبارتی در این فضا، محتوا به صورت خود تولید، توزیع به صورت خودگردان و فرآیند انتخاب کردن و دریافت نیز به صورت خودگزین است (خازنی، ۱۳۹۴: ۲۱۶).

یکی از چالش‌های جدید حقوق کیفری مقابله با جرائم سایبری است، به بیان دیگر با توجه به گستردگی و شبکه‌ای بودن فضای سایبر، باید اذعان داشت مقابله با جرائم سایبری به جهت گستردگی خسارت و کثرت بزه دیدگان، فرامرزی بودن و مشکلات کشف و تعقیب مجرم و بسیاری ویژگی‌های دیگر تنها با یک راهبرد جنایی مشارکتی می‌تواند کارآمد و مؤثر صورت گیرد، آن چه این نظر را تقویت می‌کند این است که جرائم سایبری در غیاب جرائم سنتی اتفاق نمی‌افتند و در واقع جایگزین جرائم سنتی نمی‌شوند، بلکه در کنار آن‌ها قرار می‌گیرند، یعنی جرائم سنتی مانند قتل، ضرب و جرح، زنا، سرقت و کلاهبرداری‌های سنتی کماکان اتفاق می‌افتند، نتیجه این است که منابع، نیروها و امکانات موجود دستگاه عدالت کیفری دچار فرسایش و کمبود می‌شوند و امکان مواجهه با همه این جرائم از آن‌ها سلب می‌شود (مهدوی ثابت و مرادی، ۱۳۹۶: ۹۹).

برای مقابله همه جانبه و کارآمد با این جرائم، اتخاذ یک سیاست جنایی فراگیر با مشارکت گسترده جامعه مدنی، کاربران سایبر و سازمان های مردم نهاد ضروری است. در پرتو یک سیاست جنایی مشارکتی هر یک از این گروه‌ها باید در مراحل مختلف فرآیند جنایی یعنی پیشگیری و مقابله با جرم، کشف جرم و

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

تعقیب مجرم، مرحله رسیدگی به جرم و مجازات مجرم نقش آفرینی کنند تا ضمن کاستن از بار دستگاه عدالت کیفری به مقابله هرچه گسترده تر و دقیق تر با جرم پرداخته شود، چرا که کنترل بزه به جهات مختلف فراتر از ظرفیت نهادهای رسمی عدالت کیفری است و باید به واگذاری بخشی از سازگارهای تأمین کننده امنیت و عدالت به مردم، سازمان های مردم نهاد و نهادهای غیر دولتی پرداخت.

سیاست جنایی مشارکتی، یعنی مشارکت جامعه مدنی و نهادهای غیر دولتی در فرآیندهای جنایی (کیفری و غیرکیفری)؛ مشارکت مردم می‌تواند به روند رسیدگی کمک شایانی نماید، هم از نظر سرعت رسیدگی و هم این که فرهنگ سازی در این زمینه می‌تواند به گزارش دهی و همکاری با مسئولین و همچنین پیشگیری از وقوع جرم کمک نماید (فرهمند، ۱۳۹۶: ۱۳۴).

سیاست جنایی مشارکتی یا سیاست جنایی توأم با شرکت وسیع جامعه، یعنی در نظر گرفتن آثار ضرورت حیاتی ایجاد اهرم‌های تقویتی دیگری به غیر از پلیس یا قوه قضائیه به منظور اعتبار بخشیدن بیشتر به یک طرح سیاست جنایی است که به وسیله قوه مجریه و قوه مقننه تهیه و تدوین می‌گردد. استفاده از قدرت رسانه‌های جمعی، انجمن‌ها و شهروندان در ایجاد توافق و هماهنگی درباره سیاست جنایی ضروری است. پی بردن به اهمیت این موضوع و توجه به آن در عمل، باید به شرکت دادن مردم در سیاست جنایی با کلیه تغییراتی که این کار به دنبال می‌آورد بینجامد؛ نه بدین لحاظ که از نظر عقیدتی طرفدار حضور و مداخله کمتر دولت باشیم بلکه به خاطر واقع گرایی است؛ زیرا مشارکت عامه مردم در سیاست جنایی به کارآیی آن می افزاید. به علاوه این واقع گرایی ما را در جهت مردمی (دموکراتیزه کردن زندگی محلی نیز سوق می‌دهد (لازرژ، ۱۳۹۶: ۱۲۶).

یکی از نمودهای سیاست جنایی مشارکتی در زمینه سایبر، کاستن از اختیار نهادهای دولتی و نظارتی در امر فیلترینگ و تفویض حداقل قسمتی از این امر به برخی از شهروندان و کاربران شریف فضای سایبر، که رویکردی سنجیده و ملایم تر نسبت به مسئله فیلترینگ دارند، می‌باشد. این امر موجب افزایش دقت و هوشمند سامانه‌های فیلتر کننده برای اجتناب از اشتباه در فیلترینگ نیز می‌شود. نمونه دیگری از سیاست جنایی مشارکتی در جرائم سایبری رعایت ادب و نزاکت در اتاق‌های گپ و گفت و گو است که در صورت عدم پایبندی به آن، کاربران دیگر، شخص هنجار شکن را از ادامه حضور در اتاق گپ محروم می-کنند (حاجی ده آبادی و سلیمی، ۱۳۹۳: ۸۳-۸۲).

سیاست جنایی مشارکتی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم را در بر می‌گیرد که با همکاری وسیع جامعه مدنی و نیروهای دولتی مانند پلیس، سازمان زندان ها، سازمان

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

محیط زیست، جنگل بانی و ... با دستگاه قضایی انجام می‌شود. در این سیاست جنایی، برای پیشگیری از جرم و مبارزه با آن از اسباب و وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود که می‌توان برای اعمال آن، از طریق مختلف مانند فرهنگ سازی، آموزش، مفهوم دینی امر به معروف و نهی از منکر بهره برد. یکی از طرق نظارت بر جرائم سایبری، توسط نهادهای مدنی و اشخاص و با مشارکت مردم است که می‌تواند مصداقی از امر به معروف و نهی از منکر باشد و موجب پیشگیری از جرائم سایبری شود، مربوط به نظارت بر ورودی‌ها است که سعی می‌شود از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری شود (وطنی و اسدی، ۱۳۹۵: ۱۲۲). در این مقاله نگارندگان به دنبال پاسخ گویی به سوالات ذیل هستند که سیاست جنایی مشارکتی در خصوص جرایم سایبری دارای چه رویکردی باید باشد؟ سیاست جنایی مشارکتی جمهوری اسلامی ایران در حوزه سالم سازی فضای سایبر از محتوای مجرمانه تا چه میزان از ظرفیت‌های ممکن برای رسیدن به هدف مذکور استفاده نموده است؟

مفهوم شناسی تحقیق

۱-سیاست جنایی

در تعاریف مضیق این مفهوم،که در واقع از تعاریف اولیه سیاست جنایی محسوب می‌شدند، سیاست جنایی مترادف با سیاست کیفری به کار گرفته می‌شد و سیاست جنایی در این تعبیر، به سیاست «برخورد با جرم و بزهکاری پس از ارتکاب آن»، محدود می‌شد. هر چند که در تعاریف اولیه سیاست جنایی، رویکرد انحصاری، مبارزه با جرم و کیفر بزهکاران و به بیان دیگر سیاست کیفری بوده است، اما به تدریج در کنار مقابله و جزادهی به بزهکار، بحث پیشگیری از بزه نیز در میان جرم‌شناسان قوت پیدا کرد و سیاست جنایی از «سیاست کیفر» به «سیاست کیفر و پیشگیری» تحول پیدا کرد.کسانی همچون، فون لیست[1]، مرل و ویتو[2] و استفانی، لواسور و بولک[3] ازین دیدگاه به سیاست جنایی پرداخته‌اند. لیکن از منظر، سیاست جنایی در سطح حقوق کیفری یا جرم‌شناسی محدود نمانده و خود مفهومی مستقل و رشته مطالعاتی نوینی شناخته می‌شود. بدین سبب، در تعریف موسع سیاست جنایی، واژگانی جدید (عمدتاً متفاوت با آنچه در تعاریف مضیق به کار رفته است)، دیده می‌شود.

سیاست جنایی موسع علاوه بر قواعد حقوقی، عملکرد نهادهایی مختلف را که اجرای قواعد مزبور را

1. Vonlist
2. Merl and Vito
3. Stefani, Levasseur and Bouloc

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

به عهده دارند در بر می‌گیرد. این نهادها عبارتند از: پلیس، دادسراها، دادگاه‌ها، اداره زندانها، اداره آموزش و تربیت مراقبتی مجرمان، نهادهای پیشگیری از جرم و ادارات خدمات اجتماعی. بنابراین مجموعه‌ای از فعالیت‌های نهادی (رسمی) وجود دارد که همچون خود قانون جزء سیاست جنایی قرار می‌گیرند. شیوه‌ی عملکرد نهادها و قواعد حقوقی، نظام عدالت جنایی و نظام کیفری با هم ترکیب می‌شوند و ساختاری به نام «نظام سیاست جنایی» شکل می‌گیرد[1].

به این ترتیب، سیاست جنایی در مفهوم موسع را می‌توان به «سیاست جنایی ماهوی» شامل بزه انگاری، انحراف انگاری و پاسخ گذاری و «سیاست جنایی شکلی» شامل آیین‌های رسیدگی به بزه، تعیین پاسخ به آن (پاسخ دهی)، تعریف مراجع پاسخ دهی [رسیدگی کننده) و سازمان‌های متولی اجرا و اعمال پاسخ به بزه و نیز پاسخ دهی به انحراف توسط جامعه مدنی تقسیم نمود[2].

۲- سیاست جنایی مشارکتی

سیاست جنایی مشارکتی، یعنی مشارکت جامعه مدنی و نهادهای غیر دولتی در فرآیندهای جنایی (کیفری و غیرکیفری)؛ مشارکت مردم می‌تواند به روند رسیدگی کمک شایانی نماید، هم از نظر سرعت رسیدگی و هم این که فرهنگ سازی در این زمینه می‌تواند به گزارش دهی و همکاری با مسئولین و همچنین پیشگیری از وقوع جرم کمک نماید .

سیاست جنایی مشارکتی یا سیاست جنایی توأم با شرکت وسیع جامعه، یعنی در نظر گرفتن آثار ضرورت حیاتی ایجاد اهرم‌های تقویتی دیگری به غیر از پلیس یا قوه قضائیه به منظور اعتبار بخشیدن بیشتر به یک طرح سیاست جنایی است که به وسیله قوه مجریه و قوه مقننه تهیه و تدوین می‌گردد. استفاده از قدرت رسانه‌های جمعی، انجمن‌ها و شهروندان در ایجاد توافق و هماهنگی درباره سیاست جنایی ضروری است. به لحاظ نظری قلمرو یا دامنه سیاست جنایی مشارکتی شامل تمام مراحل تدوین و اجرای سیاست جنایی می شود که در این میان، مرحله اجرای سیاست جنایی که شامل مرحله پیشگیری و مرحله واکنش به پدیده مجرمانه می باشد بیشتر مطرح و از اهمیت بسزایی برخوردار است و در همین قلمرو، مرحله پاسخ دهی واکنشی که مشارکت مردم را در بر دارد اهمیت و گستردگی بیشتری را به خود اختصاص می دهد؛ چرا که این مرحله، مرحله گسترده ای است که در واقع تمام مراحل مختلف فرایند کیفری از بدو وقوع و ارتکاب جرم و تعقیب آن را تا مرحله اجرای حکم کیفری و بازپذیری اجتماعی

۱. حاجی ده آبای، محمدعلی؛ خاقانی اصفهانی، مهدی؛ گونه شناسی سیاست کیفری فنی در قبال جرم رمزنگاری اطلاعات از منظر آزادی گرایی و امنیت گرایی، فصلنامه آموزه های حقوق کیفری، شماره ۵، بهار و تابستان ۱۳۹۲، ص۱۰۷.

۲. نجفی ابرندآبادی، علی حسین؛ سیاست جنایی، دانشنامه علوم جنایی اقتصادی، زیر نظر امیرحسن نیازپور، تهران: انتشارات میزان، چاپ دوم، ۱۳۹۸، ص۵۵۷.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

بزهکار دربر می‌گیرد و تمام ارکان جامعه مدنی می‌توانند در آن ایفای نقش نمایند. بدین ترتیب در کنار اهرم‌های پاسخ دهی دولتی به پدیده مجرمانه، امکان مشارکت فعال شهروندان و نهادهای جامعه مدنی نیز در فرآیند کیفری فراهم شده و پاسخ به جرم صرفا جنبه رسمی و دولتی محض نخواهد داشت[1].

این تعاریف و تعاریف مشابهی که از سیاست جنایی مشارکتی شده است، همساز با تعریف خود سیاست جنایی است، جز اینکه به بعد تکامل یافتهٔ آن و حضور مردم و نهادهای مردمی در فرایند آن تأکید می‌شود. پذیرش مشارکت مردمی به عنوان فصل مقوّم سیاست جنایی، از آن رو است که حضور مردم و نهادهای مدنی، رسانه های گروهی، فضای سایبر، شبکه های اجتماعی مجازی و...، در مرحلهٔ تدوین قوانین، جرم انگاری، کیفرگذاری و اساساً شکل گیری سیاست جنایی تقنینی اثرگذار است. همچنین، در سیاست جنایی قضایی عادلانه بی اثر نیست، چنانکه در زمینهٔ اقناع بزهدیده و بازپذیری اجتماعی بزهکار نقش مثبت دارد. این نقش در همکاری با پلیس در زمینه های مختلف به ویژه در عرصهٔ پیشگیری از جرم محسوس است[2].

۳- فضای سایبر

(Cyber) در زبان انگلیسی پیشوند و در زبان فارسی پسوند کلمات جدید و امروزی متصل می‌شود تا به آن‌ها معنا و مفهوم دهد به گونه‌ای که مرتبط با فضای رایانه یا برخط (Online) باشد. سایبر از کلمه Cyberspace مشتق شده است که به مطالعه مکانیزم‌های مورد استفاده در کنترل و تنظیم سیستم‌های پیچیده اعم از انسان یا ماشین اطلاق می‌شود و اصطلاح فضای سایبر یا دنیای مجازی آنلاین اصطلاحی است که نخستین بار توسط ویلیام گیبسون در رمانی با عنوان نیورومانسر در سال ۱۹۸۵ مورد استفاده قرار گرفت[3]. از آن زمان تاکنون فضای سایبر را به معنای مکانی غیر فیزیکی و مجازی می‌شناسیم. فضای سایبر، یک فضای واقعی، اما مفهومی است که در آن ارتباطات و انتشار اطلاعات از طریق شبکه‌های کامپیوتری صورت می‌گیرد[4] و با عنایت به ارزیابی سنجه‌های متفاوت از مفهوم فضای سایبر می‌توان گفت که فضای سایبر، محیطی تشکیل یافته از سامانه‌ها و شبکه‌های ارتباطی متصل به هم است که قابلیت هر نوع رفتار متناسب با محیط مبادله داده، ذخیره و انتشار اطلاعات را دارد.

---

۱. رستمی، ولی؛ مشارکت مردم در فرآیند کیفری – بررسی سیاست جنایی کشورهای غربی، فصلنامه حقوق، مجله دانشکده حقوق و علوم سیاسی، شماره ۲، تابستان ۱۳۸۹، ص۱۶۱.

۲. وحیدی، عبدالملک، شیدائیان، مهدی و میرخلیلی، سید محمود؛ مباني و جلوه¬های قرآني سیاست جنایي مشارکتي، فصلنامه پژوهش حقوق کیفری، دوره نهم، شماره ۳٤، بهار ۱٤۰۰، صص۳۵-۳٦.

۳. باستانی، برومند؛ جرائم کامپیوتری و اینترنتی جلوه¬ای نوین از بزهکاری، تهران: انتشارات بهنامی، چاپ اول، ۱۳۸۳، ص۵۵.

٤. کرامتی معز، هادی؛ بزه دیده شناسی کودکان در شبکه¬های مجازی، تهران: انتشارات دادگستر، چاپ اول، ۱۳۹۹، صص صص۲۳-۲۴.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

۴- حکمرانی فضای سایبر

حکمرانی فضای سایبر را می‌توان نحوه ایجاد ارزش‌ها، هنجارها و استانداردهای رسمی و غیررسمی برای رفتار دولت و بازیگران غیردولتی (بخش خصوصی و نهادهای مدنی) در نسبت فضای مجازی دانست. ایجاد سازوکارهای قانونی بهتر برای رسیدگی و مقابله با جرائم سایبری بین المللی، قواعد شفاف ملی برای اجرای قانون و طراحی نظام حفاظتی یکپارچه داده ها ازجمله نتایج حکمرانی فضای سایبر است[۱].

۵- ماهیت و انواع جرایم سایبری

جرم سایبری عبارت است از هرگونه تخلف از قانون کیفری که دانش فناوری رایانه‌ای را در ارتکاب، تحقیق و پیگرد شامل شود؛[۲] موسسه ملی عدالت در گزارش خود زیر عنوان «واحدهای جرم سایبری اختصاصی»[۳] جرم سایبری را هر رفتار غیرقانونی می‌داند که دانش فناوری رایانه‌ای برای ارتکاب جرم به کار گرفته می‌شود. در این گزارش قید شده که فضای سایبر نسبت به جرم می‌تواند دو حالت داشته‌باشد؛ حالت فعال که رایانه برای نفوذ در فایل‌ها و ربایش پول و رفتارهای غیرقانونی از این دست به کار گرفته می‌شود و حالت انفعال که رایانه نقش تسهیل کننده یا راهنما برای خریداران یا کالا ها به ویژه در پرونده‌های قاچاق مواد مخدر دارد[۴].

بر پایه قانون مجازات اسلامی فصل جرایم رایانه‌ای و قانون آیین دادرسی کیفری می توان گفت که جرم سایبری در حقوق کیفری ایران به جرمی گفته می‌شود که یا بر ضد داده یا رایانه رخ دهد یا با دستاویز رایانه یا فضای سایبر رخ دهد. با این حال گستره بزه سایبری از جهت ابزار و وسیله بودن ناروشن است.

یکی از تقسیم بندی کلی از جرایم، تقسیم به جرایم طبیعی و جرایم قراردادی است. در مفهوم طبیعی و تعیین مصادیق آن در ادبیات جزایی تا حدی اختلاف نظر به چشم می خورد از جمله جرایم تصنعی، جرایم ناشی از فناوری اطلاعات می باشد. شاید بتوان گفت جرایم طبیعی بیشتر تحت سیطره ارزش های مذهبی و شرعی است و یا سنن کهن قضایی در باب آنها جاری و ساری است. به عبارت دیگر، قوانین قدیمی و کلاسیک برای این جرایم در نظر گرفته می شود؛ اما جرایم قراردادی مخصوصاً جرایم ناشی از فن آوری مدرن از امور حادثند. در بحث از جرایم طبیعی و قراردادی یکی از موارد، اثر ارتکاب

۱. فیروزآبادی، ابوالحسن؛ درآمدی بر حکمرانی فضای مجازی، تهران: انتشارات دانشگاه امام صادق و مرکز ملی فضای مجازی، چاپ اول، ۱۳۹۹، ص٤٤.

2. Keyser,mike,the council of Europe convention on cybercrime, journal of transnational law and policy, volume 12,2003, p290.

3. Dedicated Cyber Crime Unites.

4. Edgar, stacey, morality and machines: perspectives on computer ethics, jones and Bartlett publishers, second edition,2003, p167.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

این جرایم بر مرتکب است. احساس شرم در جرایم طبیعی وجود دارد اما در جرایم قراردادی خیر. عنصر مادی جرایم سنتی یا کلاسیک و مرسوم به دلیل بسترهای متفاوت ارتکاب آن و اشکال مختلف سناریوی مجرمانه طبعا عنصر مادی هر جرم با جرم دیگر تفاوت دارد. به هر حال هنگام تبیین عنصر مادی جرایم سایبری باید به شکل یکسان ارتکاب آنها یا دیگر اجزای عنصر مادی توجه کرد. فناوری واحد بستر واحدی ایجاد می کند که جرایم در این بستر شکل های خاص و ثابتی می‌یابند[1].

یکی دیگر از نقاط افتراق جرایم ارتکابی در دنیای فیزیکی با فضای سایبر این است که بسیار اتفاق می‌افتد که میان محل حضور مرتکبین جرایم و بزه دیدگان فاصله‌ای بس طولانی وجود دارد. البته بدون شک یکی از دلایلی که مرتکبین جرایم این فضا را گزینش کرده اند این است که بدون ملاقات و مواجهه فیزیکی با قربانیانشان می‌توانند به نتایج مجرمانه شان نائل شوند[2].

بنابراین در جرایم محیط سایبر، اولاً تعداد بزه دیدگان بسیار بالاست و شاید از مرز هزاران و میلیون ها نفر هم فراتر رود، ثانیا معمولا نمی توان آمار دقیقی از تعداد بزه دیدگان داشت، چه جرایم سایبر در شبکه شیوع می یابند و حالت اشاعه جرم ارتکابی که در بسیاری موارد به صورت خودکار صورت می گیرد، بسیاری از سیستمهای رایانه ای و اطلاعات را درگیر خود می سازد و این امر قابل شمارش نیست. در واقع این طبیعت فضای تکنولوژیک فضای سایبر است که موجد پیدایش جرایمی خودکار شده است که مرتکب فقط در قدم اول تحقق جرم نقش دارد و نه در استمرار آن. به عبارت دیگر در ارتکاب این جرایم مرتکب آغازگر است. اما شاید هیچ گاه ادامه دهنده نباشد و این امر جرایم مستمری را آفریده است که فاعل آن در استمرارش نقشی ندارد. بنابراین نرخ ارتکاب جرم هم بالاست و در یک لحظه از زمان به میزان بسیار زیادی ممکن است واقع شود. برای نمونه ممکن است بتوان هزاران سند و اطلاعات رایانه ای را در لحظه ای از زمان جعل کرد و یا به صورت غیرمجاز کپی کرد و تکثیر کرد. از این رو «ارتکاب جرایم جمعی» در محیط سایبر یک ویژگی نسبتا معمول است[3].

در یک تقسیم بندی، این جرایم به طور کلی، در دو دسته قرار گرفته است:

۱) جرایم کامپیوتری که با قوانین کلاسیک قابل مجازات هستند و نیاز به جرم انگاری جدید ندارند.

---

۱. خرم آبادی، عبدالصمد؛ جرایم فناوری اطلاعات، رساله دکتری، رشته حقوق کیفری و جرم شناسی، دانشگاه تهران، ۱۳۹٤، ص۳۵.

۲. جلالی فراهانی، امیرحسین؛ درآمدی بر آیین دادرسی کیفری جرایم سایبری، معاونت حقوقی و توسعه قضایی قوه قضائیه مرکز مطالعات راهبردی و توسعه قوه قضاییه، تهران: انتشارات خرسندی، ۱۳۸۹ چاپ اول، ص۷۶.

۳. فضلی، مهدی؛ مسئولیت کیفری در فضای سایبر، تهران: معاونت حقوقی و توسعه قضایی قوه قضائیه مرکز مطالعات توسعه قوه قضاییه، انتشارات خرسندی، چاپ دوم، ۱۳۸۹، ص۷۱.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

۲) جرایمی که حسب توصیه سازمانهای بین المللی و منطقه‌ای[1] نیاز به وضع قوانین جدید دارند.

دسته اول، در همان سه گروه جرایم سنتی مشتمل بر جرایم علیه اشخاص، جرایم علیه اموال و جرایم علیه امنیت و آسایش عمومی، قابل توضیح می باشند[2].

دسته دوم، در سه گروه به شرح ذیل تقسیم شده اند:

۱) جرایمی که ارتکاب آنها قبل از پیدایش فناوری اطلاعات، به هیچ وجه امکان پذیر نبوده است و جدید بودنشان موجب جرم انگاری آنها شده است (مانند هک)؛

۲) جرایمی که تفاوت ماهیتی آنها با جرایم سنتی، موجب جرم انگاری مجزا برای آنان شده است (مانند جعل کامپیوتری)؛

۳) جرایمی که خطرناک تر شدن ارتکاب آنها نسبت به جرایم سنتی، مدد جرم انگاری مجزا شده است. (مانند پورنو گرافی کودکان[3])

به نظر می‌رسد این تقسیم بندی جامعیت لازم برای ادای مقصود نسبت به جرایم این فضا را دارد.

انجمن مطالعات جهان اسلام
Islamic World Studies Association
جمعیة دراسات العالم الاسلامی
فصلنامه علمی -پژوهشی
پژوهشهای سیاسی جهان اسلام

روش تحقیق

تحقیق حاضر از نوع مطالعات تحلیلی و توصیفی به وسیله کتابخانه ای - اسنادی انجام می‌شود.

به صورت روش تحقیق کتابخانه‌ای، برای جمع آوری اطلاعات بعد از ماخذ شناسی و گردآوری منابع، از ابزارهای فیش، و فرم‌های مربوطه به نکته برداری خواهیم پرداخت؛ بدین صورت که بعد از ماخذیابی کتب و اسناد مربوطه به موضوع، فهرست موقت از مطالب مورد نیاز را تهیه و سپس با آماده سازی فیش‌ها، مرحله‌ی فیش برداری شروع و مطالب با استفاده از تکنیک ماخذ گذاری به روش علمی تنظیم خواهد شد.

یافته ها

۱. نقش سیاست جنایی مشارکتی در پیشگیری اجتماعی از جرایم سایبری

جهت سالم سازی فضای سایبر در مباحث مربوط به پیشگیری از جرم، تدابیر پیشگیرانه اجتماعی مربوط

---

۱. مانند سازمان ملل، شورای اروپا و غیره

۲. ابوذری، مهرنوش؛ پیشین، ص۲۷.

۳. خرم آبادی، عبدالصمد، جزوه جرایم فناوری اطلاعات، کانون جنبش نرم افزاری دانشکده حقوق سیاسی دانشگاه تهران، ۱۳۹۰، صص۲۳ - ۲۹.

[Downloaded from priw.ir on 2026-02-03]

[DOR: 20.1001.1.23222980.1400.11.4.7.1]

به مرحله پیش از ارتکاب جرم می باشند. در موضوع سالم سازی فضای سایبر و نیز سالم سازی کاربری این فضا، تدابیر اجتماعی مورد نظر اعم است از تدابیری که موجب کاهش انتشار محتوای مجرمانه و نامناسب بوده و تدابیری که موجب مصون سازی کاربران به ویژه کاربران کودک و نوجوان که آسیب پذیرترین قضر کاربران فضای سایبر هستند، می‌باشد.

۱-۱. مشارکت در تولید محتوا

یکی از تدابیر مؤثر جهت سالم سازی فضای سایبر و نیز سالم سازی کاربری این فضا، تولید محتوای متناسب است. لکن با توجه به گستردگی فضای سایبر، روشن است که جهت اثربخش بودن چنین راهکاری، مشارکت نهادهای دولتی و غیر دولتی و اقشار مختلف جامعه مدنی لازم است.

سرویس های ارائه محتوا و مدیریت آن‌ها یکی دیگر از سیاست های پیشگیری اجتماعی به شمار می‌رود که به دنبال ارائه محتواهای مطلوب و غیر مجرمانه 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 ویژه ای به ارائه محتواهای مناسب برای کاربران در این فضا دارند. نمود این توجه را می توان در تأکید کشورها بر ارتقای فرهنگ ملی، ارزش های 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 سیاست گذاری، تصمیم گیری، ارائه پیشنهادات و همچنین اعمال نظارت و مدیریت بر سازمان های مرتبط با تولید محتوای فضای مجازی، سطح محتوای مطلوب را در جامعه افزایش دهد (شاملو و کاظمی جویباری، ۱۳۹۸: ۲۳).

یکی از کشورهایی که در بحث تولید محتوا در فضای سایبر، سرمایه گذاری وسیعی انجام داده، کشور کاناداست. در این کشور علاوه بر اینکه نهادی دولتی بنام «مرکز فرهنگ کانادایی برخط»، متولی تولید محتوا در فضای سایبر است، تلاش برای جلب مشارکت عمومی جهت تولید محتوای مناسب سایبری، با جدیت و حمایت دولت صورت می‌گیرد. به عنوان مثال یکی از موارد تحت حمایت مرکز فرهنگ کانادایی برخط، صندوقی تحت عنوان «صندوق سرمایه گذاری مشارکت» است. این صندوق برای کمک به طرح های ابتکاری میان مؤسسات و سازمان‌های غیر انتفاعی، عمومی و خصوصی به منظور برقراری ارتباط همه کانادایی ها با ثروت‌های میراثی کانادا از طریق دسترس پذیر ساختن مجموعه های فرهنگ کانادایی که در اختیار سازمان های فرهنگی استانی، شهری و محلی قرار دارد، در اینترنت به زباهای رسمی،

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

طراحی شده است. همچنین صندوق شبکه های پژوهشی در حوزه رسانه های نوین نیز یکی از برنامه های دیگری است که مورد حمایت مرکز فرهنگ کانادایی برخط قرار گرفته است هدف این صندوق، کمک بهساخت ظرفیت تحقیق و توسعه در کانادا و پیشرفت نوآوری در حوزه محتوای فرهنگی سایبری است. تحت حمایت این صندوق، گروهی از مشارکت کنندگان بخش عمومی و خصوصی جهت تولید محتوای مناسب سایبری فعالیت می‌کنند (عاملی و حسنی، ۱۳۹۱: ۱۸).

تولید محتوا در رسانه‌های جمعی به طور معمول نیاز به مهارت‌ها و آموزش تخصصی دارد. در مقابل، اغلب تولیدات رسانه‌های اجتماعی مجازی، به مهارت‌ها و آموزش تخصصی نیاز ندارد. هر کسی با دسترسی به اینترنت می‌تواند وسایل تولید رسانه‌های مجازی را به کار بیندازد (کرامتی معز و میرخلیلی، ۱۳۹۹: ۲۴-۲۵)، اقداماتی که لازم است انجام شده در زمینه صیانت و سالم‌سازی محتوا انجام شود عبارت از: تأمین بستر حقوقی حمایت از تولید و عرضه محتوا و خدمات داخلی. ایجاد زیرساخت جمع‌آوری، ذخیره و تحلیل داده‌های عظیم شبکه‌ای، پیاده‌سازی سامانه احراز هویت کاربران خدمات ارتباطی کشور (کرامتی معز، ۱۳۹۹: ۱۷۲).

در ایران نیز، در دهمین جلسه شورای عالی فضای مجازی، در تاریخ ۱۱ آذرماه ۱۳۹۱ بر اساس ماده ۹ اساسنامه مرکز ملی فضای مجازی، سیاست گذاری در خصوص تشویق و ترغیب مستمر بخش های خصوصی و مردمی برای فعال شدن در عرصه تولید محتوای مطلوب فضای مجازی و گسترش بازار کسب و کار و اشتغال زایی در این عرصه در چارچوب مصوبات شورای عالی و نیز سیاست گذاری جهت حمایت حداکثری از مؤسسات، تشکل ها و نیروهای مردمی و متعهد و انقلابی در عرصه تولید محتوا در چارچوب مصوبات شورای عالی، بعنوان وظایف این کمیسیون شناخته شده است. همچنین شورای عالی فضای مجازی، مشارکت با بخش خصوصی را در جلسه بیست و ششم مورخ ۱۳۹۴/۹/۲۵، به صورت یک امر مستقل و به عنوان یک سیاست تلقی کرده است. گرچه به نظر می‌رسد محور این سیاست گذاری، بیش‌تر اقتصادی است تا فرهنگی، اما به هر وصف، به رسمیت شناختن ورود بخش خصوصی به سیاست‌های مرتبط با فضای سایبری را می‌توان به فال نیک گرفت (علیزاده طباطبایی، ۱۳۹۵: ۲۶۸).

۱-۲. مشارکت در آموزش و ارتقاء سواد سایبری

امروزه سواد تنها به معنای خواندن و نوشتن و توانایی درک مطلب نیست. در دنیای امروز لزوماً این مسئله را نمی‌توانیم سواد بدانیم و موضوع خیلی پیچیده‌تر از این‌ها است. امروزه یادگیری دانش الکترونیک و فناوری‌های جدید هم می‌توانند در این تعریف جای بگیرند. زمانی که اجتماع رو به سمت پیچیدگی

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

می‌رود، افراد باید بافرهنگ‌تر و باسوادتر شوند. کسی هم که در چنین شرایطی نتواند سیستم موجود را تحلیل کند کارش به سمت تنش و آسیب می‌رود[1].

همگام با رشد گسترده فناوری اطلاعات، تجارت و انواع خدماتی که از طریق آنلاین در دسترس هستند، از طریق رسانه دیجیتال به بخش جدایی ناپذیر و پیش شرط مشارکت موثر در زندگی فرهنگی، اقتصادی و اجتماعی تبدیل شده اند. از سوی دیگر نمی‌توان از تهدیدهایی که این تکنولوژی برای سلامت و امنیت افراد ایجاد می‌نماید غافل ماند.

اهمیت خانواده و توجه به نقش کلیدی آن در پیشرفت و توسعه جامعه در دین مبین اسلام و نیز فرهنگ اصیل ایرانی همواره مورد توجه و تأکید بوده است. چیزی که پیشرف‌های فناورانه، جهان غرب را با توهم بی‌نیازی از آن مواجه ساخت و سبب شد با وجود رشد گسترده و شتابان علم و نوآوری و حتی ابرقدرت شدن در سطح جهانی، همواره با مشکلات و اختلالات روحی از جمله افسردگی، خشونت و بزهکاری افراد جامعه خود دست و پنجه نرم کند و نتواند جامعه‌ای بالنده به لحاظ معنوی داشته باشند (کرامتی معز، ۱۳۹۹: ۱۶۰).

چنانچه بتوان در ابتدا توصیه ها و آموزش های لازم را به والدین منتقل و آنها را با خطرها و در عین حال مزایا و مطلوبیت های فضای اینترنتی آشنا کرد، می توان امیدوار بود تا حدود زیادی اهداف این تدابیر به ثمر بنشیند. متاسفانه این نوع پیشگیری نیز در کشورمان آن طور که باید، مورد توجه قرار نمی گیرد، هر چند که امروزه در مدارس و بعضا محیط خانواده تلاش هایی در جهت آموزش افراد در این مورد انجام شده است، اما متاسفانه برنامه ای هدفمند و یکپارچه در این مورد وجود ندارد، تا بتوان با توجه به آن آموزش افراد را پیگیری کرد (عطارزاده و انصاری، ۱۴۰۰: ۱۷۰).

در همین راستا لازم است به کودک بیاموزیم چه اطلاعاتی در دایره اطلاعات شخصی قرار دارد و از طرف دیگر در صورت انتشار آنلاین آنها، این اطلاعات دیگر قابل حذف کردن نیستند. لازم است به کودکان در مورد تبعات انتشار عکس و یا ویدئو تصویر و با بیان احساسات به افراد غریبه آگاهی‌های لازم داده شود. به عنوان نمونه، یک برنامه آموزشی برای والدینی که فرزندانشان با فضای سایبر سرو کار دارند، می تواند حاوی نکاتی نظیر آموزش کاربری مسئولانه و ایجاد توانایی انتخاب گزینه های مناسب به هنگام حضور در فضای سایبر و به عبارت بهتر نحوه حضور صحیح و مفید در این فضا، نحوه اتخاذ تصمیمات مناسب درباره محتوایی که می خواهند مشاهده کننده و آموزش نحوه مواجهه با محتوای نامناسبی که

۱. برای اطلاعات بیشتر در زمینه سواد مجازی و موضوعات حقوقی آن ر.ک به (یزدان‌پناه و بیات کمیتکی، ۱۳۹۹: ۹۲۱-۹۳۷).

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

ممکن است مشاهده گردد و کاهش اثرپذیری از آن و عواقب آن، باشد. البته روشن است که ابتدا باید به خود والدین آموزش داد تا بدانند چگونه این راهکارها را نسبت به فرزندان خود اتخاذ نمایند. این مهم از طریق ایجاد کمپین های آموزشی از سوی نهادهای عمومی دولتی یا غیردولتی نظیر شهرداری ها با نهادهای خصوصی از جمله کنشگران فضای سایبر نظیر ارائه دهندگان خدمات شبکه ای، اپراتورهای موبایل و یا سازمانهای مردم نهاد، قابل تحقق است.

۱-۳. استفاده از ظرفیت‌های مشارکت مردمی در اجرای سیاست‌های پیشگیرانه

پیشگیری مشارکتی از جرم یکی از شاخه‌های اصلی سیاست جنایی مشارکتی است. این رویکرد یکی از بخش های اصلی سیاست گذاری کشورها در زمینه پیشگیری از جرم است. رویکرد مذکور در دهه ۸۰ میلادی در انگلستان در قالب اجرای طرح ها و پروژه های مدیریتی آغاز شد (جزینی و جهانتاب، ۱۳۹۶: ۱۹۳).

در این رویکرد، پیشگیری از جرم به یک وظیفه همگانی تبدیل می‌شود. رویکرد مشارکتی با یکی کردن و متمرکز کردن افراد و سازمان‌ها، آنها را به ایجاد روابطی داوطلبانه، سودمند (به طور متقابل) و نوآورانه تشویق می‌کند (رجبی تاج امیر، ۱۳۹۸: ۶۶).

این رویکرد با سایر رویکردها در هدف مشترک است و بر این اصل تکیه دارد که نهادهای عوامل و سازمان-هایی که بر تأثیرگذاری بر عوامل جرم زا توانایی، مسئولیت یا صلاحیت دارند باید با آرمانی مشترک با یکدیگر متحد شوند؛ به گونه ای که با اهداف و اقدامات متضاد، کارهای یکدیگر را خنثی نکنند و مانند آنها در پی کاهش جرم و افزایش ایمنی ساکنان جوامع باشند.

رویکرد مشارکتی بر توسعه راهبردهای اجتماعی، که خود مبتنی بر نیازهای محلی است، متمرکز است و به دنبال درگیر کردن شهروندان و سازمان‌های مردم نهاد در برنامه های پیشگیری است. در نهایت، این پیشگیری در پی این ایده ظهور کرده است که پیشگیری از جرم بدون کمک و مشارکت مردم نمی تواند نتیجه مطلوبی داشته باشد؛ زیرا جرم معضلی اجتماعی است و کنترل آن وظیفه هر شهروند در کنار دولت است (قورچی بیگی، ۱۳۸۸: ۳۵۳)، پس هر چه مشارکت مردم، جامعه محلی و سازمان‌های مردم نهاد در امر به بیشتر و ملموس‌تر باشد، در مقابل میزان پایداری و موفقیت برنامه های پیشگیری افزایش خواهد یافت.

انجمن ها یا سازمان‌های مردم نهاد سهم عمده ای در اداره جامعه و تدوین برنامه اقدام در دنیای نوین برعهده دارند. دولت ها دیگر نمی‌توانند آن‌ها را نادیده بگیرند؛ بلکه باید در جریان مدرنیته از توانایی

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

آنها برای پیشرفت و پرکردن کاستی های قدرت خود بهره ببرند. آنان تا اندازهای قدرت پیدا کرده‌اند که می‌توانند به عنوان همکار دولت در پروژه های پیشگیری از جرم شرکت کنند و یا اینکه خود عهده دار تدوین پروژه باشند و دولت از دستاوردهای آنان استفاده کنند. آن‌ها حتی می‌توانند به حمایت از بزه دیدگان برخاسته و در دادگاهها نیز حضور داشته باشند. به موازات این پیشرفت، حوزه پیشگیری از جرائم سایبری نیز به شدت مورد توجه انجمن های مردم نهاد متعددی در بسیاری از کشورهای دنیا بوده است. این سازمان ها در دولت های مختلف اقدامات متعددی را در حوزه نرم افزارهای نظارتی و افزایش سواد سایبری انجام داده‌اند. در ایران هم حدود چند سال است که انجمن سواد رسانه ای ایران تشکیل شد که در همایش و چندین کتاب و دو پودمان (مهارت های سواد رسانه ای و تربیت مربی سواد رسانه ای 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 (شاملو و کاظمی جویباری، ۱۳۹۸: ۲۷-۲۸).

۱-۴. نقش آفرینی رسانه‌ها

یکی از کارکردهای اجتماع تحکیم عقاید و ارزشهای مشترک میان اعضاء خود است و همین کارکرد در کنترل اجتماعی به عنوان یک تئوری مبنایی برای پیشگیری اجتماعی به کار می‌آید. از این رو برنامه های پیشگیرانه ای که با محوریت رسانه ها طرح ریزی می شوند، در عداد سازوکار پیشگیری اجتماعی قلمداد می گردند. زیرا رسانه های گروهی در ایجاد یک جریان غالب از این ارزش‌ها و دیدگاه‌های مشترک نقش بسزایی دارند.

رسانه ها از یک سو با آموزش روش‌های مقابله با جرایم و تنویر افکار عمومی، نقش پیشگیرانه را ایفا می نمایند و با اطلاع رسانی به افزایش مکانیزمهای نظارتی و کنترل یاری می رسانند، و از سوی دیگر تکلیف خود را در آموزش جامعه نیز فراموش نمی کنند. بدین معنا که رسانه ها باید بتوانند واکنش جامعه در مقابل این افراد و پدیده را به سمت جنبه های انسانی تر و علمی تر پیش برده و محیط اجتماع را برای زیست جمعی مساعدتر نمایند. این به معنای روشن نمودن اذهان و ادراک مخاطبان از محیط اجتماعی، بواسطه تعلیم رفتارهای مطلوب اجتماعی و ارزش های اخلاقی است که سبب تقویت سرمایه اجتماعی و بالا رفتن اعتماد عمومی و ایجاد نظامی سالم خواهد گردید. رسانه های جمعی دارای قدرت درشعاع وسیعی میان توده های مردم می‌باشند. پس می توان آنها را مانند نهادهای اجتماعی مورد شناسایی قرار داد.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

۲. تدابیر وضعی مشارکتی

با همه‌ی محاسن و معایبی که در خصوص پیشگیری وضعی مطرح می‌شود؛ امروزه خیلی از کشورهای توسعه یافته و جوامع مردم سالار نیز با طرح دلایل مختلف به سمت اولویت بخشی به این گونه از پیشگیری و یا استفاده‌ی تلفیقی هم زمان با سایر شیوه ها دلالت شده‌اند (دارابی، ۱۳۹۷: ۱۳۱-۱۳۲)؛ بنابراین پیشگیری وضعی بر خلاف پیشگیری اجتماعی مبتنی بر تقویت ارزش‌های جامعه، متعالی کردن نهادهای آن، بررسی ریشه های بزهکاری و قطع آن نیست بلکه به طور ساده بر کاهش فرصت ها و موقعیت های ارتکاب جرم تکیه دارد. در واقع به جای پرداختن به انگیزه و نیات درونی افراد که تغییر آنها دشوار می باشد سعی دارد راه های دست یابی مرتکب به موضوع جرم یا بزه دیده و افزایش زحمت و خطر برای مرتکب بپردازد تا از این رهگذر راهکاری عملی برای پیشگیری از وقوع جرم ارائه نماید.

۲-۱. تدابیر نظارتی مشارکتی

نظارت و مقابله پیشگیرانه با بزهکاری را می‌توان مهم‌ترین و موثرترین جنبه مشارکت جامعه مدنی در امر پیشگیری از جرم دانست. تکیه بر نظارت دولتی رسیدن به اهداف بر شمرده شده را به تنهایی محقق نمی‌سازد و بنابراین برای پیشگیری از ارتکاب جرم و یا انحرافان و تا به هنجاری های رو تکیه بر نظارت مردمی و عمومی و اجتناب ناپذیر است. البته به قول ریموندگسن، جرم شناس فرانسوی اگرچه نظارت عامه مردم مطلوب و مهم است اما نباید از حدی تجاوز کند و به عبارتی بایستی حدود و ثغور آن در هر سیاست جنایی کاملا مشخص باشد (گسن، ۱۳۹۷: ۸۱).

در فضای سنتی، نمونه هایی همچون نظارت بر محله و همسایگی و مشارکت و همکاری با پلیس محلی در پیشگیری محلی و تقویت آماج ها و استفاده از پلیس خصوصی و گروه‌های مراقبت از شهروندان، جلوه هایی از مشارکت نهادها و عوامل غیر دولتی در امر نظارت هستند (رستمی، ۱۳۸۴: ۱۴۰).

نکته قابل توجه در امر نظارت مشارکتی این است که برای تحقق این شکل از نظارت از هر روش و یا راهکاری که استفاده شود، خانواده در مرکز توجه قرار می گیرد. بنابراین اولین محیطی که توجه متولیان و مجریان تدابیر پیشگیرانه اجتماعی را به خود جلب می کند، خانواده و به تبع آن والدین است. از مصادیق نظارت مشارکتی در فضای سایبر استفاده از پتانسیل فراهم کنندگان خدمات در حوزه ارتباطات آنلاین است که بیشترین نقش را این زمینه ایفا می کنند. استفاده از پتانسیل این فراهم کنندگان خدمات در واقع مشارکت دادن بخش خصوصی در امر حاکمیتی نظارت است. این مشارکت با بخش خصوصی در ایران نیز به خوبی اجرا شده است.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

۲-۱-۱. نظارت توسط والدین

جهت نظارت بر فعالیت‌های فرزندان در فضای سایبر لازم نیست والدین با فرزندان خود برای اجتناب از مخاطرات فضای آنلاین مشاجره و یا درگیری داشته باشند و یا در بازگو کردن مخاطرات این فضا به شکلی اغراق آمیز با فرزندان برخورد کنند. بلکه لازم است والدین بدانند چگونه فرزند آن‌ها اطلاعات را در فضای مجازی انتشار می دهند و چگونه افراد غریبه می‌توانند به راحتی به اطلاعات آن‌ها دسترسی داشته باشند (اتحادیه بین المللی مخابرات[1]، ۲۰۱۶: ۲۲).

والدین، محافظان و آموزگاران باید از ماهیت دقیق سایت‌های مختلف و درک مخاطرات این فضا توسط کودکان مطلع باشند. همچنین والدین بایستی کامپیوتر را در محیطی عمومی در منزل قرار دهند و هنگامی که کودکان در حال استفاده از آن هستند حضور داشته باشند[2]. در صورت عدم امکان حضور در آن محیط، روش‌های دیگری را برای مراقبت نزدیک بر کودک خود نظیر استفاده از ابزارهای فنی نظارتی پیدا کنند. در خانواده های بزرگتر که ممکن است چندین سیستم در آن وجود داشته باشد، بهتر است تمام آنها در یک محیط قرار داشته باشد. به علاوه لازم است والدین در مورد سایت هایی که کودک از آنها بازدید می‌کند و دانستن در مورد اینکه چگونه زمان خود را در آنجا سپری می کند، آگاهی داشته باشند (علیزاده طباطبایی، ۱۳۹۵: ۲۸۷).

۲-۱-۲. نظارت توسط ارائه کنندگان خدمات دسترسی و میزبانی

در ایران نیز یکی از مصادیق نظارت را می‌توان در ماده ۷۴۹ قانون مجازات اسلامی بخش تعزیرات (ماده ۲۱ قانون جرایم رایانه‌ای ۱۳۸۸) یافت که مطابق آن، ارائه کنندگان خدمات دسترسی و میزبانی امکان نظارت بر داده‌های افراد را دارند و بر این اساس برای آن‌ها مستولیتی جهت پاسخ‌گویی به نهادهای دولتی نیز شناسایی شده است. به طور کلی می‌توان گفت که این مواد قانونی، ارائه دهندگان خدمات به ویژه رساها را تبدیل به عامل نظارتی غیرمستقیم دولت‌ها کرده است.

در حوزه جرائم سایبری چند نهاد به موجب قانون مشمول برخی تکالیف پیشگیرانه در راستای فیلترینگ[3] هستند، به طوری که می‌توان آن‌ها را در شمار مدیران مکان‌ها دانست. نخست، بر اساس ماده

1. Interational Telecommunication Union (ITU).

۲. نرم افزارهای زیادی تحت عنوان «نرم افزار کنترل والدین» ایجاد شده اند و حتی در برخی سایت ها نیز تدابیر نظارتی برای والدین فراهم شده است. به عنوان مثال می¬توان به نرم افزار EyeGuardian که یک نرم افزار کاربردی مبتنی بر رایانش ابری برای Facebook می¬باشد، اشاره نمود.

۳. فیلتر اینترنتی یا فیلترینگ، عبارت است از اعمال ممیزی و محدود کردن و نظارت ساختاریافته و هدفدار بر دسترسی به محتوای وبگاه‌ها و استفاده از خدمات اینترنتی که از دیدگاه متولیان فرهنگی و سیاسی هر کشور برای مصرف عموم مناسب نیست، اعمال فیلتر معمولاً به وسیله ارائه‌دهندگان خدمات اینترنتی انجام می‌شود، ولی تعیین سطح، مصادیق و سیاست‌های فیلترینگ با دولت‌ها

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

۷۴۹ قانون مذکور ارائه دهندگان خدمات دسترسی مکلف شده اند تا بر اساس فهرست و ضوابط فنی ارائه شده از سوی کارگروه تعیین مصادیق محتوای مجرمانه، محتوای مجرمانه را پالایش و فیلتر کنند. ارائه دهندگان خدمات دسترسی، سازمان با شرکتی است که به عنوان واسطه میان کاربر و اینترنت عمل کرده و امکان اتصال به اینترنت را برای آنان فراهم می کند. آیین نامه نحوه ارائه خدمات اطلاع رسانی و اینترنت، این اشخاص را به عنوان شرکت ها و یا موسسات و مراکز ارائه کننده خدمات اطلاع رسانی و اینترنت تعریف کرده و حدود فعالیت ها و وظایف آنها بر شمرده است. آیین نامه جمع آوری و استناد پذیری ادله الکترونیکی مصوب ۱۳۹۳ نیز در بند الف ماده ۱ ارائه دهندگان خدمات دسترسی را اشخاصی دانسته که امکان ارتباط کاربران را با شبکه های رایانه ای یا مخابراتی و ارتباطی داخلی یا بین المللی یا هر شبکه مستقل دیگر فراهم می آورند از قبیل تأمین کنندگان، توزیع کنندگان، عرضه کنندگان خدمات دسترسی به شبکه های رایانه ای یا مخابراتی.

همچنین مطابق ماده ۶۶۷ قانون آیین دادرسی کیفری، ارائه دهندگان خدمات دسترسی موظفند داده های ترافیک را حداقل تا شش ماه پس از ایجاد حفظ نمایند و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند و بر اساس ماده ۶۶۸ قانون آیین دادرسی کیفری ارائه دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجادشده را حداقل تا پانزده روز نگهداری کنند همچنین در خصوص اپراتورهای تلفن همراه نیز پیش بینی مواردی جهت نظارت این ارائه دهندگان خدمات بر محتوای سایبری پیش بینی شده است.

به عنوان مثال در پیش نویس نقشه مهندسی فرهنگی شرکت خدمات ارتباطی رایتل، اپراتور رایتل به عنوان یکی از فراهم کننده خدمات در ایران بر اساس ضوابط مقرر توسط شورای عالی انقلاب فرهنگی خط مشی خود را در زمینه نحوه ارائه خدمات به مشترکین تنظیم کرده است. بخشی از خط مشی این فراهم کننده خدمات صراحتاً یک همکاری مشارکتی در تنظیم مقررات در زمینه کنترل و نظارت بر محتوا است. از جمله این خط مشی‌ها می توان به تدوین ساز و کار نظارتی بر محتوا، تبلیغات و خدمات است اشاره نمود. این فراهم کننده خدمات هیات متخصصی را برای تیین محتوا و پایش آن تشکیل داده است که از جمله وظایف این هیات تدوین سازوکار نظارتی بر محتوا، تبلیغات و خدمات تعیین ضوابط فرهنگی

است. به طور کلی دو راهبرد برای فیلتر کردن محتواهای غیرمجاز وجود دارد. راهبرد اول مبتنی بر لیستهای سیاه و سفید سایت‌ها است و راهبرد دوم بر مبنای برچسبهای محتوایی از طریق تعریف کردن کلیدواژه‌های خاص که برای فیلتر کردن سایتها صورت می‌گیرد که روش دوم به دلیل ضریب خطایی که در دسترسی به سایت‌های سالم ایجاد میکند، انتقادات زیادی را برانگیخته است (سعد، ۱۳۹٤: ۹۸).

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

انتخاب و همکاری با شرکت های همکار در موضوعات محتوا، خدمات و تبلیغات، پایش فرهنگی محتوای چند رسانه ای، پایش فرهنگی خدمات ارزش افزوده، پایش فرهنگی تبلیغات تلویزیونی، چاپ، مطبوعات و...)، پایش فرهنگی فروشگاه های عرضه خدمات رایتل، پایش اخبار مرتبط با تبلیغات، خدمات و محتوا، رصد اخبار مرتبط با تبلیغات، خدمات و محتوا می‌باشد.

۲-۱-۳. ایجاد فضای سبز سایبری یا محیط‌های حفاظت شده در فضای سایبر

پیشرفت فناوری اطلاعات و ارتباطات و ایجاد امکانات مختلف و جذاب برای تمامی افراد و گروه های سنی از جمله کودکان و نوجوانان در فضای سایبر، موجب شده که حضور کودکان و نوجوانان در این فضا، تا حدودی گریزناپذیر باشد. در حقیقت کودکانی که در دهه ۹۰ متولد شده اند، کسانی هستند که همیشه به تکنولوژی شبکه دسترسی داشته اند و لذا محروم کردن این بومی های دیجیتال از استفاده از امکانات فضای سایبر، غیر ممکن است و از سوی دیگر این امکانات آزادی همراه با خطر را به آنها اعطا کرده است. کودکان ممکن است در این فضا در معرض محتوای نامناسب، محتوای خشونت آمیز و یا ارتباطات نامطلوب قرار گیرند. به همین دلیل است که باید یک رویکرد جامع برای اطمینان از اینکه آن‌ها بصورت سالم و ایمن از آزادی که در این فضا به آنها داده شده استفاده می کنند، در پیش گرفته و از راهکارها و امکانات مختلف و با مشارکت کنشگران مختلف، در این خصوص بهره برداری شود.

یکی از راهکارهایی که در راستای صیانت از کودکان در فضای سایبر وجود دارد، ایجاد فضاهای سبز[1] یا فضاهای حفاظت شده[2] است (کاترین. مونتگومری[3]، ۲۰۰۰: ۱۴۵). این امکان عبارت است از ایجاد داوطلبانه فهرست هایی از موارد مناسب برای کودکان و فراهم کردن محیط و بستری که به کودکان اجازه دهد از طریق مرورگر یا خدمات برخط یا پالایشگر های روی سرور فقط به این محیط دسترسی داشته و محتوای ارائه شده در فهرست مزبور را دریافت نمایند (گزارش کمیسیون حفاظت از کودکان برخط (آنلاین) به کنگره ایالات متحده آمریکا، ۱۳۹۶: ۵۳).

در این روش زیر ساخت و بستر موجود، مستقل از اینترنت بوده و به نوعی شبکه ای مستقل برای استفاده اختصاصی کودک و نوجوان با امکانات متعدد ایجاد شده و از طریق ارائه کننده خدمات، در صورت درخواست کاربر، در اختیار وی قرار داده می‌شود. البته جهت کارآمدی و اثربخشی این تدبیر، لازم است برای رده های سنی مختلف، فضاهای اختصاصی و امکانات متفاوتی در نظر گرفته شود. به عنوان مثال می-

1. Greenspaces.
2. Walled Garden.
3. Kathryn C. Montgomery.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

توان در فضای اختصاصی رده سنی زیر ۱۰ سال، صرفا امکانات وب ۱ را در اختیار کودک قرار داد، اما برای رده سنی ۱۰ سال به بالا، امکان دسترسی به امکانات وب ۲ در این شبکه اختصاصی نیز وجود داشته باشد.

علاوه براین باید محتوای مناسب هر رده سنی در فضای حفاظت شده مربوطه باشد. در حقیقت این فضای سبز یا محیط حفاظت شده، می‌تواند جایگزین مناسبی برای کودکان، جهت استفاده از امکانات اینترنت و آماده شدن جهت ورود مرحله به مرحله به دنیای پرخطر و بیکران اینترنت باشد. لذا ارائه کننده خدمات می‌تواند این امکان را فراهم نماید که با درخواست و تایید والدین، رمز عبوری[1] جهت پرش از این محوطه حفاظت شده و دسترسی به محیط اینترنت، به مرور و پس از رسیدن به سن خاصی امکان پذیر گردد. البته بهتر است که این دسترسی نیز با رعایت ترتیب و شرایط خاصی ایجاد شود (علیزاده طباطبایی، ۱۳۹۵: ۲۸۷).

۲-۱-۴. شورای عالی فضای مجازی

اولین نهاد تأسیس شده در رابطه با فضای مجازی، شورای عالی فضای مجازی است که در ۱۷ اسفند ماه ۱۳۹۰ به وجود آمد. این شورا فرا قوه‌ای است و این بدان معنا است که وابسته به هیچ نهاد یا قوه‌ای نیست. شورای عالی فضای مجازی به مانند شورای عالی انقلاب فرهنگی، در قانون اساسی نیامده است و هر دو با حکم رهبر زمان خود تأسیس شده است. شورای عالی انقلاب فرهنگی با حکم امام خمینی «ره» و شورای عالی فضای مجازی با حکم مقام معظم رهبری «دامه برکاته» شروع به فعالیت نموده است (منصورآبادی، میرخلیلی و کرامتی معز، ۱۴۰۰: ۲۷).

مقام معظم رهبری وظایفی را در تشکیل شورای عالی فضای مجازی به این شورا محول کرد که عبارت‌اند از:

اشراف کامل و به‌روز نسبت به فضای مجازی در سطح داخلی و جهانی؛

تصمیم‌گیری نسبت به نحوه مواجهه فعال و خردمندانه کشور از جهت سخت‌افزاری، نرم‌افزاری و محتوایی در چارچوب مصوبات شورای عالی فضای مجازی؛

نظارت بر اجرای دقیق تصمیمات در همه سطوح؛

با توجه به لزوم عهده‌داری نقش سیاست‌گذاری و نظارت عالی بر پروژه‌های مرتبط با فضای مجازی

---

۱. برای داشتن رمز عبور مناسب و مطمئن باید ترکیبی از روش‌های مختلف را به کار گرفت. برای ساختن رمز عبور مناسب، شیوه های متفاوتی وجود دارد. با جست وجویی ساده در اینترنت، می توانید با بیشتر این روش ها آشنا شوید. اما به طور کلی، کارشناسان مسائل امنیتی همواره تأکید می کنند که رمز عبور مناسب باید ترکیبی از حرف کوچک، وی، اعداد و علائم باشد. البته شما می توانید روش خاص خود را هم داشته باشید، اما به یاد داشته باشید که اگر برای تعیین رمز عبور روشی خاص خود دارید آن را به هیچ کدام از دوستان و اطرافیان خود آموزش ندهید (سهلانی، ۱۳۹۷: ۱۹۷).

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

کشور توسط یک نهاد در کشور، در این حکم از شورای عالی فضای مجازی به عنوان نقطه کانونی متمرکز برای سیاست‌گذاری، تصمیم گیری و هماهنگی در فضای مجازی کشور یاد می‌شود(منصورآبادی، میرخلیلی و کرامتی معز، ۱۴۰۰: ۲۷).

از آن‌جایی‌که شورای عالی فضای مجازی در امر تولید محتوا و نظارت بر آن در فضای مجازی ایفای نقش می‌کند، به نوعی می‌تواند در امر پیشگیری از بزه‌دیدگی کودکان در شبکه‌های مجازی نیز تاثیرگذار باشد. «شبکه‌هایی نظیر فیس‌بوک و توییتر ابزاری برای انتشار محتوا هستند که در صورت فقدان نظارت می‌توانند خسارات جبران‌ناپذیری در حوزه فردی و عمومی به بار بیاورند، اما شورای عالی فضای مجازی از طریق اعمال نظارت دقیق بر این فضا و از بین بردن زمینه‌های ارتکاب جرم در شبکه‌های اجتماعی فیس‌بوک و توییتر می‌تواند از بزه‌دیدگی پیشگیری کند (عمرانی، ۱۳۹۴: ۸۲)، تا قبل از تشکیل شورای عالی فضای مجازی سازوکار مشخصی برای نظارت بر این گونه شبکه‌ها وجود نداشت، ایجاد شورا می‌تواند خلأ موجود در این حوزه را به‌خوبی پوشش دهد.

۲-۱-۵. وجوب تعامل مردم با پلیس فتا

امروزه اساس کار پلیس فتا جامعه محوری است و تلاش برای رضایت و جلب مردم برای مشارکت با پلیس فتا، در اولویت های اصلی ناجا قرار گرفته است. یکی از مهم ترین ماموریت های پلیس برقراری نظم و امنیت در جامعه است و این امر میسر نمی‌شود مگر با مشارکت مردم و مردمی بودن فعالیت‌های پلیس فتا. ایجاد حس آرامش و امنیت همان اندازه که در فضای حقیقی مهم است در فضای سایبری نیز حائز اهمیت است. به دست آمدن امنیت و آرامش در فضای سایبر محقق نمی شود جز با تعامل پلیس فتا و مردم.

در یکی از اقدامات اخیر پلیس فتا طرح راه‌اندازی «فیلترینگ هوشمند»[1] است، تفاوت فیلترینگ جدید با فیلترینگ قبلی روی آدرس URL ، در این است که روش فعلی فیلترینگ جزء روش‌های مقدماتی و ابتدایی است و هر چقدر مکانیزم نرم‌افزار فیلترینگ از نظر فنی پیشرفته‌تر شود، احتمال خطا و اشتباه در تصمیم‌گیری کمتر خواهد شد. بر اساس این طرح، درصد خطای سامانه فیلترینگ کشور کاهش پیدا می‌کند (میرشفیعی، ۱۳۹۹: ۱۳۱)

هم‌اکنون اگر درون سایتی که دارای چندین صفحه است، یک محتوای مجرمانه وجود داشته باشد، با استفاده از نرم‌افزار فعلی فیلترینگ، ناگزیر کل سایت فیلتر می‌شود، اما اگر این هوشمندسازی اجرایی

۱. قانون گسترش راهکارهای اجرایی عفاف و حجاب مصوب ۱۳۸۴ شورای عالی انقلاب فرهنگی، تنها سند حقوقی است که از «فیلترینگ هوشمند» در آن نام برده شده و تأکید بر تسریع ایجاد آن شده بود.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

شود، می‌توان تنها بخش مد نظر را فیلتر کرد و دسترسی به مابقی محتوای سایت امکان‌پذیر باشد، و این موضوع باعث کاهش قابل توجه حجم فیلتر خواهد شد (منصورآبادی، میرخلیلی و کرامتی معز، ۱۴۰۰: ۴۴).

رابطه پلیس با مردم رابطه اقتصادی نیست که برای کسب درآمد یا به دست آوردن مشتری و بازار پر سود باشد بلکه ناجا ملزم به دفاع از حقوق اجتماعی و امنیتی ملت است و در فضای سایبری نیز مانند فضای حقیقی پلیس وظیفه دارد با نیاز مندی ها و مشکلات مردم در این فضا آشنا باشد و امنیت سایبری مردم جامعه را فراهم کند.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

نتیجه گیری

با وجود تمام مزیت هایی که دنیای سایبر برای بشر داشته است، انقلاب فناوری اطلاعات و ارتباطات به واسطه ویژگی‌های بی‌همتایی که دارد (برای مثال، ناشناختگی و عدم رویارویی چهره به چهره بزه کار با بزه دیده ، دشواری کشف بزه و شناسایی بزه کار، کثرت بزه دیدگان به واسطه فرامکانی و فرا مانی بودن بستر ارتکاب جرم)، بیش از هر فناوری دیگری، نیمه تاریک پررنگ تری دارد، زیرا طبق یک قانون نانوشته، «هرچه دستاوردها و پیشرفت های بشر ساخته والاتر باشند، بهره برداری سوء از آن نیز فزون‌تر است» و می-توان گفت که پیش از این، هیچ پیشرفتی عمیق‌تر از فناوری‌های اطلاعاتی و ارتباطی زندگی بشر را تحت تأثیر قرار نداده است. با توجه به وابستگی روزافزون بشریت به فضای سایبر، بزه دیدگی ما نیز روند تصاعدی خواهد داشت.

علی‌رغم سرمایه گذاری مادی و معنوی حاکمیت در امر پالایش، عملاً به واسطه مشکلات زیادی که در استفاده از آن وجود دارد، بسیاری از افراد برای دسترسی به حقوقی مشروع خود، با نرم افزارهای پولی و رایگان به راحتی مبادرت به دور زدن پالایش می‌نمایند. لذا به نظر می‌رسد که ظرفیت ها و رویکردها و تدابیر متعدد قابل اتخاذ جهت نیل به اهداف نظام سالم سازی فضای سایبر از محتوای مجرمانه مورد غفلت قرار گرفته و لازم است با احصای ویژگی‌های فضای سایبر به عنوان یک رسانه و نیز یک دنیای جدید که به نوعی می‌توان گفت افراد در آن زندگی می‌کنند، الزامات سالم سازی فضای سایبر و انواع تدابیر قابل اتخاذ در این خصوص که هماهنگ با اقتضائات این فضا و نیز موثر در جهت نیل به اهداف نظام سالم سازی باشند با کمک جوامع مدنی و سازمان‌های مردم نهاد احصا گردد.

. به نظر می‌رسد در راستای پیش گیری کنشی از جرایم سایبری، هیچ ابزاری به اندازه «آموزش» نمی‌تواند مؤثر واقع شود؛ آموزشی که هم زمان با آغاز شکل گیری شخصیت یعنی از دوران کودکی - نه پس از آن که تغییر شخصیت دشوار می‌شود - تا دوران نوجوانی و جوانی ادامه یابد. هر چه این آموزش کندتر یا با وقفه همراه باشد، رشد اخلاق سایبری و نیز درونی سازی هنجارهای اجتماعی را با دشواری مواجه می‌کند.

[Downloaded from priw.ir on 2026-02-03]

[DOR: 20.1001.1.23222980.1400.11.4.7.1]

فهرست منابع

خازنی، محمد حسن(۱۳۹۴). قدرت در جامعه شبکه ای؛ کند و کاوی در کتاب قدرت ارتباطات، فصلنامه نقد کتاب علوم اجتماعی، شماره‌های ۵ - ۶ .

حاجی ده آبادی، محمدعلی و سلیمی، احسان(۱۳۹۳). اصول جرم انگاری در فضای سایبر(با رویکردی انتقادی به قانون جرائم رایانه ای)، فصلنامه مجلس و راهبرد، دوره ۲۱، شماره ۸۰.

جزینی، علیرضا و جهانتاب، محمد(۱۳۹۶). پیشگیری مشارکتی از جرم، تهران: انتشارات دانشگاه علوم انتظامی امین، چاپ اول.

سهلانی، حسین(۱۳۹۷). آشنایی با تهدیدات فضای سایبر، تهران: انتشارات دانشگاه علوم انتظامی امین، چاپ اول.

شاملو، باقر و کاظمی جویباری، مهدی(۱۳۹۸). موانع اثربخشی راهبردهای پیشگیرانه از جرائم علیه امنیت اخلاقی در فضای مجازی، فصلنامه رهیافت پیشگیری؛ دوره دوم، شماره اول.

دارابی، شهرداد(۱۳۹۷). پیشگیری از جرم در مدل مردم سالار سیاست جنایی، تهران، انتشارات میزان، چاپ دوم.

رجبی تاج امیر، ابراهیم(۱۳۹۸). جرم شناسی، تهران: انتشارات دانشگاه علوم انتظامی امین، چاپ اول.

رستمی، ولی(۱۳۸۴). سیاست جنایی مشارکتی در جمهوری اسلامی ایران، رساله دکتری، رشته حقوق کیفری و جرم شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران.

عاملی، سعیدرضا و حسنی، حسین(۱۳۹۱). دوفصایی شدن آسیب ها و ناهنجاری های فضای مجازی: مطالعه تطبیقی سیاست گذاری‌های بین‌المللی، تحقیقات فرهنگی، سال پنجم، بهار ۱۳۹۱، شماره اول.

عطارزاده، سعید و انصاری، جلال(۱۴۰۰). حقوق جزای اختصاصی: جرایم رایانه‌ای، تهران: بنیاد حقوقی میزان، چاپ دوم.

عمرانی، گلسا(۱۳۹۴). بررسی جرم‌شناختی بزه‌دیدگی جنسی در شبکه‌های اجتماعی فیس‌بوک و توییتر، پایان‌نامه کارشناسی ارشد، رشته حقوق کیفری و جرم‌شناسی، دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی.

علیزاده طباطبایی، زهراسادات(۱۳۹۵). سیاست جنایی کارآمد جهت سالم سازی فضای سایبر از محتوای مجرمانه و کاربری آن، رساله دکتری، رشته حقوق کیفری و جرم شناسی، دانشگاه تهران.

فرهمند، مجتبی(۱۳۹۶). جلوه‌های عدالت ترمیمی در حقوق کیفری ایران، تهران: بنیاد حقوقی میزان، چاپ اول.

قورچی بیگی، مجید(۱۳۸۸). پیشگیری چند نهادی از جرم: مفاهیم، مبانی و چالش‌ها، مجموعه مقالات نخستین همایش ملی پیشگیری از جرم، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا.

کرامتی معز، هادی(۱۳۹۹). بزه دیده شناسی کودکان در شبکه‌های مجازی، تهران: انتشارات دادگستر، چاپ اول.

کرامتی معز، هادی و میرخلیلی، سید محمود(۱۳۹۹). پیشگیری رشدمدار از بزه دیدگی کودکان در شبکه‌های اجتماعی مجازی (مطالعه موردی معلمان منطقه پنج شهر تهران)، فصلنامه مطالعات پیشگیری از جرم، دوره پانزدهم، شماره ۵۶.

گسن، ریموند(۱۳۹۷). جرم شناسی نظری، ترجمه مهدی کی نیا، تهران: مجمع علمی و فرهنگی مجد، چاپ هفتم.

گزارش کمیسیون حفاظت از کودکان برخط (آنلاین) به کنگره ایالات متحده آمریکا(۱۳۹۶). حفاظت از کودکان برخط (آنلاین)؛ فناوری‌ها و روش‌ها، مترجم ویراستار علمی: سید آرش وکیلیان، مرکز توسعه فناوری اطلاعات و رسانه های دیجیتال وزارت فرهنگ و ارشاد اسلامی.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]

لازرژ، کریستین(۱۳۹۶). درآمدی به سیاست جنایی، ترجمه دکتر علی حسین نجفی ابرند آبادی، تهران: انتشارات میزان، چاپ ششم.

منصورآبادی، عباس؛ میرخلیلی، سید محمود و کرامتی معز، هادی(۱۴۰۰). پیشگیری از بزه‌دیدگی کودکان در شبکه‌های اجتماعی مجازی با تأکید بر نقش نظارتی شورای عالی فضای مجازی و پلیس فتا، فصلنامه مطالعات پلیس بین‌الملل، دوره دوازدهم، شماره ۴۶.

مهدوی ثابت، محمدعلی و مرادی، قاسم(۱۳۹۶). سیاست جنایی ایران در فضای سایبر، فصلنامه مطالعات علوم اجتماعی، دوره ۳، شماره ۴.

میرشفیعی، نسترن سادات(۱۳۹۹). جرایم سایبری و بزه دیدگی دختران، تهران: انتشارات دادگستر، چاپ اول.

وطنی، امیر و اسدی، حمید(۱۳۹۵). سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم، پژوهشنامه حقوق اسلامی، سال هفدهم، شماره اول.

یزدان‌پناه، زین‌العابدین و بیات کمیتکی، مهناز(۱۳۹۹). نقش سواد رسانه در تحقق گفتمان حقوق شهروندی، فصلنامه مطالعات حقوق عمومی، دوره ۵۰، شماره ۳.

Interational Telecommunication Union (ITU) (2016). Guidelines For Children On Child Online Protection.

Kathryn C. Montgomery (2000), Children's Media Culture In The New Millennium: Mapping The Digital Landscape, The Future Of Children.

به این مقاله این‌گونه ارجاع دهید: DOI: ۱۰.۲۱۸۵۹/priw-۱۱۰۴۰۷

نظری، سید غنی؛ جعفرزاده، سیامک؛ نیک خواه سرنقی، رضا (۱٤۰۰)، «نقش سیاست جنایی مشارکتی در پیشگیری از جرایم سایبری در ایران» فصلنامهٔ پژوهشهای سیاسی جهان اسلام، س۱۱، ش٤، زمستان ۱٤۰۰، صص ۱۷٤-۱۵۱.

[Downloaded from priw.ir on 2026-02-03]
[DOR: 20.1001.1.23222980.1400.11.4.7.1]