



Conceptual model of cybercrime criminal policy in Iran

Reza Sobhkhiz¹

Babak Pourghahramani²

Ali Saffari³

Article type: Article extracted from the doctoral dissertation



Received: 2021.11.27

Accepted: 2021.4.29

DOR: 20,1001,1,25381946./SSJ.2021,97092

Abstract

Today, the use of information and communication technology and the cyberspace platform has overshadowed many aspects of human life; As the relationships of people in this context have led to the formation of the title of “cyber communities”. The dimension of security and public order is the most important element in the stability of any society; Cyber communities are no exception to this and seek to outline their criminal policies to ensure the security of life, property and dignity of citizens as well as the security of public institutions in the context of cyberspace. In Iran, due to the high rate of Internet penetration and the large number of users, creating a criminal policy to manage and control cyber anomalies is of great importance and priority; Accordingly, in this category, by examining the documents and studying the library, the trends and approaches of the criminal policy of the Islamic Republic of Iran in cyberspace are explained, as a result, a conceptual model of relative cybercrime-related criminal policy for scientific and practical development is presented.

Key Words

Criminal policy, Cyberspace, Cyberspace, Cybercrime

1. PhD Student in Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Research Sciences Branch, Islamic Azad University, Tehran, Iran, reza122onlymorning@gmail.com

2. Associate Professor, Department of Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Maragheh Branch, Islamic Azad University, Maragheh, Iran, b.pourghahramani@yahoo.com

3. Associate Professor, Department of Criminal Law and Criminology, Faculty of Law, Theology and Political Science, Shahid Beheshti University, Tehran, Iran, a-saffary@sbu.ac.ir

الگوی مفهومی سیاست جنایی جرایم سایبری در ایران

رضا صبح خیز^۱

بابک پورقهرمانی^۲

علی صفاری^۳

نوع مقاله: مقاله مستخرج از رساله دکتری

تاریخ پذیرش نهایی: ۱۴۰۰/۲/۹

تاریخ دریافت: ۱۳۹۹/۹/۷



فصلنامه مطالعات راهبردی ناجا، سال ششم، شماره ۲ (پیاپی ۲۰) - تابستان ۱۴۰۰ * ۱۵۴-۱۲۹

DOR: 20,1001,1,25381946./SSJ.2021,97092

چکیده

امروزه، استفاده از فناوری اطلاعات و ارتباطات و بستر فضای سایبری در بسیاری از ابعاد زندگی بشر سایه افکنده است؛ به طوری که روابط افراد در این بستر منجر به شکل گیری عنوان "جوامع سایبری" گردیده است. بعد امنیت و نظم عمومی مهم ترین رکن در پایداری هر جامعه است؛ جوامع سایبری نیز از این امر مستثنی نبوده و به دنبال 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 ناهنجاری های سایبری از اهمیت و اولویت به سزایی برخوردار است؛ بر این اساس، در این مقوله، با بررسی اسناد و مدارک و مطالعه کتابخانه ای، روندها و رویکردهای سیاست جنایی جمهوری اسلامی ایران در فضای سایبری تبیین گردیده و در نتیجه، الگوی مفهومی از سیاست نسبی جنایی مرتبط با فضای سایبری برای اقدامات علمی و عملی توسعه ای ارائه شده است.

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

مقدمه

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

۱. دانش آموخته 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 جرم شناسی، 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 در مجموع، به پایش جرم می‌پردازند (مهدوی ثابت، ۱۳۹۵: ۱۲). اصطلاح سیاست جنایی که عموماً به کتاب فوئر باخ در سال ۱۸۰۳ منتسب می‌شود، مدت‌ها با "جنبه‌های نظری و عملی نظام کیفری" مترادف مانده‌است. مطابق نظر فوئر باخ، سیاست جنایی شامل مجموعه شیوه‌های سرکوبگری می‌شود که دولت از طریق پیش‌بینی و به‌کار بستن آنها بر ضد بزه واکنش نشان می‌دهد. این معنا از سیاست جنایی، همچنان مورد نظر بعضی از 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؛ هنگامی که مارک آنسل نشریه "آرشیوهای سیاست جنایی" را در سال ۱۹۷۵ تأسیس نمود، در نخستین اقدام، بر ضرورت عدم محدود و خلاصه کردن سیاست جنایی، به حقوق کیفری تأکید کرد و با تلاش برای برجسته کردن ویژگی دوگانه آن - یعنی "دانش مشاهده و مطالعه" و "فن" یا "راهبرد روش‌مند واکنش بر ضد بزه"، پیشنهاد کرد که سیاست جنایی "واکنش سازمان‌یافته و مطالعه‌شده جامعه بر ضد اقدام‌ها و فعالیت‌های بزهکارانه، منحرفانه و یا ضد اجتماعی" تعریف شود (دلماس مارتی، ۱۳۹۳، ۲: ۶۳).

در دیدگاه مارک آنسل، سیاست جنایی، نخست، علاوه بر جرم - که یک مفهوم قانونی است - به انحراف (کژروی) - که یک مفهوم اجتماعی است - نیز می‌پردازد؛ دوم اینکه، علاوه بر سرکوب و مجازات بزهکاری، به پیشگیری از آن توجه دارد؛ سوم اینکه، علاوه بر 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 - یعنی سیاست کیفری - به سمت مفهوم موسع - به معنای امروزی آن - تحول می‌یابد (لازرژ، ۱۳۹۰: ۱۵). بدین ترتیب، می‌توانیم بگوییم که سیاست جنایی در پایان سده بیستم - یعنی حدود دو سده پس از فوئر باخ - شامل کلیه اقدام‌های سرکوبگرانه (کیفری و غیر کیفری) و پیشگیرانه با ماهیت‌های مختلف می‌شود که دولت و جامعه مدنی، هر یک به صورت مستقل و یا با یک مشارکت سازمان‌یافته، از آنها در قالب روش‌های مختلف به منظور سرکوب بزهکاری و بزهکاران و نیز پیشگیری از بزهکاری و انحراف استفاده می‌کنند (لازرژ، ۱۳۹۰: ۱۷).

دل‌ماس مارتی تعریف فوئر‌باخ را گسترش داده و سیاست جنایی را «مجموعه روش‌هایی که هیئت اجتماع با توسل و با به‌کار بستن 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 هسته اصلی یا مرکز شدیدترین فشار با رؤیت‌پذیری بسیار بالا در سیاست جنایی حضور پُررنگی دارد؛ اما شیوه‌های کیفری مقابله با بزه در قلمرو سیاست جنایی تنها نیستند؛ بلکه حول آنها، شیوه‌های دیگر پایش اجتماعی از گونه غیر کیفری (مانند رسیدگی و ضمانت اجراهای اداری و مدنی)، غیر سرکوبگر (مانند پیشگیری، جبران و ترمیم خسارت بزه‌دیده، میانجی‌گری) و گاه غیر دولتی (رویه‌های سرکوبگر شبه‌نظامیان و شبه پلیس‌های خصوصی، اقدام‌های اعتراضی از نوع اقدامات سازمان عفو بین‌الملل بر ضد 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

از آنجا که 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؛ به طوری که سیاست جنایی از لحاظ کاربردی، دارای چهار حالت زیر است:

۱. **سیاست جنایی تقنینی**؛ که همان تدبیر قانون‌گذار در مورد واکنش بر ضد جرم است.

۲. **سیاست جنایی قضایی**؛ که در واقع، نحوه برداشت دادگستری (قوه قضاییه) از سیاست جنایی تقنینی است.

۳. **سیاست جنایی اجرایی**؛ با وجود استقلال قوای سه‌گانه، حکومت ناگزیر است که برای اجرای قوانین داخلی از قوه مجریه بهره‌برد. این بدان معناست که قوه مجریه نیز از سیاست خاص خود برخوردار است؛ بنابراین، سیاست جنایی اجرایی عبارت است از نحوه درک و اجرای قوانین و احکام قضایی در مورد پایش جرم و واکنش‌های خود آن.

۴. **سیاست جنایی مشارکتی**؛ این جنبه از سیاست جنایی ممکن است در بردارنده حالت‌های پیشین باشد. به بیان دیگر، ممکن است سیاست جنایی مشارکتی با سیاست جنایی تقنینی، سیاست جنایی قضایی و یا سیاست جنایی اجرایی در ارتباط باشد. 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 شهادت و در مرحله حکم مانند واگذاری طفل به خانواده‌های 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 در خصوص سیاست جنایی آمده‌است، ارائه می‌گردد.

تعریف فوئر باخ: اصطلاح سیاست جنایی برای اولین بار توسط فوئر باخ آلمانی در سال ۱۸۰۳ به‌کار برده شد. او در کتاب خود - حقوق کیفری - 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».

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

تعریف مارک آنسل: به نظر مارک آنسل، سیاست جنایی به‌طور هم‌زمان، 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 ضد 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 روش‌هایی می‌شود که هیئت اجتماع از طریق آنها پاسخ‌گویی به پدیده 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، هر کدام با نگاه و رویکرد زمانی و مکانی منحصر به فرد خود، تعریفی از سیاست جنایی ارائه داده‌اند. در حال حاضر، با توجه به رشد فزاینده جرایم سایبری و تأثیرگذاری فضای سایبری بر زندگی بشری، به نظر می‌رسد که نیاز است نسبت به ترسیم سیاست جنایی 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 دکتر 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

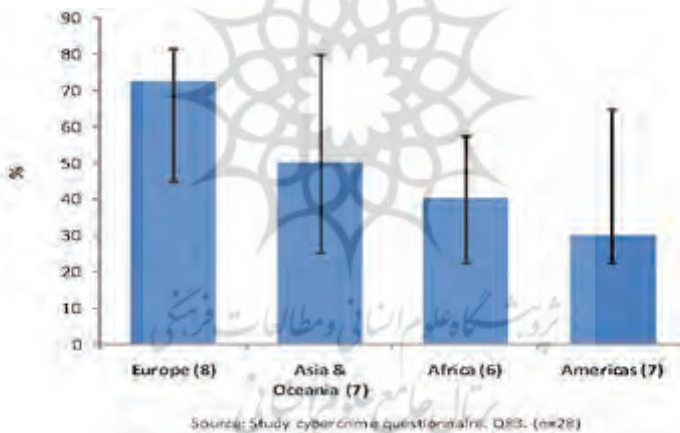
در سیاست جنایی معمولاً دو موضوع مورد توجه قرار می‌گیرد: اول، بررسی فرآیند جرم‌انگاری؛ دوم، بررسی شبکه‌های پاسخ به پدیده مجرمانه یا جرم. در زیر، هر یک از آنها به‌طور مختصر شرح می‌شود.

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 متخصصان رایانه به مطالعه و بررسی همه‌جانبه این پدیده روی آورند؛ به‌طوری که 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 کشورهای نسبت به رسیدگی و نیز تعارض قوانین این کشورها در برخورد با جرایم سایبری شده‌است.

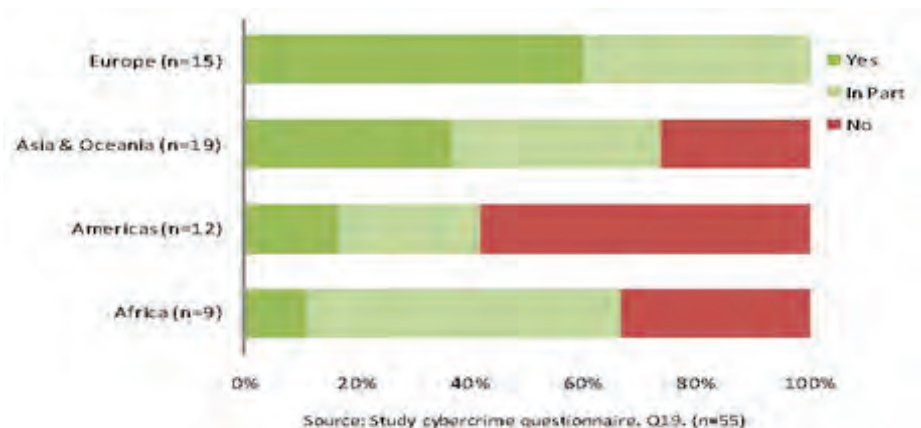
همان‌طور که می‌دانیم، حقوق بین‌الملل شاخه‌ای از حقوق عمومی است که شامل مجموعه قوانین و مقرراتی است که بر جامعه بین‌المللی حاکم است و در آن جامعه، قابلیت اجرایی دارد (ضیایی بیگدلی، ۱۳۹۶: ۲). جامعه بین‌الملل دارای تابعان بین‌المللی است که همان کشورها و سازمان‌های بین‌المللی محسوب می‌شوند. یکی از مهم‌ترین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

بین‌المللی مطرح می‌شود، مجموعه قوانین و قواعد همکاری‌های بین‌المللی کشورها و سازمان‌ها در مواجهه با پدیده جرم است. سازمان ملل متحد به‌عنوان بزرگ‌ترین سازمان بین‌المللی، به نوبه خود، به حوزه جرم توجه ویژه‌ای داشته‌است و با ایجاد دفتر مبارزه با جرم (UNODC) در بطن خود به دنبال ایجاد معیارهای سازنده در سطوح مختلف همکاری‌های بین‌المللی تابعین خود در مواجهه و مقابله با پدیده جرم است. این دفتر در ابتدا در جهت مبارزه با پدیده جرایم موادمخدر به وجود آمد و در حال حاضر، با توجه به ماهیت بین‌المللی جرایم سایبری در این حوزه نیز متمرکز شده‌است؛ به طوری که در سال ۲۰۱۳ با انتشار پیش‌نویس سندی با عنوان "مطالعه جامع بر جرایم سایبری" نگرانی‌های خود را در این مورد ابراز کرد. براساس این گزارش و برابر آمارهایی که دفتر مقابله با جرم و موادمخدر سازمان ملل در سال ۲۰۱۳ کسب کرده‌است، بیش از نیمی از کشورها گزارش داده‌اند که بین ۵۰ تا ۱۰۰ درصد از جرایم سایبری که پلیس با آنها برخورد کرده‌است، ابعاد فراملی داشته‌است (دفتر مقابله با جرم سازمان ملل، ۲۰۱۳: ۴۹).



نمودار ۱. درصد اعمال مجرمانه سایبری

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



نمودار ۲. وضعیت قانون‌گذاری جرایم سایبری در سطح بین‌الملل

تحقیق فوق‌نشان می‌دهد که حدود یک‌سوم از کل کشورهای پاسخ‌دهنده معتقد بودند که چارچوب‌های قانونی ملی آنها برای جرایم فرامرزی "کافی" بوده‌است. ۴۰ درصد دیگر از آنها چارچوب‌های قانونی ملی را "ناحدودی" کافی می‌دانستند.

مطالعات نشان می‌دهد که به‌دلیل قابلیت‌های فنی رایانه‌ها و اجزای مرتبط 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 گسترش سامانه‌های رایانه‌ای از محیط رایانه و شبکه داخلی به سطح بین‌المللی گسترش پیدا کرده‌است و موجب خلق نسل جدید جرایم رایانه‌ای - یعنی جرایم در محیط سایبری - شده‌است که ماهیت و خاصیت کاملاً فراملی و بین‌المللی دارد. به‌هر حال، امروزه، جرایم سایبری تبدیل به یک پدیده مجرمانه کاملاً بین‌المللی شده‌است. 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 هر جایی از دنیا می‌توانند مورد پیگرد قانونی قرار گیرند اما با وجود این، تفاوت‌های منطقه‌ای نیز نقش مهمی را در این امر بازی می‌کنند.

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

مورد استفاده 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 امکان 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 با توجه 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 قوانین ملی کشورها ارائه کرده‌اند. از جمله سازمان‌های بین‌المللی و منطقه‌ای پیش‌رو و اقدامات انجام‌شده در این زمینه می‌توان به سازمان همکاری و توسعه اقتصادی^۱، شورای اروپا، انجمن بین‌المللی حقوق جزا^۲، سازمان ملل، 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 در خصوص جرایم سایبر، به کنفرانس بوداپست در اواخر سال ۲۰۰۱ م. برمی‌گردد که در آن، بیشتر کشورهای اروپایی همراه کانادا، ژاپن و آفریقای جنوبی و آمریکا مصوبه‌ای به نام "کنوانسیون جرایم سایبر" را امضا نمودند. در مجموع، بیش از ۳۲ کشور بر مصوبات کنفرانس بوداپست صحه گذاشتند؛ اما روسیه، اسلواکی، ترکیه، لیتوانی، لوکزامبورگ، چک، دانمارک و بوستنی 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، تخریب تعامل میان داده‌های سامانه‌ای از طریق حمله به شبکه‌های بزرگ، دسترسی غیرقانونی به کدهای برنامه‌های حساس، تخطی از قوانین کی‌رایت 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 حقوق دانان 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 گسترش 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 شورای نگهبان قرار گرفته است. دومین واکنش در مقابل جرایم رایانه‌ای، از طریق وضع "قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای" به عمل آمد. این قانون در تاریخ ۸۱/۱۰/۴ به تصویب مجلس شورای اسلامی و در تاریخ ۸۱/۱۰/۱۰ به تأیید شورای نگهبان رسید. ماده ۱۳ قانون مذکور، نقض حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مورد حمایت این قانون را جرم تلقی کرده و برای آن، مجازاتی معادل ۹۱ روز تا ۶ ماه حبس و جزای نقدی تعیین کرده است. 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 مجلس شورای اسلامی به عمل آمد. به موجب ماده ۱۳۱ این قانون، جعل اطلاعات و داده‌های رایانه‌ای، تسلیم و افشای غیرمجاز اطلاعات و داده‌ها و سوءاستفاده مالی از طریق رایانه (کلاهبرداری و اختلاس)، جرم تلقی شده و مرتکب حسب‌مورد، به مجازات جرم ارتكابی محکوم می‌شود. چهارمین واکنش قانونی از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۷۷ و ۶۶ و ۶۷ و ۶۸ و ۶۹ و ۷۴ و ۷۵ و ۷۶ این قانون، کلاهبرداری، جعل، دستیابی، افشای غیرمجاز اسرار تجاری، نقض حقوق مربوط به مالکیت معنوی (کپی رایت) و ... که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود، جرم تلقی شده و برای آن مجازات تعیین گردیده است. پنجمین واکنش قانونی نیز تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ می‌باشد.

۲. بررسی شبکه‌های پاسخ به جرایم سایبری

اصولاً حق مجازات و کیفر، از حقوق ذاتی دولت‌ها و از مولفه‌های حق حاکمیت است؛ چراکه مجازات‌ها اصولاً از جنبه عمومی و غیرشخصی برخوردار است و واگذاری حق تنبیه به جامعه مدنی به دلیل حب و بغض و نابرابری جای ایراد است؛ بنابراین، 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 سست‌ترین پاسخ‌ها به جرم به اقتضای سن تحول بشری، پاسخ‌های سرکوبگر کیفری بوده است؛ اما در کنار این پاسخ‌ها، ضمانت‌اجراهای دیگری همانند

صنفا، ادارى، انتظامى و انضباطى نيز در سياست جنايى به وجود آمده است كه با وجود دارا بودن وصف حقوقى، اين دسته از ضمانت اجراها با وجود برخوردارى از جنبه تنبيهى، كيفرى قهرآمى محسوب نمى شوند. در كنار اين پاسخها، برخى از پاسخها با وصف پيشگيرانه نيز وجود دارد كه در دو سطح اجتماعى و وضعى ارائه داده مى شود (مهدوى ثابت، ۱۳۹۵: ۱۲). به طور كلى، پاسخ به جرايم سايبى را مى توان در دو سطح به شرح زير تبين نمود: ۱. شبكه پاسخهاى كنىشى (پيشگيرانه) نسبت به جرايم سايبى كه اغلب به دو شاخه وضعى و اجتماعى تقسيم بندى مى شوند؛ ۲. شبكه پاسخهاى واكنشى (سر كوبنده) نسبت به جرايم سايبى كه به دو شاخه قهرآمى و غير قهرآمى تقسيم مى گردند. در زير به شرح هريك از اين موارد پرداخته مى شود.

۱-۲. شبكه پاسخهاى كنىشى (پيشگيرانه) نسبت به جرايم سايبى

نمود تأثير پذيرى ديگر سياست جنايى از نظريه ها و آورده هاى علمى، به ويژه، جرم شناسى پيشگيرى، ظهور راهبرد پيشگيرى از بزه كارى و بزه دیده شدن شهروندان است كه در واقع، به دنبال کاهش مناسبتهاى مداخله اى نظامهاى كيفرى، ادارى و انضباطى در برابر بزه كارى و تخلفات، با هدف صرفه جويى در هزينه هاى مادى اجتماعى انسانى است كه اين مداخله براى كنىشگران جرم - يعنى بزه كار، بزه دیده و جامعه، به طور كلى، به بار مى آورد.

امروزه، پيشگيرى به عنوان يك راهبرد نظام مند سياست جنايى، از يك سو، مبتنى بر قوانين و مقرراتى است كه به طور مستقيم^۱ يا غير مستقيم^۲، اقدامهاى عمومى يا ويژه اى را ضابطه مند و نهاد يا سازمان خاصى را براى مديريت و اجراى آنها در سطح محلى، وزارتى يا در مقياس مى تعريف و تاسيس مى كنند و از سوى ديگر، مبتنى بر ابتكارها و رويه هاى خودجوش و عملى است كه متوليان نهادهاى عمومى (مانند شهردار، فرماندار، استاندار، فرمانده پليس، شورى تأمين) يا نهادهاى جامعوى (مانند انجمن حمايت از شكجهديدگان، انجمن مبارزه با اعتياد، انجمن حمايت از زنان خشونت دیده، انجمن حمايت از محيط زيست براى پيشگيرى از بزه كارى اتخاذ کرده و به اجرا مى گذارند) (نجفى ابرنآبادى، ۱۴۰۲: ۱۴).

۱. مانند قانون ارتقاى سلامت ادارى و مقابله با فساد مصوب ۱۳۹۰/۸/۷، قانون مبارزه با قاچاق کالا و ارز مصوب ۱۳۹۲/۱۰/۳، با اصلاحات مصوب ۱۳۹۴/۷/۲۱ و قانون مجازات قاچاق اسلحه و مهمات و دارندگان سلاح و مهمات غير مجاز مصوب ۱۳۹۰/۷/۱۶ ماده ۱۹ در ايران يا قانون پيشگيرى از بزه كارى مصوب ۵ مارس ۲۰۰۷ در فرانسه.

۲. مانند نهادهاى فرزندخواندگى و تكليف تربيت فرزندان توسط والدين در قانون مدنى يا حمايت از كودكان در معرض خطر بزه ديدگى و بزه كارى پيشگيرى رشدمدار - در قانون حمايت از كودكان و نوجوانان بى سرپرست و بدسرپرست مصوب ۱۰ مهر ۱۳۹۲ با ماده ۱۱۴ قانون آيين دادرسى كيفرى مصوب ۱۳۹۲ كه بايد با احتياط و رعايت كامل 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 مدنظر است که در اصطلاح، به آن پیشگیری جامعه‌مدار^۱ یا محیط اجتماعی^۲ 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^۳ 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 - که رایج‌ترین شکل پیشگیری غیرکیفری است - بر مبنای شناسایی عوامل مختلف محیطی بزهکاری به منظور خنثی کردن یا دست کم، کاهش آثار آنهاست. در واقع، پیشگیری جامعه‌مدار از بزهکاری با بهبود شرایط زندگی در یک محیط معین، به‌طور مستقیم بر رفتار مجرمانه تأثیر می‌گذارد (پورقهرمانی، ۱۳۹۵: ۱۸۲).

بر این اساس، پیشگیری محیطی بستگی به نوع جرایم، شرایط و اقتضائات محیطی خاص 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 آشفته‌بازار 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 در جهت 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 علاوه بر محاسن زیاد خود، معایب و خطرات زیادی نیز به همراه دارد. این فضا و دسترسی به محتویات آن، جزو حق افراد شمرده می‌شود (نصاری، ۱۳۹۰: ۸۷) و بنابراین، نمی‌توان مانع دسترسی افراد، به خصوص جوانان و نوجوانان شد و چنین واکنشی، علاوه بر ضمانت اجرایی ملی و بین‌المللی، از منظر جرم‌شناسی نیز قضیه را بغرنج‌تر خواهد ساخت. 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 ناشی از 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 اطلاع‌رسانی‌ها 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 مورد نظر 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 بوده است (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 کاربران اینترنت تعداد اهداف احتمالی جرایم سایبری را کاهش می‌دهد؛ همانند آموزش‌هایی از طریق برنامه‌های آموزش عمومی، آموزش در مدرسه، کتابخانه‌ها، مراکز IT و دانشگاه‌ها و مشارکت در برنامه‌های عمومی و خصوصی (دستور، جمشیدی‌نسب، ۱۳۹۳: ۱۲۳).

۳. تدوین کدهای رفتاری: یکی دیگر از روش‌های پیشگیری اجتماعی جامعه‌مدار، تدوین "کدهای رفتاری" برای مشاغل گوناگون و الزام به آگاهی از مفاد آن است. منظور از کد رفتاری، مجموعه قواعد 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، دانش‌آموزان و... و نیز هدایت صحیح آنها به مقصد سایبری‌شان است (باقری اصل، ۱۳۸۷: ۳۸). یک کد رفتاری می‌تواند به‌وسیله هر سازمانی، اصولاً برای الزام اعضای سازمان و تعیین مبنایی برای روند انضباطی برقرار شود (شایگان و سروستانی، ۱۳۸۸: ۴۱).

به‌طور کلی، 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^۲، تمامیت^۳ و دسترس‌پذیری^۴ 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 شرایط اقتصادی: برخی از جرایم سایبری همانند کلاهبرداری سایبری، سرقت سایبری و ... با انگیزه‌های مالی ارتکاب می‌یابند که خود ناشی از عوامل اجتماعی مانند فقر و بیکاری هستند. بیکاری با پیامدهای مادی و روانی خود در درازمدت، نوعی احساس نفرت را نسبت به جامعه فعال به‌وجود آورده‌است (گریکار، ۲۰۰۱: ۹). افزون بر این، احساس 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 نسبت به 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 شورای عالی انقلاب فرهنگی، سازمان صداوسیما، شورای عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات، وزارت فرهنگ و ارشاد، نیروی انتظامی، وزارت آموزش و پرورش 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 - 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 در معرض 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 مواد مخدر.

این عوامل خطر، تأثیر متقابلی بر یکدیگر داشته و همدیگر را کامل می‌کنند. در پیشگیری باید نسبت به چهار سطح ذکر شده، مدیریت و اقدام لازم صورت گیرد. به نظر می‌رسد که در خصوص ارتکاب جرایم سایبری، عوامل موصوف نقش مستقیم و غیرمستقیمی 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 در مقابل عوامل خطر، نقش حمایتی را بر عهده دارند و عبارتند از: 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 فراهم می‌کند و تجارب منفی را تنبیه می‌کند. بر این اساس، برخی مداخله‌های خانواده‌مدار که برای پیشگیری از اختلالات رفتاری و بزه‌کاری طرح‌ریزی می‌شوند، بدین گونه قابل تقسیم هستند:

۱. برنامه دیدارهای خانگی زودهنگام و آموزش‌های پیش‌دستانی؛ 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 می‌کند، خانواده و بالطبع والدین است؛ بنابراین، چنانچه بتوان در ابتدا، توصیه‌ها و آموزش‌های لازم در مورد فضای سایبری و رایانه‌ای را به والدین منتقل و آنها را با خطرها و درعین حال، 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 آموزش و پرورش در حمایت از اطفال و نوجوانان در معرض خطر، جایگاهی منحصر به فرد و بی‌بدیل است. گرایش اطفال و نوجوانان به بزه کاری ناشی از اختلال در کارکردهای رشدی، جامعه‌پذیری و پایشی نخستین مراجع جامعه‌پذیری کودک - یعنی خانواده، مدرسه، همسالان و رسانه‌ها - است. اطفال در معرض خطر، به‌ویژه از نظر خانوادگی، در معرض آسیب‌های اختلال کارکردی هستند و بنابراین، خانواده آنها، خود، محتاج اقدامات مداخله‌ای حمایتی است. نظام آموزش و پرورش، ابزار رسمی اجتماع برای انتقال ارزش‌ها و هنجارهای پذیرفته‌شده اجتماعی به کودکان و نوجوانان است. کودک در سنین مدرسه در شرایط حساسی قرار دارد که هم می‌توان نشانه‌های اولیه اختلالات رفتاری را در وی کشف کرد و هم قابلیت اصلاح رفتار و بازگشتن وی به مسیر رشد مطلوب در این سنین بسیار قوی است. به عبارت دیگر، دانش‌آموزان الگوپذیری مطلوبی از معلمان خود دارند؛ پس اگر معلمان الگوهای محیطی مناسبی را در جهت تطبیق دانش‌آموزان با ارزش‌های جامعه ارائه دهند، دانش‌آموزان نیز سعی می‌کنند که خود را با قوانین اجتماعی هماهنگ سازند (فهیمی، ۱۳۸۰: ۲۹۶). بر این اساس، معلمان باید آموزش صحیح استفاده از 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 نهادینه کردن نحوه استفاده با اینترنت و رایانه است.

۳.۲. عوامل حمایتی در زمینه همسالان: کودکان و نوجوانان در مسیر رشد، مراحل متعدد و مختلفی را طی می‌کنند و هر مرحله از رشد آنها تحت تأثیر عواملی است که ابعاد رشدی، جامعه‌پذیری و پایشی آنها را تحت تأثیر قرار می‌دهد. از آنجاکه در دوره نوجوانی نیاز به استقلال و احساس هویت فردی در فرد تقویت شده و فرد با احساس برابری مشابهت، نیاز به امنیت، تعلق

و احترام خود را از طریق گروه همسالان تأمین می‌کند، به‌همین دلیل، نفوذ گروه همسالان بر وی افزایش می‌یابد. سهولت یادگیری کودکان و نوجوانان از همسالان، احساس مشابهت و عدم سلسله‌مراتب بین همسالان و نیز کارکرد نامطلوب خانواده کودکان و نوجوانان در معرض 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 منظور ما در اینجا غیر از اینترنت (مثل رادیو، تلویزیون، روزنامه و ...) است. امروزه، نفوذ روزافزون رسانه‌ها در ابعاد مختلف فردی و اجتماعی زندگی انسان‌ها غیرقابل انکار است و بنابراین، ویژگی‌های رسانه می‌تواند در وضعیت‌های خاص دوران کودکی و نوجوانان نقش به‌سزایی داشته باشد؛ چراکه بر اساس تحقیق انجام‌شده، بیشترین تماشاگران تلویزیون در شهر تهران، کودکان کمتر از ۱۵ سال هستند (شیخوندی، 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 خود را تکرار نموده و از روش‌های دراماتیک، هیجانی و اغراق‌آمیز برای ایجاد جاذبه در مخاطبان بهره‌برند. استفاده از قابلیت رشدی، جامعه‌پذیری و پایشی رسانه در قالب برنامه‌های حمایتی، از ضروری‌ترین بخش‌های برنامه جامع حمایت از اطفال و نوجوانان در معرض خطر می‌باشد (آجرلویی، ۱۳۹۱: ۲۲). با این توضیح، واضح است که بسیاری 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 - که غالب کودکان از آن بهره‌مند هستند - نیز می‌توانند از طریق پخش فیلم آموزش کودکان و یا کارتون مرتبط با رایانه، اینترنت و ... در زمینه پیشگیری از انحرافات سایبری و رایانه‌ای کمک به‌سزایی کند (پورقهرمانی، ۱۳۹۵: ۲۱۰).

شبکه‌های پاسخ‌دهنده نسبت به پیشگیری اجتماعی رشدمدار از جرایم سایبری

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

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

پیشگیری وضعی از جرایم سایبری

همان‌طور که در ابتدای بحث پیشگیری به‌طور خلاصه گفته شد، پیشگیری وضعی بر این فرض استوار است که یک انسان متعارف در همه زمینه‌ها، خواسته یا ناخواسته، به‌طور منطقی و حساب‌شده عمل کرده و از خطرات شدید دوری می‌کند؛ یعنی در صورتی تن به خطر می‌دهد که عایدات یا منافع حاصل از آن عمل، ارزشمند باشد؛ حال اگر این فرض در مورد 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، قاعدتاً مجرمان بالقوه از ارتکاب جرم منصرف خواهند شد (نجفی ابرندآبادی، ۱۳۸۲).

پیشگیری وضعی برخلاف پیشگیری اجتماعی نمی‌خواهد با به‌سازی محیطی و نظایر آن، تمایلات مجرمانه را از بین ببرد؛ بلکه هدف، نوعی توان‌گیری غیر کیفری از طریق تقویت آمار جرم و ... است. در پیشگیری وضعی به جای اثرگذاری بر شخصیت فرد و تغییر آن (که زمان‌بر و یا حتی گاهی غیر ممکن است) با ایجاد تغییر در موقعیت ماقبل بزه‌کاری، فرایند تصمیم‌گیری مرتکب مختل می‌شود. در این نوع پیشگیری هم مثل مدیریت آماری، خطرپذیری جرم^۱ پیش‌بینی نقش محوری دارد. موقعیت پر از خطر باید شناسایی گردد. موقعیت پر از خطر ممکن است ناشی از 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، با اعمال روش‌های فیزیکی (مادی) یا تغییر و پایش موقعیت‌های مناسب برای ارتکاب جرم می‌توان وقوع آن را ممتنع و خنثی ساخت؛ بدین طریق، از ورود به وادی پیچیده سلسله عوامل متعدد انسانی و اجتماعی جرم و تحلیل و برخورد با آنها احتراز می‌گردد» (صفاری، ۱۳۸۰: ۲۸۳).

در زمینه پیشگیری وضعی از جرایم سایبری باید اذعان داشت که با وجود انتقادات وارده بر آن، باز هم از جایگاه خاصی برخوردار است. یکی از دلایلی که می‌توان جهت توجیه پیشگیری

۱. مدیریت خطرپذیری درباره حذف، کاهش، انتقال منفی حوادث و بهره‌جستن از فرصت‌های احتمالی سخن می‌گوید. هدف اصلی مدیریت خطرپذیری، تغییر دادن محیط است.

وضع‌ی از این جرایم عنوان نمود، همین قابلیت‌ی است که فضای تبادل اطلاعات فراهم آورده‌است. همان‌طور که گفته شد، ماهیت جرم مبتنی بر رایانه به گونه‌ای است که نمی‌توان با دست‌تهی مرتکب آن شد و باید علاوه بر 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 تا پیشگیری وضعی در جرایم رایانه‌ای با تمام کاستی‌های آن دنبال شود، بحث شبکه‌های اطلاع‌رسانی رایانه‌ای است. تقریباً 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 تحت نظارت دولت و مقررات قانونی لازم‌الاجرا هستند. درحقیقت، این شبکه‌ها پل ارتباطی ما با فضای تبادل اطلاعات هستند و به این ترتیب، اگر در این پل ارتباطی اقدامات پیشگیرانه وضعی مؤثری اعمال شود، 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 سبب جرم و مجرم قرار داد. آنچه که امروزه، در قالب نصب دیوار آتشین در این شبکه انجام می‌شود، چیزی جز پیشگیری وضعی نمی‌باشد (جلالی فراهانی، ۱۳۸۳: ۱۱۰)؛ بنابراین، در اینجا به مجرمان اجازه داده نمی‌شود که به راحتی به مقصود خود نائل شوند؛ همچنین، با پیدایش پدیده‌هایی مانند پلیس گشت سایبر، پیشگیری وضعی در این فضا جلوه دیگری 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 منحصر به فرد فضای تبادل اطلاعات مربوط می‌شود. در این

فضا، شخص می تواند برخلاف دنیای فیزیکی، در یک زمان، در چند نقطه ظاهر شود و با انجام یک عمل بر چند نقطه تأثیر بگذارد؛ به عنوان مثال، یک مجرم می تواند از طریق شبکه به تعداد بسیاری رایانه میزبان متصل شود و به طور هم زمان، 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 تأثیر گذاری فضای تبادل اطلاعات است که نسبت به دنیای فیزیکی، حوزه بسیار گسترده تری را در بر می گیرد؛ به عنوان مثال، گستره تأثیرهای مخرب نشر مطالب تحریک آمیز بر ضد امنیت ملی یا مطالب توهین آمیز نسبت به مقدسات مذهبی یا تصاویر حاوی هرزه نگاری در این فضا بر کسی پوشیده نیست (پورقهرمانی، ۱۳۹۵: ۲۱۵).

تدابیر پیشگیرانه وضعی

در مورد هر جرمی و با توجه به موضوع آن می توان تدابیر وضعی متناسبی اتخاذ کرد. در خصوص تدابیر پیشگیری وضعی از جرایم و در راستای برقراری امنیت، می توان یکی از روش های زیر را در پیش گرفت:

۱. دشوار ساختن ارتکاب جرایم سایبری برای مجرمان بالقوه از طریق ایجاد موانع به منظور 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 دسته بندی کرده اند: تدابیر محدود کننده یا سلب کننده دسترسی، ناشناس کننده و رمزنگارها، تدابیر صدور مجوز و تدابیر نظارتی (سادوسکای، جورج و دیگران، ۱۳۸۴: ۲۲۱).

شبکه های پاسخ دهنده نسبت به پیشگیری وضعی از جرایم سایبری

اغلب شبکه های پاسخ دهنده در پیشگیری وضعی، ارتباطی مستقیم با ساختار حاکمیتی دارند؛ چراکه تغییر در وضعیت های مختلف، تنها با دسترسی به زیرساخت های فناوری اطلاعات و ارتباطات هر کشوری مقدور می باشد. در جمهوری اسلامی ایران، این شبکه ها عبارتند از شورای عالی امنیت ملی، شورای عالی فضای مجازی، قوه قضائیه، نیروی انتظامی و وزارت فناوری اطلاعات و ارتباطات.

۲.۲. شبکه پاسخ‌های واکنشی (سرکوبنده) نسبت به جرایم سایبری

اصولاً در پاسخ‌دهی به رفتارهای مجرمانه، از جمله جرایم رایانه‌ای تا زمانی که امکان توسل به پاسخ‌های 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 که پیش‌تر گفته شد، نتوان فرایند گذار از اندیشه به اعمال مجرمانه رایانه‌ای را از مرتکبان این جرایم سلب کرد و به عبارت دیگر، در صورتی که پاسخ‌های کنشی جرم‌شناسی نسبت به 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 منصف 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؛ هرچند که 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

قانون جرایم رایانه‌ای مصوب ۱۳۸۸ بدون ذکر تعریف از جرایم رایانه‌ای در ۵۶ ماده و سه بخش جرایم و مجازات‌ها، مقررات آئین 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. جرایم بر ضدّ صحت و تمامیت 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.

نقطه حائز اهمیت این است که برای اولین بار در فصل ششم از بخش اول در این قانون برای اشخاص حقوقی نیز مسئولیت کیفری تدوین شده است.

شبکه‌های پاسخ‌دهنده کیفری نسبت به جرایم سایبری

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

ب. پاسخ‌های غیر کیفری

رویکرد پاسخ‌های غیر کیفری 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 عدالت‌ترمیمی می‌باشد.

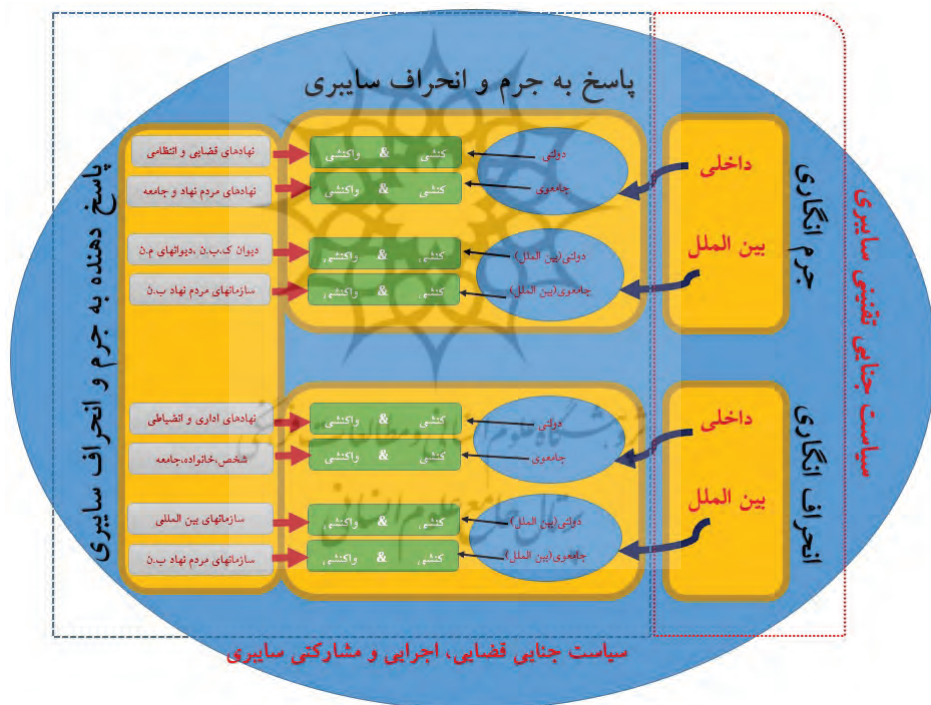
۱. پاسخ‌های تأمینی: پاسخ‌های تأمینی اغلب نسبت به اشخاص حقوقی حقوق خصوصی که با عنوان مؤسسات اینترنتی یا ارائه‌دهندگان خدمات دسترسی و میزبانی یا ارائه‌دهندگان خدمات اطلاع‌رسانی و اینترنتی (رساء) فعالیت دارند، اعمال می‌شود. این پاسخ‌ها اغلب تعطیلی موقت محل کسب تا انحلال محل و نیز تذکر و لغو پروانه و ...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

۲. پاسخ‌های سیاسی: با توجه به اینکه جرایم سایبری فراملی هستند، پس می‌توانند تهدیدی نسبت به کشورها و جوامع باشند و در سطح جهانی نیز صلح و امنیت بین‌المللی را تهدید نمایند؛ بنابراین، چه‌بسا تهدیدات و خطرات سایبری از کشوری نسبت به کشور دیگر ممکن است که روابط دو کشور را برهم زند و چه‌بسا پیامدهای سیاسی و واکنشی را در پی داشته باشد (نور محمدی، ۱۳۹۰: ۲۸)؛ به عبارت دیگر، دولت‌ها در وضعیتی نیستند 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 از پیش طراحی شده است. قواعد بین‌المللی خاصی در این زمینه وجود ندارد ولی با این همه، کشورها می‌توانند در مقابل این حملات، پاسخ‌ها و

اقدام‌های مقابله به مثلی انجام دهند (پورقهرمانی، ۱۳۹۵: ۲۷۱). شبکه‌های پاسخ‌دهنده غیر کیفری نسبت به جرایم سایبری شبکه‌های پاسخ‌دهنده کیفری به جرایم سایبری در ایران عبارتند از: ثمن‌ها و اتحادیه‌ها، قوه قضائیه، نیروی انتظامی و شورای عالی امنیت ملی.

الگوی مفهومی تحقیق

در این گفتار، الگوی مفهومی تحقیق برگرفته از مبانی نظری تحقیق ارائه می‌گردد. در این الگو، کلیات و روابط جامعی از متغیرهای مستقل، وابسته و تعدیل‌گرای احصاء شده از مبانی در قالب الگوی مفهومی به شرح شکل زیر ارائه گردیده است.



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

و تعریف گردیده‌است. در مفهوم اول، جرم‌انگاری و انحراف‌انگاری به‌عنوان ابعاد و واکنش‌های داخلی و بین‌المللی به‌عنوان مولفه‌ها تدوین گردیده‌اند و در مفهوم دوم، شبکه پاسخ‌دهنده و شبکه پاسخ، هر کدام به‌عنوان ابعاد مفهوم و پاسخ‌های دولتی - جامعه‌ی و نیز دولت (بین‌الملل) - جامعه‌ی (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 آنها پاسخ‌گویی به پدیده جنایی در فضای سایبری را سامان می‌بخشد. حسب تعریف بالا و با لحاظ قراردادن الگوی مفهومی احصایی و سنجش 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، خلأ مهارتی و آموزشی در بعد قضایی، 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 با توجه به بعد فراملی آثار و تبعات بزه‌های سایبری نیازمند تلاش، همکاری و تعامل بین‌المللی می‌باشد. با همه این اوصاف، اولین گام در جهت ترسیم صحیح سیاست جنایی در قبال جرایم سایبری، الگوسازی است. الگوها به‌دنبال چستی‌ها 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 احصایی در الگوها می‌توان ارتباط‌سازی بین این حوزه‌ها را از طریق الگوهای اجرایی و نقشه‌راه ترسیم نمود تا به یک سیاست منسجم، صحیح و دقیق منجر شود.

فهرست منابع

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

- اولریش زیبر (۱۳۸۲)، جرایم رایانه‌ای، ترجمه محمد علی نوری، تهران: گنج دانش
- آئین دادرسی کیفری ایران
- باستانی برومند (۱۳۸۸)، جرایم کامپیوتری و اینترنتی؛ جلوه‌ای نوین از بزه کاری، تهران: بهنامی
- بای؛ حسینعلی، پورقهرمانی؛ بابک (۱۳۸۸)، بررسی فقهی حقوقی جرایم رایانه‌ای، تهران: پژوهشگاه علوم و فرهنگ اسلامی
- پاکزاد، بتول (۱۳۸۸)، تروریسم سایبری؛ رساله دکتری در حقوق جزا و جرم‌شناسی، تهران: دانشکده حقوق دانشگاه شهید بهشتی (ره)
- پلومان، ادوارد (۱۳۸۰)، حقوق بین‌الملل؛ ارتباطات و اطلاعات، ترجمه بهمن آقایی، تهران: کتابخانه گنج و دانش
- پورقهرمانی، بابک (۱۳۹۵)، سیاست جنایی ایران در قبال جرایم رایانه‌ای، تهران: شهر دانش
- حافظ‌نیا، محمدرضا (۱۳۹۱)، جغرافیای سیاسی فضای مجازی، تهران: انتشارات سمت
- حسینی، سید محمد (۱۳۹۴)، سیاست جنایی در اسلام و در جمهوری اسلامی ایران، تهران: انتشارات سمت
- زندی، محمد رضا (۱۳۹۴)، تحقیقات مقدماتی در جرایم سایبری، تهران: انتشارات جنگل
- شیرزاد، کامران (۱۳۸۸)، جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل، تهران: شرکت نشر بهینه‌فراگیر
- صبح‌خیز، رضا (۱۳۹۸)، جرایم سایبری در نظام حقوقی ایران و جهان، تهران: انتشارات دانشگاه علوم انتظامی
- ضیایی بیگدلی (۱۳۸۶)، حقوق بین‌الملل عمومی، تهران: انتشارات گنج دانش
- قانون جرایم رایانه‌ای مصوب سال ۸۸ ایران
- قانون مجازات اسلامی ایران
- گرکی، مارکو (۱۳۹۰)، جرایم سایبری راهنمایی برای کشورهای در حال توسعه، ترجمه مرتضی اکبری، تهران: پلیس فتا
- لازرژ، کریستین (۱۳۹۹)، درآمدی بر سیاست جنایی، ترجمه علی حسین نجفی ابرندآبادی، تهران: انتشارات میزان
- مصوبات کنوانسیون بوداپست ۲۰۰۱
- می‌ری دلماس، مارتی (۱۳۹۳)، نظام‌های بزرگ سیاست جنایی، ترجمه علی حسین نجفی

ابرندابادی، تهران: بی جا

- _____ (۱۳۸۳)، بررسی ابعاد حقوقی فناوری اطلاعات، تهران: مرکز مطالعات راهبردی و توسعه قضایی

- _____ (۱۳۷۶)، نشریه بین‌المللی سیاست جنایی (ش ۴۴، ۴۳، ۱۹۹۴)، ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور

- _____ (۱۹۹۰)، شورای اروپا جرم رایانه‌ای، توصیه‌نامه شماره ۸۹، ترجمه دبیرخانه شورای عالی انفورماتیک، سازمان برنامه و بودجه کشور

