الگوی مفهومی سیاست جنایی جرایم سایبری در ایران

رضا صبح‌خیز[1]
بابک پورقهرمانی[2]
علی صفاری[3]

نوع مقاله: مقاله مستخرج از رساله دکتری
تاریخ دریافت: ۱۳۹۹/۹/۷ تاریخ پذیرش‌نهایی: ۱۴۰۰/۲/۹
فصلنامه مطالعات راهبردی ناجا / سال ششم / شماره بیستم- تابستان ۱۴۰۰ * ۱۲۹-۱۵۴

چکیده

امروزه، استفاده از فناوری اطلاعات و ارتباطات و بستر فضای سایبری در بسیاری‌از ابعاد زندگی بشر سایه افکنده است؛ به‌طوری‌که روابط افراد در این بستر منجر به شکل‌گیری عنوان "جوامع سایبری" گردیده‌است. بعد امنیت و نظم عمومی مهم‌ترین رکن در پایداری هر جامعه است؛ جوامع سایبری نیز از این امر مستثنی نبوده و به‌دنبال ترسیم سیاست جنایی خود برای تضمین امنیت جانی، مالی و حیثیتی شهروندان و نیز تأمین امنیت نهادهای عمومی در بستر فضای سایبری هستند. در ایران نیز با توجه ضریب بالای نفوذ اینترنت و حجم وسیع کاربران، ترسیم سیاست جنایی برای مدیریت و پایش ناهنجاری‌های سایبری از اهمیت و اولویت به‌سزایی برخوردار است؛ بر این اساس، در این مقوله، با بررسی اسناد و مدارک و مطالعه کتابخانه‌ای، روندها و رویکردهای سیاست جنایی جمهوری اسلامی ایران در فضای سایبری تبیین گردیده و درنتیجه، الگوی مفهومی از سیاست نسبی جنایی مرتبط با فضای سایبری برای اقدامات علمی و عملی توسعه‌ای ارائه شده‌است.

واژگان کلیدی: سیاست جنایی، فضای سایبری، فضای مجازی، جرایم سایبری

مقدمه

رسالت و هدف سیاست جنایی هر جامعه، درواقع، تضمین امنیت جانی، مالی و حیثیتی شهروندان، از یک سو و تأمین امنیت نهادهای عمومی آن، از سوی دیگر است(لازرژ، ۴۲:۱۳۹۰). عنوان و لفظ سیاست جنایی که آن را به فویر باخ آلمانی نسبت می‌دهند، به حقوق جزای کاربردی مربوط می‌شود

۱. دانش‌آموخته دکتری رشته حقوق کیفری، دانشکده حقوق، الهیات و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
reza122onlymorning@gmail.com
۲.دانشیار گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق، الهیات و علوم سیاسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران (نویسنده مسئول)
b.pourghahramani@yahoo.com
۳. دانشیار گروه حقوق کیفری و جرم شناسی، دانشکده حقوق، الهیات و علوم سیاسی، دانشگاه شهید بهشتی، تهران، ایران
a-saffary@sbu.ac.ir

که موضوع آن، مدیریت و پایش جرم را تشکیل می‌دهد. به نظر می‌رسد که سیاست جنایی در مفهوم باخی آن، در پایش جرم، توفیقی به دست نیاورده‌است؛ به همین جهت، پس از جنگ دوم جهانی، پایش و مدیریت جرم و خطرپذیری آن دیگر در انحصار مطلق حقوق کیفری نیست بلکه پیرامون آن نهادهایی به وجود آمدند که درمجموع، به پایش جرم می‌پردازند(مهدوی ثابت، ۱۲:۱۳۹۵).

اصطلاح سیاست جنایی که عموما به کتاب فوئر باخ در سال ۱۸۰۳ منتسب می‌شود، مدت‌ها با "جنبه‌های نظری و عملی نظام کیفری" مترادف مانده‌است. مطابق نظر فوئرباخ، سیاست جنایی شامل مجموعه شیوه‌های سرکوبگری می‌شود که دولت از طریق پیش‌بینی و به‌کاربستن آنها بر ضدّ بزه واکنش نشان می‌دهد. این معنا از سیاست جنایی، همچنان موردنظر بعضی‌از نویسندگان معاصر نیز هست. با وجود این، امروز شاهد آنیم که سیاست جنایی، از حقوق کیفری، جرم‌شناسی و جامعه‌شناسی جنایی جدا شده‌است و مفهوم مستقلی به خود گرفته‌است؛ هنگامی‌که مارک آنسل نشریه "آرشیوهای سیاست جنایی" را در سال ۱۹۷۵ تأسیس نمود، در نخستین اقدام، بر ضرورت عدم محدود و خلاصه‌کردن سیاست جنایی، به حقوق کیفری تأکید کرد و با تلاش برای برجسته‌کردن ویژگی دوگانه آن ـ یعنی "دانش مشاهده و مطالعه" و "فن" یا "راهبرد روش‌مند واکنش بر ضدّ بزه"، پیشنهاد کرد که سیاست جنایی "واکنش سازمان‌یافته و مطالعه‌شده جامعه بر ضدّ اقدام‌ها و فعالیت‌های بزهکارانه، منحرفانه و یا ضد اجتماعی" تعریف شود(دلماس مارتی، ۱۳۹۳، ۲: ۶۳).

در دیدگاه مارک آنسل، سیاست جنایی، نخست، علاوه‌بر جرم ـ که یک مفهوم قانونی است ـ به انحراف(کژروی) ـ که یک مفهوم اجتماعی است ـ نیز می‌پردازد؛ دوم‌اینکه، علاوه‌بر سرکوب و مجازات بزهکاری، به پیشگیری از آن توجه دارد؛ سوم‌اینکه، علاوه‌بر اقدام‌های جزایی و نظام کیفری، بر تدبیرها و نظام‌های اجتماعی، فرهنگی، اخلاقی و ... و نیز بر همه آنچه که در بهداشت و پیشگیری اجتماعی از بزهکاری مؤثر است، تکیه می‌کند و بدین‌سان، سیاست جنایی از مفهوم سنتی مضیق ـ یعنی سیاست کیفری ـ به‌سمت مفهوم موسع ـ به‌معنای امروزی آن ـ تحول می‌یابد(لازرژ، ۱۳۹۰: ۱۵). بدین‌ترتیب، می‌توانیم بگوییم که سیاست جنایی در پایان سده بیستم ـ یعنی حدود دو سده پس از فوئرباخ ـ شامل کلیه اقدام‌های سرکوبگرانه(کیفری و غیرکیفری) و پیشگیرانه با ماهیت‌های مختلف می‌شود که دولت و جامعه مدنی، هر یک به‌صورت مستقل و یا با یک مشارکت سازمان‌یافته، از آنها در قالب روش‌های مختلف به‌منظور سرکوب بزهکاری و بزهکاران و نیز پیشگیری از بزهکاری و انحراف استفاده می‌کنند(لازرژ، ۱۷:۱۳۹۰).

دلمـــاس مارتی تعریف فوئرباخ را گســـترش داده و سیاست جنایی را «مجموعه روش‌هایی که هیئت اجتماع با توسل و با به‌کاربستن آنها، پاسخ‌های مختلف به پدیده جنایی را سازمان می‌بخشد» تعریف نمود. بدین ترتیب، سیاست جنایی با جنبه‌های نظری و عملی اشکال مختلف پایش اجتماعی بزه و انحراف مترادف به نظر می‌رسد. ناگفته پیداست که حقوق کیفری، به‌عنوان هســـته اصلی یا مرکز شدیدترین فشار با رؤیت‌پذیری بسیار بالا در سیاست جنایی حضور پُررنگی دارد؛ اما شیوه‌های کیفری مقابله‌با بزه در قلمرو سیاست جنایی تنها نیســـتند؛ بلکه حول آنها، شیوه‌های دیگر پایش اجتماعی از گونه غیرکیفری(مانند رسیدگی و ضمانت اجراهای اداری و مدنی)، غیرسرکوبگر(مانند پیشگیری، جبران و ترمیم خســـارت بزه‌دیده، میانجی‌گـــری) و گاه غیردولتی(رویه‌های سرکوبگر شبه‌نظامیان و شبه‌پلیس‌های خصوصی، اقدام‌های اعتراضی از نوع اقدامات سازمان عفو بین‌الملل بر ضدّ نقض حقوق بشر یا اقدام‌های انضباطی که یادآور برخی گونه‌های انتظام حرفه‌ای در صنف‌ها یا اتحادیه‌ها و ... است) نیز وجود دارد(لازرژ، ۱۳۹۰: ۷۰).

سیاست جنایی

ازآنجاکه جرم‌شناسی به شاخه‌های مختلفی چون جامعه‌شناسی جنایی، زیست‌شناسی جنایی و ... تقسیم می‌شود، سیاست جنایی نیز رشته‌ای کاربردی محسوب می‌شود و شکل‌های گوناگونی به خود می‌گیرد؛ به‌طوری‌که سیاست جنایی ازلحاظ کاربردی، دارای چهار حالت زیر است:

۱.**سیاست جنایی تقنینی؛** که همان تدبیر قانون‌گذار درمورد واکنش بر ضدّ جرم است.

۲.**سیاســـت جنایی قضایی؛** که درواقع، نحوه برداشت دادگســـتری(قوه قضاییه) از سیاست جنایی تقنینی است.

۳.سیاســـت جنایی اجرایی؛ با وجود استقلال قـــوای سه‌گانه، حکومت ناگزیر است که برای اجرای قوانین داخلی از قوه‌مجریه بهره ببرد. این بدان‌معناست که قوه‌مجریه نیز از سیاست خاص خود برخوردار است؛ بنابراین، سیاست جنایی اجرایی عبارت است از نحوه درک و اجرای قوانین و احکام قضایی درمورد پایش جرم و واکنش‌های خود آن.

۴.سیاست جنایی مشارکتی؛ این جنبه از سیاست جنایی ممکن است دربردارنده حالت‌های پیشین باشـــد. به بیان دیگر، ممکن است سیاست جنایـــی مشارکتی با سیاست جنایی تقنینی، سیاست جنایی قضایی و یا سیاست جنایی اجرایی در ارتباط باشد. درواقع، در اینجاست که بحث جامعه مدنی در سیاست جنایی متجلی می‌گردد. در این رویکرد، مردم به اقتضای بافت حکومت

در مراحل مختلف اجرایی، قضایی، انتظامی، مهار و پایش جرم، مشارکت می‌جویند. مشارکت مردم در محاکمات جنایی در نهادهایی مانند هیئت منصفه، در کشف جرم از طریق راه‌هایی چون ادای شهـادت و در مرحله حکم مانند واگذاری طفل به خانواده‌هـای جایگزین(به‌موجب حکم دادگاه اطفال) و یا اجرای مراسم رجم(سنگسار) در حقوق کیفری اسلامی، نمونه‌هایی از سیاست جنایی مشارکتی به شمار می‌روند(نجفی ابرند آبادی، ۱۳۸۲: ۳۲).

در زیر، مهم‌ترین تعریف‌هایی که درخصوص سیاست جنایی آمده‌است، ارائه می‌گردد.

تعریف فوئر باخ: اصطلاح سیاست جنایی برای اولین‌بار توسط فوئر باخ آلمانی در سال ۱۸۰۳ به‌کـار برده شد. او در کتاب خود ـ حقوق کیفری ـ تعریفی از سیاست جنایی بدین مضمون ارائه می‌دهد: «سیاست جنایی مجموعه‌ای از شیوه‌های سرکوبگرانه‌ای است که دولت با استفاده از آن، به پدیده مجرمانه واکنش نشان می‌دهد».

تعریـف دوندی یو وابر: در سـال ۱۹۳۸ استاد وابر در مقام تعریـف سیاست جنایی، دوباره تعبیری را به‌کار می‌برد که یادآور دیدگاه‌های فوئر باخ است:«سیاست جنایی یک هنر و فن است و موضوع آن کشف‌شیوه هایی است که مبارزه بر ضدّ جرم را میسر می‌سازد. سیاست جنایی همه شیوه‌هایی که ممکن است دولت‌ها اختیار داشته باشند و بر ضدّ بزهکاری به‌کار برند را دربرمی‌گیرد. سیاسـت جنایی پیشگیری را دربرنمی‌گیرد. بـا اینکه امر پیشگیری، از وظایف دولت است اما اگر برای مهار و پایش جرم مؤثر واقع نشود، وظیفه دوم دولت ـ که همان سیاست جنایی است ـ اعمال می‌شود؛ یعنی واکنش تنبیهی و سرکوبگرانه جرم».

تعریف مارک آنسل: به نظر مارک آنسل، سیاست جنایی به‌طورهم‌زمان، علم مشاهده و هنر یا استراتژی اصولی و سازمان‌یافته واکنش ضد جنایی است. بر اساس این تعریف، می‌توان گفت که سیاست جنایی در مکتب دفاع احقاقی نوین، دارای دو جنبه علمی(نظری) و فنی(کاربردی) است. از دیدگاه علمی، همان‌گونه که جرم‌شناسی علم علت‌شناسی جرم است، سیاست جنایی نیز علم مشاهده، تجربه و آزمایش واکنش بر ضدّ جرم است. از طرفی، از دیدگاه کاربردی نیز همان‌طور که جرم‌شناسی به چهارراه علوم موصوف است، سیاست جنایی را نیز می‌توان یک فن توصیف نمود.

تعریف دلماس مارتی: در سال ۱۹۸۳، دلماس مارتی(یکی از دانشجویان مارک آنسل) باز هم مفهوم سیاست جنایی را توسعه داد. سیاست جنایی در تعبیر دلماس مارتی، شامل کلیه شیوه‌ها و روش‌هایـی مـی شود که هیئت اجتمـاع از طریق آنها پاسخ‌گویی به پدیـده جنایی را سازمان می‌بخشد(مهدوی ثابت، ۱۳۹۵: ۳۴).

سیاست جنایی جرایم سایبری

سیاست جنایی در جرایم سایبری را نیز می‌توان در قالب‌های ارائه‌شده در بالا تبیین نمود. همان‌طور که ملاحظه گردید، علما و دانشمندان حقوق، هرکدام با نگاه و رویکرد زمانی و مکانی منحصربه‌فرد خود، تعریفی از سیاست جنایی ارائه داده‌اند. درحال‌حاضر، با توجه به رشد فزاینده جرایم سایبری و تأثیرگذاری فضای سایبری بر زندگی بشری، به نظر می‌رسد که نیاز است نسبت‌به ترسیم سیاست جنایـــی منحصر به این فضا اهتمام ویژه‌ای مبذول گردد اما در اینجا و در تعریف سیاست جنایی، به نظر می‌رسد که در تبیین و تدوین سیاست جنایی مختص فضای سایبری می‌توان از قالب عام دکتـــر دلماس مارتی استفاده نمود و چنین بیان داشت که سیاست جنایی جرایم سایبری شامل کلیه شیوه‌ها و روش‌هایی می‌شود که هیئت اجتماع از طریق آنها پاسخ‌گویی به پدیده جنایی در فضای سایبری را سازمان می‌بخشد.

موضوع سیاست جنایی در جرایم سایبری

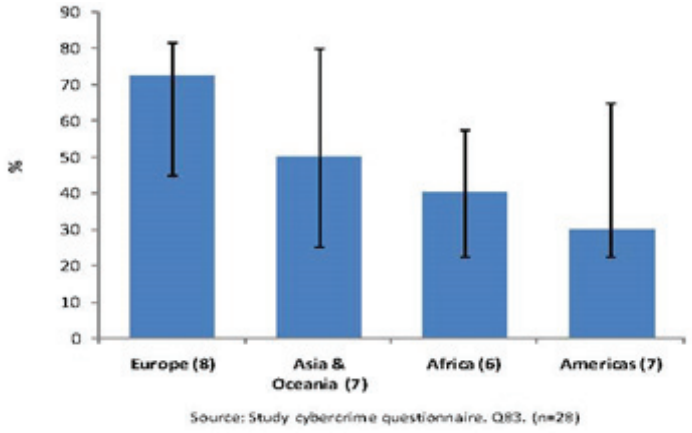
در سیاست جنایی معمولاً دو موضوع موردتوجه قرار می‌گیرد: اول، بررسی فرآیند جرم‌انگاری؛ دوم، بررسی شبکه‌های پاسخ به پدیده مجرمانه یا جرم. در زیر، هر یک از آنها به‌طور مختصر شرح می‌شود.

۱.بررسی فرآیند جرم‌انگاری

جرم سایبری اغلب دارای بُعد بین‌المللی است و بیشتر مواقع عناصر مرتبط با جرم سایبری ریشه در سطح بین‌المللی دارد. ابعاد بین‌المللی این نوع از جرایم موجب شده‌است تا افراد مختلف از جمله جرم‌شناسان، حقوق‌دانان و متخصصانِ رایانه به مطالعه و بررسی همه‌جانبه این پدیده روی آوردند؛ به‌طوری‌که تدوین قوانین و اجرای مجازات با توجه به فراملی بودن ماهیت جرایم سایبری به مسئله پیچیده‌ای به‌ویژه در حقوق بین‌الملل تبدیل شده‌است؛ چراکه وقوع این نوع جرایم، موجب تشدید خلأهای قانونی و قضایی حاکم در حقوق بین‌الملل، همانند صلاحیت دادگاه‌های کشورها نسبت‌به رسیدگی و نیز تعارض قوانین این کشورها در برخورد با جرایم سایبری شده‌است.

همان‌طـــور که می‌دانیم، حقوق بین‌الملل شاخه‌ای از حقوق عمومی است که شامل مجموعه قوانیـــن و مقرراتـــی است کـــه بر جامعه بین‌المللی حاکـــم است و در آن جامعـــه، قابلیت اجرایی دارد(ضیایی بیگدلی،۲:۱۳۹۶). جامعه بین‌الملل دارای تابعان بین‌المللی است که همان کشورها و سازمان‌های بین‌المللی محسوب می‌شوند. یکی از مهم‌ترین مسائلی که در روند شکل‌گیری قواعد

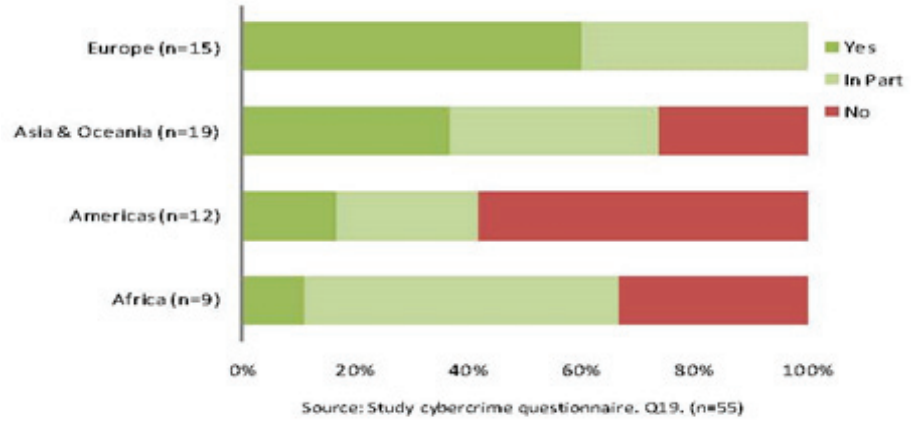
بین‌المللی مطرح می‌شود، مجموعه قوانین و قواعد همکاری‌های بین‌المللی کشورها و سازمان‌ها در مواجهه با پدیده جرم است. سازمان‌ملل‌متحد به‌عنوان بزرگ‌ترین سازمان بین‌المللی، به نوبه خود، بـــه حوزه جرم توجه ویژه‌ای داشته‌است و با ایجـــاد دفتر مبارزه با جرم(UNODC)[1] در بطن خود به‌دنبال ایجاد معیارهای سازنده در سطوح مختلف همکاری‌های بین‌المللی تابعین خود در مواجهه و مقابلـــه با پدیده جرم است. این دفتر در ابتدا در جهت مبارزه با پدیده جرایم موادمخدر به‌وجود آمد و درحال‌حاضر، با توجه به ماهیت بین‌المللی جرایم سایبری در این حوزه نیز متمرکز شده‌است؛ به‌طوری‌که در سال ۲۰۱۳ با انتشار پیش‌نویس سندی با عنوان "مطالعه جامع بر جرایم سایبری" نگرانی‌هـــای خـــود را در این مورد ابراز کرد. براساس این گزارش و برابر آمارهایی که دفتر مقابله با جرم و موادمخدر سازمان‌ملل در سال ۲۰۱۳ کســـب کرده‌است، بیش از نیمی از کشورها گزارش داده‌اند که بین ۵۰ تا ۱۰۰ درصد از جرایم سایبری که پلیس با آنها برخورده کرده‌است، ابعاد فراملی داشته‌است(دفتر مقابله با جرم سازمان ملل،۲۰۱۳:۴۹).



نمودار ۱. درصد اعمال مجرمانه سایبری

نمودار بالا نشان می‌دهد که کشورهای اروپایی، بالاترین نسبت جرایم سایبری بین‌المللی را دارا هستند. این نهاد در بررسی دیگری در پاسخ به این سؤال که «آیا قانون‌ملی چارچوب موجود برای جرایم سایبری را در ابعاد ملی کافی می‌داند یا خیر؟» به تحلیلی به شرح نمودار ۲ رسید.

1. United Nations Office on Drugs & Crime



نمودار۲. وضعیت قانون‌گذاری جرایم سایبری در سطح بین‌الملل

تحقیــق فوق نشان می‌دهد که حدود یک‌ســوم از کل کشورهای پاسخ‌دهنده معتقد بودند که چارچوب‌هــای قانونــی ملی آنها برای جرایــم فرامرزی "کافی" بوده‌اســت. ۴۰ درصد دیگر از آنها چارچوب‌های قانونی ملی را "تاحدودی" کافی می‌دانستند.

مطالعــات نشــان می‌دهد که به‌دلیل قابلیت‌های فنــی رایانه‌ها و اجزای مرتبــط با آن، امکان ذخیره‌سازی، انتقال، استفاده از داده‌ها از طریق شبکه‌ها و نیز ایجاد ارتباط و انتقال سریع در سطح وسیع بین سامانه‌های رایانه‌ای، ماهیت فراملی جرایم سایبری افزایش یافته‌است؛ به‌طوری‌که دامنه گســترش سامانه‌های رایانه‌ای از محیط رایانه و شبکه داخلی به سطح بین‌المللی گســترش پیدا کرده‌است و موجب خلق نسل جدید جرایم رایانه‌ای ـ یعنی جرایم در محیط سایبری ـ شده‌است که ماهیت و خاصیت کاملاً فراملی و بین‌المللی دارد. به‌هرحال، امروزه، جرایم سایبری تبدیل به یــک پدیده مجرمانه کاملاً بین‌المللی شده‌اســت. در این راستا، تعدادی از کشورها نحوه همکاری قانونی دوطرفه‌شان را بر اساس اصل مجرمیت دوگانه قرار می‌دهند. پیگردها در سطح جهانی، در کل، محدود به جرایمی هستند که در همه کشورهای شرکت‌کننده "جرم" شمرده می‌شوند. اگرچه تخلفاتی وجود دارد که در هرجایی از دنیا می‌توانند مورد پیگرد قانونی قرار گیرند اما با وجود این، تفاوت‌های منطقه‌ای نیز نقش مهمی را در این امر بازی می‌کنند.

جرم‌انگــاری محتوای غیرقانونی در کشورهای مختلف، متفــاوت است. موضوعاتی که از لحاظ قانونی می‌توانند در کشوری منتشر شوند، ممکن است در کشور دیگری غیرقانونی باشند. فناوری

مورداستفاده رایانه، به‌طور عمده، در دنیا یکسان است. جدا از مقوله‌های زبانی و نوع قدرت، تفاوت‌های خیلی اندکی بین سامانه‌های رایانه‌ای و تلفن‌های همراه فروخته‌شده در آسیا و مواردی که در اروپا به فروش رسیده است، وجود دارد. موقعیتی مشابه در رابطه با اینترنت وجود دارد. به‌خاطر استانداردسازی، پروتکل‌های مورد استفاده در کشورهای قاره آفریقا با مواردی که در ایالت‌متحده آمریکا استفاده شده‌است، یکسان است. استانداردسازی امکانِ دسترسی کاربران سراسر دنیا را به خدمات یکسان اینترنتی فراهم می‌سازد. جرایم سایبری با توجه به خصیصه فراملی و فراسرزمینی خود، تعاون و همکاری بین‌المللی را ایجاب می‌کند و پدیده‌ای است که به‌دلیل شرایط خاص و ماهیت بین‌المللی بودن، نوعی سیاست جنایی یکسان را به‌دنبال می‌آورد. در کشورهای پیشرفته، قانون‌گذاران باتوجه به نیاز جامعه، انواع مختلفی از اعمال مجرمانه مرتبط با رایانه را شناسایی و در قالب قوانین کیفری خود گنجانده‌اند و هم‌زمان با این اقدامات پراکنده کشورها، مراجع بین‌الملل نیز فعالیت خود را در این زمینه آغاز و با دسته‌بندی جرایم شناخته‌شده، فهرست‌هایی از این‌گونه جرایم را به‌عنوان الگوی واحد و راهنما برای تدوین قوانین‌ملی کشورها ارائه کرده‌اند. از جمله سازمان‌های بین‌المللی و منطقه‌ای پیش‌رو و اقدامات انجام‌شده در این زمینه می‌توان به سازمان همکاری و توسعه اقتصادی[1]، شورای اروپا، انجمن بین‌المللی حقوق جزا[2]، سازمان‌ملل، سازمان اینترپل(سازمان پلیس جنایی بین‌المللی)، کنوانسیون بوداپست، اقدام گروه هشت(در سال ۱۹۹۹) و اقدام مؤسسه مک‌کانل اشاره نمود. اما مهم‌ترین گردهمایی و مصوبه درخصوص جرایم سایبر، به کنفرانس بوداپست در اواخر سال ۲۰۰۱م. برمی‌گردد که در آن، بیشتر کشورهای اروپایی همراه کانادا، ژاپن و آفریقای جنوبی و آمریکا مصوبه‌ای به نام "کنوانسیون جرایم سایبر" را امضا نمودند. درمجموع، بیش از ۳۲ کشور بر مصوبات کنفرانس بوداپست صحه گذاشتند؛ اما روسیه، اسلواکی، ترکیه، لیتوانی، لوکزامبورگ، چک، دانمارک و بوسنی هنوز بدان نپیوسته‌اند. در این کنفرانس، چارچوب مشخصی برای جرایم سایبر مورد تأیید قرار گرفت و به‌عنوان مصوبه ثبت گردید. شاخص‌های اصلی تأییدشده شامل دسترسی غیرقانونی به اطلاعات رایانه‌ای و شبکه‌های رایانه‌ای از طریق نفوذ در داده و دستکاری در آنها، تخریبِ تعامل میان داده‌های سامانه‌ای از طریق حمله به شبکه‌های بزرگ، دسترسی غیرقانونی به کدهای برنامه‌های حساس، تخطی از قوانین کپی‌رایت و نقض حقوق تألیف نظری اینترنت و تکثیر غیرقانونی موسیقی و فیلم روی اینترنت و تخریب اطلاعات هستند. این کنفرانس به‌عنوان اولین همایش فراملی درباره جرایم سایبر در کانون توجه حقوق‌دانان اینترنتی

1. OECD
2. AIDP

قرار گرفت و پس از آن تاریخ، همچنان در حال توسعه و گسترش است(باستانی، ۱۳۸۸: ۷۲).

در جمهوری اسلامی ایران نیز با گســترش استفاده از فناوری اطلاعات و بستر فضای سایبری، قوانین مرتبط با آن نیز وضع و توسعه پیدا کرد. نخستین واکنش قانونی ایران در برابر بعضی از جرایم رایانه‌ای، قانون اصلاح مطبوعات مصوب ۷۹/۱/۳۰ بود که مورد تأیید شورای‌نگهبان قرار گرفته‌است. دومیــن واکنش در مقابل جرایم رایانه‌ای، از طریق وضــع "قانون حمایت از حقوق پدیدآورندگانِ نرم‌افزارهای رایانه‌ای" به‌عمل آمد. این قانون در تاریخ ۸۱/۱۰/۴ به تصویب مجلس‌شورای‌اسلامی و در تاریخ ۸۱/۱۰/۱۰ به تأیید شورای نگهبان رسید. ماده ۱۳ قانونِ مذکور، نقض حقوق پدیدآورندگانِ نرم‌افزارهای رایانه‌ای موردحمایتِ این قانون را جرم تلقی کرده و برای آن، مجازاتی معادل ۹۱ روز تا ۶ ماه حبس و جزای نقدی تعیین کرده‌است. البته اشکالاتی بر این قانون وارد است که در این مقال نمی‌گنجد. سومین واکنش قانونگذار ایران در مقابل جرایم رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرایم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس‌شورای‌اسلامی به عمل آمد. بــه موجــب ماده ۱۳۱ این قانون، جعــل اطلاعات و داده‌های رایانه‌ای، تســلیم و افشای غیرمجاز اطلاعــات و داده‌هــا و سوءاستفاده مالی از طریق رایانه(کلاهبرداری و اختلاس)، جرم تلقی شده و مرتکب حســب‌مورد، به مجازات جرم ارتکابی محکوم می‌شود. چهارمین واکنش قانونی از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس‌شورای‌اسلامی به عمل آمده‌است. به موجب مواد ۷۷و ۶۶و ۶۷و ۶۸و ۶۹و ۷۴و ۷۵و ۷۶ این قانون، کلاهبرداری، جعل، دستیابی، افشای غیرمجــاز اسرارِ تجاری، نقض حقــوق مربوط‌به مالکیت معنوی(کپی رایت) و ... که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی شده و برای آن مجازات تعیین گردیده‌است. پنجمین واکنش قانونی نیز تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ می‌باشد.

۲. بررسی شبکه‌های پاسخ‌به جرایم سایبری

اصــولا حق مجــازات و کیفر، از حقوق ذاتی دولت‌هــا و از مولفه‌های حق حاکمیت است؛ چراکه مجازات‌ها اصولا از جنبه عمومی و غیرشخصی برخوردار است و واگذاری حق تنبیه به جامعه مدنی به‌دلیــل حــب و بغض و نابرابری جای ایراد است؛ بنابرایــن، حق پاسخ به جرم، یک انتخاب کلان حاکمیتی محسوب می‌گردد که با نظام سیاسی هر کشور در ارتباط می‌باشد. در سیاست جنایی، این پاسخ، قهرآمیز و کیفری است و ســست‌ترین پاسخ‌ها بــه جرم به اقتضای سن تحول بشری، پاسخ‌هــای سرکوبگر کیفری بوده‌است؛ امــا در کنار این پاسخ‌ها، ضمانت اجراهای دیگری همانند

صنفی، اداری، انتظامی و انضباطی نیز در سیاست جنایی به‌وجود آمده‌است که با وجود دارا بودن وصـف حقوقی، این دسته از ضمانت اجراها با وجود برخورداری از جنبه تنبیهی، کیفری قهرآمیز محسوب نمی‌شوند. در کنار این پاسخ‌ها، برخی از پاسخ‌ها با وصف پیشگیرانه نیز وجود دارد که در دو سطح اجتماعی و وضعی ارائه داده می‌شود(مهدوی ثابت، ۱۲:۱۳۹۵). به‌طورکلی، پاسخ به جرایم سایبـری را می‌توان در دو سطح به شرح زیر تبیین نمود: ۱. شبکه پاسخ‌های کنشی(پیشگیرانه) نسبت‌به جرایم سایبری که اغلب به دو شاخه وضعی و اجتماعی تقسیم‌بندی می‌شوند؛ ۲. شبکه پاسخ‌های واکنشی(سرکوبنده) نسـبت‌به جرایم سایبری که بـه دو شاخه قهرآمیز و غیرقهرآمیز تقسیم می‌گردند. در زیر به شرح هریک از این موارد پرداخته می‌شود.

۲ـ۱. شبکه پاسخ‌های کنشی(پیشگیرانه)نسبت‌به جرایم سایبری

نمود تأثیرپذیری دیگر سیاست جنایی از نظریه‌ها و آورده‌هایِ علمی، به‌ویژه، جرم‌شناسی پیشگیری، ظهـور راهبرد پیشگیری از بزه‌کاری و بزه‌دیده شدن شهرونـدان است که درواقع، به‌دنبال کاهش مناسبت‌های مداخله‌ای نظام‌هایِ کیفـری، اداری و انضباطی در برابر بزه‌کاری و تخلفات، با هدف صرفه‌جویی در هزینه‌هایِ مادی اجتماعی انسانی است که این مداخله برای کنشگران جرم ـ یعنی بزه‌کار، بزه‌دیده و جامعه، به‌طورکلی، به بار می‌آورد.

امروزه، پیشگیری به‌عنـوان یک راهبرد نظام‌مند سیاست جنایی، از یک‌سو، مبتنی‌بر قوانین و مقرراتی است که به‌طور مستقیم[1] یا غیرمستقیم[2]، اقدام‌های عمومی یا ویژه‌ای را ضابطه‌مند و نهاد یـا سازمان خاصی را برای مدیریت و اجرای آنها در سطح محلی، وزارتی یا در مقیاس ملی تعریف و تأسیـس می‌کنند و از سوی دیگـر، مبتنی‌بر ابتکارها و رویه‌هـای خودجوش و عملی است که متولیان نهادهای عمومی(مانند شهردار، فرماندار، استاندار، دادستان، فرمانده پلیس، شورای تأمین) یا نهادهای جامعوی (مانند انجمن حمایت از شکنجه‌دیدگان، انجمن مبارزه با اعتیاد، انجمن حمایت از زنان خشونت‌دیده، انجمن حمایت از محیط زیست برای پیشگیری از بزه‌کاری اتخاذ کرده و به اجرا می‌گذارند(نجفی ابرندآبادی،۱۴:۲۰۱۲).

---

۱. مانند قانون ارتقای سلامت اداری و مقابله با فسـاد مصوب ۱۳۹۰/۸/۷، قانون مبارزه با قاچاق کالا و ارز مصوب ۱۳۹۲/۱۰/۳، با اصلاحات مصـوب ۱۳۹۴/۷/۲۱ و قانـون مجازات قاچاق اسلحه و مهمات و دارندگان سلاح و مهمات غیرمجاز مصوب ۱۳۹۰/۷/۱۶ ماده ۱۹ در ایران یا قانون پیشگیری از بزه‌کاری مصوب ۵ مارس ۲۰۰۷ در فرانسه.

۲. مانند نهادهای فرزندخواندگی و تکلیف تربیت فرزندان توسط والدین در قانون‌مدنی یا حمایت از کودکان درمعرض خطر بزه‌دیدگی و بزه‌کاری پیشگیری رشدمدار ـ در قانون حمایت از کودکان و نوجوانان بی‌سرپرست و بدسرپرست مصوب ۱۰ مهر ۱۳۹۲ یا ماده ۱۱۴ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ که باید با احتیاط و رعایت کامل حقوق متهم اعمال گردد.

پیشگیری اجتماعی از جرایم سایبری

منظور از پیشگیری اجتماعی، مجموعه اقدامات و تدابیری است که بر خود فرد تأثیر می‌گذارند و از این طریق، خلأ و ناهنجاری‌ها را برطرف می‌کنند. تدابیر و اقدامات پیشگیری اجتماعی به دو دسته تقسیم می‌شوند: زمانی که تأثیرگذاری بر محیط‌های پیرامون انسان مدّنظر است که در اصطلاح، به آن پیشگیری جامعه‌مدار[1] یا محیط اجتماعی[2] گفته می‌شود و زمانی که تأثیرگذاری در مراحل مختلف رشد کودک و نوجوان ناسازگار منحرف یا بزهکار اعمال می‌شود، که به آن، پیشگیری فردمدار و یا رشدمدار[3] گفته می‌شود؛ که در زیر به آنها پرداخته می‌شود(پورقهرمانی،۱۳۹۵:۱۸۱).

الف. پیشگیری اجتماعی جامعه‌مدار(محیط اجتماعی) از جرایم سایبری

پیشگیری جامعه‌مدار یا محیطی ـ که رایج‌ترین شکل پیشگیری غیرکیفری است ـ برمبنای شناسایی عوامل مختلف محیطی بزهکاری به‌منظور خنثی کردن یا دست کم، کاهش آثار آنهاست. درواقع، پیشگیری جامعه‌مدار از بزهکاری با بهبود شرایط زندگی در یک محیط معین، به‌طورمستقیم بر رفتار مجرمانه تأثیر می‌گذارد(پورقهرمانی،۱۳۹۵:۱۸۲).

بر این اساس، پیشگیری محیطی بستگی‌به نوع جرایم، شرایط و اقتضائات محیطیِ خاصِ خود را می‌طلبد و یک امر ثابت و کلی که شامل تمامی جرایم باشد، نیست؛ بلکه یک امر نسبی تلقی می‌شود و بسته به نوع و ویژگی‌های هر جرمی، ممکن است متفاوت باشد و جرایم سایبری هم از این قاعده مستثنا نیست.

با توجه به موضوع و ماهیت جرایم سایبری، مهم‌ترین مواردی که می‌تواند پیشگیری جامعه‌مدار از وقوع جرایم سایبری تلقی شود، به‌همراه شبکه مرتبط به شرح زیر است:

۱.فرهنگ‌سازی: فرهنگ عبارت از مجموعه آداب‌وسنن حاکم بر جامعه در یک دوره زمانی خاص است. امروزه، بسط و گسترش روزافزون فضای سایبری و توسعه آن موجب گردیده‌است که آداب‌وسنن حاکم بر جوامع نیز دستخوش تغییر و تحول بنیادین قرار بگیرد. در این آشفته بازار فرهنگی که اغلب فرهنگ و تمدن غربی با توجه به کسب قدرت اولیه در این حوزه، از جایگاه ویژه‌ای برخوردار است و درصدد گسترش نفوذ خود با استفاده از همین فضای مجازی و تحمیل آداب و سنن تمدن غربی به سایر جوامع، ملل، تمدن‌ها و فرهنگ‌ها است. در این میان، جامعه ایرانی نیاز

1. Community Based Prevention
2. Social Environment Prevention
3. Developmental Prevention

دارد که با اساس قراردادن معیارهای ایرانی و اسلامی، هرچه سریع‌تر درجهت فرهنگ‌سازی سالم و صحیح در بستر فضای سایبری قدم بردارد.

۲. **اطلاع‌رسانی و آگاه‌سازی:** با گسترش فناوری‌های اطلاعات و فضای سایبری، محال است که کشوری بتواند درون مرزهایش مخفی شده و خود را بی‌نیاز از جهان و جهانیان بداند؛ اما روشن است که این فضا علاوه‌بر محاسن زیاد خود، معایب و خطرات زیادی نیز به‌همراه دارد. این فضا و دسترسی‌به محتویات آن، جزو حق افراد شمرده می شود(نصاری،۱۳۹۰: ۸۷) و بنابراین، نمی‌توان مانع دسترسی افراد، به‌خصوص جوانان و نوجوانان شد و چنین واکنشی، علاوه‌بر ضمانت اجراهای ملی و بین‌المللی، از منظر جرم‌شناسی نیز قضیه را بغرنج‌تر خواهدساخت. بنابراین، آموزش صحیح و به‌موقع در محیط‌های علمی(کران و دیگران، ۲۰۰۹، ۳: ۲۵۱) می‌تواند در آگاه‌سازی افراد در زمینه استفاده از چنین فضاهایی مؤثر باشد. همگام با آموزش می‌توان از اطلاع‌رسانی به‌عنوان یکی از مبانی پیشگیری و مقابله عمومی با جرایم رایانه‌ای در جامعه یاد کرد(گریکار،۲۰۰۱:۹).

در بسیاری از موارد، اطلاع‌رسانی مؤثر و به‌هنگام می‌تواند حجم خسارت‌های ناشی‌از جرایم سایبری را تا حد قابل‌ملاحظه‌ای کاهش دهد(معاونت کشف جرایم ناجا، ۱۳۷۹، ۳: ۱۰۳) که البته نقش رسانه‌های گروهی را در این زمینه نباید نادیده گرفت. یکی از انواع مهم اطلاع رسانی‌ها که اغلب مردم با آن روبه‌رو هستند، ارائه اخبار و یا گزارش‌های خبری در رسانه‌های عمومی است. در این قبیل اخبار سعی می‌شود که ضمن آشنا ساختن عموم یا اقشار خاصی از جامعه(متناسب با گستره خبری رسانه و حوزه پخش خبر) با موضوع موردنظر و آموزش غیرمستقیم درمورد مقابله با این جرایم، از ایجاد تشویق عمومی جلوگیری گردد(معاونت کشف جرایم ناجا، ۱۳۷۹، ۳: ۱۰۵). در این میان، آموزش فناوری اطلاعات به زبان خود فناوری، از اهمیت بسزایی برخوردار است؛ به عبارت دیگر، اگر آموزش موارد فرهنگی، مذهبی، ارزش‌های اخلاقی و حتی آسیب‌ها و تهدیدهای فناوری در خود آن پیاده‌سازی شود، موفقیت آن بیشتر خواهد بود. به هر حال، نباید این مسئله را کتمان کرد که در میان کاربران رایانه‌ای، بهره‌برداری مشروع و سودمند یک حلقه مفقوده محسوب می‌شود. هنوز بسیاری از مردم با کارکردهای اصلی این فناوری و خطرات آن آشنا نیستند و اغلب ابزارهای رایانه‌ای و ارتباطی را یک وسیله سرگرمی تلقی و در همین حد از آن بهره‌برداری می‌کنند؛ حال آنکه، هدف سازندگان از تعبیه گزینه‌های سرگرمی، رفع خستگی کار جدی با این ابزارها بوده‌است(باقری اصل و جلالی فراهانی، ۱۳۸۷: ۳۳)؛ بنابراین، اگر کاربران آگاه باشند که مؤسسات مالی آنها با ایمیلی که درخواست گذرواژه با جزئیات حساب بانکی کنند، هرگز با آنها

تماس نخواهند گرفت، آنها قربانی حملات فیشینگ یا کلاهبرداری هویت نخواهند شد. آموزش‌های کاربـــران اینترنت تعداد اهداف احتمالی جرایم سایبری را کاهش می‌دهد؛ همانند آموزش‌هایی از طریق برنامه‌های آموزش عمومی، آموزش در مدرسه، کتابخانه ها، مراکز IT و دانشگاه‌ها و مشارکت در برنامه‌های عمومی و خصوصی(دستور، جمشیدی‌نسب، ۱۳۹۳: ۱۲۳).

۳. تدویـــن کدهای رفتاری[1]: یکی دیگر از روش‌های پیشگیری اجتماعی جامعه‌مدار، تدوین "کدهـــای رفتاری" برای مشاغل گوناگـــون و الزام به آگاهی از مفاد آن است. منظور از کد رفتاری، مجموعه قواعـــد وضع‌شده برای دست‌اندرکاران یک حوزه خاص است تا آنها با ماهیت کار خود و همچنین، عواقبی که در اثر نقض شرایط حاکم بر آن متحمل خواهند شد، آشنا گردند. آنچه در اینجا لازم است، شناسایی نیازهای هر گروه اعم از تجار، صنعتگران، پژوهشگران، دانش آموزان و... و نیـــز هدایت صحیح آنها بـــه مقصد سایبری‌شان است(باقری اصـــل،۳۸:۱۳۸۷). یک کد رفتاری می‌تواند به‌وسیله هر سازمانی، اصولا برای الزام اعضای سازمان و تعیین مبنایی برای روند انضباطی برقرار شود(شایگان و سروستانی، ۱۳۸۸: ۴۱).

به‌طورکلی، با کدهای رفتاری می‌توان گروه‌های خاصی را که وظیفه‌ای به آنها سپرده شده‌است را در برابر اعمالشان پاسخ‌گو دانست. از جمله این گروه‌ها، گروه مشاغلی هستند که در حوزه‌های مختلف به فعالیت می‌پردازند و از آنجا که به متصدیان شبکه‌ای خود، داده‌های واجد ارزشی واگذار می‌کنند تا با رعایت سه اصل محرمانگی[2]، تمامیت [3]و دسترس‌پذیری[4] آنها را به کار گیرند، ضروری است که متناسب با حرفه، نوع و میزان اطلاعات و دیگر شرایط، کد رفتاری لازم‌الاجرای مربوط را برای آنها تدوین کنند(جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱۳۹).

۴. بهبود شـــرایط اقتصادی: برخی از جرایم سایبـــری همانند کلاهبرداری سایبری، سرقت سایبری و ... با انگیزه‌های مالی ارتکاب می‌یابند که خود ناشی‌از عوامل اجتماعی مانند فقر و بیکاری هستند. بیکاری با پیامدهای مادی و روانی خود در درازمدت، نوعی احساس نفرت را نسبت‌به جامعه فعال به‌وجود آورده‌است(گریکار،۹:۲۰۰۱). افزون بر این، احســـاس بیهودگی و درنهایت، احساس بریدن از جامعه، حالت بی‌تفاوتی، خصومت و سرانجام، انتقام‌جویی را در ذهن بیکاران ایجاد می‌کند که با گذشت زمان می‌تواند خطر بزرگی برای نظم اجتماعی، اخلاقی و فرهنگی یک کشور محسوب

1. Codes of Conduct
2. Confidentiality
3. Integration
4. Availability

شود(نجفی ابرند آبادی، ۱۳۸۲: ۳۳۲).

شبکه‌های پاسخ‌دهنده نسبت‌به پیشگیری اجتماعی جامعه‌مدار از جرایم سایبری

شبکه‌های پاسخ‌دهنده به پیشگیری جامعه‌مدار از جرایم سایبری بر اساس سیاست‌های کلان و کلی ابلاغی از طرف مقام معظم رهبری و نیز دولت ترسیم می‌گردد و بر این اساس و با توجه به برنامه‌های ابلاغی چهارم، پنجم و ششم، می‌توان گفت که در این راستا، نهادهایی همانند شورای‌عالی انقلاب فرهنگی، سازمان صداوسیما، شورای‌عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات، وزارت فرهنگ و ارشاد، نیروی انتظامی، وزارت آموزش‌وپرورش و همچنین، انجمن‌ها، ثمن‌ها و اتحادیه‌های فعال در حوزه‌های اجتماعی همگی می‌توانند نقش سازنده‌ای به عنوان یک شبکه پاسخ‌دهنده در پیشگیری اجتماعی جامعه‌مدار داشته باشند.

ب. پیشگیری اجتماعی رشدمدار از جرایم سایبری

با تعریف پیشگیری رشدمدار به‌عنوان مداخله روانشناختی ـ اجتماعی زودرس در پیشگیری از رفتارهای مجرمانه و با توجه به مسیر رشد کودک تا رسیدن به جوانی و بزرگسالی، دو عامل زیر باید مورد توجه قرار گیرد:

۱.عوامل خطر

عوامل خطر در چهار سطح بررسی می‌گردد؛ به عبارت دیگر، در حالت کلی، عواملی که کودکان و جوانان را درمعرض خطر قرار می‌دهد را می‌توان در چهار قلمرو دسته‌بندی کرد:

۱،۱. عوامل خانوادگی:

- صلاحیت ناکافی یا مسئله‌دار والدین؛
- نظارت ضعیف والدین؛
- درآمد خانوادگی ناچیز، فقر و انزوا؛
- خشونت خانوادگی، سوءاستفاده و فراموشی؛
- اختلاف خانوادگی.

۲،۱. عوامل فردی

- رفتارهای پرخاشگرانه و تکانشی زودرس؛
- فراوانی زمان صرف‌شده با دوستان بدون نظارت؛
- فراوانی رفت‌وآمد با جوانان بزهکار.

۳،۱. عوامل تحصیلی

- بازدهی تحصیلی ضعیف؛

-رفتار توأم با آشوبگری و اخلال و رعب؛

- نداشتن تعهد در مدرسه؛

- غیبت و فرار؛

- عقب‌ماندگی تحصیلی؛

- نداشتن برنامه و سازماندهی در مدیریت تحصیلی.

۴،۱. عوامل محلی

- منزل مسکونی ناسالم، شرایط و وضعیت بد زندگی در محله؛

- ازهم‌گسیختگی و عدم احساس تعلق به آن محله؛

- جابه‌جایی زیاد در سطح محله؛

- فقدان منابع و امکانات برای نوجوانان؛

- فقدان دورنمای شغلی؛

- در دسترس بودن موادمخدر.

ایــن عوامل خطر، تأثیر متقابلی بــر یکدیگر داشته و همدیگر را کامل می‌کنند. در پیشگیری باید نســبت‌به چهــار سطح ذکرشده، مدیریــت و اقــدام لازم صورت گیرد. به نظــر می‌رسد که درخصوص ارتکاب جرایم سایبری، عوامل موصوف نقش مســتقیم و غیرمســتقیمی در بزه‌کاری، بویژه در سنین کودکی و نوجوانی، دارند که نیاز است در قالب یک پژوهش کامل مورد بررسی قرار گیرد(ابراهیمی،۱۳۸۸: ۱۹۷).

۲. عوامل حمایت‌کننده

عوامل حمایت‌کننده عواملی هستند که درمقابل عوامل خطر، نقش حمایتی را برعهده دارند و عبارتنداز:

۱،۲. عوامل حمایت‌کننده خانوادگی: خانواده یک شبکه ارتباطی است و نظامی است که در آن شبکه‌های ارتباطی و قواعد منظمی حاکم است و افراد آن دارای حال، گذشته و آینده‌ای مشترک هستند. خانواده مکانی است که کودک با همه تجارب خویش به آن بازمی‌گردد و این تجارب در خانواده شناسایی، درک و ارزشیابی می‌گردد و با تشویق تجارب مثبت، موجبات بالندگی افراد را فراهــم می‌کند و تجارب منفی را تنبیه می‌کند. بر این اساس، برخی مداخله‌های خانواده‌مدار که برای پیشگیری از اختلالات رفتاری و بزه‌کاری طرح‌ریزی می‌شوند، بدین‌گونه قابل‌تقسیم هستند:

۱. برنامه دیدارهای خانگی زودهنگام و آموزش‌های پیش‌دبستانی؛ ۲. خانواده درمانی و آموزش پدر و مادر؛ ۳. حفظ خانواده(گراهام، ۲۰۰۱، ۳۱۲).

اولین محیطی که توجه متصدیان پیشگیری رشدمدار را به خود جلب می کند، خانواده و بالطبع والدین است؛ بنابراین، چنانچه بتوان در ابتدا، توصیه‌ها و آموزش‌های لازم درمورد فضای سایبری و رایانه‌ای را به والدین منتقل و آنها را با خطرها و درعین‌حال، مزایا و مطلوبیت‌های فضای سایبر آشنا کرد، می‌توان امیدوار بود که تا حد زیادی این تدابیر به ثمر بنشیند(باقری اصل و جلالی،۱۳۸۷: ۳۴).

۲,۲. عوامل حمایت‌کننده در مدرسه: بعد از خانواده، جایگاه مدرسه و نظام آموزش‌وپرورش در حمایت از اطفال و نوجوانانِ درمعرض خطر، جایگاهی منحصربه‌فرد و بی‌بدیل است. گرایش اطفال و نوجوانـــان به بزه‌کاری ناشی‌از اختلال در کارکردهای رشدی، جامعه‌پذیری و پایشیِ نخســـتین مراجعِ جامعه‌پذیریِ کودک ـ یعنی خانواده، مدرسه، همسالان و رسانه‌ها ـ است. اطفال درمعرض خطر، به‌ویژه از نظر خانوادگی، درمعرض آسیب‌های اختلال کارکردی هستند و بنابراین، خانواده آنهـــا، خود، محتاج اقدامات مداخله‌ای حمایتی است. نظـــام آموزش‌وپرورش، ابزار رسمی اجتماع بـــرای انتقال ارزش‌ها و هنجارهای پذیرفته‌شـــده اجتماعی به کودکان و نوجوانان است. کودک در سنین مدرسه در شرایط حســـاسی قرار دارد که هم می‌توان نشانه‌های اولیه اختلالات رفتاری را در وی کشف کرد و هم قابلیت اصلاح رفتار و بازگشتن وی به مســـیر رشد مطلوب در این سنین بســـیار قوی است. به‌عبارت‌دیگر، دانش‌آموزان الگوپذیری مطلوبی از معلمان خود دارند؛ پس اگر معلمان الگوهای محیطی مناسبی را درجهت تطبیق دانش‌آموزان با ارزش‌های جامعه ارائه دهند، دانش‌آموزان نیز سعی می‌کنند که خود را با قوانین اجتماعی هماهنگ سازند(فهیمی،۱۳۸۰: ۲۹۶). بـــر این اساس، معلمان باید آموزش صحیح استفاده‌از رایانه و اینترنت را در قالب محتوای مباحث درسی به دانش‌آموزان آموزش دهند و حتی معلمان می‌توانند سایت‌هایی با محتوای آموزشی ایجاد و در اختیار آنها قرار دهند؛ همچنین، می‌توان از طریق ابزارهایی همچون نصب تابلوهای مرتبط با اینترنت و خطرات آن و نیز از طریق برگزاری دوره‌های آموزشی در قالب نمایش و فیلم به نتیجه نائل شد که این اقدام آموزشی مانعی در راستای نهادینه‌کردن نحوه استفاده با اینترنت و رایانه است.

۳,۲. عوامل حمایتی در زمینه همســـالان: کودکان و نوجوانان در مســـیر رشد، مراحل متعدد و مختلفـــی را طـــی می‌کنند و هر مرحلـــه از رشد آنها تحت‌تأثیر عواملی اســـت که ابعاد رشدی، جامعه‌پذیری و پایشی آنها را تحت‌تأثیر قرار می‌دهد. ازآنجاکه در دوره نوجوانی نیاز به استقلال و احســـاس هویت فردی در فرد تقویت شده و فرد با احساس برابری مشابهت، نیاز به امنیت، تعلق

و احترام خود را از طریق گروه همســالان تأمین می‌کند، به‌همین‌دلیل، نفوذ گروه همســالان بر وی افزایش می‌یابد. سهولت یادگیری کودکان و نوجوانان از همســالان، احساس مشابهت و عدم سلسله‌مراتب بین همسالان و نیز کارکرد نامطلوب خانواده کودکان و نوجوانان درمعرض خطر، از مهم‌ترین دلایلی است که طراحی برنامه‌های حمایتی با استفاده از نفوذ گروه همسالان را از اهمیت ویژه‌ای برخوردار می‌کند(مهدوی، ۱۳۹۰: ۴۹۴)؛ بر این اساس، همسالان که می‌توانند دانش‌آموزان، هم‌بازی‌ها، همسایگان یا افراد بزرگ‌تر خانواده باشند، می‌توانند برای دوستان و همسالان خود در استفاده صحیح از اینترنت نقش به‌سزایی را ایفا کنند؛ بنابراین، نقش همسال و همبازی کودک در تلقین رفتارهای مثبت یا منفی بسیار مهم و حائز اهمیت است(پورقهرمانی،۱۳۹۵:۲۰۹).

۴،۲. عوامل حمایت‌کننده رسانه‌ای: هرچند که اینترنت هم می‌تواند جزو رسانه تلقی شود ولی منظــور ما در اینجا غیر از اینترنت(مثل رادیو، تلویزیون، روزنامه و ...) است. امروزه، نفوذ روزافزون رسانه‌ها در ابعاد مختلف فردی و اجتماعی زندگی انسان‌ها غیرقابل‌انکار است و بنابراین، ویژگی‌های رسانه می‌تواند در وضعیت‌های خاص دوران کودکی و نوجوانان نقش به‌سزایی داشته باشد؛ چراکه بــر اساس تحقیق انجام‌شده، بیشترین تماشاگران تلویزیــون در شهر تهران، کودکان کمتر از ۱۵ سال هستند(شیخاوندی، ۱۳۷۹: ۲۴۴)؛ بنابراین، اهمیت رسانه‌ها در این زمینه دوچندان می‌شود. رسانه‌ها می‌توانند کارکرد مثبت هر یک از نهادهای تربیتی کودکان را تقویت کنند، پیام‌های هنجاری خــود را تکرار نموده و از روش‌های دراماتیک، هیجانی و اغراق‌آمیز برای ایجاد جاذبه در مخاطبان بهره برند. استفاده از قابلیت رشدی، جامعه‌پذیری و پایشی رسانه در قالب برنامه‌های حمایتی، از ضروری‌ترین بخش‌های برنامه جامع حمایت از اطفال و نوجوانان درمعرض خطر می‌باشد(آجرلویی، ۱۳۹۱:۲۲). بــا این توضیح، واضح است که بســیاری از خانواده‌ها به‌خصوص در مناطق محروم و روستانشین از اینترنت و محیط مجازی اطلاعاتی ندارند تا سلامت کارکرد آن را آموزش دهند؛ بر این اساس، رسانه‌ها به‌خصوص تلویزیون ـ که غالب کودکان از آن بهره‌مند هستند ـ نیز می‌توانند از طریق پخش فیلم آموزش کودکانه و یا کارتون مرتبط با رایانه، اینترنت و ... در زمینه پیشگیری از انحرافات سایبری و رایانه‌ای کمک به‌سزایی کند(پورقهرمانی،۱۳۹۵:۲۱۰).

شبکه‌های پاسخ‌دهنده نسبت‌به پیشگیری اجتماعی رشدمدار از جرایم سایبری

برخلاف پیشگیری جامعه‌مدار، شناسایی شبکه‌های پاسخ‌دهنده در پیشگیری رشدمدار آسان‌تر است؛ چراکه در این نوع پیشگیری، نخســت، با نهادهای محدود و خاصی مواجه هستیم و دوم، با

مرتکبان محدود ـ که سنین کودکان و نوجوانان را شامل می‌گردد. به نظر می‌رسد که این شبکه‌ها عبارتند از خانواده، وزارت آموزش‌وپرورش و صداوسیما.

پیشگیری وضعی از جرایم سایبری

همان‌طورکــه در ابتدای بحث پیشگیری به‌طورخلاصه گفته شد، پیشگیری وضعی بر این فرض اســتوار است که یک انســان متعارف در همــه زمینه‌ها، خواسته یا ناخواســته، به‌طور منطقی و حساب‌شده عمل کرده و از خطرات شدید دوری می‌کند؛ یعنی درصورتی تن به خطر می‌دهد که عایدات یا منافع حاصل از آن عمل، ارزشمند باشد؛ حال اگر این فرض درمورد مجرمان درست باشد، می‌توان گفت که اگر به هر شکل بتوان خطرپذیری جرم را افزایش داد یا جاذبه و منفعت حاصل از آن را کاهش داده یا از بین برد، قاعدتا مجرمان بالقوه از ارتکاب جرم منصرف خواهند شد(نجفی ابرندآبادی،۱۳۸۲).

پیشگیــری وضعی برخــلاف پیشگیری اجتماعی نمی‌خواهد با به‌ســازی محیطی و نظایر آن، تمایلات مجرمانه را از بین ببرد؛ بلکه هدف، نوعی توان‌گیری غیرکیفری از طریق تقویت آمار جرم و ... است. در پیشگیری وضعی به جای اثرگذاری بر شخصیت فرد و تغییر آن(که زمان‌بر و یا حتی گاهــی غیرممکن است) با ایجاد تغییر در موقعیــت ماقبل بزه‌کاری، فرایند تصمیم‌گیری مرتکب مختل می‌شود. در این نوع پیشگیری هم مثل مدیریت آماری، خطرپذیری جرم[1] پیش‌بینی نقش محوری دارد. موقعیت پر از خطر باید شناسایی گردد. موقعیت پر از خطر ممکن است ناشی‌از یک بزه‌دیده حمایت‌نشده، مکان حمایت‌نشده و ... باشد(پاک نهاد، ۱۳۸۸: ۲۴۱).

در هر حال، در رویکرد وضعی به پیشگیری، اعتقاد بر این است که «جرم قابل پیش‌بینی بوده و صرف‌نظر از اینکه مرتکب تحت‌تأثیر چه عاملی بوده، از طریق کاهش فرصت‌های ارتکاب و آماج‌های آن، بــا اعمال روش‌های فیزیکی(مادی) یا تغییــر و پایش موقعیت‌های مناسب برای ارتکاب جرم می‌توان وقوع آن را ممتنع و خنثی ساخت؛ بدین‌طریق، از ورود به وادی پیچیده سلســله عوامل متعدد انسانی و اجتماعی جرم و تحلیل و برخورد با آنها احتراز می‌گردد»(صفاری، ۱۳۸۰: ۲۸۳).

در زمینــه پیشگیری وضعی از جرایم سایبری باید اذعــان داشت که با وجود انتقادات وارده بر آن، بــاز هم از جایگاه خاصی برخوردار اســت. یکی از دلایلی که می‌توان جهت توجیه پیشگیری

۱. مدیریــت خطرپذیــری دربــاره حــذف، کاهــش، انتقــال منفــی حــوادث و بهــره جســتن از فرصت‌هــای احتمالی ســخن می‌گویــد. هدف اصلــی مدیریت خطرپذیری، تغییر دادن محیط است.

وضعی از این جرایم عنوان نمود، همین قابلیتی است که فضای تبادل اطلاعات فراهم آورده‌است. همان‌طورکــه گفته شد، ماهیت جرم مبتنی‌بر رایانه به گونــه‌ای است که نمی‌توان با دست تهی مرتکب آن شد و باید علاوه‌بر صرف اندیشه کافی، ابزارها و لوازم موردنیاز را هم در اختیار داشت؛ اما این بدین معنا نیست که برای ارتکاب قسمت عمده‌ای از این جرایم باید تخصص و مهارت فوق‌العاده داشت، بلکه اگر فرد از دانش کافی جهت بهره‌برداری ابتدایی از سامانه‌های رایانه‌ای برخوردار باشد، زمینه برای وقوع جرم مساعد می‌شود؛ از این رو، آنچه در پیشگیری وضعی از جرایم رایانه‌ای دنبال می‌شود، این است که با اتخاذ تدابیر فنی، از بهره‌برداری این‌گونه قابلیت‌های جرم‌برانگیز این فضا جلوگیری شود؛ به عبارت دیگر، مخاطبان اصلی پیشگیری وضعی از جرایم رایانه‌ای کسانی هستند که از تخصص و مهارت بالایی برخوردار نیستند و بیشتر سعی می‌کنند با امکاناتی که فضای تبادل اطلاعات در اختیار آنها قرار می‌دهد، مرتکب جرم شوند، نه اینکه خود دست به ابتکار عمل بزنند که در این صورت، از پیشگیری وضعی کاری ساخته نخواهد بود. دلیل مهم دیگری که باعث شده است تــا پیشگیری وضعی در جرایم رایانه‌ای با تمام کاستی‌های آن دنبال شود، بحث شبکه‌های اطلاع رسانی رایانه‌ای است. تقریبا می‌توان گفت که هرگونه اقدامی در فضای تبادل اطلاعات، مستلزم این است که از طریق شبکه‌های اطلاع‌رسانی رایانه‌ای بدین فضا وارد شویم؛ آن هم شبکه‌هایی که در دنیای امروز، به‌طور تخصصی فعالیت می‌کنند و هر یک به ارائه یک نوع خدمات در فضای تبادل اطلاعات می‌پردازند و از همه مهم‌تر اینکه تحت‌نظارت دولت و مقررات قانونی لازم‌الاجرا هستند. درحقیقت، این شبکه‌ها پل ارتباطی ما با فضای تبادل اطلاعات هستند و به این ترتیب، اگر در این پــل ارتباطی اقدامات پیشگیرانه وضعی مؤثری اعمال شــود، می‌توان امیدوار بود که تا حدودی از وقوع جرایم در فضای تبادل اطلاعات جلوگیری می‌شود. این وضعیت مزیتی برای پیشگیری وضعی از این جرایم محسوب می‌شود که پیشگیری وضعی از جرایم سنتی از آن بی‌بهره است؛ چراکه در آنجا هیچ عامل مؤثری را نمی‌توان میان سیبل جرم و مجرم قرار داد. آنچه که امروزه، در قالب نصب دیــوار آتشین در این شبکه انجام می‌شود، چیزی جز پیشگیری وضعی نمی‌باشد(جلالی فراهانی ،۱۱۰:۱۳۸۳)؛ بنابراین، در اینجا به مجرمان اجازه داده نمی‌شود که به‌راحتی به مقصود خود نائل شونــد؛ همچنین، با پیدایش پدیده‌هایی مانند پلیس گشت سایبر، پیشگیری وضعی در این فضا جلــوه دیگــری نیز به خود گرفته‌است که البته با الهام از نتایج مثبت پلیس گشت پیاده، به‌عنوان یک اقدام وضعی پیشگیرانه به اجرا درآمده‌است. آخرین دلیلی که می‌توان جهت پیشگیری وضعی از جرایم رایانه‌ای ذکر کرد، به ویژگی منحصربه‌فرد فضای تبادل اطلاعات مربوط می‌شود. در این

فضا، شخص می‌تواند برخلاف دنیای فیزیکی، در یک زمان، در چند نقطه ظاهر شود و با انجام یک عمل بر چند نقطه تأثیر بگذارد؛ به‌عنوان مثال، یک مجرم می‌تواند از طریق شبکه به تعداد بسیاری رایانه میزبان متصل شود و به‌طور هم‌زمان، در فعالیت تمامی آنها اختلال ایجاد کند یا با آنها ارتباط زنده برقرار کرده و مرتکب اشکال مختلفی از عناوین مجرمانه شود. البته باید توجه داشت که این خصیصه جدا از حوزه تأثیرگذاری فضای تبادل اطلاعات است که نسبت‌به دنیای فیزیکی، حوزه بسیار گسترده‌تری را دربرمی‌گیرد؛ به‌عنوان مثال، گستره تأثیرهای مخرب نشر مطالب تحریک‌آمیز بر ضدّ امنیت‌ملی یا مطالب توهین‌آمیز نسبت‌به مقدسات مذهبی یا تصاویر حاوی هرزه‌نگاری در این فضا بر کسی پوشیده نیست(پورقهرمانی،۱۳۹۵:۲۱۵).

تدابیر پیشگیرانه وضعی

درمورد هر جرمی و با توجه به موضوع آن می‌توان تدابیر وضعی متناسبی اتخاذ کرد. درخصوص تدابیر پیشگیری وضعی از جرایم و در راستای برقراری امنیت، می‌توان یکی از روش‌های زیر را در پیش گرفت:

۱. دشوار ساختن ارتکاب جرایم سایبری برای مجرمان بالقوه از طریق ایجاد موانع به‌منظور محدود نمودن فعالیت مجرمانه آنها؛

۲. دشوار ساختن ارتکاب جرم با آگاهی دادن به کاربران ابزارهای این محیط(بزه دیدگان بالقوه).

بر اساس این دو روش، کارشناسان، تدابیر پیشگیرانه وضعی در محیط مجازی را در چهار گروه اصلی دسته‌بندی کرده‌اند: تدابیر محدودکننده یا سلب‌کننده دسترسی، ناشناس‌کننده و رمزنگارها، تدابیر صدور مجوز و تدابیر نظارتی(سادوسکای، جورج و دیگران،۱۳۸۴: ۲۲۱).

شبکه‌های پاسخ‌دهنده نسبت‌به پیشگیری وضعی از جرایم سایبری

اغلب شبکه‌های پاسخ‌دهنده در پیشگیری وضعی، ارتباطی مستقیم با ساختار حاکمیتی دارند؛ چراکه تغییر در وضعیت‌های مختلف، تنها با دسترسی‌به زیرساخت‌های فناوری اطلاعات و ارتباطات هر کشوری مقدور می‌باشد. در جمهوری اسلامی ایران، این شبکه‌ها عبارتند از شورای‌عالی امنیت‌ملی، شورای‌عالی فضای مجازی، قوه قضائیه، نیروی‌انتظامی و وزارت فناوری اطلاعات و ارتباطات.

۲،۲. شبکه پاسخ‌های واکنشی(سرکوبنده)نسبت‌به جرایم سایبری

اصــولا در پاسخ‌دهی به رفتارهای مجرمانــه، از جمله جرایم رایانه‌ای تا زمانی که امکان توسل به پاسخ‌هــای غیرسرکوبگر یا غیرقهرآمیز وجود داشته باشد؛ نباید به پاسخ‌های سرکوبگرانه متوسل شد. با این وصف، وقتی که با اتخاذ پاسخ‌های پیشگیرانه چون تدابیر پیشگیرانه اجتماعی یا وضعی کــه پیش‌تر گفته شد، نتوان فرایند گذار از اندیشه به اعمــال مجرمانه رایانه‌ای را از مرتکبان این جرایم سلب کرد و به عبارت دیگر، درصورتی‌که پاسخ‌های کنشی جرم‌شناسی نســبت‌به برخی از مرتکبان، کارایی نداشته و آنها بتوانند وضعیت پیش از بزهکاری یا پیش‌جنایی این جرایم را پشت سر گذاشته و قصد مجرمانه خود را در عالم خارج به منصه ظهور رسانده یا حداقل شروع به عملیات اجرایی آن نمایند، نوبت به اعمال پاسخ‌های سرکوبگرانه می‌رسد. حال این پاسخ‌های سرکوبگرانه می‌تواند از نوع کیفری یا قهرآمیز باشد که به لحاظ ویژگی‌های خاص جرایم رایانه‌ای، امروزه، غالب دولت‌ها، در مجموعه قوانین کیفری خود از طریق جرم‌انگاری جرایم رایانه‌ای، به پاسخ‌های سرکوبگر متوسل شده‌اند؛ هرچندکــه دولت جمهوری اسلامی ایران با تصویب قانون تجارت الکترونیک در سال ۱۳۸۲ و با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸، با توجه به نوع جرایم، مجازات‌های مختلف و متنوعی را تعیین کرده‌است؛ وانگهی در کنار پاسخ‌های کیفری، باید بر اعمال پاسخ‌های غیرکیفری(غیرقهرآمیز) نظیر پاسخ‌های اداری و انضباطی تأکید کرد.

الف.پاسخ‌های کیفری

قانــون جرایم رایانه‌ای مصوب ۱۳۸۸ بدون ذکر تعریف از جرایم رایانه‌ای در ۵۶ ماده و سه بخش جرایــم و مجازات‌ها، مقررات آئیــن دادرسی و سایر قوانین ترسیم گردیده‌است. در بخش جرایم و مجازات‌ها، جرایم را در شش دسته زیر تقسیم نموده‌است:

۱.جرایم بر ضدّ محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی که شامل "دسترسی غیرمجاز"، "شنود غیرمجاز" و "جاسوسی رایانه‌ای" می‌شود؛

۲.جرایــم بر ضدّ صحت و تمامیــت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی که "جعل رایانه‌ای" و "تخریب و اخلال در داده‌ها" با سامانه‌های رایانه‌ای و مخابراتی می‌شود؛

۳.سرقت و کلاهبرداری مرتبط با رایانه؛

۴.جرایم بر ضدّ عفت و اخلاق عمومی؛

۵.هتک حیثیت و نشر اکاذیب؛

۶. سایر جرایم.

نقطــه حائــز اهمیت این است که برای اولین بار در فصل ششم از بخش اول در این قانون برای اشخاص حقوقی نیز مسئولیت کیفری تدوین شده‌است.

شبکه‌های پاسخ‌دهنده کیفری نسبت‌به جرایم سایبری

شبکه‌های پاسخ‌دهنده کیفری به جرایم سایبری در ایران عبارتند از قوه قضائیه و نیروی‌انتظامی که برابر قانون، مسئولیت برخورد کیفری با بزه‌کاری در کشور را برعهده دارند.

ب. پاسخ‌های غیرکیفری

رویکرد پاسخ‌های غیرکیفری بیشتر از آنکه در فکر مجازات مرتکبان جرایم سایبری باشد، در پی پیشگیری از وقوع و تکرار این جرم و به‌نوعی حمایت از قربانیان با اتخاذ اصول و رویه‌های عدالت ترمیمی می‌باشد.

۱. پاسخ‌های تأمینی: پاسخ‌های تأمینی اغلب نسبت‌به اشخاص حقوقی حقوق خصوصی که با عنوان مؤسسات اینترنتی یا ارائه‌دهندگان خدمات دسترسی و میزبانی یا ارائه‌دهندگان خدمات اطلاع‌رسانی و اینترنتی(رساء) فعالیت دارند، اعمال می‌شود. این پاسخ‌ها اغلب تعطیلیِ موقت محلِ کسب تا انحلال محل و نیز تذکر و لغو پروانه و ... می‌باشند. برخی‌از پاسخ‌های فوق از طرف مقتن پیش‌بینی شده‌است و برخی دیگر، از طرف سازمان‌های مربوط بر اساس آیین‌نامه مقرر شده‌است. مقنن جرایم رایانه‌ای در کنار توصیف مسئولیت کیفری اشخاص حقوقی در ماده ۱۹، در ماده ۲۰ علاوه‌بر پاسخ‌های کیفری(که فقط جزای نقدی هستند)، پاسخ‌های تأمینی مناسبی را با توجه به شخصیت آنها مقرر نموده‌است.

۲. پاسخ‌های سیاسی: با توجه به اینکه جرایم سایبری فراملی هستند، پس می‌توانند تهدیدی نسبت‌به کشورها و جوامع باشند و در سطح جهانی نیز صلح و امنیت بین‌المللی را تهدید نمایند؛ بنابراین، چه‌بسا تهدیدات و خطرات سایبری از کشوری نسبت‌به کشور دیگر ممکن است که روابط دو کشور را برهم زند و چه‌بســا پیامدهای سیاسی و واکنشی را در پی داشته باشد(نور محمدی، ۱۳۹۰: ۲۸)؛ به عبارت دیگر، دولت‌ها در وضعیتی نیســتند که به‌طور انحصاری و به‌تنهایی قواعد بازی و سیاسی را دیکته کنند؛ از این رو، دولت‌ها در برابر این وضعیت واکنش نشان می‌دهند(مثل ویروس استاکس‌نت). این حملات سایبری اغلب ازپیش‌طراحی‌شده است. قواعد بین‌المللی خاصی در ایــن زمینه وجود ندارد ولــی با این همه، کشورها می‌توانند درمقابــل این حملات، پاسخ‌ها و

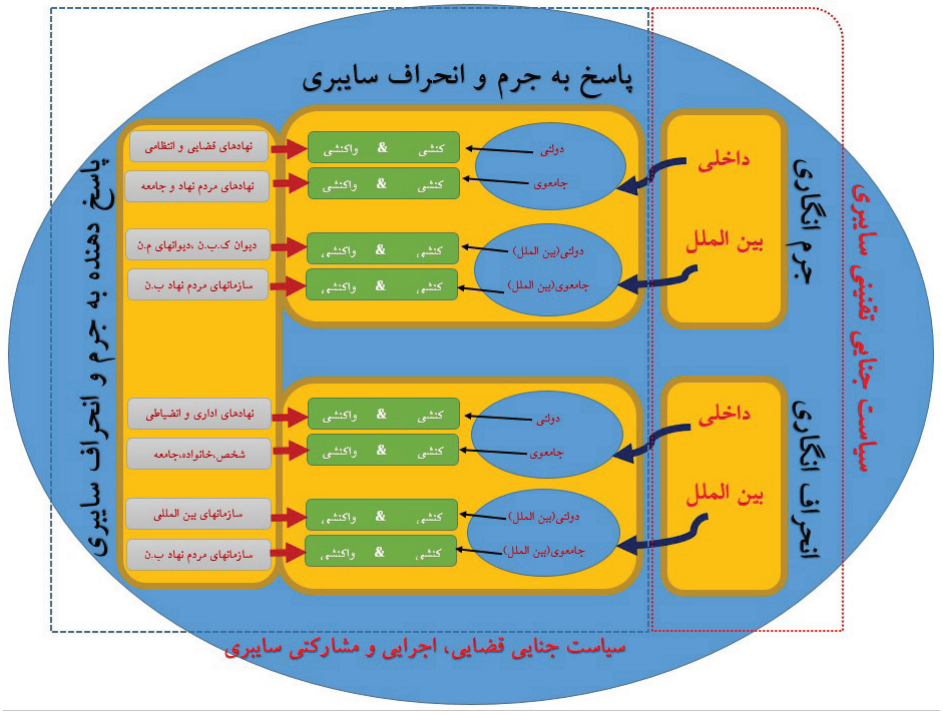
اقدام‌های مقابله‌به‌مثلی انجام دهند(پورقهرمانی،۱۳۹۵:۲۷۱).

شبکه‌های پاسخ‌دهنده غیرکیفری نسبت‌به جرایم سایبری

شبکه‌هـــای پاسخ‌دهنـــده کیفری به جرایم سایبری در ایران عبارتنـــد از: ثمن‌ها و اتحادیه‌ها، قوه قضائیه، نیروی‌انتظامی و شورای‌عالی امنیت‌ملی.

الگوی مفهومی تحقیق

در این گفتار، الگوی مفهومی تحقیق برگرفته از مبانی نظری تحقیق ارائه می‌گردد. در این الگو، کلیات و روابط جامعوی از متغیرهای مستقل، وابسته و تعدیل‌گرای احصاءشده از مبانی در قالب الگوی مفهومی به شرح شکل زیر ارائه گردیده‌است.



طبـــق شکل، مفهوم‌های سیاست جنایی تقنینی جرایم سایبـــری به‌عنوان مفهوم اول از پایش جرایم سایبری و مفهوم سیاست جنایی اجرایی به‌عنوان مفهوم دوم از پایش جرایم سایبری، تبیین

و تعریـف گردیده‌است. در مفهـوم اول، جرم‌انگاری و انحراف‌انگاری به‌عنـوان ابعاد و واکنش‌های داخلـی و بین‌المللی به‌عنوان مولفه‌هـا تدوین گردیده‌اند و در مفهـوم دوم، شبکه پاسخ‌دهنده و شبکه پاسخ، هرکدام به‌عنوان ابعاد مفهوم و پاسخ‌های دولتی ـ جامعوی و نیز دولت(بین‌الملل) ـ جامعوی(بین‌الملل) به‌عنوان مولفه‌هایی از ابعاد یادشده، تدوین گردیده‌است. روابط بین مفهوم، ابعاد و مولفه‌ها ترسیم شده‌است.

نتیجه‌گیری

سیاست جنایی جرایم سایبری شامل کلیه شیوه‌ها و روش‌هایی است که هیئت اجتماع از طریق آنهـا پاسخ‌گویی به پدیـده جنایی در فضای سایبری را سامان می‌بخشد. حسـب تعریف بالا و با لحـاظ قراردادن الگوی مفهومی احصایی و سنجـش وضعیت موجود، به نظر می‌رسد که در ابعاد مختلف سیاست جنایی جرایم سایبری همانند تقنینی، قضایی، اجرایی و مشارکتی، باید اقدامات و برنامه‌ریزی کلان و راهبردی صورت پذیرد؛ چراکه خلأها و ابهامات و سکوت قوانین در بعد تقنینی، خـلأ مهارتی و آموزشی در بعد قضایـی، خلأهای زیرساختی، واکنشی و کنشی در ابعاد اجرایی و مشارکتی همگی موجب می‌گردد که کارکرد سیاست جنایی در قبال جرایم سایبری بسیار کند، معیوب و ضعیف باشد.

الگوی مفهومی ارائه‌شده نشان می‌دهد که در جهت تکامل سیاست جرایم سایبری، باید اقدامات بین‌المللی را در حوزه‌های کنشی و واکنشی بسیار تقویت نمود و باتوجه به بعد فراملی آثار و تبعات بزه‌های سایبری نیازمند تلاش، همکاری و تعامل بین‌المللی می‌باشد. با همه این اوصاف، اولین گام در جهـت ترسیم صحیح سیاست جنایی در قبال جرایم سایبری، الگوسازی است. الگوها به‌دنبال چیستی‌ها هستند. وضعیت‌شناسی سیاست جنایی موجود موجب می‌گردد تا دانسته شود که به چه چیزهایی برای درک صحیح سیاست جنایی مرتبط نیاز است و بر اساس ابعاد، مولفه‌ها و معرف‌های احصایـی در الگوها می‌توان ارتباط‌سازی بین این حوزه‌هـا را از طریق الگوهای اجرایی و نقشه‌راه ترسیم نمود تا به یک سیاست منسجم، صحیح و دقیق منجر شود.

فهرست منابع

ـ انصاری، محمد مهدی(۱۳۹۰)، جنگ واقعی در فضای مجازی، تهران: دفتر مطالعات و برنامه‌ریزی رسانه‌ها

ـ اولریش زیبر(۱۳۸۲)، جرایم رایانه‌ای، ترجمه محمد علی نوری، تهران: گنج دانش
ـ آئین دادرسی کیفری ایران
ـ باستانی برومند(۱۳۸۸)، جرایم کامپیوتری و اینترنتی؛ جلوه‌ای نوین از بزه‌کاری، تهران: بهنامی
ـ بای؛ حسینعلی، پورقهرمانی؛ بابک(۱۳۸۸)، بررسی فقهی حقوقی جرایم رایانه‌ای، تهران: پژوهشگاه علوم و فرهنگ اسلامی
ـ پاکـــزاد، بتول(۱۳۸۸)، تروریســـم سایبری؛ رساله دکتری در حقوق جـــزا و جرم‌شناسی، تهران: دانشکده حقوق دانشگاه شهید بهشتی(ره)
ـ پلومان، ادوارد(۱۳۸۰)، حقوق بین‌الملل؛ ارتباطات و اطلاعات، ترجمه بهمن آقایی، تهران: کتابخانه گنج و دانش
ـ پورقهرمانی، بابک(۱۳۹۵)، سیاست جنایی ایران در قبال جرایم رایانه‌ای، تهران: شهر دانش
ـ حافظ نیا، محمدرضا(۱۳۹۱)، جغرافیای سیاسی فضای مجازی، تهران: انتشارات سمت
ـ حســـینی، سید محمد(۱۳۹۴)، سیاست جنایی در اســـلام و در جمهوری اسلامی ایران، تهران: انتشارات سمت
ـ زندی، محمد رضا(۱۳۹۴)، تحقیقات مقدماتی در جرایم سایبری، تهران: انتشارات جنگل
ـ شیرزاد، کامران(۱۳۸۸)، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، تهران: شرکت نشر بهینه فراگیر
ـ صبح خیز، رضا(۱۳۹۸)، جرایم سایبری در نظام حقوقی ایران و جهان، تهران: انتشارات دانشگاه علوم انتظامی
ـ ضیایی بیگدلی(۱۳۸۶)، حقوق بین‌الملل عمومی، تهران: انتشارات گنج دانش
ـ قانون جرایم رایانه ای مصوب سال ۸۸ ایران
ـ قانون مجازات اسلامی ایران
ـ گرکـــی، مارکو(۱۳۹۰)، جرایم سایبری راهنمایی برای کشورهای درحال‌توسعه، ترجمه مرتضی اکبری، تهران: پلیس فتا
ـ لازرژ، کریســـتین(۱۳۹۹)، درآمدی بر سیاست جنایی، ترجمه علی حســـین نجفی ابرندآبادی، تهران: انتشارات میزان
ـ مصوبات کنوانسیون بوداپست ۲۰۰۱
ـ مـــی ری دلمـــاس، مارتی(۱۳۹۳)، نظام‌های بزرگ سیاست جنایی، ترجمه علی حســـین نجفی

ابرندآبادی، تهران: بی‌جا
ـ ـــــــ(۱۳۸۳)، بررسی ابعاد حقوقی فناوری اطلاعات، تهران: مرکز مطالعات راهبردی و توسعه قضایی
ـ ـــــــ(۱۳۷۶)، نشریه بین‌المللی سیاست جنایی(ش۴۴،۱۹۹۴/۴۳)، ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور
ـ ـــــــ(۱۹۹۰)، شـورای اروپا جرم رایانه‌ای، توصیه‌نامه شماره ۸۹، ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور