



سال یازدهم / تابستان ۱۴۰۱

سیاست جنایی مشارکتی در فضای سایبر؛ از ضرورت و کارایی تا تدابیر اجرایی

• احسان قلعه سلیمی^۱

چکیده

یکی از بزرگ‌ترین چالش‌های دستگاه عدالت کیفری، مقابله با جرائم سایبری است. به سبب ویژگی‌های خاص جرائم سایبری، اکتفا به واکنش کیفری دولتی، در برابر گستره این جرائم کافی و کارآمد نیست؛ برای مقابله‌ی همه‌جانبه و موفق با جرائم سایبری، کاربست یک سیاست جنایی مشارکتی با همکاری گسترده سازمان‌های مردم‌نهاد، کاربران و شهروندان فضای سایبر ضروری است. تحقیق حاضر با روش توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای، ضمن بررسی امکان و ضرورت کاربست سیاست جنایی مشارکتی در فضای سایبر، درصدد شناسایی سازوکارهای اجرایی این راهبرد است. یافته‌های این پژوهش تدابیری همچون «دعوت از افراد شریف برای حضور اثرگذار در فضای مجازی»، «تشکیل گروه‌های گشت زنی خصوصی»، «تقویت هنجارهای برخط»، «تفویض قسمتی از امر تعقیب به سازمان‌های مردم‌نهاد»، «استمداد از بزهکاران پیشین برای کشف جرم»، «استفاده از هیئت‌منصفه در جریان دادرسی»، «ارائه خدمات عام‌المنفعه به‌جای مجازات» و «جبران خسارات ناشی از جرم از طریق بیمه سایبری» را به‌عنوان گزینه‌های یک راهبرد مشارکتی در کنترل و مقابله با جرائم سایبری معرفی می‌کند.

واژه‌های کلیدی: فضای سایبر، سیاست جنایی جامعوی، عدالت کیفری افقی، جرائم برخط، مشارکت شهروندان.

^۱ استادیار گروه حقوق دانشکده علوم انسانی دانشگاه مراغه

مقدمه

فناوری اطلاعات و ارتباطات در حال گسترش و تأثیرگذاری روزافزون بر جنبه‌های مختلف زندگی بشری است؛ امروزه در سایه تحولات گسترده این فناوری، شاهد شکل‌گیری نوع جدیدی از جامعه و شهروند، تحت عنوان جامعه و شهروند مجازی^۱ هستیم. سهولت استفاده از فناوری اطلاعات و ارتباطات، به عمومی شدن آن در میان اقشار مختلف، منجر شده است. در کنار امکانات بی‌شمار این فناوری جنبه‌های منفی آن، همچون هر فناوری بشر ساختی شیوع داشته و از این رهگذر جرائم سایبری به‌عنوان یکی از بزرگ‌ترین و مهم‌ترین چالش‌های حقوق کیفری نوین مطرح شده است.

غیرقابل تخمین بودن رقم سیاه جرائم سایبری (Bar, 2013: 2) و بالا بودن رقم خاکستری در این‌گونه از جرائم (Xingan Li, 2014:116) دلیل مهمی بر ناکارآمدی سیاست جنایی دولتی در قبال این دسته از جرائم است. به‌عنوان نمونه در یک تحقیق در استرالیا مشخص شد بیش از ۴۰ درصد قربانیان جرائم سایبری بنا به جهت مختلف از جمله ناامیدی از فرآیند تعقیب کیفری، تمایلی به گزارش جرم ندارند. (Cyber Security Survey, 2015: 22) به جهت وجود چنین وضعیتی است که باید اذعان نمود، مقابله با بزه سایبری فراتر از ظرفیت نهادهای رسمی عدالت کیفری و مستلزم مشارکت عموم شهروندان یا کاربست «سیاست جنایی مشارکتی»^۲ است. راهبردی که کنش و واکنش به بزه در مراحل مختلف را از گذر همکاری و مداخله شهروندان و سپردن امور به آنان جست‌وجو نماید و از ظرفیت‌های عظیم جامعه برای مقابله با جرم بهره‌برداری نماید. در این راستا دغدغه نوشتار حاضر، شناسایی راهبردها و تدابیر اجرایی سیاست جنایی مشارکتی برای مقابله با جرائم سایبری است؛ به دیگر سخن، پرسش اصلی این پژوهش آن است که چگونه می‌توان از ظرفیت‌های جامعه و شهروندان فضای سایبر برای مقابله با جرائم این فضا بهره‌برداری نمود؟ که برای پاسخ به این پرسش ابتدا امکان‌سنجی سیاست جنایی مشارکتی در دستور کار قرار گرفته است و در ادامه برخی سازوکارهای اعمال این راهبرد در فضای سایبر مطرح شده‌اند. سابق بر این نوشتار، برخی محققان (سعید رضا عاملی، ۱۳۹۷) «الگوی حکمرانی دو فضایی» را موردتحقیق قرار داده‌اند و ضمن شناسایی

۱ اصطلاح شهروندان فضای سایبر (Netizen) در مقابل سیتی‌زن (Citizen) در راستای القای مفهوم «جامعه» برای فضای مجازی، وضع شده است.

2 participatory criminal law

الگوهای حکمرانی فضای مجازی در سطح بین‌الملل مدل خاص حکمرانی در فضای مجازی را برای ایران پیشنهاد داده‌اند. در پژوهش مرتبط دیگری با عنوان «دو فضای شدن نظام حکمرانی و دولت همراه: نظام‌مندشدن و همگرایی رابطه‌ی دولت و مردم» توسط محقق مذکور (سعید رضا عاملی، ۱۳۹۴) موضوع مشارکت مردم در حکمرانی رسانه‌ای مطرح شده است. برخی پژوهشگران نیز (مهدوی ثابت و مرادی، ۱۳۹۶) موضوع دیگری که ارتباط بیشتری با نوشتار حاضر دارد یعنی «سیاست جنایی ایران در جرائم سایبری» را مورد بررسی قرار داده‌اند. همچنین بعضاً پژوهشگران موضوع سیاست جنایی مشارکتی را با رویکردهای مختلف از جمله رویکرد دینی (وحیدی، میرخلیلی ۱۴۰۰) مورد توجه قرار داده‌اند. با این همه پژوهشی یافت نمی‌شود که موضوع سیاست جنایی مشارکتی در خصوص جرائم سایبری را مورد تمرکز قرار داده باشد.

۱. سیاست جنایی مشارکتی در فضای سایبر؛ از امکان‌سنجی تا ضرورت

بسیاری از مشکلاتی که امروزه در مسیر اجرای عدالت خودنمایی می‌کند ناشی از درک تلقینی و تحمیلی از اجرای عدالت است؛ بر اساس فهم رایج گمان می‌رود تنها یک شیوه یا پارادایم برای اجرای عدالت وجود دارد و آن اجرای دولتی عدالت است. در سیاست جنایی دولتی کنشگران به جرم، محدود به نهاد رسمی دستگاه عدالت کیفری هستند و اولویت این سیاست جنایی بر واگذاری امور به ارکان رسمی دستگاه عدالت کیفری است در حالی که سیاست جنایی مشارکتی، خواهان نقش دهی به نهادها و سازمان‌های غیردولتی در مقابله با جرم است. از این روی، سیاست جنایی مشارکتی و سیاست جنایی دولتی در تقابل محض با یکدیگر نیستند؛ بلکه محل اختلاف این دو رویکرد در راهبردها و راهکارهایی است که هر یک برای رسیدن به اهداف پیشنهاد می‌کنند.

۱-۱. امکان‌سنجی سیاست جنایی مشارکتی در فضای سایبر

فضای سایبر تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را به ارمغان آورده است. در محیط سایبر از ساختار قدرت و کنترل تمرکززدایی شده و هیچ نهاد بالادستی نمی‌تواند در این فضا امر حاکمیت و کنترل را در دست گیرد. (Brenner, 2004; 55) در این محیط، اساساً نهادهای بالادستی، وجود ندارند که بر نهادهای پایین دست حاکم و ناظر باشند. این آرمان و ارمغان فضای سایبر به‌صراحت در «اعلامیه استقلال فضای سایبر» بیان شده است:

«ای دولت‌های جهان صنعتی، ای غول‌های کسل‌کننده‌ای که از فلز و شهنایت ساخته شده‌اید، من از اهالی فضای سایبرم... در جایی که ما گرد هم می‌آییم، شما از هیچ حاکمیتی برخوردار نیستید... ما هیچ دولت منتخبی نداریم و امیدواریم هیچ حکومتی در اینجا پدیدار نشود» (بارلو، اعلامیه استقلال فضای سایبر، ۱۹۹۶)^۱

با انتفای رویکرد کنترل‌کننده سلسله مراتبی و هرمی در فضای مجازی، هرچقدر از امکان توسل به رویکرد امنیت‌گرا و سرکوبی دور شده‌ایم به امکان اعمال راهبرد مشارکتی نزدیک‌تر می‌شویم چه آن‌که در جامعه مجازی عموم کاربران قدرت تأثیرگذاری را در سطحی برابر دارا هستند. از این روی مردم و سازمان‌های مردم‌نهاد به‌خوبی می‌توانند در این محیط به ایفای نقش بپردازند؛ بنا بر آنچه گفته شد استمداد از شهروندان فضای مجازی برای کنترل بحران جرم و مقابله با مجرمان مجهز به دانش فناوری اطلاعات از حیث عملی ممکن و قابل اجراست.

۲-۱. ضرورت سیاست جنایی مشارکتی

مسائل فضای ارتباطی جدید در هر سطحی تابعی از فرا متغیرهای^۲ فراوان آن است. فرا متغیر به‌مثابه عاملی است که همه‌چیز را تحت تأثیر قرار می‌دهد و دامنه اثرگذاری آن بر یک پدیده فراتر از حد تصور است. دو فرا متغیر اساسی فضای مجازی یعنی «فرا مکانی بودن و گستره بی‌انتهای» و «زمان‌گریزی» بر همه مسائل فضای سایبر از جمله نحوه نظارت، کنترل و مقابله با جرائم این فضا تأثیرگذار هستند. در کنار این فرا متغیرها عوامل دیگری چون «سهولت ارتکاب جرم» و «مرز شکنی جرم»، «دگر هویت‌پذیری» و «مشکلات کشف جرم»، «شناسایی مجرم»، «گسترده‌گی خسارات» و «کثرت بزه دیدگان»، ضرورت توسل به سیاست جنایی مشارکتی و استمداد از کاربران و شهروندان جامعه مجازی را ایجاب می‌نماید. چه آنکه به‌واسطه وجود این فرا متغیرها و ویژگی‌ها اکتفا نمودن به نهادهای رسمی عدالت کیفری به‌هیچ‌روی نمی‌تواند به کنترل جرم در این محیط منجر شود. حتی کاربست فناوری‌های نوین و روش‌های فنی-تخصصی در پیشگیری از جرائم سایبری نمی‌تواند کافی باشد. (Back, & LaPrade, 2019;1)

لذا باید اذعان داشت اتخاذ سیاست جنایی مشارکتی در فضای سایبر نه‌تنها ممکن بلکه ضروری

۱ این قطعه با این جملات آغاز می‌شود: «دولت‌های دنیای صنعتی! من از رایاسپهر می‌آیم، سرزمین تازه ذهن و خرد. به نمایندگی از آینده، از شما درخواست می‌کنم که ما را به حال خود بگذارید. کسی در بین ما به استقبال شما نخواهد آمد و به شما خوش‌آمد نخواهد گفت. شما در آنجا حق حاکمیت نخواهید داشت.»

2 Meta-factor

و گریزناپذیر است.^۱ از جمله مزایای الگوهای مشارکتی می‌توان گفت که الگوی مشارکتی الگویی منعطف، انطباق پذیر با رسانه و کارآمد است (عاملی، ۱۳۹۷: ۵۱) و سطح مناسبی از تعامل میان مردم و دولت را فراهم می‌نماید.

۲. سازوکارهای اجرایی سیاست جنایی مشارکتی در فضای سایبر

در عصر حاضر وظیفه دولت‌ها این نیست که درگیر کارهایی شوند که بخش خصوصی و شهروندان بهتر می‌توانند آن را انجام دهند. (خوارزمی، ۱۳۹۰: ۳۱) سیاست جنایی مشارکتی هم به مثابه یک الگوی مشارکتی شهروندمدار به حق امنیت شهروندان احترام می‌گذارد و بر این اعتقاد استوار است که امنیت بیشتر تنها از ترکیب بهینه و متعادل پیشگیری، ضمانت اجرا و بازپذیری بزهکار به وجود خواهد آمد از این رو در مراحل مختلف فرآیند کیفری اعم از مرحله پیشگیری از بزهکاری، کشف جرم و واکنش یا پاسخ به آن تدابیر اجرایی خاصی را توصیه می‌کند که از طریق مشارکت شهروندان و با صرف کمترین هزینه به هدف کاهش نرخ جرم در فضای سایبر می‌انجامد.

۲-۱. پیشگیری جامعوی از جرائم سایبری

استفاده از مشارکت مردم در رهیافت‌های پیشگیرانه، یکی از مهم‌ترین مراحل تحقق این رویکرد می‌باشد.^۲ مشارکت فعال اجتماعات و سایر بخش‌های جامعه مدنی، بخش اساسی پیشگیری از جرم است. راهبرد پیشنهادی حاکم بر سیاست کیفری نوین باید راهبردی فعال، پیشگیرانه و کنترل‌کننده باشد. به جهت پیچیدگی و تخصصی بودن جرائم رایانه‌ای و درعین حال سهولت ارتکاب این جرائم، پیشگیری هرچه بهتر از این جرائم در گرو مشارکت مسئولانه و همراه شدن نهادهای غیردولتی با دولت در فرآیند پیشگیری از جرم است.

۲-۱-۱. فراهم‌سازی امکان حضور کاربران شریف

استفاده سلیقه‌ای و بدون ضابطه از فیلترینگ امکان رخداد جرم به علت عدم حضور کاربران شریف را بالا می‌برد. فیلترینگ شبکه‌های ارتباطی و اجتماعی موجود در فضای مجازی، به

۱. یکی از صاحب‌نظران در این راستا بیان می‌دارد: نه به این لحاظ که از نظر عقیدتی طرفدار مداخله‌ی کمتر دولت هستیم بلکه به این خاطر که به واقع‌گرایی اعتقاد داریم باید به دنبال سیاست جنایی مشارکتی باشیم. (لازرژ، ۱۳۹۲: ۱۶۴)

۲. بکاریا در رساله جرائم و مجازات‌های خود در خصوص مشارکت ملت در پیشگیری از جرم تأکید دارد: «می‌خواهید از وقوع جرم پیشگیری کنید؟ پس بکوشید تا قوانین روشن و ساده باشد و تمام قدرت ملت در دفاع از آن بسیج شود.» (بکاریا، ۱۳۸۰: ۱۳۲)

جهت کثرت و سهولت استفاده از فیلترشکن در فضای سایبر، جز آنکه افراد اندکی را که غالباً افراد سالم و محتاط فضای سایبر هستند از استفاده و بهره بردن از این وسایل ارتباطی محروم می‌کند موجب می‌شود که متخلفان و کاربران کم سن فضای سایبر بدون نظارت اجتماعی کاربران دیگر با سهولت و سرعت بیشتری به محیط‌های ناسالم وارد شوند یا به نحوی در معرض بزه دیدگی قرار گیرند. به نظر می‌رسد برای جلوگیری از جرائم در فضای سایبر نه تنها باید از پالایش^۱ این نوع از فضاها که بسته به نوع استفاده، امکان بهره‌ی مجاز و غیرمجاز در آن‌ها متصور است، خودداری شود بلکه باید به دعوت عموم مردم و به‌ویژه افراد شریف جامعه از قبیل قضات، اعضای هیئت علمی، فرهنگیان و والدین به این فضاها پرداخت تا به واسطه‌ی «شرم حضور» این افراد، سالم‌سازی بسترهای فضای مجازی محقق گردد.

۲-۱-۲. واگذاری پالایش محتوا به شهروندان فضای سایبر

مطابق با نظریه تراز کنترل^۲، میزان کنترلی که یک فرد بر جامعه اعمال می‌کند با میزان کنترلی که بر او اعمال می‌شود، امکان وقوع کژروی و نوع کژروی را تعیین می‌کند. (Tittle, 1995: 35) بنا بر نظریه مذکور «کنترل شدن» کاربران به صورت یک‌جانبه و بدون تفویض «قدرت کنترل‌کنندگی» به آنان، میزان درگیر شدن این افراد در فعالیت‌های مجرمانه را بالا می‌برد. اعمال فیلتر و مسدود نمودن قسمتی از فضای سایبر به شیوه دولتی به جهت نگاه افراطی متصدیان فیلتر به ممنوعیت هر سایتی که مطالب آن با سلیقه فیلتر کنندگان هم‌خوان نیست^۳ و کارکرد انطباقی و نه هوشمندانه ابزارها و برنامه‌های فیلترینگ مانع دسترسی آزاد به مکان‌های عمومی مجاز شده است. (فراهانی، ۱۳۸۴: ۱۴۰) در زمینه فیلترینگ می‌توان با کاستن از اختیار نهادهای دولتی در امر فیلترینگ و تفویض حداقل قسمتی از مسئولیت، به شهروندان فضای سایبر و یا برخی از کاربران شریف فضای سایبر، ضمن اتخاذ رویکردی سنجیده و ملایم نسبت به مسئله، به جایگاه جامعه به‌عنوان بزه‌دیده توجه داشت و به یکی از نیازهای جامعه از عدالت یعنی داشتن فرصتی جهت ایجاد حس جمعی، مسئولیت و پاسخگویی

۱ واژه پالایش به‌عنوان معادل فارسی اصطلاح فیلترینگ استعمال شده است.

2 control balance

۳ آنچه به گستره این محدودیت‌ها دامن می‌زند گنجاندن طیف وسیعی از موضوعات مشکوک یا به اصطلاح خاکستری در فهرست‌های سیاه است. همچنین اصطلاحات یا تصاویر مندرج در فهرست‌های سیاه، تنها در متون یا محتواهای غیرمجاز به کار نمی‌رود و بسیار اتفاق می‌افتد که به لحاظ کاربرد آن‌ها در محتوای مجاز از دسترسی به آن‌ها جلوگیری می‌شود.

متقابل (زهر، ۱۳۸۸: ۵۰) توجه نمود و در راستای توجه به نظریه تراز کنترل میزان درگیر شدن افراد در فعالیت‌های مجرمانه را کاهش داد. نمونه‌هایی از این راهبرد را شبکه‌های اجتماعی مانند فیس‌بوک، مای اسپیس و آرکات، اتخاذ کرده‌اند. این شبکه‌ها برای سالم‌سازی محیط، به کاربران خود اختیارات گسترده‌ای از قبیل «مسدود کردن فرد مزاحم»، «ایجاد ممنوعیت برای ورود افراد متخلف به گروه‌ها» و «پنهان‌سازی پروفایل یک کاربر متخلف از جستجوی اینترنتی» ارائه داده‌اند.^۱

۲-۱-۳. تشکیل گروه‌های گشت زنی خصوصی در فضای مجازی

اشکال مختلفی از رویکردهای گشت زنی وجود دارند که می‌توانند در اجتماعات به شکلی فعال به ایفای نقش بپردازند. در اجتماع واقعی هر دو رویکرد گشت زنی پلیس محور و جامعه‌محور کم‌وبیش وجود دارد. گستردگی و گستره‌زا بودن محیط سایبر، امکان نظارت همه‌جانبه بر آن را آن‌گونه که در جامعه‌ی واقعی و با مأمور کردن پلیس یا گروه‌هایی جهت گشت زنی وجود داشت، منتفی نموده است. باین‌وجود و با اذعان به‌ضرورت نظارت بر فضای مجازی می‌توان با اقتباس از محیط واقعی، گروه‌هایی از خود کاربران را جهت نظارت و گشت زنی مأمور نمود. حضور مستمر این گروه‌ها در محیط‌های عمومی فضای مجازی به‌ویژه شبکه‌های اجتماعی و اتاق‌های گفت‌وگو ضرورت دارد. وجود این گروه‌ها و «تجویز قانونی اجازه‌ی اخطار» توسط آنان به شهروندان متخلف فضای مجازی، سلامت محیط‌های اجتماعی مجازی را تضمین می‌کند. در راستای اجرایی شدن این پیشنهاد می‌توان هزینه‌ها و بودجه موردنیاز را از جزای نقدی مجرمان سایبری تأمین نمود.

۲-۱-۴. توزیع ابزارهای مقابله‌ای در میان کاربران فضای سایبر

پدیده «انتشار» در فضای سایبر به جهت شبکه‌ای بودن آن بیش از تصور سرعت دارد. آنجا که موضوع انتشار پدیده منفی و مجرمانه است باید توزیع ابزارهای مقابله‌ای در سطح وسیع بری را

۱. برای مطالعه بیشتر در این زمینه ر. ک:

Akçayır, G. (2017). Why do faculty members use or not use social networking sites for education? *Computers in Human Behavior*, 71, 378-385.

Manca, S., & Ranieri, M. (2016). Facebook and the others. Potentials and obstacles of social media for teaching in higher education. *Computers & Education*, 95, 216-230

Halder, Debarati And Jaishankar, K. (2011), Online Social Networking And Women Victims, In: Jaishankar, K. (Ed), *Cyber Criminology: Exploring Internet Crimes And Criminal Behavior*, CRC Press.

در دستور کار قرار داد چراکه تنها از این طریق است که می‌توان بزه را کنترل نمود و از انتشار آن جلوگیری کرد. نمونه انتشار جرم در فضای سایبر، انتشار برنامه‌های مختل‌کننده نرم‌افزار و سخت‌افزار و ویروس‌ها می‌باشد؛ ویروس‌ها و کرم‌های رایانه‌ای قابلیت زایش و تکثیر تصاعدی را دارا هستند و لذا امکان بزه دیدگی مجدد به واسطه انتشار ویروس بسیار بالا و محتمل است. با توزیع برنامه‌های ویروس‌یاب و ویروس‌کش به صورت فراگیر در میان کاربران و تسلیح آنان به برنامه‌های مقابله‌ای، علاوه بر اینکه از شیوع و گسترده شدن بیشتر خسارت نسبت به شخص بزه‌دیده جلوگیری می‌شود، از بزه‌دیده شدن دیگران هم پیشگیری به عمل می‌آید. برخی از سازوکارهای عملی پیشگیری از جرم توسط وبسایت‌ها و میزبانان فضای سایبر امکان یافته است؛^۱ این امکانات باید تقویت و بیش از این به کاربران شناخته شود.

به‌عنوان یک تجربه موفق در این زمینه می‌توان به تلاش‌های «مرکز آموزش جامعه»^۲ در کشور اندونزی اشاره نمود که در دوان همه‌گیری کرونا اقدام به آموزش سواد رسانه‌ای و توزیع ابزارهای پیشگیری از جرم سایبری میان شهروندان نموده است.^۳

۲-۱-۵. تقویت هنجارهای فضای سایبر

جریان سازی و تقویت هنجارها و عرف سایبر و جهت‌دهی به آن توأم با برانگیختن حس تعهد و مسئولیت کاربران که یک تجلی تمام‌عیار از «سیاست جنایی مشارکتی» است تا حد زیادی می‌تواند در ایمن‌سازی فضای سایبر، پیشگیری از جرم و مقابله با آن مؤثر باشد. ترغیب کاربران رعایت نزاکت (Cirton, 2009: 21) به ایمن‌سازی محیط سایبر و واکنش به ناهنجاری در این فضا، با تفهیم این واقعیت به شهروندان فضای سایبر که جامعه‌ی مجازی زیستگاه دوم ایشان است، در سالم‌سازی فضای سایبر و مقابله با جرم بسیار مؤثر و راهگشاست. در بعضی موارد

۱. شبکه‌های اجتماعی به افراد برای محافظت از خود در برابر مورد مزاحمت واقع شدن، گزینه‌های گسترده‌ای را مانند قرار دادن ارزیابی‌های امنیتی، قفل کردن آلبوم‌های شخصی و صفحات پیام، جلوگیری از مشاهده‌ی اطلاعات شخصی یک شخص توسط دیگران و پنهان ساختن پروفایل یک نفر از جستجوی اینترنتی و روش‌های گوناگون دیگر ارائه می‌دهند. در همین راستا تقویت و شناساندن امکانات موجود به کاربران و افزودن بر ظرفیت پیشگیری پذیری فضای سایبر باید در دستور کار قرار گیرد.

2. Community Learning Center

۳. برای مطالعه بیشتر در این زمینه ر.ک:

Nurhayati, S., Musa, S., Boriboon, G., Nuraeni, R., & Putri, S. (2021). Community Learning Center Efforts to Improve Information Literacy in the Community for Cyber Crime Prevention during a Pandemic. *Journal of Nonformal Education*, 7(1), 32-38

هنجارهای تعریف نشده‌ای که می‌توان از آن به‌عنوان «رفتار متعارف بر خط» نام برد، اگرچه به صورت کمرنگ وجود دارد^۱ و کاربران فضای مجازی خواه‌ناخواه ملزم به رعایت آن می‌شوند؛ باید تقویت هرچه بیشتر این هنجارها در دستور کار قرار داد.

هنجار سازی که مطابق با تحلیل هیرشی^۲ از رهگذر ایجاد تعلق خاطر، به اعتقاد و اهتمام به رعایت هنجارها می‌انجامد، باید در فضای مجازی حول محور دو اصل «نفی آزار رسانی»^۳ و «رعایت کرامت انسانی»^۴ صورت گیرد. با نفی اضرار، آزار رسانی به دیگران خواه از جنس انتشار ویروس و بدافزار^۵ و خواه از جنس هر نوع خسارت دیگر، نامطلوب شناخته می‌شود و با تأکید بر کرامت انسانی از تمامیت شخصیت معنوی افراد در مقابل بزه‌های شایع در فضای مجازی از قبیل توهین و انتشار اکاذیب و... از آبروی افراد حمایت می‌شود.

۲-۲. مشارکت جامعه‌ی در کشف جرم سایبری

راهبرد مشارکتی با به جریان انداختن تعقیب از طریق افشا، اعلام جرم و اقامه‌ی شکایت توسط تشکل‌ها، انجمن‌ها یا سندیکاها با مشارکت «گروه اجتماعی» معنا و مفهوم خود را می‌یابد^۶

۱ رعایت ادب و نزاکت و احترام به عقاید یکدیگر در اتاق‌های گپ و گفت‌وگو نمونه‌ای از هنجارهای موجود فضای مجازی است. در مواردی که افرادی این هنجارها را رعایت نکنند، توسط مدیران سایت یا دیگر کاربران از ادامه استفاده از امکانات آن سایت یا فضای مجازی محروم می‌شوند.

۲ در تحلیل هیرشی، قیدوبند عبارت است از وابستگی شدید، پایبندی و تعهد، اشتغال خاطر و وارد شدن و مشارکت کردن در امور جامعه و اعتقاد و احترام به اخلاقیات و هنجارهای قراردادی جامعه. (نجفی ابرندآبادی، هاشم بیگی، ۱۳۹۰: ۷۶)

۳ مستند این اصل قاعده فقهی «لا ضرر و لا ضرار فی الاسلام» است. مضمون این قاعده آن است که ضرر در اسلام مشروعیت ندارد و هرگونه ضرر و اضرار در اسلام نفی شده است از این روی کاربرد قاعده مذکور در مقام بیان نهی مردم از اضرار به یکدیگر است.

۴ در بستر فقه و حقوق اسلامی، حفظ کرامت انسان به‌طور عام یکی از مقاصد عام شریعت شمرده می‌شود و افراد به‌کرات به التزام به آن در حق یکدیگر توصیه شده‌اند و مستند اصلی آن آیه شریفه «لقد کرما بنی آدم» (اسراء، ۷۰) است.

۵ برای مطالعه بیشتر در این زمینه مراجعه کنید به: کربلایی حسنی، اشرف، ۱۳۹۳، احکام فقهی مترتب بر ایجاد ویروس در فضای مجازی بر اساس قاعده لاضرر، همایش الکترونیکی پژوهش‌های نوین در علوم و فناوری، به‌صورت الکترونیکی، شرکت علم محوران آسمان، http://www.civilica.com/Paper-EMAA_01_07_01-EMAA.html.

۶ در برخی کشورها مانند آمریکا، رویکرد «تعقیب اجتماعی» یا مردمی مطرح و اجرا گردد که به امر تعقیب و بیژگی اجتماعی می‌دهد. در این راستا مقامات تعقیب، ضمن ارتباط با مقامات محلی و شهروندان به شناسایی و کشف جرائم و مسائل مرتبط با جرم می‌پردازند. (E.Casey Foundation, ۲۰۰۳, ۲۵)

(دلماست مارتی، ۱۳۸۷: ۳۸). مشارکت مردم در این مرحله، جلوه‌ای از خصوصی‌سازی تعقیب و کشف جرم محسوب می‌شود که در اروپا و آمریکا در حال گسترش است. پرداخت مقداری از بودجه دستگاه عدالت کیفری رسمی برای کشف جرائم سایبری به سازمان‌های مردم‌نهاد و ایجاد تسهیلات و تشویق سازمان‌های مردم‌نهاد فعال به جهت گزارش جرم و پرداخت قسمتی از جریمه نقدی توسط مجرم به این نهادها می‌تواند بخشی از یک راه‌حل برای اقناع این سازمان‌ها برای همکاری با دولت در مقابله با جرم باشد.^۱

۲-۱. متعهد نمودن کاربران به گزارش جرم سایبری

مشارکت عمومی در عرصه‌ی سایبر، امکان کشف جرم را تا حد قابل‌توجهی بالا می‌برد در واقع به جهت گستردگی فضای سایبر امکان نظارت کامل بر آن توسط پلیس سایبر غیرممکن و محال می‌نماید لذا تنها در صورتی می‌توان از «رقم سیاه بزهکاری»^۲ در جرائم سایبری کاست که آحاد جامعه نسبت به ارتکاب جرم حساس بوده و تعهد اجتماعی خود را در گزارش بزه به ضابطین دادگستری انجام دهند. باید با متعهد سازی کاربران به گزارش جرم، به افزایش کارایی نهادها و کاهش هزینه‌های انسانی و مادی کشف و پیگرد این جرائم کمک نمود. گسترش مشارکت مردمی، به ترویج «فرهنگ مشارکت» نیازمند است. این متغیر به لحاظ ساختاری اهمیت بالایی در تداوم مشارکت مردمی دارد. (سعیدی، ۱۳۹۲: ۶۳) مشارکت مردم در مقابله با جرائم سایبری هنگامی به صورت پویا و فعال دنبال می‌شود که حس تعهد و مسئولیت در جامعه زنده باشد و افراد به همان اندازه که در جامعه واقعی نسبت به رفتار و کنش‌های دیگران حساس هستند در فضای مجازی نیز به کنترل و واکنش بپردازند. متأسفانه افکار عمومی در بسیاری از موارد همچنان بر این باور است که تنها پلیس و دستگاه قضایی وظیفه مقابله با جرم را دارند. رسانه‌ها و دستگاه‌های اطلاع‌رسانی جامعه می‌بایست از انتظار مردم از دستگاه رسمی عدالت کیفری برای مقابله با جرم بکاهند. گام نخست برای ترویج فرهنگ مشارکت برای کنترل جرائم سایبری، توجیه، تفهیم و آموزش آنان نسبت به خطر مضاعف این جرائم است (Lee,)

۱ در واقع دشوار است که بخش‌های مختلف را ترغیب کرد که به‌جای پیگیری اهداف و وظایف محوله قانونی خود، به کار گروهی و فرا بخشی در زمینه مقابله با جرم روی آورند و بخشی از بودجه و وقت خود را صرف امور غیر از آنچه به‌طور خاص از آن‌ها انتظار می‌رود، نمایند.

۲ "رقم سیاه بزهکاری" عبارت است از تفریق بزهکاری واقعی یعنی تمامی جرائمی که در یک زمان و مکان معین اتفاق می‌افتد با جرائمی که توسط پلیس کشف و برای آن‌ها پرونده تشکیل شده است.

16: 2019) با تفهیم این مطلب، انتظار مردم نسبت به ساماندهی یک‌جانبه امور توسط نهادهای قضایی و پلیس کاسته می‌شود.

۲-۲-۲. دخالت سازمان‌های مردم‌نهاد و بزهکاران پیشین در فرآیند کشف جرم

سایبری

در عصر جدید شاید هیچ جرمی را نظیر جرائم سایبری نتوان سراغ داشت که بزهکاران آن بدین شکل معادلات شناسایی را برای مأمورین تحقیق پیچیده ساخته باشند. (کوره‌پز، ۱۳۹۳: ۱۱۲) خصوصی‌سازی تعقیب در جرائم سایبری شاید بخشی از راه‌حل برای ساده‌سازی کشف و تعقیب جرائم قلمداد شود. اعطای فرصت اعلام جرم، اقامه دلیل و اعتراض به مراجع قضایی توسط سازمان‌های مردم‌نهاد در خصوص جرائم سایبری علاوه بر اینکه از بار دادسرا می‌کاهد این بستر را فراهم می‌نماید که در آینده، با پیدایش سازمان‌های فنی و تخصصی، فرآیند تعقیب مجرمان سایبری به سازمان‌های تعقیب خصوصی که متشکل از افراد متبحر در زمینه «جرم یابی سایبری» و حقوق کیفری فناوری اطلاعات هستند، سپرده شود؛ مهم‌ترین امتیاز این رویکرد به‌روز شدن شیوه‌های تعقیب کیفری و تسریع در روزآمد شدن اطلاعات فنی و کشف علمی جرائم است. خوشبختانه ماده ۶۶ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ یک گام بلند در راستای تحقق سیاست جنایی مشارکتی در مرحله کشف و تعقیب جرائم برداشته است این ماده مقرر می‌دارد: «سازمان‌های مردم‌نهادی که اساسنامه آن‌ها در زمینه حمایت از اطفال و نوجوانان، زنان، اشخاص بیمار و دارای ناتوانی جسمی یا ذهنی، محیط زیست، منابع طبیعی، میراث فرهنگی، بهداشت عمومی و حمایت از حقوق شهروندی است، می‌توانند نسبت به جرائم ارتكابی در زمینه‌های فوق اعلام جرم کنند و در تمام مراحل دادرسی جهت اقامه دلیل، شرکت و نسبت به آراء مراجع قضائی اعتراض نمایند.» هرچند این ماده از سازمان‌هایی که به‌طور تخصصی در زمینه سایبر فعالیت دارند نام نبرده است لکن درصد بالایی از جرائم سایبری را می‌توان به اعتبار بزه دیدگی زنان و کودکان و... تحت شمول آن قرار داد.^۱

۱ علاوه بر ماده مذکور، قانون‌گذار در ماده ۴۸ قانون تجارت الکترونیک نیز به موسسه‌های قانونی و مدنی حمایت از مصرف‌کننده اختیار داده است که به‌عنوان شاکی اقامه دعوا نمایند و از این رهگذر به توسعه‌ی دامنه شکایت پرداخته است.

علاوه بر این نباید از یاد برد که بزهکاران پیشین می‌توانند بخشی از بار کشف و تعقیب جرائم را به دوش بگیرند. بهره‌گیری از دانش فنی و تجربیات ملموس و مستقیم آن‌ها به‌عنوان افرادی خبره در کشف جرم بسیار راهگشاست.^۱ در سال ۲۰۰۳ در استرالیا، استفاده از دانش و تخصص یک مجرم منجر به دستگیری سازنده یک ویروس که خسارات عظیمی بر سخت‌افزارهای رایانه‌ای وارد کرده بود، گردید.^۲

۲-۳. واکنش‌های جامعه‌ی - تخصصی به بزه سایبری

یکی از مشکلات اساسی رسیدگی به جرائم نوین، عدم آشنایی قضات با موضوع و ماهیت جرم است این مشکل در جرائم سایبری که با سرعتی شتابان روزبه‌روز در حال پیشرفت است، پیوسته تداوم دارد و نقطه پایانی برای آن قابل‌تصور نیست. «استفاده از تخصص و تبحر کارشناسان» و «حضور هیئت‌منصفه در جریان دادرسی» می‌تواند قاضی را در تعیین مصداق جرم و مجازات قانونی مناسب یاری نماید.

۲-۳-۱. ارائه خدمات عام‌المنفعه سایبری به‌جای مجازات

در جرائم سایبری که از سنخ جرائم با درجه خفیف محسوب می‌شوند، ارائه‌ی خدمات عام‌المنفعه به‌جای مجازات و نشست و گفت‌وگوی بزه‌دیده و بزهکار می‌تواند تدابیر یک راهبرد مشارکتی در مرحله رسیدگی به جرم محسوب شود. لکن نباید به این مهم بی‌توجه بود که هر نوع واکنشی به جرم باید با توجه به پاسخگویی بزهکار باشد. (غلامی، ۱۳۹۱: ۲۴) کار عام-المنفعه یکی از مصادیق مهم مشارکت توأمان بزهکار و جامعه در فرآیند اصلاح و درمان بزهکار

۱ یکی از نظریات که در ذیل جرم‌شناسی انتقادی (Critical Criminology) مورد بحث قرار گرفته، نظریه «جرم‌شناسی محکومین» (Convict Criminology) است به عقیده طرفداران «جرم‌شناسی محکومین»، اغلب جرم‌شناسان بدون آنکه حتی یک روز حبس را تحمل کرده باشند، به ایراد سخن در زمینه جرم، مجرم و کیفر می‌پردازند و نظریات مختلف، با عبارات جذاب ارائه می‌کنند. نمونه‌هایی از نقش دهی به «گروه بزهکاران پیشین» در زمینه اعتیاد کارنامه موفق‌تری را در مقابله با جرم ارائه داده است. با استفاده از این افراد در کشف جرائم، علاوه بر اینکه مسئله حمایت، هدایت و به‌ویژه اشتغال پس از اتمام دوران محکومیت نیز تا حدی مرتفع شده و فرد مرتکب، به لحاظ دارا شدن و تکمیل تخصص خود در یک شغل شرافتمندانه در زمان محکومیت، می‌تواند به آینده‌ای پاک از جرم و مجرمیت امیدوار باشد، اعتمادبه‌نفس این افراد افزایش یافته و به‌نوعی احساس مفید بودن می‌کنند.

۲. جهت دسترسی به اطلاعات بیشتر در این زمینه ر.ک:

Australian federal police 1991- 2003. Annual reports at:
www.usdoj.gov/criminal/cybercrime/comrade.htm

است و به مجرم نشان می‌دهد که هرچند جامعه از مجرمیت او متأثر شده است، با این همه می‌تواند به او به‌عنوان یک عنصر سودمند و سازنده - نه مخرب و زیان‌بار- نیز بنگرد. فرآیند مزبور یک فلسفه عدالت ترمیمی را به همراه دارد که بر مبنای آن بزهکار یک‌سری خدمات عام‌المنفعه عمومی را انجام می‌دهد که این امر منجر به اشتغال و کسب تجربه‌های نوین نیز می‌شود. (جمشیدی، ۱۳۹۰: ۲۴۱) خوشبختانه بستر اجرای این راهبرد در خصوص مجرمین رایانه‌ای به جهت برخورداری از تخصص کافی کار با رایانه بسیار هموار و مساعد است. با اتخاذ چنین تدبیری، اولاً جامعه از نیروی فنی و دانش تخصصی بزهکار بهره‌مند می‌شود. ثانیاً ضمن سلب توان بزهکار در زمان ارائه خدمات عام‌المنفعه، امکان کسب درآمد و شناساندن تخصص بزهکار به جامعه فراهم می‌شود که این امر خود موجب، شرمسار سازی سازنده، جامعه‌پذیری و اشتغال وی پس از خروج او از دستگاه عدالت کیفری است.

۲-۳-۲. نهادینه‌سازی حضور متخصصان فناوری اطلاعات در جریان دادرسی

پیدایش روزافزون جرائم جدید و شیوه‌های نوین جرم، امر تعقیب جرائم سایبری را با مشکل روبه‌رو می‌نماید. در جرائم سایبری اثبات جرم، دشوار و فنی است لذا حمایت مضاعف از بزه‌دیده نسبت به سایر جرائم ضرورت بیشتری دارد؛ چه آن‌که داده‌ها و سوابق رایانه‌ای یا دلایل اتهام در جرائم سایبری بیش از ادله‌ی سایر جرائم قابلیت امحاء و تخدیش پذیری دارند، بسیار ناپایدار و فرارند و در بسیاری از موارد، متهم قبل از رسیدگی به اتهام، این مدارک را از بین می‌برد یا ادعای بی‌اعتباری ادله را مطرح می‌سازد. لذا برای شناسایی و گاهی بازبازی ادله‌ی جرم، در کنار ابزارهای خاص و پیشرفته به نیروی باتجربه و ماهر نیاز است. (جلالی فراهانی، ۱۳۸۹: ۲۱۳) بسیاری از قضات و حقوقدانان، از ماهیت، نوع و ابعاد مختلف جرمی که باید به جرم انگاری یا اعمال مجازات آن پردازند کم‌اطلاع هستند. این معضل تا آنجا پیش می‌رود که در اکثریت قریب به اتفاق جرائم سایبری شخص مرتکب، به‌مراتب بیش از قاضی رسیدگی کننده به موضوع و ابعاد جرم اشراف اطلاعاتی دارد و به‌راحتی می‌تواند جریان دادرسی را منحرف نماید. از این رو ابقای صلابت و اقتدار دستگاه عدالت کیفری در استمداد از نهادهای غیردولتی متخصص در امور فناوری اطلاعات و ارتباطات است. به نظر می‌رسد برای حل این مشکل می‌بایست حضور متخصصان فناوری در محاکم جرائم سایبری از امور الزامی برای شروع و ادامه

دادرسی دانست.^۱ با اتخاذ چنین رویکردی، می‌توان بخش گسترده‌تری از آنچه در حال حاضر به کارشناسان ارجاع می‌شود را به متخصص محول نمود و نابرابری اطلاعاتی و فنی محاکم و بزه دیدگان در برابر مجرمان را تعدیل نمود.

۲-۳-۳. حضور کاربران در جریان دادرسی

حضور «هیئت‌منصفه»^۲ در مرحله‌ی رسیدگی به‌عنوان جلوه‌ی تام راهبرد مشارکتی گام مهمی برای کارآمدی هرچه بیشتر محاکم رسیدگی کننده به جرائم سایبری است؛ هیئت‌منصفه نماینده افکار عمومی است و وجدان جمعی را در محاکمات تجلی می‌بخشد و باعث می‌شود که انتظارات مردم از عدالت و قضاوت توسط خود مردم بیان شود. بنابراین اعتماد عمومی نسبت به تصمیمات قضایی بیشتر می‌شود. (رستمی، ۱۳۸۶: ۱۴۶) ضرورت وجود نهاد هیئت‌منصفه در جرائم سایبری از این جهت قابل توجیه است که اعضای هیئت‌منصفه برخلاف قاضی دادگاه، نگاه غیر منصوص و موسع‌تری به واکنش دارند؛ خود را مکلف به پیروی از یک نص قانونی نامتناسب با وضعیت مجرم نمی‌بینند و ضمن اینکه به تناسب جرم و مجازات توجه دارند، درصددند که تناسب بین مجازات و شخصیت مجرم هم لحاظ شود. این امر، یعنی؛ «فردی شدن مجازات‌ها» در خصوص جرائم سایبری ضرورتی مضاعف دارد چراکه مجرمان سایبری مجرمانی با ویژگی‌های خاص خود هستند که در بسیاری از جرائم نقطه مقابل مجرمان سنتی از حیث هوش، قدرت تطبیق با محیط و سایر ویژگی‌ها هستند.^۳

۲-۳-۴. جبران خسارات ناشی از جرم از طریق بیمه سایبری

گسترده‌ی خسارات ناشی از جرم از جمله ویژگی‌های جرائم سایبری است. خسارات ناشی از جرم سایبری شامل خسارات مادی و معنوی می‌شود. در فضای مجازی گاه انتشار یک بدافزار و

۱ در کشورهای دارای نظام حقوقی انگلوساکسون، مشارکت سازمان‌های غیردولتی در پیشگاه برخی از مراجع تحت عنوان «دوستان دادگاه» وجود دارد. دوست و یار دادگاه، نه طرف دعوا به شمار می‌رود و نه شخص ثالث. مرجع رسیدگی کننده با توجه به صلاحیت، تجربه و تخصصی که این گروه‌ها دارند، از آن‌ها می‌خواهد تا دیدگاه‌های خود را به صورت کتبی یا شفاهی در اختیار آن مرجع بگذارد (رضانی قوام‌آبادی، ۱۳۹۰: ۲۱۸). در این حالت، سازمان‌های غیردولتی می‌توانند اطلاعات، نظرات و تجربه و تحلیل‌ها و دلایل حقوقی خود را به شعبه رسیدگی کننده ارجاع دهند. این شعبه می‌تواند از این سازمان‌ها بخواهد بیانیه مکتوبی در مورد موضوع خاصی ارائه نمایند. (کوشکی، ۱۳۹۲: ۶۷)

2 jury

۳ به‌طور نمونه بسیاری از هکرها در فضای سایبر افراد کم سنی هستند که از یک‌سو ممکن است به جهت صغر مسئولیت کیفری نداشته باشند و از سوی دیگر گسترده‌ی خسارت آن‌ها به‌مراتب بیش از جرائم کلاسیک است که برحسب معیار صدمه باید به مجازات سنگینی برسند.

گاه توهین به یک شخص گستره‌ای از خسارات مادی و معنوی را پدید می‌آورد. جبران خسارات و بازگشت به حالت قبل از جرم مسئله مهمی است که انتظار می‌رود از طریق سازوکارهایی تحصیل شود. یکی از جلوه‌های مشارکت سازمان‌های مردم‌نهاد در زمینه جبران خسارات ناشی از جرم، نهاد بیمه می‌باشد؛ در واقع بیمه سایبر می‌تواند به‌عنوان تضمینی برای جبران خسارت‌های ناشی از جرم و مخاطرات موجود در فضای سایبر ایفای نقش کند. ممکن است مسببان زیان‌های رایانه‌ای شناسایی یا مسئول شناخته نشوند یا نتوانند همه خسارت‌های وارده را از آن‌ها بازستانند در چنین وضعیتی بیمه سایبری می‌تواند پاسخگوی مسئولیت احتمالی کاربران باشد.^۱ این تدبیر با ایجاد اطمینان به جبران زیان‌های وارده در فضای سایبر اعتماد ذی‌نفعان این حوزه را تأمین می‌کند و با رویکردی کنشگرانه و پیشگیرانه، جبران‌ناپذیری زیان‌های سایبری را به حداقل می‌رساند. (کلانتری و سجادی، ۱۳۹۰: ۱۸۸) تقویت، ترویج و نهادینه‌سازی این صنعت در خصوص فناوری اطلاعات و ارتباطات برای به حداقل رساندن خسارات در فضای سایبر و ارتقاء امنیت در این فضا، در گرو حمایت از سازمان‌های خصوصی بیمه‌گذار، اطلاع‌رسانی و اقناع کاربران فضای مجازی است.

نتیجه‌گیری

عموماً راهبردهای حکمرانی متمرکز، دستوری، عمودی و سلسله‌مراتبی نه مطلوب شهروندان است و نه متبوع آنان. این وضعیت در خصوص فضای سایبر به جهت فرا متغیرهای این فضا از جمله گستردگی و فرامرزی بودن، تمرکز گریزی و ساختار شبکه‌ای آن به مراتب تشدید یافته است. لذا ضرورت دارد که برای کنترل جرم در فضای سایبر در یک راهبرد مشارکتی و فراگیر از شهروندان و کاربران جامعه مجازی استمداد نمود. لکن مقدم بر هر امری باید «چگونگی

۱ عمده پوشش‌های بیمه‌ای در فضای سایبری را می‌توان در بخش خسارات مالی، سرقت اطلاعات صنعتی و فردی، وقفه در تجارت و نیز ارتباطات دانست که پوشش‌های ارائه شده در بخش ارتباطات عمدتاً به سه دسته کلی تقسیم می‌شود:

(۱) پوشش بیمه شخص ثالث؛ شامل پوشش از دست دادن یا خرابی سیستم‌های اطلاعاتی، اخاذی در فضای سایبری و نیز کلاهبرداری در زمان انتقال پول الکترونیکی

(۲) بیمه مسئولیت شخص ثالث؛ شامل پوشش آلوده شدن سیستم‌ها به ویروس و بدافزار و نیز دزدیده شدن کارت‌های تجاری و اعتباری

(۳) بیمه استثنائات؛ شامل پوشش محرومیت از سیستم‌های ارتباطی راه دور همانند بد کار کردن ماهواره یا پست‌های ارتباطی شرکت و نیز عملیات غیرمنصفانه و کلاهبرداری از سوی شرکت ارائه‌دهنده خدمات الکترونیک.

استفاده از مشارکت شهروندان» یا «سازوکارهای اجرایی مشارکت شهروندان در فضای مجازی» شناسایی شود. موضوعی که پژوهش حاضر متکفل پرداختن به آن بود. بر مبنای یافته‌های این پژوهش در راستای استفاده از ظرفیت جامعه برای کنش و واکنش به بزه‌هایی که در فضای سایبر ارتکاب می‌یابند، در سه سطح «پیشگیری»، «کشف جرم» و «واکنش به جرم» می‌توان تدابیر اجرایی خاصی را معرفی نمود.

در مرحله پیشگیری از جرم، با تعدیل مسدودسازی فضاها و فیلترینگ به شیوه جاری و «واگذاری پالایش محتوا به شهروندان فضای سایبر»، خروج کاربران شریف از فضاهای مجازی منتفی می‌شود و این مهم یعنی «حضور حداکثری کاربران شریف» نظارت‌های غیررسمی در فضای سایبر را تقویت نموده و به پیشگیری مؤثری از بزهکاری می‌انجامد. علاوه بر این «تشکیل گروه‌های گشت زنی خصوصی»، «توزیع ابزارهای مقابله‌ای» و «تقویت هنجارهای بر خط» روش‌ها و تدابیر مناسب دیگری برای بهره‌برداری از ظرفیت اجتماع در مرحله پیشگیری از جرم می‌باشند که دو مورد اول گزینه‌های در دسترس و قابل اجرا برای متصدیان اجرایی پیشگیری از جرم، از جمله پلیس فتا است و مورد اخیر نیازمند توجه و اقدام سازمان‌های فرهنگی پرشمار در کشور است.

در مرحله کشف جرم نیز «متعهد سازی شهروندان به گزارش رفتار مجرمانه» مستلزم اقدامات بنیادین فرهنگی-تربیتی است که می‌توان، بخشی از آن را به دوش متولیان تعلیم و تربیت در مدارس محول نمود. علاوه بر این «تفویض امر تعقیب به سازمان‌های مردم‌نهاد و استمداد از بزهکاران پیشین برای کشف جرم» روش‌های کارآمدی دیگری هستند که با اعمال آن، مشکل بالابودن رقم سیاه و خاکستری در فضای سایبر تا حدودی برطرف می‌گردد. لکن در حال حاضر به جهت فقدان نص قانونی امری غیرممکن به نظر می‌رسد و مستلزم تجویز قانون‌گذار است.

اما در مرحله پاسخ به بزهکار، «ارائه خدمات عام‌المنفعه سایبری به جای مجازات» اقدام مؤثری است که در حال حاضر با وجود نهادهای ارفاقی مختلف در قانون مجازات اسلامی، از جمله جایگزین‌های حبس و ماده ۸۴ امکان اعمال آن توسط دادرسان وجود دارد. «حضور متخصصان فناوری اطلاعات در جریان دادرسی» و کمک به قضات توسط ایشان موضوع دیگری است که در راستای تأمین عدالت قضایی از تیرئه بی‌جهت مرتکبان ممانعت به عمل می‌آورد چه آن‌که غالباً، بزهکاران سایبری در خصوص فضای سایبر از حیث فنی تخصص بیشتری

نسبت به دادرسان داشته و این وضعیت خواه‌ناخواه در به انحراف کشیده شدن مسیر دادرسی و نتیجتاً تبرئه بی‌جهت مرتکب مؤثر می‌باشد. از سوی دیگر، «حضور کاربران فضای سایبر در جریان دادرسی»، می‌تواند مانع از محکومیت بی‌جهت متهم گردد، چه آن‌که بعضاً عرف و هنجار فضاهای سایبر نظیر شبکه‌های اجتماعی و چت روم‌ها متفاوت از عرف و هنجار فضای واقعی است و این موضوع در تحقق یا عدم تحقق برخی جرائم مؤثر است، لذا ضروری است بعضی شهروندان و کاربران فضای مجازی در جلسه دادرسی حاضر بوده و دادرس را در شناخت هنجارهای فضای سایبر یاری رسانند. همچنین «جبران خسارات ناشی از جرم از طریق بیمه» می‌تواند به‌عنوان جلوه دیگری از راهبرد جنایی مشارکتی در دستور کار قرار گیرد و به‌واسطه آن از ضررهای ناشی از جرم شهروندان کاسته شود، موضوعی که نیازمند فرهنگ‌سازی یا الزام قانونی دست‌کم در مورد شرکت‌های تجاری و... است.

منابع

- بارلو، جان پری (۱۹۹۶) اعلامیه استقلال فضای سایبر.
- بکاریا، سزار (۱۳۸۰) رساله جرائم و مجازات‌ها ترجمه محمدعلی اردبیلی، انتشارات میزان، چاپ دوم.
- جلالی‌فراهانی، امیرحسین، (۱۳۸۳) «پیشگیری از جرائم رایانه‌ای»، مجله حقوقی دادگستری، شماره ۴۷.
- جلالی‌فراهانی، امیرحسین، (۱۳۸۴) «پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، مجله فقه و حقوق، سال دوم، پاییز.
- جلالی‌فراهانی، امیرحسین، (۱۳۸۸) تفتیش و توقیف رایانه‌ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری، انتشارات روزنامه رسمی جمهوری اسلامی ایران.
- جمشیدی، علیرضا، (۱۳۹۰) سیاست جنایی مشارکتی، تهران انتشارات میزان، چاپ نخست.
- خوارزمی، شهین دخت (۱۳۹۰) شئون انسانی در فضای مجازی، انتشار یافته در فضای مجازی؛ ملاحظات اخلاقی، حقوقی و اجتماعی، انتشارات دانشگاه تهران.
- دلماس-مارتی، می ری (۱۳۸۱) نظام‌های بزرگ سیاست جنایی، ترجمه، علی حسین نجفی ابرندآبادی، تهران، انتشارات میزان، چاپ اول.
- رستمی، ولی (۱۳۸۶) مشارکت مردم در فرآیند کیفری (بررسی سیاست جنایی کشورهای غربی)، فصلنامه حقوق دانشگاه تهران سال ۳۷، شماره ۲.
- زهر، هوارد (۱۳۸۸) کتاب کوچک عدالت ترمیمی، ترجمه: حسین غلامی، انتشارات مجد، چاپ دوم.
- سعیدی، محمدرضا (۱۳۹۳) درآمدی بر مشارکت مردمی و سازمان‌های غیردولتی، انتشارات سمت، چاپ سوم.
- عاملی، سعید رضا (۱۳۹۷) الگوی حکمرانی دوفضایی، انتشارات امیرکبیر.
- غلامی، حسین، (۱۳۹۱) عدالت ترمیمی، انتشارات سمت، چاپ سوم.
- کلانتری رضا، سجادی هادی (۱۳۹۰) بیمه سایبر و نقش آن در توسعه اعتماد به خدمات تجارت الکترونیکی، همایش ملی اقتصاد و تجارت الکترونیکی، وزارت ارتباطات و فناوری اطلاعات، اصفهان، نشر طوبی نصف جهان.
- کوشکی، غلامحسین (۱۳۹۲) سازمان‌های غیردولتی: از انفعال تا مشارکت رو به فعال در تعقیب دعوای عمومی (با نگاهی به قانون آیین دادرسی کیفری)، پژوهش حقوق کیفری، شماره ۴.
- لازرژ، کریستین، (۱۳۹۲) درآمدی بر سیاست جنایی، ترجمه علی حسین نجفی ابرندآبادی، انتشارات میزان، چاپ چهارم

- محمد کوره‌پز، حسین؛ میرخلیلی، محمود؛ توجهی، عبدالعلی؛ بهره‌مند، حمید؛ (۱۳۹۳) نیمرخ جرم‌شناختی بزهکاران سایبری، پژوهش حقوق کیفری، سال سوم، شماره نهم.
- نجفی ابرنآبادی، علی حسین؛ هاشم بیگی، حمید؛ (۱۳۹۰) دانشنامه جرم‌شناسی، انتشارات گنج دانش، چاپ دوم.
- Barlow, John Perry (1996) Declaration of Cyberspace Independence.
- Bekaria, Caesar (1380), treatise on crimes and punishments, translated by Mohammad Ali Ardabili, Mizan Publishing House, second edition.
- Akçayır, G. (2017). Why do faculty members use or not use social networking sites for education? *Computers in Human Behavior*, 71, 378-385.
- Australian federal police 1991- 2003. Annual reports at: www.usdoj.gov/criminal/cybercrime/comrade.htm
- Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(2), 1-4. <https://www.doi.org/10.52306/02020119KDHZ8339>
- Bar Wolfgang, (2013) Legal challenges in the fight against cybercrime, Cybercrime—Threat, intervention, defence BKA Autumn Conference, 12 - 13 November 2013
- Brenner Susan W. (2004) Toward a Criminal Law for Cyberspace: Distributed Security, *Boston University Journal of Science & Technology Law*, Vol. 10, No. 2, 2004 0
- Citron, K. D. (2009). Law's expressive value in combating cyber gender harassment. *Michigan Law Review*, 108, 373-415.
- Cyber Security Survey (2015) MAJOR AUSTRALIAN BUSINESSES, Australian Cyber Security Centre.
- , E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(2), 5-22.
- Halder, Debarati And Jaishankar, K. (2011), Online Social Networking And Women Victims, In: Jaishankar, K. (Ed), *Cyber Criminology: Exploring Internet Crimes And Criminal Behavior*, CRC Press.
- Jaishankar.k (2011).*Cyber Criminology, Exploring Internet Crimesand Criminal Behavior*.Boca Raton.CRC Press.
- Lee, S., Choi, K., Choi, S., & Englander
- Jalali-Farahani, Amirhossein, (2013) "Prevention of computer crimes", *Law Journal of Justice*, No. 47.
- Jalali-Farahani, Amirhossein, (2004) "Situational prevention of cyber crimes in the light of human rights standards", *Jurisprudence and Law Journal*, second year, autumn.
- Jalali-Farahani, Amirhossein, (2008) Searching and confiscating computers and obtaining electronic evidence in criminal investigations, publications of the official newspaper of the Islamic Republic of Iran.
- Jamshidi, Alireza, (1390) Participatory Criminal Policy, Tehran, Mizan Publications, first edition.

- Khwarazmi, Shahin Dokht (2010) Human affairs in the virtual space, published in the virtual space; Ethical, legal and social considerations, Tehran University Press.
- Delmas-Marti, May Ray (2012) The Great Systems of Criminal Politics, translated by Ali Hossein Najafi Abrandabadi, Tehran, Mizan Publications, first edition.
- Rostami, Vali (2016) People's participation in the criminal process (review of the criminal policy of Western countries), Tehran University Law Quarterly, 2017, No. 2.
- Zohr, Howard (1388) Small Book of Restorative Justice, translated by Hossein Gholami, Majd Publications, second edition.
- Saeedi, Mohammad Reza (2013) An Introduction to People's Participation and Non-Governmental Organizations, Samt Publications, third edition.
- Ameli, Saeed Reza (2017) Two-space governance model, Amirkabir Publications.
- Gholami, Hossein, (1391) Restorative Justice, Samt Publications, third edition.
- Kalantari Reza, Sajjadi Hadi (2018) Cyber insurance and its role in developing trust in e-commerce services, National Economy and E-commerce Conference, Ministry of Communications and Information Technology, Isfahan, Toubi Neseef Jahan Publishing House.
- Koshki, Gholam Hossein (2012) Non-Governmental Organizations: From Passivity to Active Participation in Prosecuting Public Lawsuits (Looking at Criminal Procedure Law), Criminal Law Research, No. 4.
- Lazarge, Christian, (2012) An Introduction to Criminal Policy, translated by Ali Hossein Najafi Abrandabadi, Mizan Publications, 4th edition
- Mohammad Korepaz, Hossein; Mir Khalili, Mahmoud; Atari, Abdul Ali; Bohrmand, Hamid; (2013) Criminological Profile of Cybercriminals, Criminal Law Research, 3rd year, 9th issue.
- Manca, S., & Ranieri, M. (2016). Facebook and the others. Potentials and obstacles of social media for teaching in higher education. Computers & Education, 95, 216-230
- Nurhayati, S., Musa, S., Boriboon, G., Nuraeni, R., & Putri, S. (2021). Community Learning Center Efforts to Improve Information Literacy in the Community for Cyber Crime Prevention during a Pandemic. *Journal of Nonformal Education*, 7(1), 32-38
- Najafi Abrandabadi, Ali Hossein; Hashem Beigi, Hamid; (1390) Encyclopedia of Criminology, Ganj Danesh Publications, second edition.
- Tittle, Charles R. (۱۹۹۵) Control Balance: Toward a General Theory of Deviance, Westview Press, Inc Boulder, CO 80301, United States of America
- Xingan Li, (2014) PHENOMENAL EXPLORATION INTO IMPACT OF ANONYMITY ON LAW AND ORDER IN CYBERSPACE, *Kriminologija i socijalna integracija* Vol.22 Br.2.