پژوهشنامه حقوق اسلامی، سال هفدهم، شمارهٔ اول (پیاپی ۴۳)، بهار و تابستان ۱۳۹۵، صص۹۹-۱۲۶

سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم

امیر وطنی *
حمید اسدی **

تاریخ دریافت: ۱۳۹۵/۱۰/۲۰
تاریخ پذیرش: ۱۳۹۵/۱۲/۱۴

چکیده

پیشگیری و مقابله با جرائم، محور اصلی سیاست جنایی هر کشور محسوب می شود که برای تحقق آن، از ابزارها و امکانات مختلفی در انواع مهم سیاست جنایی تقنینی، قضایی و مشارکتی بهره‌برداری می‌گردد. با گسترش فضای مجازی و بهره‌برداری افراد از رایانه و اینترنت و امکان وقوع جرم علیه فناوری اطلاعات، تدوین سیاست جنایی مناسب علیه جرائم سایبری از اهمیت بسزایی برخوردار است. سیاست جنایی تقنینی، وظیفه قانون‌گذاری در یک کشور است که در خصوص جرائم سایبری، قانون‌گذار در قوانین و مقررات مربوط، گاه به‌طور ضمنی و گاه به‌طور صریح به استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر پرداخته است که یکی از مهم‌ترین موارد آن، مصوبات شورای عالی فضای مجازی است. در سیاست جنایی مشارکتی، برای پیشگیری از جرم و مبارزه با آن از اسباب و وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود. یکی از طرق نظارت بر جرائم سایبری، توسط نهادهای مدنی و اشخاص و با مشارکت مردم که می‌تواند مصداقی از امر به معروف و نهی از منکر باشد و موجب پیشگیری از جرائم سایبری شود، مربوط به نظارت بر ورودی‌ها و خروجی‌هاست که سعی می‌شود از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری شود که از مهم‌ترین طرق آن، استفاده از رمز عبور در رایانه و نرم‌افزار ضد پایش است. در سیاست جنایی قضایی که در تصمیم‌ها و رویه‌های قضایی دادسراها و دادگاه‌ها منعکس می‌شود، قوه قضائیه با رویکرد پیشگیرانه در خصوص جرائم سایبری با کمک نهادهایی مانند مرکز ماهر

* عضو هیئت علمی دانشگاه خوارزمی vatani_amir@yahoo.com
** دانشجوی دکتری فقه و حقوق جزا دانشگاه خوارزمی (نویسنده مسئول) hamidassadi90@gmail.com

(مرکز مدیریت امداد و هماهنگی عملیات رخداد) و مرکز آپا (مرکز آگاهی رسانه، پشتیبانی و امداد رایانه‌ای) و پلیس فتا فعالیت می‌نماید.

واژگان کلیدی:

سیاست جنایی، جرائم سایبری، سیاست جنایی تقنینی، سیاست جنایی قضایی، سیاست جنایی مشارکتی.

مقدمه

در جهان امروز، رسانه‌ها با انتقال اطلاعات جدید و مبادله افکار و عقاید عمومی، در راه پیشرفت و تمدن بشری، نقش بزرگی را به عهده گرفته‌اند، به‌طوری که عصر امروز را عصر ارتباطات نامیده‌اند. رسانه‌های گوناگون اعم از دیداری، نوشتاری و شنیداری می‌توانند افکار و عقاید مردم را تحت تأثیر قرار دهند چرا که رسانه‌های نامحدود امروزی، نقش بسیاری در فرهنگ‌سازی و هنجارآفرینی در جامعه دارند. اگر رسانه به نحو صحیحی در راستای فرهنگ یک جامعه مورد استفاده قرار گیرد می‌تواند موجب القای سریع بسیاری از مفاهیم گردد و از وقوع بسیاری از معضلات و جرائم در جامعه پیشگیری نماید. برعکس اگر محتوای رسانه‌ها بدون هدف و کارشناسی تنظیم شده باشد، می‌تواند تأثیرات منفی بسیاری بر جامعه داشته باشد و حتی منجر به وقوع جرائم و انحرافات در جامعه گردد.

یکی از وسایل مورد استفاده عمده در جامعه کنونی، رایانه و به ویژه بهره‌گیری از اینترنت برای انتقال اطلاعات در فضای مجازی است. وقوع جرم علیه فناوری اطلاعات در فضای مجازی که با نام جرائم سایبری شناخته می‌شود، محدوده بزرگی از جرائم را دربر می‌گیرد که با توجه به استفاده گسترده اشخاص از فضای مجازی در امور مختلف ارتباطات تجاری، اقتصادی، فرهنگی، علمی، هنری، سیاسی و ... اهمیت دو چندان می‌یابد؛ ازاین‌رو، در سیاست جنایی جوامع، بر این مسئله و پیشگیری از وقوع و مقابله با آن باید توجه لازم مبذول شود.

با توجه به اهداف مذکور، سؤال اصلی در پژوهش حاضر آن است که سیاست جنایی ایران در خصوص جرائم سایبری جهت پیشگیری و مقابله با این جرائم

چیست؟ به نظر می‌رسد با توجه به اهمیت این جرائم، سیاست جنایی در این زمینه غافل نبوده و به بررسی این مسئله پرداخته است. در این زمینه هم در قانون‌گذاری، اقدامات قضایی و هم نقش نهادهای مشارکتی را می‌توان مهم تلقی کرد. برای بررسی این مسئله لازم است انواع مختلف سیاست جنایی در این مسئله بررسی شود. به همین سبب در این مقاله ابتدا مفاهیم جرائم سایبری، مفهوم و انواع سیاست جنایی به نحو مختصر بیان شده و سپس سیاست جنایی تقنینی، قضایی و مشارکتی ایران در جرائم سایبری به نحو مجزا بررسی خواهد شد.

۱. مفهوم‌شناسی

در ابتدا مفهوم جرائم سایبری و سیاست جنایی بیان شود تا شناسایی دقیق مفهوم اصطلاحی، بتوان محدوه بحث را مشخص نموده و وارد مبحث شد:

۱-۱. مفهوم‌شناسی جرائم سایبری

واژه سایبر از نظر لغوی به معنای مجازی و غیرملموس و مترادف لغت «Cybernetes» است. سایبر از لغت یونانی «Virtual» انگلیسی معادل مفهوم سکاندار یا راهنما مشتق شده است. سایبر در زبان انگلیسی، پیشوند و در زبان فارسی پسوندی است که به کلمات جدید و امروزی متصل می‌شود تا به آن‌ها معنا و مفهوم دهد؛ به‌گونه‌ای که مرتبط با فضای رایانه یا برخط باشد. به عبارت دیگر، سایبر به مطالعه مکانیزم‌های مورد استفاده در کنترل و تنظیم سیستم‌های پیچیده اعم از انسان یا ماشین اطلاق می‌شود. سایبر در فارسی به مجاز و مجازی ترجمه شده است؛ اما این ترجمه گویای دقیق این واژه نیست زیرا محیط سایبر محیطی است حقیقی و واقعی نه دروغین و مجازی و فقط به شکل مادی و ملموس احساس شدنی نیست و این نکته کافی نیست که به آن مجاز و مجازی اطلاق شود (پرویزی، ۱۳۸۴، ص۳۸). اما سایبر در اصطلاح به همه محیط‌هایی گفته می‌شود که اساس فعالیت آن‌ها بر مبنای پردازش و طبق سامانه صفر و یک کار می‌کنند. سایبر در زبان عموم مردم به‌غلط اینترنت نامیده می‌شود درحالی‌که اینترنت یک شبکه رایانه‌ای بین‌المللی بزرگ است که نظیر آن چندین شبکه بزرگ مثل یو زنت، تله نت و ... وجود دارد. تعداد این شبکه‌های بزرگ بالغبر ۱۹ شبکه است (پرویزی، ۱۳۸۴، ص۴۰).

اصطلاح فضای سایبر یا دنیای مجازی آنلاین، اصطلاحی است که نخستین‌بار توسط ویلیام گیبسون[1] با عنوان نیورومانسر در سال ۱۹۸۴ مورد استفاده قرار گرفت. فضای سایبر در این تعریف، شبکه‌هایی است که از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند و تمام اطلاعات راجع به روابطِ افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طور کلی هر آنچه در کره خاکی به صورت فیزیکی و ملموس وجود دارد، در این فضا به شکل دیجیتالی وجود داشته و قابل استفاده و دسترسِ کاربران بوده و از طریق رایانه، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط باشند.

در زبان فارسی، فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرار کنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد (عاملی،۱۳۹۰، ص۲۳).

جرائم سایبری در اصطلاح به جرائمی گفته می‌شود که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد (جاویدنیا، ۱۳۸۸، ص۲۲۵). امروزه بسیاری از جرائم سنتی، هم‌زمان با پیشرفت فناوری اطلاعات و ارتباطات به‌شدت متحول شده و به جرائم سایبری تبدیل شده‌اند (پرویزی، ۱۳۸۴، ص۴۶). جرائم سایبری نیز به جهت گسترش خود، رفته‌رفته جانشین عباراتی چون جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. به جرائم سایبر، جرائم علیه فناوری اطلاعات نیز گفته می‌شود (پرویزی، ۱۳۸۴، ص۴۰).

واژه رایانه به‌گونه‌ای دقیق و جامع نمی‌تواند گستردگی این محیط را نشان دهد زیرا بسیاری از ابزار و وسایل امروزی با داده‌هایی کار می‌کنند که اساساً به آن‌ها رایانه اطلاق نمی‌شود. ازاین‌رو عبارت‌هایی مانند جرم‌های رایانه‌ای یا جرم‌های اینترنتی نیز نمی‌توانند به‌گونه‌ای دقیق جرم‌های ارتکابی مربوط به این حوزه را پوشش دهند. برای نمونه یک سامانه ضبط و پخش الکترونیکی، رایانه نیست؛ اما به‌طور کلی در زیرمجموعه جهان سایبر قرار می‌گیرد.

۱-۲. مفهوم‌شناسی سیاست جنایی

پیدایش اصطلاح «سیاست جنایی» توسط فویر باخ ، حقوق‌دان آلمانی، در پایان قرن ۱۸، به «حکمت‌گرایی» در برخورد با جرم مربوط بوده و زائیده آن است (حسینی، ۱۳۸۳، صص ۲۱و۲۲؛ لازرژ ، ۱۳۸۱، ۱۰و۱۱؛ نجفی ابرند آبادی، ۱۳۷۸، ص۵).

اولین کاربردهای سیاست جنایی در معنایی معادل «حقوق کیفری» یا «سیاست کیفری» که مبتنی بر «جرم ـ مجازات» و «قانون ـ قضا» می‌باشد، بوده است (حسینی، ۱۳۸۳، ص۲۳) فویر باخ نیز همین کاربرد سیاست جنایی را مدنظر قرار داده است (نجفی ابرند آبادی، ۱۳۷۸، ص۹). وی مفهوم مضیقی از این اصطلاح داده است. او در تعریف خود تنها به وسایل قهرآمیز و تنبیهی اشاره دارد که نظام کیفری برای مقابله با مجرمان در اختیار دارد. از سوی دیگر این وظیفه تنها به عهده دولت نهاده شده و تأمین امنیت را از وظایف خاص دولت به شمار آورده است. همچنین او، تنها به مبارزه علیه جرم (که در قانون جرم‌انگاری شده و برای آن مجازات تعیین شده) پرداخته است و به انحرافات اجتماعی توجهی نکرده است (لازرژ، ۱۳۸۱، ص۱۱؛ حسینی، ۱۳۸۳، ص۲۳؛ رشادتی، ۱۳۸۷، ص۳۴۰؛ محمدنژاد، بی‌تا، ص۴۱؛ نوربها، ص۱۳۷۸) اما باید دانست سیاست جنایی تنها متکی به سیاست کیفری نیست (کی نیا، ۱۳۷۳، ص۵۰). تعریف دیگر از سیاست جنایی، تعریف فون لیست[۲] دانشمند آلمانی از سیاست جنایی است. او می‌گوید: «سیاست جنایی، مجموعه منظم اصولی است که دولت و جامعه به وسیله آن‌ها مبارزه علیه بزه را سامان می‌بخشد». فون لیست برخلاف فویرباخ، علاوه بر دولت، جامعه‌مدنی را نیز مسئول سازماندهی و تأمین امنیت می‌داند اما او نیز مانند فویر باخ، سیاست جنایی را محدود در سیاست کیفری نموده است (لازرژ، ۱۳۸۱، صص ۱۱و ۱۲؛ حسینی، ۱۳۸۳، صص ۲۲و۲۳؛ رشادتی، ۱۳۸۷، ص۳۴۰).

کوش دانشمند فرانسوی (قرن ۲۰) در تعریف سیاست جنایی می‌گوید: «یک علم کاربردی که هدف آن موفقیت عملی در سازماندهی عقلانی و مؤثر مبارزه با جرم است (لازرژ، ۱۳۸۱، ص۱۳؛ رشادتی، ۱۳۸۷، ص۳۴۰). دندی یو د وابر[۳] دانشمند دیگر فرانسوی، بیش ازیک ربع قرن، بعد کوش، تعریفی شبیه او از سیاست جنایی ارائه می‌دهد: به نظر او «سیاست جنایی یک هنر و فن است که موضوع آن کشف روش‌هایی

است که مبارزه مؤثر علیه جرم را میسر می‌سازد». به نظر او سیاست جنایی همه شیوه‌های در اختیار دولت را دربر نمی‌گیرد؛ چرا که موجب محو پدیده مجرمانه نمی‌گردد (لازرژ، ۱۳۸۱، صص۱۲و۱۳؛ حسینی، ۱۳۸۳، ص۲۳) همان‌گونه که دیدیم این چهار دانشمند تعریف مضیقی از سیاست جنایی ارائه داده و آن را محدود به سیاست کیفری و مبارزه با جرم کردند (باصری، ۱۳۸۷، ص ۳۳).

در مقابل این نظر، عده‌ای دیگر از دانشمندان، تفسیر موسعی از سیاست جنایی ارائه داده‌اند که علاوه بر حقوق کیفری و سایر نظام‌های حقوقی، نظام جامعه (مردم و سازمان‌های غیردولتی) را نیز در مبارزه با جرم و پیشگیری سهیم می‌دانند (باصری، ۱۳۸۷، ص ۳۳). یکی از آن‌ها آنسل قاضی فرانسوی است. او معتقد است همان‌طور که قلمروی بزهکاری، از جرم به انحراف تسری یافته، سیاست جنایی نیز علاوه بر جرم باید به امر پیشگیری از نارسایی‌های کارکردی جرم‌زا یعنی عوامل اجتماعی زمینه‌ساز ارتکاب جرم، تعمیم داده شده و کلیه انحرافات را در بر بگیرد. همچنین در این امر، قوای عمومی دولت، به معنای اعم باید در برنامه‌ریزی، سیاست‌گذاری و اجرای آن شرکت کنند. در دیدگاه آنسل، سیاست جنایی به معنای اعم اولاً، علاوه بر جرم، انحراف را نیز در بر می‌گیرد و علاوه بر مجازات به پیشگیری نیز توجه دارد؛ ثانیاً، علاوه بر نظام کیفری به تدابیر نظام اجتماعی نیز توجه دارد؛ ثالثاً، سیاست جنایی از مفهوم سیاست کیفری خارج شده و به مثابه سیاست عمومی یک کشور یا یک دولت است (لازرژ، ۱۳۸۱، صص ۱۵-۱۳؛ حسینی، ۱۳۸۳، ص۲۳، محمدنژاد، ۱۳۸۴، ص۴۱).

یکی دیگر از دانشمندان، خانم «می ری دلماس مارتی»[۴] نیز مانند آنسل تعریف موسعی از سیاست جنایی ارائه می‌دهد. او معتقد است: «سیاست جنایی، مجموعه روش‌هایی است که هیئت (پیکر) اجتماع با استفاده از آن‌ها، پاسخ به پدیده مجرمانه را سامان می‌بخشد» (نجفی ابرند آبادی، ۱۳۷۸، ص۹). از دیدگاه او: اولاً، سیاست جنایی ماهیت صرفاً کیفری ندارد و صرفاً از نظام کیفری ناشی نمی‌شود؛ بلکه سایر نظام‌های حقوقی مانند نظام حقوقی اداری، انضباطی، اجتماعی، مالیاتی و ... را نیز در بر می‌گیرد؛ ثانیاً، علاوه بر پاسخ‌های نهادهای رسمی دولت با رعایت تشریفات خاص علیه پدیده مجرمانه، پاسخ‌های منبعث از جامعه مدنی و نهادهای مختلف مردمی را نیز دربر

می‌گیرد؛ ثالثاً، از دولت به کل پیکر اجتماع تعبیر می‌کند به شرط آنکه بدنه اجتماعی پاسخ‌های خود را سازمان‌دهی کرده باشد؛ رابعاً، پدیده مجرمانه هم جرم و هم انحراف را شامل می‌شود و در نهایت، سیاست جنایی، علاوه بر سرکوب کردن و مجازات، اقدامات پیشگیرانه علیه جرم و انحراف را نیز شامل می‌شود (لازرژ، ۱۳۸۱، صص۱۶و۱۷؛ حسینی، ۱۳۸۳، صص۲۳و۲۴؛ رشادتی، ۱۳۸۷، ص۳۴۱).

عده‌ای دیگر از دانشمندان نیز در تعریف سیاست جنایی عنصر پیشگیری از جرم را بسیار مهم می‌دانند: کلین اسکراد در تعریف سیاست جنایی می‌گوید: «شناخت وسایلی که مقنن به منظور پیشگیری از بزه و حمایت از حقوق طبیعی شهروندان، منطبق با گرایش خاص هر دولت می‌تواند بیابد». کریسپینی نیز با همین رویکرد سیاست جنایی را چنین تعریف می‌کند: «سیاست جنایی دانشی است که فعالیتی را که دولت باید به منظور پیشگیری و سرکوبی جرائم بسط دهد، بررسی می‌کند» (حسینی، ۱۳۸۳، ص۲۳).

در همه تعاریف ارائه شده عناصر بزه، بزهکار، بزهکاری، واکنش سرکوبگرانه، پیشگیرانه یا اصلاحی، به‌عنوان ارکان تعریف ملحوظ‌اند (حسینی، ۱۳۸۳، ص۲۴). پس می‌توان گفت تعریف سیاست جنایی در پایان قرن بیستم بدین نحو بوده است: «سیاست جنایی، کلیه اقدام‌های سرکوب‌گرانه (کیفری) و غیر کیفری و پیشگیرانه با ماهیت‌های مختلف را شامل می‌شود که دولت و جامعه مدنی هر یک به نحو مستقل و یا با مشارکت سازمان‌یافته یکدیگر، از آن‌ها در قالب روش‌های مختلف به منظور سرکوبی بزهکاری و بزهکاران و نیز پیشگیری از جرم و انحراف استفاده می‌کنند» (لازرژ،۱۳۸۱، صص۱۶و۱۷).

با توجه به تعاریف موسع ارائه شده از سیاست جنایی می‌توان ویژگی‌هایی را که در تعاریف آمده است بدین نحو خلاصه کرد: اول آنکه سیاست جنایی، علاوه بر تبیین جرم و مجازات، محدوده پیشگیری، درمان، اصلاح و حتی ماقبل پیشگیری از جرم را نیز مدنظر قرار می‌دهد؛ ویژگی دیگر آن است که سیاست جنایی تنها محدود به دولت نیست و سایر نهادهای غیردولتی و مردم را نیز در بر می‌گیرد؛ علاوه بر آن، سیاست جنایی مجموعه‌ای گسترده از اقدامات متفاوت است نه یک اقدام و یک تدبیر، و ویژگی آخر آنکه سیاست جنایی به انحراف نیز توجه دارد. در این تعاریف موسع،

سیاست جنایی محدود به جرم و مجازات نیست و با توجه به اینکه پیشگیری از جرم و نقش نهادهای غیر دولتی و مردم در تعریف جایگاه مهمی دارند، سیاست جنایی دارای دامنه بسیار وسیعی است. با توجه به این می‌توان گفت، هدف سیاست جنایی، مبارزه منطقی و عاقلانه با بزهکاری است که اعم از پیشگیری و تنبیه و سرکوبگری است که در موضوع پیشگیری، علاوه بر پیشگیری از وقوع جرم به انحرافات اجتماعی نیز توجه دارد (محمدنژاد، ۱۳۸۴، ص۴۱).

اگر بخواهیم یک تعریف جامع که در بردارنده تمام ویژگی‌های سیاست جنایی باشد و آن را محدود نکند می‌توان این تعریف را از سیاست جنایی ارائه نمود: *«مجموعه‌ای از جهت‌گیری‌ها و اقدامات متفاوت دولت، نهادهای غیردولتی و مردم در مهار بزهکاری است که علاوه بر مبارزه با جرم و توجه به مجازات‌ها و اصلاح مجرمین، مرحله پیشگیری و حتی ماقبل آن را نیز دربر می‌گیرد».*

۲. انواع سیاست جنایی

بر اساس دسته‌بندی‌های کلی سیاست جنایی بر سه قسم است: ۱. سیاست جنایی تقنینی؛ ۲. سیاست جنایی مشارکتی؛ ۳. سیاست جنایی قضایی.

۲-۱. سیاست جنایی تقنینی

دولت با وضع قوانین ویژه افراد را به رعایت و اتخاذ اقدامات و تدابیر و مقررات امنیتی لازم و اولیه ملزم می‌نماید. در واقع سیاست جنایی تقنینی، وظیفه قانون‌گذاری در یک کشور است که در کشور ما بر اساس قانون اساسی بر عهده مجلس شورای اسلامی و در موارد خاص بر عهده نهادهای دیگر گذاشته شده است. البته فرآیند قانون‌گذاری توسط مجلس انجام می‌شود اما در فرآیند تهیه و تنظیم یک پیش‌نویس قانونی تا تصویب آن، تحقیقات علمی، افکار عمومی، روشنفکران، گروه‌های فشار، سازمان‌های مستقل، احزاب و به‌ویژه رسانه‌های گروهی در آگاه‌سازی مردم، نحوه تصویب، نوع تصویب، مفاد قوانین آینده و ... نقش مهمی را بر عهده دارند (باصری، ۱۳۸۷، ص۳۶؛ سوتهیل و دیگران، ۱۳۸۳، ص۲۰۲؛ خالصی، ۱۳۸۳، ص۳۲) بنابراین لازم است قانون‌گذار برای تصویب قوانین و تنظیم سیاست جنایی مناسب و کارآمد، به واقعیت‌ها،

حقـایق جامعـه، ارزش‌هـای اخلاقـی، محـدود نمـودن دخالـت حقـوق جـزا، اسـتفاده از یافته‌های جرم‌شناسی و کیفرشناسی و اسـتفاده از ضـمانت اجراهـای غیـر کیفـری توجـه داشته باشد؛ به این معنا که تلاش قانون‌گذار بر این باشد تا از وقوع بزه جلوگیری نمایـد و به توده مردم اخلاق پسندیده را بیاموزد نه آنکه دائماً به جرم‌زایی پرداختـه و مجـازات را سنگین‌تر نماید. همچنین سیاست مقنن باید هم‌پای توسـعه و تحـول جامعـه پیشـرفت کند (محمدنژاد، ۱۳۸۴، ص۴۱).

۲-۲. سیاست جنایی قضایی ـ مشارکتی

این نوع از سیاست جنایی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم را دربرمی‌گیرد که با همکاری وسیع جامعه مدنی و نیروهای دولتی مانند پلـیس، سـازمان زندان‌ها، سازمان محیط زیست، جنگل بانی و .. با دستگاه قضایی انجام می‌شود.

اهداف سیاست جنایی مشارکتی عبارتنـد از: اول، جلـب افکـار عمـومی در افـزایش کارآیی این نهادها و کاهش هزینه‌هـای انسـانی و مـادی کشـف و پیگـرد جـرائم اسـت؛ هـدف دیگـر مشـارکت مـردم در حـل و فصـل دعـاوی مبتنـی بـر صـلح و سـازش، میانجی‌گری، تلطیف مجازات‌هـا، همکـاری در مشـخص شـدن مجـازات‌هـا، کمـک بـه زندانیان نیازمند، گذر از عـدالت کیفـری بـه عـدالت ترمیمـی ـ قضـایی اسـت (باصـری، ۱۳۸۷، ص۳۷)؛ هدف سوم، اعتبار بخشیدن به طرح سیاست جنـایی تنظـیم شـده توسـط قوه مقننه و قوه مجریه است و هدف چهارم، فراهم کـردن زمینـه اجـرای سیاسـت‌هـا بـا استفاده از قدرت رسانه‌ها، انجمن‌ها و شهروندان است (لازرژ، ۱۳۸۱، ص۱۳۹).

۲-۳. سیاست جنایی قضایی

این نوع از سیاست جنایی در تصمیم‌ها و رویه‌های قضایی دادسراها و دادگاه‌ها مـنعکس می‌شود که ابزارهایی چون حضور هیئت منصفه، مشاوران، دادرسان مردمی می‌توانـد بـر آن تأثیر گذارد. در این بخش، اموری مانند انعطاف مجازات‌ها، تخفیف و تشدید، تعلیـق مجازات، آزادی مشروط، فردی کردن کیفرها، استفاده از اقدامات تأمینی، مسـئله عـدالت کیفری، تشویق طـرفین بـه صـلح و سـازش و ... در دادگـاه‌هـا و توسـط قضـات مطـرح می‌گردد (باصری، ۱۳۸۷، ص۳۶؛ لازرژ، ۱۳۸۱، ص۱۲۳).

۳. ویژگی‌های خاص جرائم (فضای) سایبری نسبت به جرائم سنتی

یکی از مهم‌ترین ابزارهای ارتکاب جرائم سایبری استفاده از اینترنت است. اینترنت در معنای عمومی به معنای مجموعه‌ای از شبکه‌ها است که اولاً به صورت فیزیکی به هم متصلند، ثانیاً می توانند با یکدیگر ارتباط برقرار کند و منابع اطلاعاتی را با هم به اشتراک بگذارند و ثالثاً قادرند در کنار هم به صورت یک شبکه واحد عمل کنند (دانایی، ۱۳۸۸، ص۱۷۱).

از سرویس‌های موجود در اینترنت که به‌عنوان کلید سرویس‌های دیگر به شمار می‌آید، پست الکترونیک است. در این سرویس، متن یا هر پرونده کامپیوتری دیگری توسط یک دستور ظرف چند ثانیه به آدرس‌های مورد نظر در هر نقطه‌ای از دنیا و به هر نوع کامپیوتری ارسال می‌شود (دیندار فرکوش و صدری نیا، ۱۳۸۸، ص۱۴۰). کاربران اینترنت می توانند با استفاده از سرویس پست الکترونیک با سایر کاربران پیام مبادله کنند (دانایی، ۱۳۸۸، ص۱۷۲). یکی دیگر از سرویس‌های موجود در اینترنت، وبلاگ‌ها و وب‌سایت‌ها هستند. با اتصال به شبکه اینترنت، دسترسی به بانک‌های اطلاعاتی در تمام عرصه‌ها از جمله تجارت، حقوق، پزشکی، علوم و... فراهم می‌گردد. افراد می‌توانند با مراجعه به وبلاگ‌ها و وب‌سایت‌ها به آخرین اطلاعات مورد نیاز خود، در تمامی زمینه‌ها دسترسی پیدا کنند (دیندار فرکوش و صدری نیا، ۱۳۸۸، ص۱۴۲).

در اینترنت مزایایی وجود دارد که استفاده از آن را راحت‌تر نموده و مجرمان در روزگار کنونی، به ارتکاب جرائم سایبری به نسبت جرائم سنتی علاقه بیشتری دارند. به‌طور کلی ویژگی‌های این سرویس اطلاعاتی عبارتند از: گستردگی حوزه دسترسی، سرعت دسترسی، سهولت دسترسی، تنوع کاربردها و صرفه‌جویی (دانایی، ۱۳۸۸، صص۱۷۱و۱۷۲) که در ذیل برخی موارد آن به‌طور خلاصه ذکر می‌شود:

۳-۱. امکان گمنامی و ناشناخته بودن

از جمله ویژگی‌های منحصر به‌فرد این فضا، امکان گمنامی و ناشناخته بودن در آن است. به دیگر سخن، ناشناختگی از اصول حاکم بر جرائم جهان مجازی است (جوان جعفری، ۱۳۸۹، ص۱۷۶) نامرئی بودن این جرأت را به افراد می‌دهد که به هر جا می‌خواهند سرک بکشند و کارهایی انجام دهند که در دنیای واقعی انجام نمی‌دهند.

۳-۲. افزایش فرصت‌ها

این یک واقعیت محض است که فناوری‌های جدید علاوه بر ابزار قوی برای ارتکاب جرم، فرصت‌های ارتکاب را نیز افزایش می‌دهد. فضای سایبر بسیاری از امور خرد و کلان اجتماعی را در امن‌ترین، خلوت‌ترین و راحت‌ترین موقعیت، در مقابل دیدگان افراد قرار می‌دهد. این فرصت مغتنم در کنار دیگر شرایط مهیا، حتی کسانی که متعهد به رعایت هنجارهای اجتماعی هستند را وسوسه می‌کند، تا روحیات پلیدشان را بروز دهند. لذا به عقیده عده‌ای این فضا مصداق بارز بهشت امن هنجارشکنان است (جلالی فراهانی، ۱۳۸۹، ص۱۷). سایبر یک فضای سیال است که هیچ‌گونه حد و مرزی را نمی‌شناسد و از مرزهای جغرافیایی دنیای واقعی در آن خبری نیست. طبیعی است که مجرمین با تأسی از این نقطه‌ضعف‌ها، فرصت ارتکاب جرائم بیشتر و انتخاب‌های کلان‌تری نیز دارند. فرصت[۵] در اینجا یعنی فراهم بودن مقتضیات و فقدان موانع. به همین دلیل است که اکثر صاحب‌نظران در عرصه‌های پیشگیری، قائل به کاهش فرصت‌ها در زمینه جرائم‌اند.

۳-۳. آسانی و سرعت ارتکاب جرائم

از ویژگی‌های دیگر این فضا می‌توان به آسانی و سرعت ارتکاب جرائم در آن اشاره کرد. مجرمین سنتی اغلب در فرآیند گذار از اندیشه به عمل[۶] و ارتکاب یک جرم تام، زمان و فاصله زیادی را طی می‌کردند. شاید یکی از عوامل کندی وقوع پدیده بزهکارانه در جهان واقعی بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، آماج بزه و مکان ارتکاب بزه است. حال اینکه ساختار فضای مجازی به‌گونه‌ای است که در آن قرابت مکانی میان سه عنصر فوق ضرورتی ندارد (جوان جعفری، ۱۳۸۹، ص۱۷۶)؛ لذا امروزه به مدد تکنولوژی‌های نوین، مرتکب اغلب با یک کلیک می‌تواند به عرصهٔ ارتکاب جرم راه پیدا کند. مثلاً در ارتکاب جرم کلاهبرداری دیگر به عوامل و ارکان خاص این جرم در دنیای مادی از جمله مانورهای خاص متقلبانه و تعاملات رو در روی افراد با هم نیازی نیست. چرا که سایبر امکان بردن اموال دیگری را به سادگی فشردن تنها چند کلید و انجام عملیاتی پیش پا افتاده ممکن ساخته است.

۳-۴. فقدان ابزارهای نظارتی و حاکمیتی

مجرمین در فضای سایبر به معنای واقعی کلمه از آزادی عمل و آزادی اراده برخوردارند. چرا که هیچ قدرت تحکیم‌کننده و هیچ نیرو و اهرم بازدارنده‌ای وجود ندارد. دنیای جدید موقعیتی را به وجود آورده که افراد فارغ از هرگونه نظارت و کنترل در خلوت خود در مقابل رایانه قرار بگیرند، و به راحتی وارد فضای افسارگسیخته‌ای شوند که اثری از عوامل دولتی و جامعهٔ محدودکنندهٔ آزادی نیست (عالی‌پور، ۱۳۸۳، ص۹۹). این فضا مالک خصوصی و دولتی ندارد. تابع آیین‌نامه‌ای جهانی نمی‌باشد و هیچ قانون‌گذار عمومی در آن وجود ندارد .عدم وجود ضوابط دقیق در دنیای مجازی باعث شده که از آن به‌عنوان «غرب وحشی جدید» تعبیر شود (جوان جعفری، ۱۳۸۹، ص۱۷۱).

۳-۵. عدم پای‌بندی به محدودیت‌های زمانی و مکانی

در فضای سایبر پایبندی کمتری به محدودیت‌های زمانی ـ مکانی دیده می‌شود. این وضعیت اساساً به رشد چشم‌گیر فناوری‌های اطلاعات و ارتباطات الکترونیکی مربوط می‌شود. جوامع شبکه‌ای این امکان را فراهم آورده‌اند تا زمان و مکان محو شوند. یک تراکنش متقلبانه می‌تواند از فاصلهٔ هزاران مایل و در کسر هزارم ثانیه ارتکاب یابد و در عین حال یک آزارگر می‌تواند بزه دیدهٔ خویش را از فاصلهٔ بسیار دور و به صورت زنده آماج گفتار تمسخرآمیز خویش قرار دهد (ویلیامز، ۱۳۹۱، صص۴۹-۵۰).

۳-۶. بین‌المللی (فرامرزی) بودن

مهم‌ترین خصیصه فضای سایبر بین‌المللی بودن یا به عبارت بهتر فرامرزی بودن آن است. شبکه‌های پیشین به صورت محلی یا حداکثر منطقه‌ای قابل بهره‌برداری بودند. اما به مدد سیستم‌های بی‌سیم و باسیم، نظیر شبکه‌های ماهواره‌ای یا خطوط فیبر نوری، این امکان فراهم گشته است (جلالی فراهانی، ۱۳۸۴، ص۱۴۲).

۴. سیاست جنایی تقنینی در جرائم سایبری

در قوانین و مقررات مربوط به فضای سایبر قانون‌گذار گاه به‌طور ضمنی و گاه به‌طور صریح به استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر پرداخته که در زیر به

آن‌ها اشاره می‌شود: نخست مصوبات شورای عالی فضای مجازی است. این شورا به تاریخ ۱۷ اسفند ۱۳۹۰به فرمان رهبری تشکیل و موظف گردید تا به‌طور کامل و روز آمد بر فضای درونی و بیرونی اینترنت اشراف داشته و امنیت این فضا را تأمین سازد. در مصوبه این شورا با موضوع توسعه فضای مجازی سالم، مفید و امن به شماره ۹۴/۱۰۰۱۵۱/ش مصوب ۹۴/۱/۳۰ به تعریف فضای مجازی ایمن پرداخته شده است. در این مصوبه آمده: «فضای ایمن فضایی است متشکل از شبکه‌های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش‌های اسلامی و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی از قبیل سن، جنس، شغل و تحصیلات از محتوا و خدمات مورد نیاز بهره‌مند شوند و حتی‌الامکان در برابر محتوا و رفتارهای آسیب‌زا محفوظ بمانند».

در عنوان این مصوبه هرچند به توسعه فضای مجازی سالم، مفید و ایمن پرداخته شده است اما در تعریفی که از فضای ایمن ارائه شده، به نظر می‌رسد فضای ایمن به لحاظ محتوایی مدنظر بوده یعنی فضایی که محتوای آن در چارچوب مبانی اسلامی باشد. به عبارت بهتر در این مقرره قانون‌گذار صرفاً به پالایش محتوا توجه داشته درحالی‌که پالایه یک اقدام حفاظتی محسوب نمی‌شود (فضلی، ۱۳۸۸، ص۱۱۱). دلیل این امر این است که پالایه همواره از سوی مقامات دولتی و برای پاک‌سازی یک وب سایت یا سایت از اطلاعاتی که به لحاظ مضمون با مبانی اخلاقی و اسلامی ناسازگاراند به کار رفته و جنبه حفاظتی ندارد درحالی‌که آنچه در حفاظت از اطلاعات مالی مدنظر است این است که از اطلاعات مالی حفاظت به عمل آید تا این اطلاعات، افشاء، تخریب، محو و ... نشوند که این حفاظت می‌تواند هم از سوی اشخاص حقیقی و هم حقوقی باشد.

در مصوبه دیگر، این شورا با موضوع سیاست‌های سامان‌دهی خدمات پیامکی ارزش افزوده و پیامک انبوه در شبکه‌های ارتباطی به شماره ۹۳/۱۰۳۶۸۱/ش مورخ ۹۳/۱۱/۱ در بند ۴ آمده: «به منظور حفظ و صیانت از اطلاعات خصوصی مخاطبان پیام و براساس قوانین به ویژه قانون جرائم رایانه‌ای، ارائه‌دهندگان خدمات ارتباطی و ارائه‌دهندگان خدمات محتوایی، حق واگذاری، فروش و یا در اختیار قرار دادن این اطلاعات به دیگران را ندارند». در این مصوبه نیز هرچند به حفاظت و حراست از

اطلاعات اشاره شده، اما تنها به حفاظت از اطلاعاتی که مربوط به حریم خصوصی شهروندان است، پرداخته شده و به اطلاعات مالی به‌طور خاص توجهی نشده است (جاویدنیا، ۱۳۸۸، ص۵). دلیل این امر چندان مشخص نیست اما به نظر می‌رسد یا وصف اطلاعات مالی برای مقنن ناشناخته بوده و ازاین‌رو حمایتی از این اطلاعات به عمل نیاورده و یا اطلاعات مالی را نیز بخشی از اطلاعات شخصی افراد قلمداد نموده و آن‌ها را همانند اطلاعات شخصی مشمول حمایت قرار داده است. به این استدلال این خدشه وارد می‌شود که اولاً از اطلاعات مالی اشخاص حقوقی در این قالب نمی‌توان حفاظت نمود؛ ثانیاً اقداماتی هم که جهت حفاظت از اطلاعات شخصی به عمل آمده، تدابیر واسطه‌ای هستند. این تدابیر، تدابیری هستند که در پی تنظیم مقررات مناسب برای حفاظت از اطلاعات‌اند (جوان جعفری، ۱۳۸۹، ص۵).

در مصوبه دیگر این شورا در خصوص طرح‌های کلان مرکز ملی فضای مجازی کشور جهت تدوین لایحه بودجه و در تصویب‌نامه این شورا در خصوص شرح وظایف، اختیارات و اعضای کمیسیون عالی فضای مجازی، به ارتقای امنیت سایبری پرداخته شده است، اما هیچ سخنی از چگونگی حفاظت از اطلاعات مالی به میان نیامده است. در این مصوبه، قانون‌گذار به تولید محتوای فضای مجازی به صراحت توجه نموده است درحالی‌که مفهوم امنیت و ابعاد آن در این‌جا تشریح نشده است. از منظر حقوقی، امنیت سایبری در دو مفهوم مضیق و موسع به کار می‌رود. در مفهوم مضیق به معنای اتخاذ تدابیر فنی پیش‌گیرانه برای حفاظت و حراست از اطلاعات در بستر سامانه‌های رایانه‌ای و مخابراتی است (احسانی مؤید، ۱۳۸۹، ص۱۲). در این مفهوم، اقدامات غیرفنی جایگاهی نداشته و اشخاص موضوع مستقیم تدابیر امنیتی قرار نمی‌گیرند اما در مفهوم موسع، دو قسم از تدابیر واسطه‌ای و تدابیر مستقیم یا اصلی اعمال می‌شود. این تدابیر به تدابیر پیش‌گیرانه وضعی اعم از تدابیر نظارت انسانی یا فنی گفته می‌شود که برای تأمین امنیت دو موضوع زیر به کار می‌رود: نخست اطلاعات رایانه‌ای که از مرحله ورود یا تولید تا ذخیره و انتشار و مورد استفاده قرار گرفتن در معرض انواع رفتارهای مخرب و مختل‌کننده است که این رفتارها موجب نابودی یا افشای اطلاعات مالی در این فضا می‌شود و دوم، سیستم‌ها و شبکه‌های رایانه‌ای و مخابراتی که سیستم و شبکه نیز همچون اطلاعات آسیب‌پذیر بوده و از آن‌جا که مقوم

آن‌ها اطلاعات است، اقداماتی نظیر انتشار ویروس، اختلال در کارکرد و بازدهی، ممانعت از ترافیک و دسترسی به اطلاعات و...، امنیت آن‌ها را به شدت تهدید می‌کند، ازاین‌رو برای امنیت اطلاعات و سیستم، از اقدامات پیش‌گیرانه وضعی استفاده می‌شود. امنیت اطلاعات نیز به فرآیند حفاظت از اطلاعات در برابر کارهای غیر مجاز شامل دسترسی، استفاده، افشا، اختلال، تغییر، مطالعه، بازرسی و ضبط گفته می‌شود (حسن بیگی، ۱۳۸۴، ص۱۱). هرچند در مقرره پیش‌گفته، امنیت سایبری به‌گونه‌ای عام مورد استفاده قرار گرفته و اشاره‌ای به تعبیر اطلاعات مالی نشده اما امنیت اطلاعات نیز در گستره امنیت سایبری می‌گنجد و اطلاعات مالی نیز جزء مصادیق آن به شمار می‌آید. در ماده ۲ اساسنامه مرکز ملی فضای مجازی «به مقابله با تهدیدات فضای سایبر با استفاده از تدابیر فنی» پرداخته شده است. یکی از مهم‌ترین تهدیدات در حوزه سایبر، تهدیداتی است که علیه محرمانگی و اصالت اطلاعات مالی صورت می‌گیرد. قانون‌گذار در همین ماده به‌طور صریح خود به این امر اشاره کرده که برای از بین بردن تهدیدات مذکور از تدابیر فنی استفاده شود.

در مصوبه دیگر این شورا در خصوص تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه سال ۱۳۹۳ نیز در بند چهارم مقرره دوم به ایجاد شبکه‌ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتال پرداخته است. در این مقرره، قانون‌گذار تنها به امنیت شبکه توجه داشته و اشاره‌ای به امنیت اطلاعات نکرده است. امنیت شبکه به فرآیند ایمن‌سازی گفته می‌شود که طی آن یک شبکه با استفاده از استانداردهای امنیتی در مقابل انواع مختلف تهدیدات اعم از داخلی و خارجی امن می‌شود؛ به عبارت دیگر، امنیت شبکه ناظر به حفاظت از شبکه در مقابل حملات است که گاه این حملات منجر به تخریب کل شبکه و گاه منجر به دسترسی غیرمجاز به منابع و اطلاعات می‌شود. با این حال در امنیت شبکه، متخصصان بیش‌تر بر عملکرد صحیح سیستم کامپیوتری تمرکز دارند؛ درحالی‌که در امنیت اطلاعات، بیش‌تر، تأکید بر حفاظت از اطلاعات خصوصاً اطلاعات با ارزش اشخاص است تا در پرتوی این حفاظت بتوان از ضررهای هنگفتی که ممکن است در اثر رفتارهای مخرب به اشخاص وارد آید جلوگیری نمود. تدابیر پیشنهاد شده در این ماده، جهت خدمت‌رسانی امن به کاربران، همگی در قالب تدابیر پیش‌گیری فنی‌اند. در این مقرره از میان تدابیر فنی تنها

به رمزنگاری و امضای دیجیتال اشاره شده، درحالی‌که این دو راهکار بیش‌تر جهت تأمین امنیت خود اطلاعات و نه شبکه در معنی یاد شده به کار می‌روند؛ ازاین‌رو بهتر می‌بود مقنن به‌طور تمثیلی به این تدابیر می‌پرداخت تا لااقل بتواند امنیت شبکه را در قالب این اقدامات به‌طور کامل تأمین سازد. در مصوبه دیگر، این شورا تحت عنوان سیاست‌های حاکم بر برنامه‌های رایانه‌ای، در بند ۱۰ به حفظ حریم خصوصی و حمایت از حقوق مصرف‌کننده اشاره شده، اما تدابیر واسطه‌ای پیش‌بینی شده در این بند نیز تنها ناظر به حفظ حریم خصوصی است و اطلاعات مالی اشخاص حقوقی تحت شمول این مقرره قرار نمی‌گیرند. با این حال حمایت از حقوق مصرف‌کننده می‌تواند شامل حمایت از اطلاعات مالی مشتریان نیز شود که این مشتریان، هم می‌توانند اشخاص حقوقی و هم اشخاص حقیقی باشند. در مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه مصوب ۱۳۸۰ قانون‌گذار در بند ب ماده ۶ به استفاده از تدابیر فنی جهت صیانت از شبکه‌ها و اطلاعات تصریح کرده است. در این بند آمده: «سیستم بارو[۷] مناسب به منظور صیانت شبکه‌ها از تخریب، فریب و سرقت اطلاعات به‌کار می‌رود». در این مقرره، قانون‌گذار به امنیت اطلاعات به‌طور صریح پرداخته است. اطلاعات به کار رفته در این متن مطلق است و شامل اطلاعات مالی و غیر مالی می‌گردد. در این مقرره تنها به حفاظت از اطلاعات در برابر سرقت، تخریب و فریب اشاره شده درحالی‌که بهتر بود مقنن به حفاظت از اطلاعات در برابر تهدیدات به نحو مطلق اشاره می‌کرد. راهکار فنی ارائه شده در این ماده نیز تنها فایروال است و مقنن به سایر تدابیر فنی وقعی ننهاده است. در آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنتی نیز در مادهٔ ۸-۳-۵ استفاده از تدابیر فنی جهت تبادل اطلاعات در فضای سایبر را منوط به موافقت مرجع ثبت‌کننده اطلاعات نموده است. قانون‌گذار، استفاده از این تدابیر را تنها جهت انتقال و مبادله اطلاعات در سیستم پیشنهاده داده و مشخص نیست که آیا یک شخص حقیقی یا حقوقی می‌تواند اطلاعات خود را در سیستم با استفاده از الگوریتم رمزنگاری ذخیره سازد حتی اگر قصد تبادل آن اطلاعات را نداشته باشد؟ اطلاعات به‌کار رفته در این مقرره نیز مطلق است و شامل هرگونه اطلاعاتی اعم از مالی و غیر مالی می‌شود. در این بند آمده: «به‌کارگیری هرگونه رمز برای تبادل اطلاعات

مستلزم کسب موافقت مراجع مربوط و ثبت مشخصات، الگوریتم و کلید رمز مربوط و همچنین مشخصات متقاضی در دبیرخانه شورای عالی اطلاع‌رسانی یا مرجعی که معرفی می‌نماید، می‌باشد و در غیر این صورت ممنوع است». در سایر موارد، این آیین‌نامه نیز به حفظ و حراست از حریم خصوصی اطلاعات و ارتباطات اشاره شده که پیش‌تر، قانون‌گذار، تدابیر واسطه‌ای را پیش‌بینی نموده و تنها اطلاعات خصوصی را ملحوظ نظر قرار داده است. در بند ه ماده ۱ آیین‌نامه استنادپذیری ادله الکترونیک مصوب ۱۳۹۳ آمده: «برای حفاظت از داده‌ها باید زنجیره حفاظتی ایمن که امکان ردیابی داده‌ها را از مبداء تا مقصد فراهم می‌سازد، در نظر گرفت». در ماده ۳۸ این آیین‌نامه نیز به روش‌های توقیف داده‌ها پرداخته شده که اکثر راهکارهای ارائه شده در این مقرره تدابیر فنی‌اند. در این ماده، واژه داده‌ها به‌طور مطلق استعمال شده و می‌تواند هم ناظر به اطلاعاتی که در مورد حریم خصوصی است و هم اطلاعات مالی باشد؛ اما نکته قابل توجه این است که هرچند قانون‌گذار به استفاده از تدابیر فنی جهت حفاظت از مطلق اطلاعات پرداخته است، اما این ماده ناظر به اطلاعاتی است که جنبه اثباتی دارند و قرار است به‌عنوان ادله الکترونیک مورد استفاده قرار گیرند. به عبارت دیگر قانون‌گذار در این مقرره، به استنادپذیری این اطلاعات به جهت داشتن ارزش اثباتی توجه نموده است و اقدامش جنبه پسینی دارد و نه جنبه پیشینی. در قوانین موجود در حوزه فضای سایبر نیز به بحث حمایت از اطلاعات پرداخته شده است. برای نمونه در ماده ۴۰ قانون جرائم رایانه‌ای آمده: «در توقیف داده‌ها با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم به روش‌هایی از قبیل چاپ، کپی‌برداری، غیر قابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری عمل می‌شود». واژه «از قبیل» نشان می‌دهد تدابیر فنی ذکر شده در این ماده حصری نیستند و تمثیلی‌اند و می‌توان از سایر تدابیر فنی نیز در توقیف داده‌ها استفاده کرد. تدابیر فنی پیش‌بینی شده در این ماده جهت حفظ و حراست از داده‌هایی مورد استفاده قرار می‌گیرند که در کشف یا اثبات جرائم به کار می‌روند. ازاین‌رو، استفاده از این تدابیر یک اقدام تمهیداتی قضایی یا اقدام چاره‌ساز است و نه یک تدبیر پیش‌گیرانه غیر کیفری که اختصاصاً برای حفاظت از اطلاعات مالی پیش از ارتکاب جرم به‌کار رود. این تدابیر برای توقیف تمام داده‌ها صرف نظر از مالی یا غیرمالی بودن استفاده می‌شوند.

۵. سیاست جنایی قضایی ایران در جرائم سایبری

این نوع سیاست جنایی از میان رویه‌های مختلف قابل استنباط است که قوه قضائیه در رأس این نهادها با رویکرد پیشگیرانه اقدام به آن می‌نماید اما در کنار آن، نهادهای دیگر نیز می‌توانند با قوه قضائیه همکاری کنند. قانون اساسی در بند ۵ اصل ۱۵۶، اقدام مناسب برای پیشگیری از جرم را وظیفه قوه قضائیه دانسته است. با توجه به بند ۴ این اصل به نظر می‌رسد در این‌جا قانون‌گذار قانون اساسی به دنبال پیشگیری غیرکیفری بوده است (بیات و دیگران، ۱۳۸۷، ص۱۲۶). چنانچه در معناشناسی پیشگیری گفتیم، پیشگیری به معنای مانع ایجاد جرم شدن است و در سه مرحله پیش از وقوع جرم، وقوع جرم، و پس از آن جایگاه دارد. از یک دیدگاه می‌توان گفت، قوه قضائیه تنها پس از وقوع جرم وارد می‌شود و وظیفه پیشگیری از جرم به معنای خاص آن را بر عهده ندارد چرا که پیشگیری برعهده مقامات اجرایی است. پیشگیری در برنامه کوتاه‌مدت، وظیفه دستگاه‌های انتظامی است که این قوا از طریق گشت‌های پلیسی متفرق کردن افراد شرور و ... به پیشگیری می‌پردازند و یا پیشگیری در برنامه بلندمدت که همان پیشگیری اجتماعی است از وظایف آموزش و پرورش و سازمان‌های مربوط به مسائل ارتباط جمعی است. آن‌ها معتقدند، قوه قضائیه برای پیشگیری از وقوع جرم نقش مدیریتی دارد و سیاست‌گذاری می‌کند، اما اجرای سیاست‌ها بر عهده نهادهای اجرایی است (بیات و دیگران، ۱۳۸۷، صص۱۲۷–۱۲۸). البته از دیدگاه دیگر پیشگیری پس از وقوع جرم نیز وظیفه قوه قضائیه است؛ بدین معنا که کشف جرم، تعقیب مجرم و مجازات مرتکبین، پس از وقوع جرم، در راه پیشگیری از وقوع جرم و اصلاح مجرمین است. پس جنبه‌های اصلاح گرانه و درمانی مجازات همه می‌توانند در پیشگیری از جرم مؤثر باشند.

تدابیری که قوه قضائیه در این جایگاه از آن استفاده می‌کند، شامل مواردی چون اتخاذ تدابیر بازپرورانه، مشاوره‌درمانی، مددکاری، کاهش عناوین کیفری، زندان‌زدایی و اعمال مجازات‌های جایگزین زندان، بازگرداندن زندانی به دامان خانواده، بازپروری زندانیان، بسترسازی برای ایجاد اشتغال در زندان، آزادی مشروط از زندان، کیفرزدایی که جزء سیاست‌های استراتژی توسعه قضایی است، می‌باشد (نقره‌کار، ۱۳۸۱/۹/۲۱، بخش اول).

در مرحلـه پـیش از وقـوع جـرم نیـز قـوه قضـائیه بـا هـدف پیشـگیری از جـرم از راهکارهایی چون تأمین عدالت و رفاه اجتماعی، مبارزه با فقر و گرفتـاری، تـأمین امنیـت اجتماعی با استفاده از سـازوکارهای ارعـابی و بازدارنـده، حمایـت از خـانواده، بـا جلـب همکاری دستگاه‌های مختلف دولتی و غیردولتی ماننـد مـدارس، رسـانه‌هـا، سـازمان‌هـای غیردولتی، تشکل‌های مردمی، پلیس و خود مـردم، دامنـه آمـوزش را بـه همـه نهادهـای اجتماعی گسترش می‌دهد و اقدام به پیشگیری از جرم و مقابله با جـرم مـی‌نمایـد (چالـه چاله، ۱۳۸۷، ص۵۳).

در کنار قوه قضائیه مراکز بی‌شماری در عرصه فضـای سـایبر فعالیـت مـی‌کننـد کـه عملکرد این مراکز نیز بعدی پیشگیرانه دارد که از جمله آن‌هـا مـی‌تـوان بـه مرکـز مـاهر (مرکز مدیریت امداد و همـاهنگی عملیـات رخـداد) و مرکـز آپـا (مرکـز آگـاهی رسـانه، پشتیبانی و امداد رایانه‌ای) اشاره کرد. مرکـز مـاهر مرکـزی اسـت کـه زیـر نظـر سـازمان فناوری اطلاعات ایران جهت پاسخ‌گویی به رخـدادهای امنیـت کـامپیوتر در سـال ۱۳۸۵ شکل گرفت. این مرکز اهداف مختلفی را در حوزه سایبری بر عهده گرفت کـه از جملـه می‌توان به سیاست‌گذاری و توسعه و بهینـه‌سـازی روش‌هـای امنیتـی، بررسـی امکانـات بالقوه ایجاد امنیت در فضـای تبـادل اطلاعـات کشـور و کمـک بـه بالفعـل نمـودن ایـن امکانات، کمک به تشکیل گروه‌های ضربت جهت حفاظت از امنیـت اطلاعـات و شـبکه اشاره کرد. با تدقیق در اهـداف یـاد شـده بـه نظـر مـی‌رسـد هرچنـد بخـش عمـده‌ای از وظایف این مرکز تأمین امنیت اطلاعات است با این حال تـاکنون اقـدامی فنـی از سـوی مرکز جهت حفاظت از مطلق اطلاعات صورت نگرفته است. ایـن مرکـز بـیش‌تـر تـدابیر پیشگیرانه خود را در قالب تدابیر پیشگیرانه اجتماعی از جملـه هشـداردهی وآگـاه‌سـازی عمومی جهت حفاظت از اطلاعاتی که تنها مربوط به حریم خصوصـی شـهروندان اسـت و افراد آن، اطلاعات را در شبکه‌های اجتماعی خود بارگذاری نموده توجه داشـته اسـت و از توجـه بـه وصـف اطلاعـات مـالی و حتـی هشـدار در خصـوص حفاظـت از ایـن اطلاعات غافل مانده است.

مرکز آپا نیز مرکزی اسـت دانشـگاهی کـه بـا هـدف ارتقـاء آگـاهی و درک مسـائل مرتبط با امنیت اطلاعـات در میـان کـاربران و سـرویس‌دهنـدگان فضـای سـایبر از سـال ۱۳۸۶ فعالیت خود را زیر نظر دانشگاه امیر کبیر آغاز کرد. این مرکز سـعی دارد بـا ایجـاد

و استفاده از تکنولوژی مناسب امنیت اطلاعات را در مقابل حملات سایبری تأمین سازد. این مرکز نیز همانند ماهر به شهروندان هشدارهایی برای حفاظت از اطلاعاتشان در فضای سایبر می‌دهد اما این امر نافی اقدامات فنی این مرکز در حفاظت از مطلق اطلاعات نیست. دلیل این امر این است که این مرکز یک مرکز فنی مهندسی است و طبع اقداماتش با تدابیر فنی سازگارتر است.

پلیس فتا نیز که تنها نهاد پلیسی فعال در حوزه امنیت سایبری است اقدامات پیش‌گیرانه‌ای جهت حفاظت از اطلاعات مالی به عمل آورده است. این نهاد یک واحد تخصصی نیروی انتظامی است که در تاریخ ۳ بهمن ۱۳۸۹ به دستور فرمانده نیروی انتظامی ایران شروع به کار کرد. هدف اصلی تشکیل این پلیس، مقابله با جرائم سایبری و حفاظت از اطلاعات بر روی شبکه اینترنت است. پلیس در این نهاد به دو قسم تقسیم می‌شود: نخست پلیس ستادی و دوم پلیس عملیاتی. پلیس‌های ستادی بنا به دستور مقام قضایی به رصد سایت‌ها یا درگاه‌های الکترونیکی می‌پردازند و در صورت مجرمانه بودن محتوای این سایت‌ها یا صورت گرفتن یکی از جرائم مندرج در قانون در این فضا این امر را به مراجع قضایی اطلاع می‌دهند. این دسته از پلیس‌ها هر چند فی نفسه ماهیت کارشان پیشگیری از وقوع جرائم است و با گشت‌زنی در فضای سایبر تلاش می‌کنند شهروندان و یا مقامات قضایی را از تهدیدات موجود در این فضا آگاه کنند اما هیچ تدبیر فنی جهت حفاظت از اطلاعات مالی اتخاذ نکرده است و تنها به هشداردهی و آگاه‌سازی عمومی از فواید و مضرات فضای سایبر بسنده کرده که بیش‌تر این هشدارها در خصوص حفظ حریم خصوصی است. دسته دوم پلیس‌های فتا، پلیس‌های عملیاتی هستند که ماهیت عملکردشان اساساً پیگیری است و نه پیشگیری در معنای خاص. این گروه از پلیس‌ها بنا به دستور مقام قضایی در صورت تحقق یافتن جرم سعی در اعمال تدابیر واکنشی از جمله فیلتر نمودن سایت‌ها می‌کنند و اقداماتشان بیش‌تر واکنشی و در جهت پالایه محتوا است.

۶. سیاست جنایی مشارکتی ایران در جرائم سایبری

در این سیاست جنایی، برای پیشگیری از جرم و مبارزه با آن از اسباب و وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود که می‌توان برای اعمال آن، از طریق

مختلف مانند فرهنگ‌سازی، آموزش، مفهوم دینی امر به معروف و نهی از منکر بهره برد. باید بگوییم سیاست جنایی مشارکتی در میان دستورات اسلام نیز یافت می‌شود. بارزترین جلوه دستورات قرآن در این زمینه که از فروع دین اسلام نیز به شمار می‌رود، دستور امر به معروف و نهی از منکر است: «ولتکن منکم امه یدعون الی الخیر و یامرون بالمعروف و ینهون عن المنکر و اولئک هم المفلحون» (آل عمران، آیه ۱۰۴)، (رشادتی، ۱۳۸۷، ص۳۴۴).

امر به معروف و نهی از منکر به‌عنوان ابزاری برای نظارت عمومی در راه پیشگیری و بازداشتن مردم از گناه و جرم است. در واقع احکام امر به معروف و نهی از منکر با هدف پیشگیری از انحرافات اخلاقی، جرم و گناه در جامعه اسلامی تبیین شده است (چاله چاله، ۱۳۸۷، ص۵۴). به همین مناسبت در اصل هشتم قانون اساسی به این امر مهم اشاره شده است و امر به معروف و نهی از منکر، وظیفه‌ای همگانی و متقابل بر عهده مردم نسبت به یکدیگر ، دولت نسبت به مردم و مردم نسبت به دولت شناخته شده است.

یکی از طرق نظارت بر جرائم سایبری، توسط نهادهای مدنی و اشخاص و با مشارکت مردم که می‌تواند مصداقی از امر به معروف و نهی از منکر باشد و موجب پیشگیری از جرائم سایبری شود، مربوط به نظارت بر ورودی‌ها است که سعی می‌شود از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری شود. این نظارت اهمیت فراوانی در حفاظت از اطلاعات مالی دارد و حفاظت دقیقی از این اطلاعات به عمل می‌آورد به‌گونه‌ای که حتی بسیاری از سامانه‌های نظارتی اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به بخش‌هایی که در آن اطلاعات مالی ذخیره شده است را ثبت می‌کنند (اسدی، ۱۳۸۴، ص۱۵). کنترل ورودی‌ها کمک می‌کند از میزان اطلاعات مالی وارد شده، نوع و منشأ آن‌ها به ویژه در حالت‌هایی که به دلیل بالا بودن هزینه امکان به‌کارگیری کنترل‌های دو لایه و تکنیک‌های تهیه مجوز وجود ندارد، اطمینان حاصل نمود (یزدانی‌زنور، ۱۳۸۷، ص۱۷). راه‌های گوناگونی برای کنترل ورودی‌ها وجود دارد که ساده‌ترین آن استفاده از رمز عبور در رایانه است (عباسی، ۱۳۸۹، ص۲۲). بدیهی است که بالا بردن ضریب کنترل می‌تواند به مثابه مانعی در برابر مجرمان با انگیزه عمل کند و آن‌ها را در دستیابی به آماج جرم ناکام بگذارد. از دیگر

راهکارهایی که می‌تواند به‌عنوان کنترل ورودی عمل کند استفاده از شبکه‌های مجازی کاوشگر الکترونیک است. این کاوشگرها که از آن‌ها به پلیس مجازی تعبیر می‌شود وظیفه کنترل دسترسی به اطلاعات مالی را بر عهده دارند. علاوه بر نظارت ورودی نظارت بر خروجی نیز اهمیت شایانی دارد و مکمل کنترل ورودی است. در این نوع نظارت علاوه بر اینکه تمامی راه‌های خروج اطلاعات مدنظر قرار می‌گیرد، احتمال نشت اطلاعات مالی در فضای سایبر نیز توجه می‌شود. در این سیستم کنترلی تمام اطلاعات مالی که منشأ خود را ترک می‌کنند مورد بررسی و نظارت کامل قرار می‌گیرند. این نظارت به دو شکل هم‌زمان و غیر هم‌زمان صورت می‌گیرد. درحالت نخست (نظارت هم‌زمان)، ابزار الکترونیکی، مسئول یا متصدی مربوطه را از فعالیت غیرمجاز شخص در دسترسی به اطلاعات مالی در همان زمان آگاه می‌کند و به این ترتیب او می‌تواند اقدامات پیشگیرانه مقتضی را انجام دهد؛ اما در حالت دوم (نظارت غیرهم‌زمان)، بسته به میزان دقت ابزار نظارتی، صرفاً بخش‌های گزینش شده‌ای از فعالیت‌های این اشخاص ثبت می‌شود تا در فرصتی دیگر با بررسی آن‌ها موارد غیرمجاز دسترسی اشخاص به اطلاعات مالی مشخص گردد. در این حالت ابزارها و برنامه‌هایی بر روی سیستم شخص نصب می‌شود که کلیه فعالیت‌های شبکه‌ای آن حتی ضرباتی که بر روی صفحه کلیدش زده یا نقاطی که به وسیله موشواره (موس) بر روی آن‌ها کلیک کرده، ضبط می‌گردد (جلالی فراهانی، ۱۳۸۸، ص۲۵). در این کنترل، تمامی راهکارهای نظارتی در مورد خروج اطلاعات مالی مد نظر قرار می‌گیرد و تمامی اطلاعات مالی ذخیره شده دارای کدبندی مشخصی می‌شوند و بدین ترتیب از تمامیت آن‌ها حفاظت می‌شود. در ادامه به تبیین مهم‌ترین راهکار این تدبیر که استفاده از نرم‌افزار ضد پایش است می‌پردازیم.

نرم‌افزار ضد پایش، نرم‌افزاری است که برای محافظت از اطلاعات مالی در برابر ویروس‌ها به‌کار می‌رود و به نوعی همان آنتی ویروس است (حسن‌بیگی، ۱۳۸۴، ص۱۱). مهم‌ترین قسمت این برنامه موتور اسکن آن است. جزئیات عملکرد هر موتور متفاوت است ولی همه آن‌ها وظیفه شناسایی فایل‌های آلوده به ویروس را بر عهده دارند که اغلب در لابه‌لای اطلاعات مالی بارگذاری شده‌اند. در بیش‌تر موارد در صورتی که فایل آلوده به ویروس باشد ضد ویروس قادر به پاکسازی و از بین بردن آن

است. این نرم‌افزارها به دو دسته نرم‌افزار نظارت و نرم‌افزار اسکن تقسیم می‌شوند. نرم‌افزار نظارت صرفاً اقدام به تشخیص ویروس‌ها و بلاک آن‌ها می‌کند ولی نرم‌افزار اسکن ویروس‌های کشف شده را نه تنها از فایل اطلاعات مالی بلکه از کل سیستم پاک می‌کند.

نتیجه‌گیری

سایبر دربردارنده محیط‌هایی است که اساس فعالیت آن‌ها بر مبنای پردازش و طبق سامانه صفر و یک کار می‌کنند که در زبان عموم مردم به‌غلط اینترنت نامیده می‌شود و فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. بر این اساس، جرائم سایبری جرائمی است که در محیطی غیرفیزیکی علیه فناوری اطلاعات با حالات شبیه‌سازی و مجازی‌سازی ارتکاب می‌یابد. تفاوت جرائم سایبری با جرائم سنتی را می‌توان در امکان گمنامی و ناشناخته بودن، فراهم بودن مقتضیات جرم در هر زمان و مکان و فقدان موانع، آسانی و سرعت ارتکاب جرائم، فقدان ابزارهای نظارتی و حاکمیتی، عدم پای‌بندی به محدودیت‌های زمانی و مکانی و فرامرزی) بودن دانست.

دیگر مفهوم مهم در این پژوهش سیاست جنایی است که در حقوق کیفری نوین به مفهوم «مجموعه‌ای از جهت‌گیری‌ها و اقدامات متفاوت دولت، نهادهای غیردولتی و مردم در مهار بزهکاری است که علاوه بر مبارزه با جرم و توجه به مجازات‌ها و اصلاح مجرمین، مرحله پیشگیری و حتی ماقبل آن را نیز دربرمی‌گیرد» که طبق این تعریف اولاً، سیاست جنایی، علاوه بر تبیین جرم و مجازات، محدوده پیشگیری، درمان، اصلاح و حتی ماقبل پیشگیری از جرم را نیز مدنظر قرار می‌دهد؛ دیگر آنکه سیاست جنایی تنها محدود به دولت نیست و سایر نهادهای غیر دولتی و مردم را نیز در بر می‌گیرد؛ علاوه بر آن، سیاست جنایی مجموعه‌ای گسترده از اقدامات متفاوت است نه یک اقدام و یک تدبیر، و ویژگی آخر آنکه سیاست جنایی به انحراف نیز توجه دارد.

بر اساس دسته‌بندی‌های کلی سیاست جنایی بر سه قسم است: ۱. سیاست جنایی تقنینی؛ ۲. سیاست جنایی مشارکتی؛ ۳. سیاست جنایی قضایی (محمدنژاد، ۱۳۸۴، ص۳۷).

سیاست جنایی تقنینی، وظیفه قانون‌گذاری در یک کشور است که در کشور ما بر اساس قانون اساسی بر عهده مجلس شورای اسلامی و در موارد خاص بر عهده

نهادهای دیگر گذاشته شده است. در خصوص جرائم سایبری، قانون‌گذار در قوانین و مقررات مربوط، گاه به‌طور ضمنی و گاه به‌طور صریح به استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر پرداخته است که یکی از مهم‌ترین موارد آن، مصوبات شورای عالی فضای مجازی است. در مصوبه این شورا با موضوع توسعه فضای مجازی سالم، مفید و امن به تعریف فضای مجازی ایمن پرداخته شده است که فضای ایمن به لحاظ محتوایی مدنظر بوده یعنی فضایی که محتوای آن در چارچوب مبانی اسلامی باشد. همچنین در مصوبات دیگر این شورا، سیاست‌های سامان‌دهی خدمات پیامکی ارزش افزوده و پیامک انبوه در شبکه‌های ارتباطی، تولید محتوای فضای مجازی، امنیت سایبری، تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه، ایجاد شبکه با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتال جهت امنیت شبکه و ایمن‌سازی، امنیت اطلاعات و تدابیر فنی جهت صیانت از شبکه‌ها و اطلاعات و به حفاظت از اطلاعات در برابر سرقت، تخریب و فریب، سیاست‌های حاکم بر برنامه‌های رایانه‌ای، حفظ حریم خصوصی اطلاعات و ارتباطات و حمایت از حقوق مصرف‌کننده مورد تأکید قرار گرفته است.

سیاست جنایی مشارکتی، اقدامات در مرحله کشف جرم، تعقیب دادرسی و اجرای حکم را دربرمی‌گیرد که با همکاری وسیع جامعه مدنی و نیروهای دولتی مانند پلیس، سازمان زندان‌ها، سازمان محیط زیست، جنگل‌بانی و ... با دستگاه قضایی انجام می‌شود. در این سیاست جنایی، برای پیشگیری از جرم و مبارزه با آن از اسباب و وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود که می‌توان برای اعمال آن، از طریق مختلف مانند فرهنگ‌سازی، آموزش، مفهوم دینی امر به معروف و نهی از منکر بهره برد. یکی از طرق نظارت بر جرائم سایبری، توسط نهادهای مدنی و اشخاص و با مشارکت مردم که می‌تواند مصداقی از امر به معروف و نهی از منکر باشد و موجب پیشگیری از جرائم سایبری شود، مربوط به نظارت بر ورودی‌ها است که سعی می‌شود از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری شود. این نظارت اهمیت فراوانی در حفاظت از اطلاعات مالی دارد و حفاظت دقیقی از این اطلاعات به عمل می‌آورد به‌گونه‌ای که حتی بسیاری از سامانه‌های نظارتی اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به بخش‌هایی که در آن اطلاعات مالی ذخیره شده است

را ثبت می‌کنند. راه‌های گوناگونی برای کنترل ورودی‌ها وجود دارد که ساده‌ترین آن استفاده از رمز عبور در رایانه است. علاوه بر نظارت ورودی نظارت بر خروجی نیز اهمیت شایانی دارد و مکمل کنترل ورودی است. در این نوع نظارت علاوه بر اینکه تمامی راه‌های خروج اطلاعات مدنظر قرار می‌گیرد، احتمال نشت اطلاعات مالی در فضای سایبر نیز توجه می‌شود. در این سیستم کنترلی تمام اطلاعات مالی که منشأ خود را ترک می‌کنند به دو شکل هم‌زمان و غیر هم‌زمان مورد بررسی و نظارت کامل قرار می‌گیرند. در این نظارت‌ها، تمامی راهکارهای نظارتی در مورد خروج اطلاعات مالی مد نظر قرار می‌گیرد و تمامی اطلاعات مالی ذخیره شده دارای کدبندی مشخصی می‌شوند و بدین ترتیب از تمامیت آن‌ها حفاظت می‌شود که مهم‌ترین راهکار این تدبیر، استفاده از نرم‌افزار ضد پایش است که برای محافظت از اطلاعات مالی در برابر ویروس‌ها به‌کار می‌رود.

دیگر نوع سیاست جنایی، سیاست جنایی قضایی است. این نوع از سیاست جنایی در تصمیم‌ها و رویه‌های قضایی دادسراها و دادگاه‌ها منعکس می‌شود که ابزارهایی چون حضور هیأت منصفه، مشاوران، دادرسان مردمی می‌تواند بر آن تأثیر گذارد. این نوع سیاست جنایی از میان رویه‌های مختلف قابل استنباط است که قوه قضائیه در رأس این نهادها با رویکرد پیشگیرانه اقدام به آن می‌نماید اما در کنار آن، نهادهای دیگر نیز می‌توانند با قوه قضائیه همکاری کنند. علاوه بر رویکرد پیشگیرانه قوه قضائیه در سه مرحله پیش از وقوع جرم، وقوع جرم، و پس از آنکه در اصل ۱۵۶ قانون اساسی بر آن تأکید شده است، با اتخاذ پیشگیرانه چون تأمین عدالت و رفاه اجتماعی، مبارزه با فقر و گرفتاری، تأمین امنیت اجتماعی با استفاده از سازوکارهای ارعابی و بازدارنده، حمایت از خانواده، با جلب همکاری دستگاه‌های مختلف دولتی و غیردولتی مانند مدارس، رسانه‌ها، سازمان‌های غیردولتی، تشکل‌های مردمی، پلیس و خود مردم و یا تدابیر بازپرورانه، مشاوره‌درمانی، مددکاری، کاهش عناوین کیفری، زندان‌زدایی و اعمال مجازات‌های جایگزین زندان، بازگرداندن زندانی به دامان خانواده، بازپروری زندانیان، بسترسازی برای ایجاد اشتغال در زندان، آزادی مشروط از زندان، کیفرزدایی که جزء سیاست‌های استراتژی توسعه قضایی است محقق می‌شود. مراکز بی‌شماری که در عرصه فضای سایبر فعالیت می‌کنند و در عملکرد پیشگیرانه نقش مهمی دارند که

می‌توان به مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخداد) و مرکز آپا (مرکز آگاهی رسانه، پشتیبانی و امداد رایانه‌ای) و پلیس فتا اشاره کرد.

یادداشت‌ها

1. William Ford Gibson
2. Von Liszt
3. Donnedieu De Vabre
4. Mireille Delmas Marty
5. Opportunity
6. acting out
7. Firewall

کتابنامه

احسانی مؤید، فرزانه، (۱۳۸۹)، «ورود جاسوس‌ها ممنوع»، *ماهنامه اطلاعات*، شماره ۱۲، سال یازدهم.

اسدی، مریم، (۱۳۸۴)، «فناوری‌های امنیت اطلاعات: با یک دیدگاه طبقه‌بندی»، *علوم اطلاع‌رسانی*، دوره ۲۰، شماره ۳ و ۴، بهار و تابستان ۱۳۸۴، صص ۱۶-۱.

باصری، علی اکبر، (۱۳۸۷)، *سیاست جنایی قضایی کودکان و نوجوانان (در حقوق داخلی و اسناد بین‌المللی)*، تهران، خرسندی.

بیات، بهرام، و شرافتی، جعفر، و عبدی، نرگس، (۱۳۸۷)، *پیشگیری از جرم با تکیه بر رویکرد اجتماع محور (پیشگیری از جرم)*، تهران، معاونت اجتماعی ناجا (اداره کل مطالعات اجتماعی).

پرویزی، رضا، (۱۳۸۴)، *پی‌جویی جرائم رایانه‌ای*، چاپ اول، تهران، جهان جام جم.

جاویدنیا، جواد، (۱۳۸۸)، *جرائم تجارت الکترونیکی*، چاپ دوم، تهران، انتشارات خرسندی.

جلالی فراهانی، امیرحسین، (۱۳۸۴)، «پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر»، *فصلنامه فقه و حقوق*، سال دوم، پاییز ۱۳۸۴.

جلالی فراهانی، امیرحسین، (۱۳۸۹)، *درآمدی بر آیین دادرسی کیفری جرائم سایبری*، چاپ اول، تهران، خرسندی.

جلالی‌فراهانی، امیرحسین، (۱۳۸۸)، «نهادسازی برای پیشگیری از جرائم سایبری با نگاهی به قانون جرائم رایانه‌ای، در رویکرد چند نهادی به پیشگیری از جرم»، *مجموعه مقاله‌های ملی پیشگیری از وقوع جرم*، چاپ اول، تهران، معاونت آموزش و پیشگیری از ناجا.

جوان‌جعفری، عبدالرضا، (۱۳۸۹)، «جرائم سایبر و رویکرد افتراقی حقوق کیفری»، *مجله دانش و توسعه*، سال هجدهم، شماره۳۴، اسفند ۸۹.

چاله چاله، فرشید، (۱۳۸۷)، «اصول و مبانی پیشگیری از جرم»، *دادرسی*، سال دوازدهم، شماره۶۷، فروردین و اردیبهشت۱۳۸۷.

حسن‌بیگی، ابراهیم، (۱۳۸۴)، *حقوق و امنیت در فضای سایبر*، چاپ اول، تهران، مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

حسینی، سید محمد، (۱۳۸۳)، *سیاست جنایی (در اسلام و در جمهوری اسلامی ایران)*، تهران، سازمان مطالعه وتدوین کتب علوم انسانی دانشگاه‌ها (سمت)- دانشگاه تهران.

دانایی، نسرین، (۱۳۸۸)، *رسانه‌شناسی*، چاپ اول، تهران، انتشارات مبنای خرد.

دیندار فرکوش، فیروز و صدری نیا، حسین، (۱۳۸۸)، *روابط عمومی و رسانه*، چاپ سوم، تهران، نشر سایه روشن.

رشادتی، جعفر، (۱۳۸۷)، *پیشگیری از جرم در قرآن کریم*، تهران، دفتر تحقیقات کاربردی پلیس پیشگیری ناجا.

سوتهیل، کیت و پیلو، مویرا، و تیلور، کلر، (۱۳۸۳)، *شناخت جرم‌شناسی*، ترجمه سید روح الله صدیق، تهران، دادگستر.

عالی‌پور، حسن، (۱۳۸۳)، «جرائم مرتبط با محتوا: محتوای سیاه فناوری اطلاعات»، *مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات*، تهران، خردادماه.

عاملی، سید سعیدرضا، (۱۳۹۰)، *رویکرد قضایی به آسیب‌ها، جرائم و قوانین و سیاست‌های فضای مجازی*، چاپ اول، تهران، انتشارات امیرکبیر.

عباسی، مراد، (۱۳۸۹)، «حریم خصوصی، فضای مجازی و چالش‌های پیشگیرانه فراروی ناجا»، *فصلنامه علمی ـ ترویجی مطالعات پیشگیری از جرم*، سال پنجم، شماره هفدهم، صص۲۷-۵.

فضلی، مهدی، (۱۳۸۸)، *مسئولیت کیفری در فضای سایبر*، چاپ اول، تهران، انتشارات خرسندی.

کی نیا، مهدی، (۱۳۷۳)، *مبانی جرم‌شناسی*، تهران، دانشگاه تهران.

لازرژ، کریستین، (۱۳۸۱)، *درآمدی بر سیاست جنایی*، ترجمه علی حسین نجفی ابرندآبادی، تهران، میزان.

محمد نژاد، پرویز، (۱۳۸۴)، «بررسی و شناخت سیاست جنایی و اثر آن بر نظم و امنیت اجتماعی»، *اصلاح و تربیت*، شماره ۳۹ (۱۲۴پیاپی)، خرداد ماه.

محمدنژاد، علی، (۱۳۸۵)، «خشونت رسانه‌ای»، *جام جم*، ۱۳۸۵/۱۱/۱۶.

نجفی ابرندآبادی، علی حسین، (۱۳۷۸)، *تقریرات درس سیاست جنایی دوره دکترای حقوق کیفری و جرم‌شناسی*، تهران، دانشکده حقوق دانشگاه شهید بهشتی.

نقره کار، صالح،(۱۳۸۱)، «رسالت پیشگیری از وقوع جرم، وظیفه مدعی‌العموم کشور»، *حمایت*، ۱۳۸۱/۹/۲۱.

نوربها، رضا، (۱۳۸۴)، «سیاست جنایی سرگردان»، *تحقیقات حقوقی*، شماره ۲۵ و ۲۶، بهار و تابستان ۱۳۷۸، صص ۱۰۳– ۱۲۸.

ویلیامز، ماتیو، (۱۳۹۱)، *بزهکاری مجازی: بزه، انحراف و مقررات‌گذاری برخط*، ترجمه امیرحسین فراهانی و محبوبه منفرد، چاپ اول، تهران، میزان.

یزدانی زنور، هرمز، (۱۳۸۷)، «حریم خصوصی در فضای سایبر»، *مجله حقوق فناوری اطلاعات و ارتباطات*، شماره۲۷.