فصلنامه علوم خبری
سال دوازدهم، شماره ۴۶ تابستان ۱۴۰۲
صفحات ۱۰۵-۷۷

La revue science de I’information
année 12 / No 46 Été 2023
pages: 77-105

آسیب شناسی چالش های حاکم بر پیشگیری وضعی حاکم بر جرایم سایبری

امین امیریان، سید محمد موسویان

۱. نویسنده مسئول، استادیار، دانشگاه امام صادق علیه‌السلام ، تهران. رایانامه: amirian.amin@yahoo.com

۲. عضو هیات علمی دانشگاه شهید اشرفی اصفهانی، ایران، رایانامه: sm.mousaviyan@gmail.com

اطلاعات مقاله

نوع مقاله: پژوهشی

تاریخ دریافت: ۰۴/۲۰/ ۱۴۰۲

تاریخ بازنگری: ۱۴۰۲/۰۵/۲۰

تاریخ پذیرش: ۱۴۰۲/۰۵/۲۰

تاریخ انتشار: ۱۴۰۲/۰۶/۲۰

کلیدواژه‌ها: اینترنت، پیشگیری وضعی، جرایم

چکیده

جرایم سایبری عبارت است از جرایمی که در محیطی غیر فیزیکی به عبارتی در فضای سایبری و اینترنتی اتفاق می افتند که توسط قوانین مختلف جرم انگاری شده اند، با توجه به اینکه با پیشرفت های حوزه فناوری جرایم سایبری نیز متحول می شوند و روش های سنتی پاسخگوی نیاز به مقابله با این جرایم نیست لذا نیاز به روش های جدید جهت پیشگیری از این جرایم است، با توجه به این مساله پژوهش حاضر با هدف تبیین جایگاه پیشگیری وضعی از جرایم سایبری در بوته آسیب شناسی حاکم بر آن انجام گرفت. روش تحقیق توصیفی و تحلیلی است و برای جمع آوری اطلاعات از منابع کتابخانه‌ای استفاده شده است. براساس نتایج تحقیق؛ تدابیر پیشگیری وضعی از جمله؛ تدابیر محدود کننده یا سلب کننده دسترسی، تدابیر نظارتی که موارد و سوابق مشکوک، تدابیر صدور مجوز، ابزارهای ناشناس کننده و رمز گذاری، گشت اینترنتی و رصد فضای سایبری برای شناسایی موارد مشکوک و پیشگیری از جرایم احتمالی، آموزش همگانی، شناسایی و کنترل افراد خطر ساز، به افزایش خطرات ملموس ارتکاب جرم افزایش محافظت ها و مراقبت ها در فضای سایبری و... نقش اساسی در پیشگیری از جرایم سایبری دارند. از چالش ها، موانع و مشکلات پیش روی پیشگیری وضعی می توان به؛ کثرت محتواهای مجرمانه، فراملی بودن جرایم سایبری، عدم تخصص کافی مراجع قضایی و انتظامی، موقتی بودن پیشگیری وضعی، مقابله‌ی محافظه کارانه با جرم، فرصت مدار بودن، عدم شمول همه‌ی آماج ها، جابه جایی جرم، عدم شفافیت

سایبری، فضای سایبری، فضای مجازی.	برخی عبارات قانونی، افزایش احتمال بزه دیدگی و رقم سیاه جرایم سایبری، زمان بر بودن تدابیر پیشگیری وضعی اشاره کرد. کلیدواژه‌ها: اینترنت، پیشگیری وضعی، جرایم سایبری، فضای سایبری، فضای مجازی.

استناد: امیریان، امین، موسوی، سید محمد (۱۴۰۲). آسیب شناسی چالش های حاکم بر پیشگیری وضعی حاکم بر جرایم سایبری، ۱۲ (۲۳)، ۲۰-۱.

مقدمه

ویژگی‌های محیط سایبر از قبیل عدم وابستگی به زمان و مکان خاص، امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، به همراه ماهیت جرایم سایبری، وسعت جغرافیایی کشور و گسترش ارتکاب جرایم سایبری؛ عواملی هستند که شیوه‌های ارتکاب جرایم سایبری را متنوع‌تر و کشف جرایم سایبری و به دام انداختن مجرمان را سخت‌تر کرده است. در شرایط حاضر ضرورت و اهمیت کشف جرایم سایبری در برابر انواع تهدیدات و تهاجمات بر کسی پوشیده نیست و برای حفظ امنیت عمومی ضروری است. با توجه به پیچیدگی های مسیر کشف جرم و لزوم تسریع کشف و دستگیری مجرمان و تأثیر آن در کاهش میزان وقوع جرایم، لازم است در حیطه جرم یابی، راهکارهای علمی متعدد و متنوعی جهت کشف جرم مطرح شده و بکار گرفته شود در این راستا نهاد پلیس در طول زمان با توجه به تغییر و تحولات محیط های پیرامونی و انتقال جرایم به محیط سایبر دچار تغییرات و دگرگونی‌هایی در جهت پاسخ دهی به جرایم شده اند و راهبردها، ساختارها و مدل های مختلفی را در پیش گرفته و اجرا نموده اند. بدین ترتیب در کشف جرایم سایبری، بدلیل پیچیدگی‌ها و مشکلات پیش روی آن، روش‌ها و ابزارهای مختلفی نیاز است و مقابله جدی و مؤثر پلیس را می‌طلبد که با توسل به مدرن‌ترین وسایل و روش‌ها، بتواند توان مقابله با مجرمانی که مرتکب این جرایم می شوند را داشته باشد. بنابراین شناسایی عوامل تأثیرگذار بر کشف جرایم سایبری از اهمیت ویژه ای برخوردار است، به طوری که بر سرعت کشف این جرایم می‌افزاید و بدون توجه به این موضوع نمی‌توان در جهت کاهش آمار رو به رشد جرایم سایبری گام برداشت و به منظور ردیابی، تعقیب و تحت پیگرد قرار دادن و کشف ادله و اثبات جرم مجهز شد؛ در حالی که مجرمان هرچه بیشتر تلاش خواهند نمود از این ظرفیت عظیم سایبری در عرصه نا امنی‌های اجتماعی استفاده نمایند. بررسی ها نیز نشان می دهد که علی رغم تشکیل پلیس مبارزه با جرایم سایبری ضابط تخصصی تحت عنوان ضابط کشف جرایم سایبری که به صورت تخصصی به مقابله با جرایم سایبری بپردازد وجود ندارد که دلیل آن می تواند خلاء قانونی و عدم تصویب قوانین اختصاصی باشد. لذا با توجه به اینکه ادله اثبات جرم در فضای سایبری به علت الکترونیکی بودن و ویژگی های خاص آن که

متفاوت از ادله های جرایم سنتی می باشد و پلیس به منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می شود که در سایر جرایم مطرح نیست، لذا با توجه به وضعیت و شرایط خاص جرایم سایبری و ادله ها و ابزارهای ارتکاب جرایم سایبری و امکان جعل و دستکاری ادله جرایم سایبری باید به طور مفصل نقش ضابطان در کشف و تعقیب این جرایم و آسیب هایی که با آن مواجه هستند بررسی شود. پژوهش حاضر درصدد پاسخگویی به این سوالات است که ضابطان چه صلاحیتی در رابطه با جرایم سایبری دارند؟ ضابطان به چه چالش ها و آسیب هایی در کشف و تعقیب جرایم سایبری مواجه هستند.

۱ . مفهوم لغوی پیشگیری از وقوع جرم

واژه پیشگیری از نظر لغوی جلوگیری کردن، مانع شدن، دفع، صیانت، جلو بستن و نیز اقدامات احتیاطی برای جلوگیری از حوادث بد و ناخواسته معنا کرده اند (معین، ۱۳۷۷، ص ۹۳۳)، یا، به معنای منع کردن، دفع، به نگهداری برخاستن نیز آمده است (دهخدا، ج۲، ۱۳۷۷، ص ۵۹۹۱). بنابراین، پیشگیری در علم لغت به معنای مانع یا سدی است که جلوی اتفاق افتادن یک امر یا موضوع بد و ناخوشایند را می‌گیرد.

از نظر ریشه‌شناسی، کلمه پیشگیری در دو بعد به معنای پیش‌دستی کردن و به جلوی چیزی رفتن و همچنین به معنی آگاه کردن، خبردادن و هشداردادن آمده است. همچنین این واژه در مفهوم جرم‌شناسی، خارج از گستره نظام کیفری تحقق پیدا می‌کند و عبارت است از «هرگونه اقدامی که جلوگیری از ارتکاب جرم را مورد توجه قرار دهد». از منظر جرم شناسی پیشگیرانه، پاسخ‌های پیشگیرانه به پدیده مجرمانه، اقدام‌هایی است که جنبه کنشی داشته و با ماهیت غیرقهرآمیز یا در مقام سالم‌سازی جامعه یا برای رفع بحران‌های جرم‌زا و یا برای برهم زدن اوضاع و احوال ما قبل بزهکاری اتخاذ می شود (نجفی ابرندآبادی، ۱۳۸۸، ص ۵۲۵).

اصطلاح شناسی پیشگیری از وقوع جرم

پیشگیری یکی از وسایل و امکانات سیاست جنایی برای کنترل جرم است. از نظر علمی و اصطلاحی، مفهوم پیشگیری به مفاهیم مختلفی تعلق دارد؛ یعنی ترکیبی از تئوری و تجربه است. در ابتدا پیشگیری به صورت نظری مطرح می‌شد. انریکو فری یکی

از پیشگامان مکتب تحققی و از بانیان نظریه عوامل محیطی بزهکاری، پیشنهادهایی در زمینه دفاع جمعی در مقابل بزهکاری- که در واقع طرح تغییر جامعه است- را ارائه می-کند، یعنی عرف و عادات باید دگرگون شود. پاره‌ای از این نظریات کم و بیش به اجرا گذاشته شده و تجربه می‌شوند. به دنبال این تجربه، ارزیابی تأثیر این تجربیات مطرح می‌شود. به دنبال ارزیابی این تجربیات، امکان اصلاح و جرح و تعدیل نظریه قبل فراهم می‌شود و به این ترتیب، مفهوم پیشگیری یک مفهوم منطقی و عملی به خود می‌گیرد (نجفی ابرندآبادی، ۱۳۸۳، ج۱، ۷۴۱).

در اصطلاح‌شناسی، بنابراین، می‌توان گفت: مجموعه تدابیر و اقداماتی است که هدف از اعمال آن کاهش جرم و بزه، ترس و ارعاب در مجرمان برای عدم تکرار جرم‌های بعدی، جلوگیری از مجرم شدن مجرمان بالقوه، تأدیب افراد جامعه علی‌الخصوص مجرمان، با هدف افزایش نظم و امنیت عمومی و فردی، کاهش انگیزه‌ها و فرصت‌های مجرمانه در افراد جامعه، دفاع از حقوق قربانیان جرم، در چارچوب قانون می‌باشد.

پیشگیری وضعی جرم‌شناختی

در پیشگیری وضعی جرم شناختی،[۲۱] که مبنای نظری آن در جرم‌شناسی، وضعیت ماقبل بزهکاری است، با فرآیند گذار از اندیشه به عمل[۲۲] مواجه هستیم و درصدد تغییر وضعیت مشرف بر جرم هستیم تا معادله جرم به ضرر مجرم شود. به بیان دیگر، هدف اتخاذ اقداماتی است که فرآیند گذار از اندیشه به عمل را قطع کند (همان، ج۱، ۷۸۸-۷۵۱). اقدام‌های وضعی در این نوع پیشگیری، ناظر به اوضاع، احوال و شرایطی است که مجرم را در آستانهٔ ارتکاب جرم قرار می‌دهند. این اوضاع و احوال که در جرم‌شناسی وضعیت‌های ماقبل بزهکاری یا وضعیت‌های پیش‌جنائی نام دارند، فرایند گذار از اندیشه به عمل مجرمانه را تحریک یا تسهیل کرده و نقش تعیین‌کننده‌ای در آن ایفا می‌کند (همان، ۵۸۰). در پیشگیری وضعی جرم‌شناختی، اندیشه اساسی این است که گذار به عمل مجرمانه نه فقط به انگیزه‌های مجرم بستگی دارد، بلکه به خصوصیات وضعی،

---

۲۱ Criminological preventional

۲۲ Acting out

شرایط موضعی، شرایط موجود در اوضاع و احوال قبل از جرم بستگی دارد. هدف، چیره شدن به اوضاع قبل از جرم که فرد را در آستانهٔ جرمی قرار داده است.

در این نوع پیشگیری وضعی، دو اقدام اساسی می‌توان انجام داد: کاهش وضعیت‌های جرم‌زا یا وضعیت‌های موجود در آستانه ارتکاب جرم یا وضعیت‌هایی که زمینه ارتکاب جرم را فراهم می‌کند، و افزایش خطر دستگیری مجرم یا بالا بردن هزینه کیفری ارتکاب جرم برای مجرم (همان، ج۱، ۸۳۹).

پیشگیری وضعی بزه‌دیده‌شناختی

امروزه، شکل جدیدی از پیشگیری، موسوم به «پیشگیری بزه‌دیده شناختی»[۲۳] که خود از شاخه‌های «پیشگیری وضعی» از بزهکاری محسوب می‌شود، در سیاست جنایی مورد توجه و استفاده قرار گرفته است. تدابیر و اقدام‌ها در پیشگیری بزه‌دیده شناسانه ناظر به اجتناب از بزه‌دیده واقع شدن یا به عبارت دیگر، جلوگیری از بزه‌دیدگی افراد یا اموال به عنوان آماج یا هدف جرم، است. در این چارچوب، بحث مصون‌سازی، ایمن‌سازی و تقویت آن دسته از آماج‌هایی مطرح می‌شود که بزهکاران نوعاً به آنها تعرض می‌کنند. با اتخاذ و اعمال این اقدامات، هدف آن است که هزینه روانی، جسمانی و کیفری جرم برای شخص بزهکار تا حداکثر ممکن بالا رود و لااقل خود بزه‌دیده، به عنوان عنصری از وضعیت ماقبل بزهکاری یا وضعیت پیش‌جنایی، زمینهٔ جذابی را برای بزهکاران فراهم نیاورد (نجفی ابرندآبادی، ۱۳۷۹، ۱۱). و (همان، ج۱، ۸۳۶ و ۸۴۰). به دیگر سخن، در پیشگیری وضعی بزه‌دیده شناختی، هدف مداخله در وضعیت پیش‌جنایی به شکلی است که از بزه‌دیده واقع شدن هدف و یا موضوع جرم جلوگیری شود.

بنابراین، این نوع پیشگیری با تغییر وضعیت‌های ماقبل بزهکاری، مثلاً از طریق حفاظت یا تقویت حمایت از بزه‌دیده یا آماج بالقوه جرم با استفاده از دستاورد فناوری‌های نوین، دشوار کردن ارتکاب جرم، بالا بردن خطر شناسایی و دستگیری بزهکار و کاهش سود و لذت مورد انتظار مجرم از تعرض به هدف یا بزه‌دیده خاص را دنبال می‌کند و بدین‌ترتیب فرض بر این است که در چنین شرایطی، بزهکار از عملی ساختن اندیشهٔ خود

---

۲۳ Victimological Prevention

نسبت به آن بزه‌دیده یا آماج حمایت شده صرف‌نظر خواهد کرد. به عبارت دیگر، پیشگیری وضعی، «شامل مسؤول کردن کل جامعه در قبال خطر مجرمانه و خطر بزه‌دیده شناختی می‌شود؛ به گونه‌ای که اعضای آن، خود، در مراقبت از خود و اموال مشارکت کنند.» (همان، ۵۸۱)

از این رو، تفاوت پیشگیری وضعی با سایر پیشگیری‌ها در این است که در سایر پیشگیری‌ها عمده اقدامات ما ناظر به این است که افراد مجرم نشوند و عوامل جرم‌زا خنثی شوند. اما در پیشگیری وضعی، علاوه بر این بُعد، بُعد دیگری وجود دارد که ناظر به بزه‌دیده نشدن افراد و اموال است.

فون هانتیگ، جرم‌شناس مشهور آلمانی، در فصل چهارم کتاب خود (بزهکار و قربانی او، ۱۹۴۸)، اصطلاح «پیش‌استعدادها یا پیش‌زمینه‌های مجنی‌علیه» که فرد را به بزهکاری سوق می‌دهد، مورد توجه قرار می‌دهد. از دیدگاه وی بعضی طبقات همچون زنان، کودکان، سالمندان و به طور کلی افرادی که از آنها تحت عنوان «زیرهنجار»[۲۴] یاد می‌کنند و یا ناقص‌العقل‌ها»، پیش‌زمینه و استعداد قبلی برای بزه‌دیده واقع شدن دارند. به عبارت بهتر، بعضی از افراد، کشش و جاذبه ویژه‌ای بر مجرم اعمال می‌کنند که منجر به بزه‌دیدگی آنها می‌گردد. نکتهٔ قابل توجه در ارتباط با آنان، «بی‌دفاعی مطلق» آنها در برابر بزه‌دیدگی است (صفاری، ۱۳۸۴، ۴۱)، (سماواتی پیروز، ۱۳۸۴، ۱۲۶ و ۱۲۷) و (میرمحمد صادقی، ۱۳۸۱، ۱۰۰).

۵. پیشگیری وضعی در بوته جرم شناسی نظری

در این مبحث نظریات جرم شناختی مرتبط با جرایم سایبری و پیشگیری وضعی از این جرایم بررسی و توضیح داده شده است.

۵-۱ نظریه معاشرت های ترجیحی

این نظریه که از سوی ساترلند مطرح شده، بیانگر این است که جنایات و انحراف از طریق انتقال فرهنگی در گروه اجتماعی آلوده به فساد فرا گرفته می‌شود یا رخ می‌دهد

---

۲۴ subnormal

(بیات و همکاران، ۱۳۸۷). بیشتر رفتارهای بزهکارانه، درون گروه‌های نخستین، به ویژه گروه همسالان آموخته می‌شود (گیدنز، ۱۳۷۸). این نظریه بیان می‌کند که یک شخص در مقطع معینی از زمان با گروه‌ها یا محیط‌های مختلفی در تماس است. به عبارت دیگر؛ یک شخص در آن واحد، تعلقات متعددی دارد؛ هم پدر است، هم همسر است، هم مدیر خیریه مسجد است، هم دانشجو و... بدین ترتیب یک فرد در طول زندگی اش از محیط-های مختلفی عبور می کند و با محیط‌ها و تشکل های مختلفی تماس دارد. این تشکل ها و محیط‌ها هر یک مرام خاص خود را دارند که فرهنگ آن گروه را تشکیل می‌دهد. حال با توجه به اینکه فرد با هریک از این تجمعات و تشکل‌ها تماس دارد، می‌توانیم بگوییم که یک فرد همواره در معرض مرام‌های مختلف متعددی قرار دارد. کافی است که فرد با محیط‌ها و تشکل‌هایی رابطه داشته باشد که آن تشکل‌ها و محیط‌ها مجرمانه باشند و انجام اعمال نابهنجار و مجرمانه را تا حدی، مطلوب و آرمان خود بدانند. در اینجاست که فرد مرتبط با این محیط می‌تواند تحت تأثیر آن مرام و فرهنگ، ارتکاب جرم را فرا گیرد. مطابق این نظریه، فرد مجرم به جای تبعیت از آموزش‌های محیط سالم، از آموزش های محیط مجرمانه تبعیت می‌کند و آنچه محقق می‌شود، فرایند یادگیری و آموزش پدیده بزهکاری است که این در قالب تقلیدهای ترجیحی است. البته ساترلند معتقد است که اکثر افراد یک جامعه در ارتباطشان از تشکل‌هایی تبعیت می‌کنند که در مقام مذمت و منع ارتکاب جرم فعالیت می‌کنند، مخالف ارتکاب جرم هستند و درستی را ترویج می کنند. به همین جهت، اکثر افراد مرتکب جرم نمی‌شوند و این قبیل افراد در اولویت‌شان انجام مرام ها و باورهای تشکل های سالم و درست را قرار می‌دهند. نهادهای مذهبی، یکی از مصادیق تشکل‌های سالم و درست است که براساس مسائل اعتقادی و باورهای دینی افراد جامعه ما شکل گرفته و پناهگاهی امن برای جوانان ما محسوب می‌شوند. بسیاری از صاحب نظران با توجه به تحقیقات و پژوهش‌های انجام شده در جهان معتقدند که تشکل های مذهبی و اصولاً افرادی که در این گروه ها فعالیت می کنند، کمتر دچار بحران‌هایی چون بحران هویت می‌شوند و کمتر در میان ایشان بزه‌های اجتماعی گسترش یا رواج می یابد (کاویانی،۱۳۹۴، ۵۸). لذا روابط و ارتباطات می تواند افراد را به ارتکاب جرایم سایبری سوق دهد. برای مثال وقتی که در بین دانشجویان رشته کامپیوتر مرتکب

جرایم سایبری بشوند ممکن هست این مساله باعث شود بقیه نیز تمایل به این جرایم و به عبارتی یاد گرفتن متدها و روش های ارتکاب آن داشته باشند.

۲-۵ نظریه فشار ساختاری مرتن

به نظر مرتن[۲۵]، ساخت‌های اجتماعی فشارهای خاصی بر برخی افراد وارد می‌کند و آنها را وامی‌دارد که به کارهایی که از نظر جامعه نیز مجرمانه است اما سبب بقای فرد می‌شود دست یازد. مرتن این فشار را ناشی از عدم دستیابی به اهداف مقبول اجتماعی می‌داند، نظر مرتن این است که جامعه فرد را به کج رفتاری مجبور می‌کند به بیان خود او، کج رفتاری حاصل فشار های ساختاری– اجتماعی خاصی است که افراد را به کج رفتاری وا می دارد. مرتن فاصله میان اهداف فرهنگی و راه‌های نهادی شده برای نیل به اهداف را زیربنای افزایش آمار جرم می‌داند (سخاوت، ۱۳۸۱، ۵۹).

برخی از محرومیت ها و فشارهای اجتماعی و چالش های موجود در جرایم سنتی، سبب می شود برخی از افراد تمام توان خود را در دنیای دیجیتال بکار گرفته و در راستای جرایم سایبری قدم بر دارند، به طوری که برخی موارد گزارش شده برخی افراد به علت اینکه مثلا والدین در تامین نیازهای آن ناتوان بوده اند و از طرفی برخی همسالان شرایط خیلی بهتر مالی نسبت به آنها داشته اند سبب شده به هک سیستم بانکی و سرقت سایبری و... روی آوردند.

۳-۵ جایگاه نظریه خرده فرهنگی

تلاش آلبرت کوهن برای حل این مسئله بود که چگونه خرده فرهنگ بزهکاری آغاز می‌شود او دریافت که رفتار بزهکارانه اغلب در میان طبقات فرودست جامعه دیده می‌شود و بزهکاری ولگردان رایج‌ترین شکل آن به حساب می‌آید. به نظر کوهن، شکل‌گیری خرده فرهنگ بزهکار، نتیجه شرایط خانوادگی و اجتماعی خاص است که کودکان به هنگام رشد در محیط فقیر نشین با آن مواجه می‌شوند، در حقیقت فشار خرد کننده‌ی فقر عامل اصلی ایجاد رفتارهای بزهکارانه است. کوهن به این مسئله اشاره می‌کند که خانواده‌های فرودست جامعه قادر به تعلیم و تربیت صحیح فرزندان خود نیستند و در نتیجه کودکان و

---

۲۵ Merton

نوجوانانی به جامعه تحویل می‌دهند که فاقد مهارت‌های لازم جهت نیل به موفقیت‌های اجتماعی و اقتصادی هستند. با توجه به موضوع پژوهش حاضر خرده فرهنگ بزهکاری در مدارس هم می‌تواند شکل گیرد که می‌توان گفت این خرده فرهنگی به این صورت ممکن است که وقتی گروهی از دانش‌آموزان کنار هم جمع می‌شوند و یا یک گروه دوستانه را بوجود می‌آورند ممکن است این گروه به برخی از بزهکاری‌ها در کنار هم روی آورند (سخاوت،۱۳۹۱). خرده فرهنگ های بزهکارانه می توانند در بزهکاری سایبری موثر باشند برای مثال جمعی از افراد که در یک کافی نت و یا گیم نت جمع می شوند، می تواند سبب انتقال تجربیات بزهکارانه سایبری به سایرین نیز شوند.

۴-۵ نظریه‌های یادگیری اجتماعی

نظریه یادگیری اجتماعی معتقد است بزهکاری یک رفتار اکتسابی است و تمامی ابعاد آن، روش‌ها و نگرش‌های مجرمانه، از طریق روابط نزدیک با دیگران فرا گرفته می‌شود (معظمی ،۱۳۸۷، ۱۸۱). به خصوص در گروه‌های کوچک اندیشمندانی نظیر باندورا، سادرلند و تارد نظریه یادگیری اجتماعی را توسعه دادند (احمدی،۱۳۹۶، ۹۴). گابریل تارد۲۶ (۱۹۰۴-۱۸۴۳) تئوری تقلید را برای توضیح انحراف مطرح کرد. تارد شدیداً تحت تأثیر این مسأله قرار گرفته بود که تکرار چه نقش چشم‌گیری در رفتار انسان بازی می‌کند. او می‌گوید که مجرمین نظیر آدم‌های «خوب» شیوه‌های افرادی را که ملاقات کرده، شناخته یا درباره‌شان شنیده‌اند، تقلید می‌کنند ولی برعکس مردمی که تابع قانون هستند آنها از دیگر مجرمین تقلید می‌کنند. براساس نظریه‌ی تقلید (گابریل تارد) بزهکاران رفتار کسانی را که دوست دارند و برای آنها احترام قائلند دوست دارد از این رو انحراف والدین می‌تواند تاثیر بسزایی بر فرزندانشان داشته باشد. با توجه به نظریه فوق مثلاً در مدارس نیز یادگیری اجتماعی علاوه بر اینکه نقش مثبتی در تعلیم و تربیت ایفا می‌کند می‌تواند به بزهکاری سایبری نیز منجر شود، چرا که ممکن است بزهکاری سایبری در مدارس بزهکاری را از دیگر دانش‌آموزان که بزهکار هستند و گاهی مورد تشویق و تحسین سایر قرار می‌گیرند تقلید کنند.

---

۲۶ Gabriel Tard

۵-۵ نظریه انتقال فضا

نظریه انتقال فضا یا نظریه جابه جایی مکانی به عنوان یک نظریه اختصاصی جرایم سایبری در سال ۲۰۰۷ توسط جایشانکار مطرح شد. وی در این نظریه فرآیندی چرایی و چگونگی جرم سایبری را تبیین می کند. این نظریه عامل اصلی جرم سایبری را در تغییر محیط می بیند. به باور جایشانکار افراد وقتی به دنیایی با ویژگی‌های منحصر به فرد نظیر سایبر وارد می شوند به گونه‌ای متفاوت رفتار می کنند که همین رفتار به بزهکاری و بزه دیدگی شهروندان سایبری می انجامد. مؤلفه های هفت گانه این تئوری شامل: «سرکوب مرتکب در فضای فیزیکی»، «انعطاف پذیری هویت»، «نفوذ رفتارهای مجرمانه در دو فضا»، «ماهیت زمانی مکانی خاص»، «تأثیر و تأثر دو فضا»، «محدودیت های اجتماعی»، «تعارض های هنجاری دو فضا» می شود (سلیمی،۱۳۹۷، ۵۱). به نظر می رسد با در نظر گرفتن اینکه بویژه در دهه های اخیر با پیشرفت و توسعه خیلی سریع اینترنت و به عبارتی تغییر از مکان سنتی و فیزیکی به فضای سایبر زمینه های جرایم سایبر را فراهم آورد، البته می توان به خلاء فرهنگ استفاده از فضای سایبر نیز اشاره کرد که نتوانست با سرعت همزمان با پیشرفت اینترنت توسعه یابد.

۶- آسیب شناسی چالش های ناظر بر ساختار فضای سایبر و موارد فنی

۱-۶ کثرت محتواهای مجرمانه در فضاهای عمومی سایبر

با وجود فعالیت های نظارتی پلیس فتا و گشت زنی های مستمر این نیروها، کماکان فضاهای مجرمانه بسیاری وجود دارد که توسط پلیس مورد توجه قرار نگرفته است؛ به نظر می رسد هم پوشی فعالیت پلیس و کمیته تعیین مصادیق محتوای مجرمانه در این مسئله به کثرت محتواهای مجرمانه ای که نه مورد پالایش محتوا قرار گرفته اند و نه با رصد نیروهای پلیس و اقدامات نظارتی، بزهکاران شناسایی و ادامه فعالیت آنها متوقف شود، دامن زده است. همچنین بعضی از فضاها و سایت های توهین به مقدسات یا محتواهای هرزه نگاری، به جهت آن که از خارج از کشور و در کشورهایی که پلیس با آنها همکاری ندارد، اداره می شوند، امکان شناسایی و دستگیری مدیران آنها وجود ندارد و این موضوع از آن جهت که موجب تجری مرتکبان و ایجاد محیطی نا امن در فضای

مجازی ایران شده است، موضوعی قابل انتقاد است (سلیمی،۱۳۹۷، ۱۴۳). لذا با توجه به اینکه فضای سایبری بی انتها و بی عبارتی بهتر وسیع است کنترل و بررسی تمام محتوا در جهت پیشگیری از جرایم سایبری غیر ممکن و به عبارتی سخت است.

۶-۲ محدودیت های ناشی از فضای سایبر

یکی از چالش ها و آسیب های پیش روی پیشگیری پیشگیری وضعی در پیشگیری از جرایم سایبری محدودیت های ناشی از فضای سایبری است یکی از این محدودیت ها بحث حریم خصوصی است که باعث می شود نظارت بر فضای سایبری محدود شود از دیگر محدودیت ها می توان به گسترده بودن فضای سایبری اشاره کرد که پیشگیری را با چالش مواجه می کند. به هر حال ذات و ماهیت فضای مجازی و دسترسی نامحدود به آن پیشگیری وضعی از جرایم سایبری را سخت و پر هزینه می کند.

۶-۳ فراملی بودن جرایم سایبری

این جرم یک جرم مدرن است. مدرن بودن این جرم ابزاری را در اختیار مجرم قرار می دهد که در جرایم سنتی وجود ندارد برای مثال، مجرم می تواند از اتاق خواب خود، سیستم های امنیتی یا اطلاعاتی کشورهای دیگر را تخریب یا تهدید کند و در عین حال در مدت زمان بسیار کوتاهی مرتکب چندین جرم مجزا شده و خسارات قابل ملاحظه ای به بار آورد. در جرایم رایانه‌ای حضور مجرم در محل وقوع جرم لازم نیست. این امر وقوع جرایم فراملی در این جرایم را بالا برده است (سروش، ۱۳۹۳، ۱۲۱). این امر البته بدان معنا نیست که تمام جرایم این حوزه فراملی هستند بلکه تنها درصد جرایم فراملی در این حوزه بالاتر است (فهیمی، ۱۳۸۰، ۱۳۱). البته، مفهوم مرزهای ملی در عرصه فضای مجازی معنا ندارد و در واقع فضای مجازی اصلا مرزی ندارد. بحث از فراملی بودن این جرایم تنها در تطبیق جرایم این حوزه با مفاهیم رایج حقوقی بالاخص مفهوم مرز است (باستانی، ۱۳۸۳، ص ۱۳۰). بنا به طبع این جرایم و فراملی بودن این دسته از جرایم، اعمال صلاحیت دولت ها در این عرصه پیچیدگی های خاصی دارد. مرزها در فضای مجازی با مفهوم مرز در فضای واقعی یکسان نیست. مرزهای فیزیکی مبتنی بر مکان هستند و عامل اصل در آنها جغرافیا است اما در مرزهای مجازی، اصولا مفهوم مکان و

جغرافیا وجود ندارد (محوری، ۱۳۸۶، ۹۷). اصولا رشد اینترنت و گسترش مفهوم فضای مجازی، مرزها را بدان شکل شناخته شده فیزیکی از بین برده است و حتی کشورها را در اعمال حقوق نقش تعیین کننده دارند. اعمال سلطه یک کشور در داخل مرزهایش صورت می گیرد و از سوی دیگر اعمال قوانین جزایی کشور عموما بستگی تام و تمام با مرزهای کشور دارند. هر کشور تا جایی می تواند صلاحیت حقوقی یا جزایی خود را اعمال نماید که مرزهایش گسترده است. از سوی دیگر اعمال صلاحیت های حاکمیتی هم در اینترنت با مشکل مواجه است دقیقا به همین دلیل که مرزی وجود ندارد تا حیطه صلاحیت دول را از یکدیگر جدا کند. از همین رو، قدرت کنترل فعالیت ها در فضای مجازی کمترین ارتباطی به موقعیت فیزیکی ندارد. بسیاری از کشورها در برخورد با ارتباطات الکترونیکی که از مرزهای سرزمینی آنها عبور می کند از طریق متوقف کردن یا قاعده مند کردن جریان اطلاعات پاسخ داده‌اند (باستانی، ۱۳۸۳، ۱۲۹). بحث فراملی بودن فضای سایبری جرایم بین المللی و فرا ملی را به دنبال دارد که اولاً هیچ متولی بین المللی برای پیشگیری از آن وجود ندارد و از طرفی برای مثال فردی که در کشور فرانسه مستقر است ممکن است از آنجا بدون نیاز به حضور جرایمی را در ایران مرتکب بشود که این مساله فرا ملی بودن پیشگیری را با چالش مواجه می کند.

۷-آسیب شناسی تدابیر فنی پیشگیرانه وضعی در جرایم سایبری

۷-۱ کمبود تجهیزات و امکانات پلیس

شاید اگر به گوییم وسایل، امکانات و تجهیزاتی که می بایست در اختیار پلیس به خصوص آن دسته از پرسنل نیروی انتظامی که مستقیما در سطح شهر با مردم در تماس هستند، به گشت زنی مشغولند و از وقوع جرایم پیشگیری می کنند، قرار گیرد. بسیار کمتر از میزان ایده آل و مطلوب است که پلیس پیشگیری بایستی به آنها مجهز باشد بر اساس واقعیات موجود اظهار نظر کرده ایم البته ممکن است وسایل و امکاناتی که در رده های فرماندهی و مدیریت مورد استفاده قرار می گیرد مجهز و سالم و مرتب باشد از قبیل اتومبیل های فرم و نیز ساختمان ها، میزها، بی سیم ها و تلفن مانند آن اما این امکانات در رده های پایین سازمان بخصوص کلانتری ها و پاسگاه ها که عمدتا بعنوان پیشگیری

کننده از جرایم و بزهکاری محسوب می شوند، موجود نیست (گرکی، ۱۳۸۹، ۲۶۵). هم چنین لازم به ذکر است با توجه به سیالیت و پیشرفت روز افزون در حوزه اینترنت و تدابیری که مجرمان سایبری به کار می برند پلیس نیز باید از امکانات و ابزارهای لازم برای مقابله با جرایم سایبری و پیشگیری از آن برخوردار باشد این در حالی است که پلیس از امکانات لازم برخوردار نیست و این چالش بزرگی در پیشگیری از این جرایم است.

۲-۷ عدم تخصص کافی مراجع قضایی و انتظامی

از جمله چالش‌ها و خلأهای مهم موجود در این حوزه، نداشتن تخصص کافی مراجعی است که به تعقیب، کشف و رسیدگی ماهوی این جرایم می پردازند. عدم آشنایی بازرسان و قضات با رسانه های اطلاعاتی و ضعف آنها در برخورد با مسائل فنی جرایم سایبری عاملی است برای تشدید هر چه بیشتر مشکلات موجود. البته با عنایت با ماهیت نوین این جرایم، این مسأله چندان تعجب آور نیست. بسیاری از اقدامات و تلاش های صورت گرفته در بسیاری از کشورهای فاقد ساختار کیفری مناسب فضای سایبر، برای تعقیب مجرمان متوقف شده و شکایات بسیاری در این زمینه رد شده و احکام بسیاری صرفا در خصوص جنبه های حقوقی دعاوی صادر شده است که همه این امور بیانگر عدم تمایل مجریان قانون به مواجهه با مشکلات خاص پرونده های مطرح شده است، این مسأله باعث می شود که تعقیب و کشف این جرایم با مشکل مواجه شود و دادگاه ها نیز نتوانند به نحو شایسته به جرایم مزبور رسیدگی نمایند (طهماسبی و شاهمرادی،۱۳۹۷، ۱۰۶).

جرایم سایبری آن گونه که از نام آنها برمی آید، در فضای سایبری روی می دهند و بر خلاف جرایم سنتی، به جای آنکه شواهد حاصل از آن در بستر مادی، فیزیکی و ملموس باشند، دیجیتالی، شکننده و پیچیده می باشند. پیچیدگی آنها از این جهت است که رمزگشایی از این دلایل به مراتب بیش از سایر جرایم به تخصص، آموزش و مهارت نیازمند است. همچنین شکننده اند چون تعلل و تساهل مأمورین تحقیق در ضبط، نمونه برداری و نگاهداری آنها ممکن است برای همیشه آنان را از شناسایی بزهکار مأیوس سازد (تراب زاده،۱۳۸۸، ۷). زیرا دلایل دیجیتالی می تواند توسط مرتکبان به انحاء مختلف به سرعت از بین رود. از همین رو است که قانون گذار در موارد اضطراری یعنی مواقعی که

داده ها را خطر آسیب، تغییر، دست کاری و از بین رفتن تهدید می کند، حفاظت فوری از این شواهد را حتی بدون دستور مقام قضایی مجاز دانسته و برای مستنکف مجازات تعیین نموده است (طهماسبی و شاهمرادی،۱۳۹۷، ۱۰۷). در این رابطه لازم به ذکر است بویژه در ایران ضابطان از تخصص و دانش کافی در رابطه با جرایم سایبری برخوردار نیستند بلکه به نوعی همان پلیس های معمولی هستند و ممکن است دوره های کوتاه مدت در رابطه با جرایم سایبری و فضای سایبری را دیده باشند، لذا عدم تخصص ضابطان قضایی و پلیس فتا نیز یکی از چالش ها در رابطه با پیشگیری وضعی از جرایم مذکور است.

۸- چالش های حقوق بشری پیشگیری وضعی از جرایم سایبری

پیشگیری وضعی، در واقع، تغییر سبک زندگی، کار و حضور اجتماعی افراد، تغییر ساعات فعالیت روزانه، صرف‌نظر کردن از برخی علاقه‌ها و آرزوها را می‌طلبد؛ یعنی صرف‌نظر کردن افراد از برخی حقوق و آزادی‌هایشان که تحت تأثیر تدابیر وضعی، محدود و یا حتی از میان می‌روند؛ تدابیری که می‌توانند هرگونه تحرک و یا حتی هر نوع اندیشه‌ای را با تجهیزات قوی نظارتی الکترونیکی و پیشرفته شناسایی و کنترل کنند (نجفی ابرندآبادی، ۱۳۸۸، ۵۸۲). به عبارت دیگر، پیشگیری وضعی مستلزم اقدامات و تدابیری است که خلوت افراد و زندگی انسان‌ها را تحت‌الشعاع خود قرار می‌دهد. بدین‌ترتیب، پیشگیری وضعی خطر تجاوز به حریم خصوصی و خلوت افراد را که مورد حمایت مادۀ ۱۲ اعلامیۀ جهانی حقوق بشر۲۷ و مادۀ ۱۷-۱ میثاق بین‌المللی حقوق مدنی و سیاسی است، به دنبال داشته و ممکن است آثار نامطلوبی برای حقوق و آزادی های افراد به بار آورد.

اندیشه ی رعایت حقوق بشر قدمتی به درازای تمدن انسانی دارد؛ اندیشه ای که پس از جنگ جهانی دوم به اوج خود رسید؛ حکومت ها نیز در تلاشند با منطبق کردن

---

۲۷ – احدی نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه و مکاتبات خود مورد مداخله‌های خودسرانه واقع شده و شرافت و آبرویش مورد تعرض قرار گیرد.

اقدامات خود، از مقررات حقوق بشری تبعیت نمایند. این مسأله در مواردی که حقوق افراد در میان باشد، نمود بیشتری می یابد. به شرح آتی محدودیت های حقوق بشری اجرای تدابیر پیش گیرانهی وضعی بررسی می شود.

۱-۸ حریم خصوصی و چالش های نظارت

ارتباط تنگاتنگی جرایم سایبری با استفاده از اطلاعات شخصی و محرمانه، حریم خصوصی اشخاص، به طور مستقیم و غیر مستقیم، آماج فعالیت های غیر قانونی قرار می گیرد. بنابراین، اتخاذ راهکارهای پیشگیرانه مؤثر و روز آمد در این راستا از مهم ترین پیش نیازهای توسعه در جامعه اطلاعاتی است. اگر چه فناوری اطلاعات، معمولا یکی از عمده ترین دلائل نقض حریم خصوصی تلقی می گردد، راه های گوناگونی نیز وجود دارد که از طریق آن ها این فناوری، خود قادر به حمایت از محرمانگی و پیشگیری از نقض آن می باشد. امروزه رهنمودها و شیوه های محافظت از حریم خصوصی که به روش های علمی طراحی شده اند مورد استفاده قرار می گیرند. این امکانات، طیف وسیعی از تمهیدات و راهکارها از روش شناسی های طراحی شده بر مبنای اطلاع رسانی اخلاقی تا رمزنگاری به منظور محافظت از اطلاعات شخصی در مقابل استفاده غیر مجاز را در برمی گیرد (محسنی، ۱۳۹۵، ۹۳).

اجرای تدابیر پیشگیرانه وضعی، همانند بسیاری از سایر تدابیر پیشگیرانه، ممکن است محدودیت هایی ایجاد کند. از این رو، هدف پیشگیری، نمی تواند کاربرد هر وسیله، فن، اقدام و روش های خاص فراقانونی شود (نجفی ابرند آبادی، ۱۳۸۲، ۵۶۷). در بند دوم و سوم اصل ۲۶ «رهنمود پیشگیری از جرم سازمان ملل متحد سال ۲۰۰۲ به بهره گیری از تدابیر پیشگیری وضعی که به قابلیت و بدنه ی محیط اجتماعی لطمه وارد نکند و دسترسی آزاد به مکان های عمومی را محدود ننماید، تأکید شده است. در ارتباط با بند ۱ لازم به توضیح است که از نظر فنی و تخصصی، ممکن است با کاربرد تدابیر پیشگیری وضعی در فضای سایبری، شاهد برخی اختلالات همچون کاهش سرعت شبکه، بسته شدن اشتباهی برخی از سایت ها و وبلاگ ها به جهت پالایه، محدودیت های بی جهت برای ورود به برخی فضاها، اعمال محدودیت در دسترسی به شبکه های بین المللی و غیره بود. نتیجه ی اعمال این شرط رهنمود، بهره گیری از رویکردی سنجیده و ملایم تر

نسبت به ممنوعیت کامل شبکه های اجتماعی مجازی، مسئله ی پالایه و افزایش دقت و هوشمندی سامانه های پالایه است. بند ۲ این رهنمود نیز با تفویض تصمیم گیری به سازمان ها، نهادها یا اشخاصی که صلاحیت قانونی چنین امری را دارند یا بر روند و نحوه اجرا این گونه تدابیر نظارت مستقیمی دارند قابل اجرا است (محسنی و صوفی زمرد،۱۳۹۶، ۱۷۳). لذا مباحث حقوق بشری یکی از موانع پیش روی پیشگیری از جرایم سایبری است، که از مهم ترین آنها می توان به آزادی اطلاعات، حریم خصوصی و اصل براعت و... اشاره کرد.

۸-۲ فیلترینگ به مثابه ابزار سانسور

باید اذعان داشت پالایش محتوا در ایران، دسترسی آزاد به اطلاعات را با مخاطرات جدی مواجه ساخته است. رصد و فراتحلیل گزارش ها و پژوهش های مختلف داخلی و خارجی حکایت از پایمال شدن این شعبه از حق آزادی دارد. قطع نظر از محتواهای منافی عفت و مستقیم مجرمانه نظیر تارنماهای اشاعه خشونت، نفرت و خرید و فروش مواد مخدر و برخی موارد این چنینی که پالایش فضای مجازی از آنها مورد وفاق نسبی جامعه است، برخی شبکه های اجتماعی محبوب نظیر فیس بوک و تلگرام و ابزارهای نمایشگر عمومی مانند یوتیوب در ایران مسدود و بدون استفاده از ابزارهای فیلترشکن غیر قابل دسترس هستند (سلیمی،۱۳۹۷، ۸۳). همانطوری که قبلاً گفته شد فیلترینگ یا محدود کردن دسترسی یکی از راهکارهای پیشگیری وضعی در پیشگیری از جرایم سایبری است و از طرفی فیلترینگ نیز ضد حقوق بشری به مثابه جلوگیری از دسترسی به اطلاعات و به عبارتی سانسور بر فضای مجازی است که این مساله پیشگیری وضعی از جرایم سایبری را با مانع مواجه می کند.

۸-۳ تقابل پیشگیری وضعی از جرایم سایبری با آزادی بیان و جریان آزاد اطلاعات

از آنجا که این دو اصل از لحاظ ماهیت تقریبا مشابه یکدیگرند و حتی می توان آنها را لازم و ملزوم یکدیگر برشمرد و چون تدابیر پیشگیرانه از جرایم سایبر به یک شکل به آنها

تعرض می کنند، در اینجا با یکدیگر بررسی خواهند شد. همان گونه که اشاره شد، ماهیت آزادی بیان به گونه ای است که باید دیدگاهها و عقاید افراد بدون محدودیت در اختیار همگان قرار گیرد. این مبنا کاملا با آنچه فضای سایبر فراهم می آورد منطبق است و حتی زمینه های شکوفایی آن به مراتب فراتر از آنچه تصور می رفت به وجود آمده است. از سوی دیگر، تدابیر محدود کننده یا سلب کننده دسترس، به ویژه فیلترینگ، مانع بزرگی در تحقق این اصل محسوب می شوند، زیرا از جریان آزاد اطلاعات جلوگیری می کنند. دلایل مختلفی باعث ایجاد محدودیت از سوی این ابزارها می شود (جلالی فراهانی،۱۳۸۴، ۱۵۲). همانطوری که قبلاً اشاره شد برخی از تدابیر پیشگیری وضعی آزادی بیان، آزادی اطلاعات و آزادی گردش اطلاعات را محدود می کند که برخلاف رویه ها و حق های حقوق بشری است.

۹. چالش های جرم شناختی پیشگیری وضعی از جرم

از دیدگاه جرم شناختی، پیشگیری وضعی با محدودیت هایی مواجه است که در عمل موجب عدم کارایی آن شده است. این محدودیت های جرم شناختی را می توان در از دیدگاه جرم شناختی، پیشگیری وضعی با محدودیت هایی مواجه است که در عمل موجب عدم کارایی آن شده است. این محدودیت های جرم شناختی را می توان در برخورد محافظه کارانه و سطحی با جرم، عدم جامعیت آن در تحت پوشش قرار دادن تمام جرایم، فرصت مدار بودن و مواردی از این قبیل مشاهده نمود که بدان پرداخته می شود.

۹-۱ مقابله محافظه کارانه با جرایم سایبری

بسیاری از منتقدان معتقدند: پیشگیری وضعی، اذهان را از ریشه و علل اصلی جرم منحرف نموده است، لذا این تدابیر را به اقدام محافظه کارانه با جرم، با رویکردی اداری متهم کرده اند. این انتقادات با عنوان «جرم شناسی های اداری» و در تحقیقات وزارت کشور انگلستان ریشه دارد. به عبارت دیگر، این نوع پیشگیری به جای این که توجه خود را به ریشه یابی علل جرم و بزهکاری در جامعه معطوف نماید و با شناسایی این عوامل و

زمینه ها، سیاست جنایی مناسب را در قبال آنها، در پیش گیرد، به گونه ای دیگر اقدام نموده و رو به اقداماتی موقتی می آورده و راه کارهایی را پیشنهاد می نماید که ممکن است ارتباط چندانی با کاهش جرم نداشته باشد. به واقع در این شیوه ی پیشگیری از جرم، دست اندرکاران و مجریان، در مقام ریشه یابی علل و عوامل جرم نبوده، بلکه همواره در تلاشند با ارائه ی راه کارهایی برای ارتکاب جرم، مانع ایجاد نمایند و به تعبیری ارتکاب جرایم و نرخ آن را به گونه ای که برای جامعه قابل تحمل باشد، مدیریت کنند (بابایی و نجیبیان،۱۳۹۰، ۱۵۲).

۲-۹ فرصت مدار بودن پیشگیری وضعی از جرایم سایبری

موقعیت مدار بودن نیز ایرادی است که بر پیشگیری وضعی مترتب میشود؛ این موضوع با دامنه ی شمول و قلمرو اجرای این نوع پیشگیری مرتبط است. به نظر برخی از جرم شناسان، رویکرد وضعی، فقط جرایمی را در بر می گیرد یا به عبارت دقیق تر در خصوص جرایمی قابل اعمال است که فرصت مدار یا به تعبیری موقعیت مدار هستند؛ در حالی که بسیاری از جرایم شدید و خشونت آمیز بیش از آن که «فرصت مدار» باشند، تابع احساسات و کشش های درونی اند به طور کلی، فرصت مدار بودن در پیشگیری وضعی، دو مفهوم را با خود به همراه دارد؛ نخست این که، همه‌ی جرایم فرصت مدارند؛ بدین معنی که بزهکار در مسیر رسیدن به قصد مجرمانه‌ی خویش، در فرصتی مناسب اقدام خود را عملی می نماید؛ بنابراین ایراد مذکور منتفی به نظر می رسد. در این مفهوم، فرصت مداری بدین معنی است که ارتکاب جرم در کنار وجود مرتکب مصمم، به وجود یک هدف یا آماج بدون دفاع یا محافظ نیز نیاز دارد؛ بنابراین همه ی جرایم فرصت مدار هستند. اما آن چه مقصود خدشه کنندگان به رویکرد پیشگیری وضعی است، معنی دیگر فرصت مدار بودن یعنی همان مفهوم کسب سود مادی است. مقصود آن گروه از جرایمی است که ارتکاب آنها نوعا تابع به وجود آمدن فرصت مناسب در معنی جذب سود (عموما مادی) و خطر کمتر برای مرتکب است به بیان دیگر پیشگیری وضعی جرایمی را شامل می شود که بر سود و زیان مبتنی بوده و یا لااقل سود و زیان در آنها نقشی تعیین کننده دارد، در حالی که جرایمی که نه به انگیزه ی مالی بلکه به دلایل حیثیتی رخ می دهد، به

دلیل این که بر پایه ی سود و زیان حاصل از جرم استوارند، اعمال تدابیر پیش گیرانهی وضعی برای آنها امکان پذیر نمی باشد (بابایی و نجیبیان،۱۳۹۰، ۱۵۶).

بر پایه این ایراد گفته می‌شود که پیشگیری وضعی تنها دربارۀ جرم‌های فرصت‌مدار۲۸ کارآیی دارد که در آنها «سودمندی» بیش از هرچیز دیگر مهم است؛ در حالیکه بسیاری از جرایم شدید و خشونت‌آمیز بیش از آنکه «فرصت‌مدار» باشند تابع احساسات و کشش‌های درونی هستند.

۳-۹ عدم شمول همه ی آماج ها

شاید این ایراد پیشگیری وضعی از ساده بودن و یا به تعبیر دیگر ناکافی بودن اقدامات پیشگیرانهی وضعی با توجه به فن آوری های نوین و مسائل جدید ناشی می‌شود؛ چرا که اقدامات پیشگیری وضعی فقط آماجها یا موضوعاتی را شامل می شود که در عالم خارج و به شکل ملموس وجود داشته باشد و در خصوص آماج های معنوی، مانند شخصیت و یا حق طبع، راهکاری را عرضه نمی کند.

به طور کلی، آماج در پیشگیری وضعی دارای دو مفهوم است. در مفهوم نخست، اشیاء را شامل می شود و در مفهوم دوم، افراد نوع بشر را مدنظر دارد «آماج‌ها- موضوع ها» یا حتی وسایل، از این جهت، به دو گروه عمده تقسیم می شوند: آماج های مادی مانند پول یا جسم اشخاص و آماج های فکری یا معنوی که طیف متنوعی چون کرامت شخص، خلوت و زندگی خصوصی، حیثیت او یا در مقوله ای کاملا متفاوت، اطلاعات، آفرینش های فکری و غیره را در بر می گیرد (صفاری، ۱۳۸۰، ۳۰۱).

بر این اساس، پیشگیری وضعی در خصوص آماجهای معنوی مانند شهرت و مسائلی این چنینی راه حلی ندارد. در همین راستا برخی از منتقدان این ایراد کلی را مطرح کرده اند که اصولا ارزش های اخلاقی و آماج های غیرمادی در تدوین و ارائه ی این روشها کاملا نهادینه نشده اند و عدم کارایی در آنها مشهود است (بابایی و نجیبیان،۱۳۹۰، ۱۵۷).

---

۲۸ - opportunistic crimes

۹-۴ جابه جایی جرایم سایبری

پیشگیری وضعی از جرایم سایبری بر این دیدگاه مبتنی است که رفتار مجرمانه با گسستن یک حلقه از زنجیره‌ی حوادث و وقایع، قابل خنثی شدن است. بر این اساس، در صورتی که در نتیجه‌ی اتخاذ تدابیر وضعی، جرمی خنثی یا عقیم شود، این اطمینان خاطر وجود ندارد که مجرم بالقوه، برای ارتکاب جرم به دنبال فرصت دیگر در جای دیگر نخواهد رفت. تدابیر اتخاذی از سوی این نوع پیشگیری، سبب جابه جایی فعالیت های مجرمانه در مکان، شیوه ی ارتکاب و نوع جرم می شود. این نتیجه ممکن است موجب دلخوشی شهروندان در حفاظت از اموال خود یا اشخاص گردد، اما برای سیاست گذارانی که هدف آنها کاهش وقوع جرم در جامعه است، چندان خوشایند نیست؛ جابه جایی جرم موجب شده است طرفداران پیشگیری وضعی با انتقاد مواجه شوند (بابایی و نجیبیان،۱۳۹۰، ۱۶۰).

ایراد پیشگیری وضعیت‌مدار به «پدیدهٔ جابه‌جایی جرم» مربوط است. یعنی، تقویت آماج‌های جرم و حفاظت از آنها سبب می‌شود که بزهکاران ــ به‌ویژه، حرفه‌ای‌ها ــ با تغییر هدف‌های خود به هدف‌های محافظت نشده یا کمتر تقویت شده رو آورند. این تغییر و جابه‌جایی ممکن است در مکان، زمان یا آماج ارتکاب جرم باشد. همچنین، جابه‌جایی ممکن است در نوع جرم ارتکابی رخ دهد. (صفاری، ۱۳۸۱، ۲۰۵).

۹-۵ عدم شفافیت برخی عبارات قانونی در رابطه با جرایم سایبری

یکی از فروعات اصل قانونمندی عنصر شفافیت قانون است؛ برخی از نصوص در فهرست مصادیق مجرمانه، غیر شفاف و تأویل پذیر هستند. برای مثال عباراتی مانند مخالفت با اسلام (شماره ۴ از بند ب) تشویش اذهان عمومی و سیاه نمایی (شماره ۱۴ از بند ح) با شفافیت و روشنی در مصادیق خود که مقتضای اصل مذکور است، همراه نیست. حتی برخی از نصوص قانونی، نظیر تعابیر محتوای ناشی از جرایم رایانه ای یا محتوایی که برای ارتکاب جرایم رایانه ای به کار می روند ذکر شده در مواد ۷۴۹ و ۷۵۱ تعابیر بسیار پوشیده ای هستند که از نکته های نافهمیدنی این قانون به شمار می آیند. عدم شفافیت سبب شده است که عملا گستره فیلترینگ بیش از مواردی که حاوی محتواهای ناشی از جرایم رایانه ای و محتواهایی که برای جرایم رایانه ای به کار می روند، باشد

(سلیمی،۱۳۹۷، ۱۰۲). البته با بازنگری در قوانین و تصویب قوانین می توان این نقص و چالش را برطرف کرد.

۶-۹ افزایش احتمال بزه دیدگی و رقم سیاه جرایم سایبری

استفاده از ابزارهای وی. پی. ان. خارجی و پروکسی ها، علاوه بر آنکه به جهت برقراری یک ارتباط نا امن خطر بزه دیدگی کاربران را به شدت افزایش می یابد، شناسایی و کشف موقعیت جغرافیایی و محتواهای مورد استفاده کاربران با دشواری مواجه می سازد و با افزایش هزینه های کشف جرم، رقم سیاه جرم را بالا می برد. توضیح آن که وی. پی. ان.ها و پروکسی ها با ایجاد یک تونل بین کاربر استفاده کننده از این ابزارها و یک سرور ناشناس در خارج کشور باعث می شوند که در خواست های کاربر استفاده کننده از گذر سرور ناشناس مذکور برای کاربر ارسال شود و با رمزگذاری آن، ارتباط را برای شرکت های ارائه دهنده خدمات اینترنتی غیر قابل فهم نموده و بدون مشکل از آنها رد میشود. سپس آدرس هایی که توسط کاربران استفاده کننده درخواست شده به صورت رمزنگاری شده برای شخص متقاضی ارسال می شود. به این ترتیب از یک سو دسترسی ارائه دهندگان خدمات و به تبع آن پلیس به محتواهای درخواست شده کاربر قطع می شود و به این ترتیب امکان عدم شناسایی جرم بالا می رود و رقم سیاه بزهکاری افزایش می یابد و از سوی دیگر سرور خارج از کشور امکان رصد جزئیات محتواهای تقاضا شده و دسترسی های یک کاربر و به طور کلی کلیه اقدامات کاربر را خواهد داشت و به همین جهت احتمال بزهدیدگی کاربران استفاده کننده از این ابزارها از سوی سرورهای خارجی افزایش می یابد (سلیمی،۱۳۹۷، ۱۱۳). به هر حال رقم سیاه جرایم سایبری بسیار بالا است و در بیشتر مواقع این مساله پیشگیری و تعقیب مجرمان سایبری را با چالش مواجه می کند و از طرفی برخی از تدابیر پیشگیری وضعی از جرایم سایبری باعث می شود احتمال بزه دیدگی و بزهکاری افراد افزایش یابد که از نمونه آنها می توان به نصب وی پی ان ها اشاره کرد که ممکن است برخی از آنها آلوده به انواع ویروس ها باشند و سبب سوء استفاده و سرقت از کاربران باشند.

نتیجه گیری

جرایم سایبری از جمله جرایم است که در دهه های گذشته با ظهور اینترنت و گسترش استفاده از فناوری اطلاعات پا به عرصه ظهور گذاشته و به دلیل ماهیت خاص و ارتکاب آن در فضای سایبری و با توجه به پیچیدگی های مسیر کشف جرم لازم است که از فناوری ها و راهکارهای نوین و به عبارتی راهکارهای متفاوت از جرایم سنتی در کشف و تعقیب مجرمان سایبری بکار گرفته شود، به عبارتی باید راهکارهای پیشگیرانه به راهکارهای سرکوبگرانه و تعقیب اولویت داده شود، لذا در این راستا در پژوهش حاضر نقش پیشگیری وضعی در پیشگیری از جرایم سایبری، چالش ها و مشکلات پیش روی آن بررسی شده است. براساس نتایج تحقیق؛ تدابیر محدود کننده یا سلب کننده دسترسی که از ورود و ارسال داده های غیر مجاز یا غیر قانونی جلوگیری می کنند، که به نوعی موارد را به مجاز و غیر مجاز تقسیم بندی و بعد آن اجازه دسترسی می دهند و هم چنین تدابیر نظارتی که موارد و سوابق مشکوک را مورد بررسی قرار می دهد از جمله تدابیر پیشگیری وضعی هستند، تدابیر صدور مجوز از دیگر تدابیر پیشگیری وضعی از جرایم سایبری است که براساس معیارهای خاص مانند به استفاده از پسورد و... از ورود و دسترسی مجرمان سایبری جلوگیری می کند، ابزارهای ناشناس کننده و رمز گذاری نیز از دستبرد تبهکاران سایبری به داده ها و وقوع جرایم سایبری جلوگیری می کنند، هر چند امکان سوء استفاده از این ابزارها در جهت ارتکاب جرایم نیز وجود دارد. اقدامات پیشگیرانه وضعی پلیس در جرایم سایبری مرتبط با فضای مجازی شامل؛ گشت اینترنتی و رصد فضای سایبری برای شناسایی موارد مشکوک و پیشگیری از جرایم احتمالی، آموزش همگانی برای افزایش آگاهی شهروندان از فضای سایبری و جرایم سایبری از طریق رسانه های مختلف و راهکارهای نوین از دیگر اقدامات پلیس در این رابطه است، یکی دیگر از اقدامات پلیس در این رابطه شناسایی و کنترل افراد خطر ساز است. از اقدامات پیشگیرانه وضعی از جرایم با رویکرد حقوقی و جرم شناختی می توان به برهم زدن معادله جرم در فضای سایبری با افزایش خطر ارتکاب جرم که سبب دشواری ارتکاب جرم، افزایش خطر جرم، کاهش منافع، کاهش تحریک پذیری و حذف بهانه ها می شود، افزایش خطرات ملموس ارتکاب جرم از دیگر راهکارهای وضعی پیشگیری از جرایم

سایبری است که با افزایش خطر ناشی از ارتکاب جرایم سایبری سبب انصراف از جرایم احتمالی می شود، افزایش محافظت ها و مراقبت ها در فضای سایبری نیز سبب پیشگیری از جرایم سایبری و به عبارتی پاین آوردن احتمال و راه های ارتکاب این جرایم می شود.

تدابیرفنی در پیشگیری وضعی از جرایم سایبری نیز نقش اساسی دارند، از جمله این تدابیر حفاظت فیزیکی است که بکارگیری قفل ها، نگهبان ها، علایم و ابزارهای مشابه برای کنترل دسترسی به رایانه و تجهیزات مربوط به آن از جرایم سایبری پیشگیری می نمایید، از دیگر تدابیر فنی می توان به؛ کنترل فنی، کنترل مدیریتی، توسعه محافظت ها، فیلترینگ اشاره کرد. از سایر تدابیر و اقدامات حقوقی و جرم شناختی در پیشگیری وضعی از جرایم سایبری می توان به تدابیر و اقدامات مبتنی بر خانواده، راهبردهای کاهنده آثار نامطلوب، تبیین و نهادینه سازی فرهنگ استفاده صحیح از فضای سایبر، افزایش میزان تلاش برای ارتکاب جرم، تغییر مسیر بزهکاران، کاهش عوامل محرک، انگیزه زدایی اشاره کرد. تدابیر آموزشی و آگاهی سازی نیز در پیشگیری وضعی از جرایم سایبری نقش اساسی دارند، با اعلان جرم بودن یک عمل در فضای سایبری و اطلاع رسانی نسبت به آن و اعلام میزان مجازات اعمال ارتکابی می توان تا حد زیادی از ارتکاب جرایم دنیای سایبر، پیشگیری نمود؛ که در این راستا می توان از امکانانت ارتباطی مختلف، رسانه ها و ... استفاده کرد. همانطور که قبلا اشاره شد تدابیر مختلف پیشگیری وضعی در پیشگیری و جلوگیری از ارتکاب جرامی احتمالی سایبری نقش اساسی دارند، ولی این به معنای انکار چالش ها، خلاء ها و آسیب های تدابیر پیشگیری وضعی نیست لذا باید با شناسایی و آسیب شناسی موانع و چالش های پیشگیری وضعی در حد امکان در رفع و مرتفع کردن آنها تلاش کرد. یکی از چالش های اساسی در رابطه با ماهیت فضای سایبری است چرا که علاوه بر اینکه با کثرت محتواهای مجرمانه در فضاهای عمومی سایبر مواجه هستیم، فراملی بودن جرایم سایبری از دیگر چالش های اساسی پیش روی پیشگیری وضعی از جرایم سایبری است. علاوه بر ساختار خاص فضای سایبر، وجود برخی ابزارها و امکانات خاص نیز پیشگیری از جرم را با دشواری مواجه ساخته است. کمبود تجهیزات و امکانات پلیس، عدم تخصص کافی مراجع قضایی و انتظامی و... از دیگر چالش ها در این حوزه است. برخی از موانع و چالش ها مرتبط با خود تدابیر

پیشگیری وضعی به دلیل؛ موقتی بودن پیشگیری وضعی، مقابله ی محافظه کارانه با جرم، فرصت مدار بودن، عدم شمول همه ی آماج ها، جابه جایی جرم، عدم شفافیت برخی عبارات قانونی، افزایش احتمال بزه دیدگی و رقم سیاه جرایم سایبری، زمان بر بودن و ایراد اقتصادی تدابیر پیشگیری وضعی است.

پیشنهادها

برنامه های پیشگیری وضعی از جرایم بویژه جرایم سایبری بویژه برای مدارس تنظیم شود

- ارتقای سواد امنیت دیجیتالی شهروندان توسط نهادهای متولی
- تربیت نیروهای متخصص در پلیس فتا و همکاری با جرم شناسان برای اعمال تدابیر پیشگیرانه
- کاهش انگیزه های مجرمانه سایبری با برنامه های آموزشی و فرهنگ

منابع

- ابراهیمی، شهرام (۱۳۹۱)، جرم شناسی پیشگیری، چاپ دوم، تهران، میزان، شماره ۱۱.
- احمدی، حبیب (۱۳۹۶)، جامعه شناسی انحرافات، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها.
- اسلامی، ابراهیم (۱۳۹۵) جایگاه حمایت ازبزه دیدگان جرایم سایبری درمقررات کیفری حقوق داخلی و حقوق بین‌الملل، پژوهشنامه حقوق اسلامی، دوره هفدهم، شماره ۱، صص ۱۸۲-۱۵۷.
- اصلانی، حمیدرضا (۱۳۸۴)، حقوق فناوری اطلاعات، (حریم خصوصی در جامعه اطلاعاتی)، با همکاری مرکز اطلاعات ریاست جمهوری، چاپ اول، تهران: میزان.
- الهی منش، محمدرضا؛ سدره نشین، ابوالفضل (۱۳۹۱). محشای قانون جرایم رایانه ای. تهران: مجد.
- امیریان فارسانی، امین و دیگران (۱۳۹۶)، کارکردهای نظری و عملی پلیس فتا در پیشگیری از جرایم سایبری و موانع حاکم بر آن، فصلنامه علمی تحقیقات حقوقی بین المللی، (۱۰)، ۳۵، ص ۲۶۵-۲۳۷.
- آیکاو، دیوید جی (۱۳۸۳)؛ راهکارهای پیشگیری و مقابله با جرایم رایانه ای؛ ترجمه اکبر استرکی، محمد صادق روزبهانی، تورج ریحانی و راحله الیاسی؛ تهران: معاونت
- بابایی، محمدعلی؛ نجیبیان، علی (۱۳۹۰)، چالش های پیشگیری وضعی از جرم، مجله حقوقی دادگستری، شماره ۷۵: ۱۴۷ تا ۱۷۲.
- باستانی، برومند (۱۳۸۹). جرایم رایانه ای و اینترنتی جلوه ای نوین از بزهکاری. چاپ دوم. تهران: انتشارات بهرامی.
- بهره مند، حمید؛ کوره پز، حسین محمد؛ سلیمی، احسان (۱۳۹۳)، راهبردهای وضعی پیشگیری از جزایم سایبری، آموزه های حقوق کیفری (۱)،۷: ۱۷۶-۱۴۷.
- بیات، بهرام؛ جعفر شرافتی و نرگس عبدی (۱۳۸۷). پیشگیری از جرم با تکیه بر رویکرد اجتماع محور تهران: معاونت اجتماعی ناجا.
- پرویزی، رضا (۱۳۸۴). پی جویی جرایم رایانه ای چاپ اول، تهران: جهان جام جم.
- پرویزی، رضا (۱۳۸۶)؛ پی جویی جرایم رایانه ای؛ چاپ اول، تهران: جهان جام جم.
- پژوهش دانشگاه علوم انتظامی آخوندی، محمود (۱۳۸۰)، آیین دادرسی کیفری؛ چاپ نهم، تهران: وزارت فرهنگ و ارشاد اسلامی، ج ۱.

- توکلی، فخرالدین؛ مرتضوی، مرتضی (۱۳۹۹)، تعیین عومال تاثیرگذار در کشف جرایم سایبری با رویکرد دلفی، فصلنامه کارآگاه، دوره ۱۳، شماره ۵۰، ص ۱۴۸-۱۲۸.
- جاوید، مهدی (۱۳۸۸)، شناسایی نقاط جرم خیز و نقش آن در پیشگیری از وقوع جرم، زیر نظر محمد فرجیها و غلامرضا محمدنسل در پیشگیری از جرم (مجموعه مقالات نخستین همایش ملی پیشگیری از جرم)، چاپ اول، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا.
- جاویدنیا، جواد (۱۳۸۸)، جرایم تجارت الکترونیک ، ی تهران: انتشارات خرسندی، چاپ دوم.
- جعفری، مریم؛ سلیمانی، فرزاد (۱۳۹۷)، نقش پلیس در تأمین امنیت و سالم سازی فضای سایبر با رویکرد پیشگیری اجتماعی از جرایم سایبری، فصلنامه دانش انتظامی زنجان؛ (۸)، ۱۹: ۱۰۹-۸۵.
- جلالی فراهانی، امیر حسین (۱۳۸۴). پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، نشریه‌ی فقه و حقوق، سال پنجم، شماره ۱۷.
- جلالی فراهانی، امیر حسین (۱۳۸۴)، پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، مجله حقوق اسلامی، (۲)، ۶: ۱۳۲-۱۶۲.
- جلالی فراهانی، امیر حسین (۱۳۸۴)، پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، مجله فقه و حقوق، پژوهشگاه فرهنگ و اندیشه، سال دوم، شماره ۶.
- جلالی فراهانی، امیرحسین (۱۳۸۴)، پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، فقه و حقوق، سال دوم: ۱۶۲-۱۳۳.
- جلالی فراهانی، امیرحسین، و باقری اصل، رضا (۱۳۸۶)؛ پیشگیری اجتماعی از جرایم و انحرافات سایبری، نشریه ی مرکز پژوهشهای مجلس، شماره‌ی ۵۵.
- جوان جعفری، عبدالرضا و مهدی سیدزاده ثانی (۱۳۹۱)، رهنمودهای عملی پیشگیری از جرم، معاونت پیشگیری از وقوع جرم قوه قضاییه، تهران، میزان.
- حقیقتی، لیلا (۱۳۹۵)، مروری بر جرایم سایبری (با تأکید بر قوانین مجازات رایانه ای)، دومین کنفرانس ملی راهکارهای توسعه و ترویج آموزش علوم در ایران.
- حیدری نژاد، نصرالله (۱۳۹۷)، پیشگیری وضعی در جرایم سایبری از منظر حقوق کیفری ایران و جهان، قانون یار (۲)، ۶: ۴۶-۲۹.
- حیدری نژاد، نصرالله (۱۳۹۷)، پیشگیری وضعی در جرایم سایبری از منظر حقوق کیفری ایران وجهان، فصلنامه علمی و حقوقی قانون یار (۲)، ۶: ۴۳-۲۹.

- خلفی، ابوذر (۱۳۹۴)، پیشگیری از جرایم سایبری با محوریت جرم یابی، نشریه کارآگاه، شماره ۳۴.
- خلفی، ابوذر (۱۳۹۵)، پیشگیری از جرایم سایبری با محوریت جرم یابی، مجله کارآگاه، (۹)،۳۴: ۳۸-۲۳.
- خلیلی پور رکن آبادی، علی و نورعلی وند، یاسر(۱۳۹۱)، تهدیدات سایبری و تاثیرات آن بر امنیت ملی، فصلنامه مطالعات راهبردی (۱۱)، ۲.
- داتن، ویلیام (۱۳۸۴)، دگرگونی های اجتماعی در جامعه اطلاعاتی، ترجمه محمد توکل و ابراهیم کاظمی پور، ترجمه محمد توکل و ابراهیم کاظمی پور، تهران، کمیسیون ملی یونسکو
- داوری، بهاره (۱۴۰۰)، راهکار های پیشگیری وضعی از جرایم سایبری علیه خانواده متاثر از اینستاگرام، پایان نامه کارشناسی ارشد، دانشگاه شهید اشرفی اصفهانی.
- دزیانی، محمدحسن (۱۳۸۴)، اخبار جرایم سایبری؛ خبرنامهء انفورماتیک، سال بیستم، شماره۸۹ .
- دهخدا، علی‌اکبر، (۱۳۷۷)، لغت‌نامه، جلد دوم، انتشارات دانشگاه تهران.
- راجی، سید محمد هادی (۱۳۸۵) نگاهی به قانون تجارت الکترونیک، فصلنامه نشریه حقوقی گواه، بهار و تابستان، شماره ۶ و ۷.
- رایجیان اصلی، مهرداد، (۱۳۸۳)، رهیافتی نو به بنیان‌های نظری پیشگیری از جرم، مجله حقوقی دادگستری، شماره ۴۸-۴۹.
- رایجیان اصلی، مهرداد؛ سلیمی، احسان؛ نوریان، علیرضا (۱۳۹۳)، پیشگیری از جرایم رایانه ای از رهیافت نظری تا رهیافت جهانی در پرتو رهنمود پیشگیری از جرم سازمان ملل متحد، مطالعات راهبردی.
- رضوی اصل، سید محمد جعفر ؛ دارابی، شهرداد (۱۳۹۶)، کارکردها و دستاوردهای پیشگیرانه وضعی قوانین دادرسی الکترونیکی و آیین دادرسی جرایم رایانه ای، مجله پزوهش های حقوقی،شماره ۴۰: ۳۸۷-۳۶۹.
- رضوی فرد، بهزاد؛ موسوی، نعمت اله (۱۳۹۴)، محدودیت ها و راهبردهای صلاحیت در جرایم سایبری، مجله حقوقی دادگستری، دوره ۸۱، شماره ۹۸، ص ۱۰۲-۸۳.
- رضوی، محمد (۱۳۸۶)، جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها، دوره ۹، شماره ۱، ص ۱۴۰-۱۲۰.

- رضوی، محمد، (۱۳۸۶)، جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آنها»، فصلنامه دانش انتظامی، سال نهم، شماره ۱.
- زلقی، علی؛ مالمیر، محمود (۱۳۹۷)، نقش ضابطان قضایی در پیشگیری و کنترل جرایم فضای سایبری در حقوق ایران و انگلیس، فصلنامه حقوق پزشکی، ویژه نامه حقوق بشر و حقوق شهروندی.
- سخاوت، جعفر (۱۳۹۱)، جامعه شناسی انحرافات اجتماعی، نشر: دانشگاه پیام نور.
- سلیمی، احسان (۱۳۹۷)، آسیب شناسی پیشگیری از جرایم سایبری در ایران، رساله دکترا، دانشگاه قم.
- سلیمی، علی و محمد داوری (۱۳۸۵)، جامعه شناسی کجروی، مجموعه مطالعات کجروی و کنترل اجتماعی، قم: پژوهشگاه حوزه و دانشگاه.

- Casey, Eoghan (2004), Digital Evidence and Computer Crime, Academic Press
- Kent, Stephen and Millett Lynette (2011), Who Goes There? Authentication through the Lens of Privacy, National Academy Press.
- Felson, Marcus, (2008), Routine Activity Approach", Ed. by: Richard Wortley & Lorraine Mazerolle, Environmental Criminology and Crime Analysis, 1st Ed., Willan Publishing
- Katzer, Catarina, Detlef Fetchenhauer & Frank Belschak, (2010), Cyberbullying: Who Are the Victims? A Comparison of Victimization in Internet Chatrooms and Victimization in School", Journal of Media Psychology, Vol. 21(1), Hogrefe & Huber Publishers
- Kizza, Joseph M (2018). Guide to Computer Network Security, London, Springer Publications Ltd.
- Cullen, F.T. (1994). "Social Support as an Organizing Concept for Criminology: Presidential Address to the Academy of Criminal Justice Sciences". Justice Quarterly, 11.
- Hirschi, T. (1969). Causes of Delinquency. Berkeley: University of California Press
- Kumar, Shiva (2010), cyber crime - prevention & detection, Journal of Strategic Information Systems 8