حقوق و تکالیف پلیس در نظارت بر فضای سایبر در ایران و آمریکا

سیدمحمد هاشمی علوی[1]

تاریخ ارسال: ۹۷/۶/۶ تاریخ پذیرش: ۹۹/۱۲/۱۲
از صفحهٔ ۱۱۳ تا ۱۵۷

چکیده

زمینه و هدف: با عنایت به اصل آزادی و استثنایی بودن محدودیت قانونی، لازم است میزان دخالت مراجع رسمی در حریم خصوصی و میزان مداخله در فضاهای عمومی در قلمروهای حقیقی یا مجازی، به وضوح روشن باشد.

روش تحقیق: مطالعه‌ی حاضر ازنظر هدف، کاربردی است و سعی شده با روش‌های توصیفی از نوع اسنادی و از طریق مراجعه به آثار مکتوب اعم از کتب، مقاله‌های علمی و سایت‌های مرتبط، تکالیف و اختیارات پلیس در نظارت بر فضای سایبر را بررسی کند.

یافته‌ها: یافته های پژوهش نشان از ضعف و خلأ قانونی در حوزه فضای سایبر در ایران دارد. استفاده از تجربیات آمریکا در این حوزه ازجمله: امکان نصب برنامه‌های پردازش داده بر روی سرورها، ایجاد امکان صدور احضاریه و قرار تفتیش از سوی پلیس برای بررسی داده‌ها و سامانه‌های الکترونیک، تعیین استثنائات قانونی نظارت بر فضای سایبری و ایجاد چارچوب قانونی برای نظارت بر فضای سایبر از سوی پلیس در مرحله‌ی پیشگیری، می‌تواند راهگشا باشد.

نتیجه‌گیری: در ایران باوجود تلاش شبانه‌روزی مأموران نیروی انتظامی در نهادهای مختلف به‌ویژه پلیس فتا خلأهای قانونی گسترده‌ای وجود دارد که از اثرگذاری اقدامات صورت گرفته می‌کاهد ازاین‌رو در این نوشتار سعی بر آن بوده که شناخت اقدامات صورت گرفته در دو کشور آمریکا و فرانسه در حوزه‌ی جرم انگاری، پیشگیری، کشف و تعقیب جرایم بتواند در ارائه‌ی راهکارهایی برای اثرگذاری هرچه بیشتر اقدامات صورت گرفته از سوی پلیس فتای ایران راهگشا باشد.

کلیدواژه‌ها: تکالیف، اختیارات، فضای سایبر، پلیس، نظارت.

۱- کارشناس ارشد حقوقژوهشگر مرکز تحقیقات کربردی و آموزش معاونت حقوقی و امور مجلس ناجا
smh.alavi92@gmail.com

مقدمه

فضای سایبری مجموعه‌ای از ارتباطات میان اشخاص است که از طریق وسایل ارتباطی، مانند رایانه و ... انجام می‌شود و مسافت جغرافیای در آن نقشی ندارد. با توسعه‌ی رسانه‌های الکترونیکی، در کنار جرایم سنتی، فرصت‌های جدیدی نیز برای بزهکاری فراهم‌شده است. اموری از قبیل حمله‌ی ویروس‌ها، ورود غیرمجاز به وب‌سایت‌ها و هک آن‌ها، سرقت و سوءاستفاده از داده‌ها و ایراد خسارت به رایانه‌ها، در زمره‌ی رفتارهای بزهکارانه‌ای تلقی می‌شوند که قابلیت ارتکاب در محیط خارج از رایانه را ندارند. به همین ترتیب، پیشرفت فناوری رایانه، شرایط و بسترهای مناسبی برای سرقت اطلاعات، تکثیر نرم‌افزارهای غیرمجاز، سوءاستفاده از بازار سهام، تجاوز به حقوق مالکیت معنوی و مهم‌تر از همه، تهاجم فرهنگی را فراهم کرده است. با توجه به گسترش روزافزون ارتباطات در فضای مجازی و درنتیجه‌ی آن سرایت برخی اعمال مجرمانه از جهان واقعی به آن، اهمیت نظارت بر دنیای سایبر امروزه بیش از هر زمان دیگری خود را نشان می‌دهد. در این زمینه تبیین وظایف و اختیارات پلیس در نظارت بر فضای مجازی در ایران و بررسی تطبیقی آن با کشور آمریکا می‌تواند به روشن شدن هر چه بیشتر این مسئله کمک کند، به‌ویژه اینکه نظام حقوقی این در این زمینه نوپاست و جای بحث و مداقه‌ی فراوانی در این زمینه وجود دارد.

جرایم سایبری را می‌توان در چهار دسته یا طبقه‌ی کلی جای داد. این دسته‌بندی تا حدی ماهیت جرایم مزبور را نیز روشن می‌کند. ۱- جرایم کلاسیک (سنتی) با توصیف سایبری: جرایمی در این دسته قرار می‌گیرند که جرایم سنتی تلقی می‌شوند، اما در حال حاضر، به علت پیشرفت فناوری، با وسایل نوینی انجام می‌شوند. ازجمله‌ی این جرایم می‌توان به جعل و کلاه‌برداری سایبری اشاره کرد. در حال حاضر، جایی که شبکه‌های رایانه‌ای، ابزار ارتکاب جرایم سنتی نظیر کلاه‌برداری و جعل از طریق اینترنت هستند، قاضی مجبور است به علت فقدان یک قانون مدون و مشخص در این رابطه، از قوانین سنتی مانند قوانین جزایی و «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای» که آیین‌نامه‌ی آن در سال ۱۳۷۹ تصویب شد و همچنین مجازات‌هایی که در «قانون تجارت الکترونیکی» مصوب ۱۳۸۲

وجـود دارد، استفاده کند.

۲- جرایم علیه محرمانه‌گی داده‌ها و سیستم‌های رایانه‌ای و مـخابراتی: هـر نمـادی از موضوع‌ها، مفاهیم یا دستورالعمل‌ها ازجمله متن، صوت یا تصویر را که برای برقـراری ارتباط مـیان سـیستم‌های رایـانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای بـه کار گرفته‌شده و به‌وسیله‌ی سـیستم رایانه‌ای ایجاد می‌شـود، «داده محتـوا» گوینـد. ازجمله جرایمی که در این دسته جای می‌گیرنـد، مـــی‌تـوان بـــه شـــنود غیرمجـاز داده‌های مخابراتی در یک ارتباط خصوصی یا داده‌های سـری اشـاره کـرد کـه واجـد ارزش برای امـنیت داخـلی و خارجی کشور می‌باشند.

۳- جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مـــخابراتی: تـــغییر، ایـجاد، محو یا متوقف کردن داده‌های رایانه‌ای و مخـابراتی بـه‌قصـد تقلـب، غیرقابـل استفاده کـردن، تـخریب یا اختلال در داده‌ها یا امـواج الکترومغناطیسـی، ممانعـت از دستیابی اشخاص مجاز به داده‌ها بـا تـغییر رمز ورود یا رمزنگـاری ازجملـه جرایمـی هستند که در این دسته قرار می‌گیرند.

۴- جرایم مرتبط بـا مـحتوا: این دسته، جرایمی را تحت شمول خود قرار می‌دهد که در آن‌ها، رایانه به‌عنوان ابـزار و وسیله توسط مجرم برای ارتکاب جرم به کار می‌رود و صرفاً فناوری اطلاعات، زمینه‌ی ارتـکاب آن‌ها را فـراهم می‌کند. بـرای مثـال، انتشـار محتویات مستهجن، تبلیغ یا تحریک یا تشویق به انحرافات جنسـی یـا خودکشـی از طریق سـیستم رایـانه‌ای یا مخابراتی، در این دسته قرار می‌گیرند.

امروزه در نقاط مختلف دنیا، اکثـر صـــنایع و شـــرکت‌هـای تولیـدی و خـدماتی، در معرض تهدید و زوال جدی قـرار دارنـــد. درصـــد زیـــادی از ایـن شـرکت‌هـا، انـواع مختلفی از مزاحمت‌ها یـا اســـتفاده‌ی غیرمجـاز از سیسـتم‌هـای رایانـه‌ای را تجربـه کرده‌اند. در حال حاضر، این مزاحمت‌ها بیشتر به سیستم‌های بـانکی و صـنایع مـالی معطوف شده است. نـکته‌ی قابل‌توجه ایـنکه جـرایم سـایبری، عمدتاً توسط نیروهای سازمان‌یافته و طراحی و نـقشه‌ی قـبلی و نیز توسط اشخاص رقیب یا اخراج شـده از سازمان‌های مزبور انجام می‌شود. بـررسی‌های انجام‌شده در سـال‌هـای اخیـر، مبـین افزایش چـشمگیر میزان بزهکاری و گرایش‌های مـجرمانه در فـضای مجـازی اسـت.

بر اساس این بررسی‌ها، تهدیدات ناشی از جرایم سایبری به شکل مهارناپذیری رو به افزایش بوده و زیان‌های مالی فراوانی نیز بر بخش‌های مختلف وارد آورده است. ازآنجاکه در سال‌های آتی، شاهد رشد تصاعدی در کاربرد فناوری اطلاعات، خصوصاً استفاده از اینترنت خواهیم بود، مسلماً چنین تمایل و گرایش خیره‌کننده‌ای، مقارن با افزایش میزان جرایم سایبری است.

پلیس جمهوری اسلامی ایران تلاش می‌کند با بهره‌گیری از آخرین دستاوردهای فناوری اطلاعات و ارتباطات سیستم‌های پیشرفته‌ی انتظامی-امنیتی کشور، امنیت اجتماعی را بهبود بخشیده و محیطی امن توأم با آسایش عمومی برای کلیه‌ی شهروندان، در پرتو ارزش‌های اسلامی فراهم کند.

معاونت آگاهی نیروی انتظامی جمهوری اسلامی ایران، اواخر سال ۱۳۷۸، به روش‌های گوناگون شروع به جمع‌آوری اطلاعاتی پیرامون جرایم سایبری کرد و در همین راستا، تحقیقی تحت عنوان «شناخت جرایم سایبری» توسط جهاد دانشگاهی دانشگاه علم و صنعت صورت گرفت. همچنین با بهره‌گیری ازنظریات کارشناسان و متخصصان شورای عالی انفورماتیک و تشکیل جلسات متعدد با صاحب‌نظران حقوقی و انفورماتیکی، به این نتیجه دست‌یافت که تشکیل واحدهای مبارزه با جرایم سایبری ضروری است.

تلاش‌های انجام‌شده سبب تصویب و ابلاغ تشکیل اداره‌ی کل مبارزه با جرایم رایانه‌ای در زیرمجموعه‌ی معاونت آگاهی و همچنین تشکیل دایره‌ی مبارزه با جرایم رایانه‌ای در اداره‌ی آگاهی تهران بزرگ شد. بدین ترتیب، پلیس متخصص برای پیگیری پرونده‌های جرایم رایانه‌ای، از سال ۱۳۸۱ فعالیت خود را باقوت و اقتدار، رسماً آغاز کرد. در سال ۱۳۸۹ یعنی یک سال پس از تصویب قانون جرایم رایانه‌ای و الحاق آن به بخش تعزیرات قانون مجازات اسلامی، پلیس فتا رسماً آغاز به کار کرد و عهده‌دار نظارت بر فضای مجازی شد.

در ادامه مطالب پیشین لازم است اشاره شود درزمینه‌ی نظارت بر فضای سایبر در ایران دو قانون اهمیت بیشتری دارند: یکی قانون جرایم رایانه مصوب ۱۳۸۸ و دیگری قانون آیین دادرسی کیفری بخش دهم آیین دادرسی جرایم رایانه‌ای مصوب

.۱۳۹۳

در آمریکا ابتدا قانون نظارت الکترونیکی بر خارجیان در سال ۱۹۷۸ تصویب شد که با احراز شرایطی در مورد یکی با حکم رئیس‌جمهور و دیگری با حکم اجرایی قوانین فدرال اجازه نظارت بر اطلاعات الکترونیکی غیر آمریکاییان را می‌داد.

قانون حریم خصوصی ارتباطات الکترونیک مصوب ۱۹۸۶ که ابتدا منحصر به شنود تلفن‌ها بود، در ادامه شامل نظارت بر انتقال الکترونیکی داده‌ها توسط کامپیوتر نیز شد. تفاوت این قانون با قانون پیشین شمول آن بر آمریکاییان و همین‌طور شمول آن بر ایمیل بود. در سال ۱۹۹۴ قانون همکاری ارتباطاتی برای اجرای قانون The Communications Assistance for Law Enforcement Act تصویب شد که ارائه‌دهندگان خدمات الکترونیکی ISP را الزام می‌کرد به مأمورین مجاز دولتی اجازه دسترسی به شبکه ارتباطی به‌منظور نظارت الکترونیکی را بدهند. قانون وطن‌پرستی مصوب ۲۰۰۱ اجازه دسترسی مراجع قانونی بر ایمیل صوتی و سایر داده‌های ذخیره‌شده الکترونیکی را آسان‌تر کرد. همچنین اصلاحات انجام‌شده در سال در ۲۰۰۵ قانون همکاری ارتباطاتی برای اجرای قانون، ازاین‌جهت مهم است که: نظارت بر صدا بر روی پروتکل اینترنت ("Voice over IP" (VoIP را قانونی کرد. این تحقیق به دنبال این است که با توجه به قوانین فوق‌الذکر و سایر قوانین، تکالیف و اختیارات پلیس در نظارت بر فضای سایبر را در این دو کشور بررسی کند.

تعریف فضای سایبر

در تعریف سایبر و فضای سایبری گفته‌شده: «واژه سایبر ازنظر لغوی به معنای مجازی و غیرملموس و مترادف لغت انگلیسی «Cybernetes» معادل مفهوم سکاندار یا راهنما است. سایبر از لغت یونانی 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؛ به گونه‌ای که مرتبط با فضای رایانه یا برخط باشد. به‌عبارت‌دیگر، سایبر به مطالعه مکانیزم‌های مورداستفاده در کنترل و تنظیم سیستم‌های پیچیده اعم از انسان یا ماشین اطلاق می‌شود. سایبر در فارسی به مجاز و مجازی ترجمه‌شده 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؛ اما سایبر در اصطلاح به همه محیط‌هایی گفته می‌شود که اساس فعالیت آن‌ها بر مبنای پردازش و طبق سامانه صفر و یک کار می‌کنند»[1]. در یک تعریف دیگر فضای سایبر در معنایی مشابه اینترنت به کار گرفته‌شده است؛ «یک نظام الکترونیکی که به استفاده‌کنندگان کامپیوتر در سراسر جهان اجازه می‌دهد با یکدیگر ارتباط برقرار کنند یا به‌منظوری به اطلاعات دسترسی داشته باشند»[2].

بااین‌همه پلیس بر فضای سایبری نظارت می‌کند تا پیشگیری از جرم انجام دهد یا جرم انجام‌شده را کشف و درباره‌ی آن تحقیق کند. درزمینه‌ی جرم سایبری تعاریف متفاوتی ارائه‌شده است. «یک تعریف عمومی، جرم سایبری را به‌عنوان هرگونه فعالیتی که در آن رایانه‌ها یا شبکه‌ها، ابزار، هدف یا مکانی برای فعالیت تبهکاری هستند، توصیف می‌کند»[3]. در تعریفی جزیی‌تر این جرایم به «فعالیت‌های به‌واسطه‌ی رایانه که هم غیرقانونی و نامشروع هستند با بخش‌های خاص که می‌توانند از میان شبکه‌های الکترونیک جهانی هدایت شوند»[4] تعریف‌شده است.

نظارت بر فضای سایبر

در تعریف لغوی نظارت گفته می‌شود که «نظارت» از ماده «نظر» است و مرحوم «دهخدا» در کتاب لغت‌نامه ذیل واژه مذکور، آن را به نگریستن در چیزی با تأمل، چشم انداختن، حکومت کردن بین مردم و فیصله دادن دعاوی ایشان، یاری‌دادن و مدد کردن و کمک کردن و نیز به معنای چشم، بصر، دیده، فکر، اندیشه، تفکر، رویه، دقت، تأمّل، تدبّر، خیال، وهم و اعتراض آورده است. او «ناظر» را به معنای نظر کننده، نگرنده، نگاه‌کننده، بیننده، شاهد و کنایه از جاسوسی، دیده‌بان و نگاهبان

---

۱ وطنی، امیر؛ اسدی، حمید، سیاست جنایی جمهوری اسلامی ایران در جرایم سایبری با تأکید بر ویژگی‌های خاص این جرایم، پژوهشنامه حقوق اسلامی، سال هفدهم، شماره اول (پیاپی ۴۳)، بهار و تابستان ۱۳۹۵، ص ۱۰۱

2 https://dictionary.cambridge.org/dictionary/english/cyberspace

۳ صبح خیز، رضا، چالش‌های حقوقی جرایم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران، فصلنامه‌ی پژوهش‌های اطلاعاتی و جنایی، سال دهم، شماره‌ی سوم، پاییز ۱۳۹۴، ص ۱۲۲

۴ مارکو، گرکی، ترجمه‌ی اکبری، مرتضی، جرایم سایبری: راهنمایی برای کشورهای درحال‌توسعه، تهران، پلیس امنیت فضای تولید و تبادل اطلاعات (فتا)، چاپ اول، ۱۳۸۹، ص ۳۲

مطرح نموده و درنهایت «نظارت» را به معنـای نظـر کـردن و نگریسـتن بـه چیـزی، مراقبت و در تحت نظر و دیده‌بانی داشتن کاری، نگرانی دیده‌بانی بـه‌سـوی چیـزی و مباشرت معنا کرده است.[1]

ازآنجاکه واژه نظارت در یک‌رشته علمـی و در یـک حیطـه و موضـوع کـاربرد نـدارد، ازاین‌رو نمی‌توان تعریف اصطلاحی اجتماعی و واحدی از نظارت ارائـه کـرد و در هـر علم، نظارت معنا و کارکرد خاص خود را خواهد یافت؛ اما در معرفـی مفهـوم نظـارت ویژگی‌های هشتگانه زیر را در همه اقسام کاربرد این اصطلاح و واژه می‌توان دید:

اول، در هر نظارتی چهار رکن را می‌توان مؤثر دید: «ناظر» و «عامل» (نظارت‌شـونده) که البته ناظر و عامل می‌توانند در یک مصداق جمع شده و بـه‌نـوعی «خـودکنترلی» برسیم، «فرآیند تحقّق نظارت» (دیـدن و کنتـرل آگاهانـه امـور) و نهایتـاً «ابزارهـا و شیوه‌های نظارت». دوم، نظارت با عقلانیت در ارتبـاط اسـت؛ چـون نیـاز بـه دیـدن، تجزیه‌وتحلیل و تشخیص صحیح از سقیم و ... دارد. سـوم، از ویژگـی فـوق، بـه ایـن خصیصه نیز می‌توان رسید که نظارت کنشی «عامدانه و عالمانه» اسـت؛ ازایـن‌رو هـر نگاه تصادفی و از روی جهل را نظارت نمی‌نامند و از همین‌جاست که نظارت در علوم اجتماعی، سیاسی و مدیریتی، تخصّصی است که افرادِ دارای استعدادِ مناسب باید این توانایی‌ها و قابلیت‌ها را طی دوره‌هایی کسب نموده و آمـوزش ببیننـد و در آن مسـیر تربیت شوند تا از عهده مسئولیتی که بر عهده آن‌ها نهاده می‌شود، برآیند و بـه‌قـدری پیچیده است که ممکن است هر دانش‌آموخته‌ای صلاحیت نظارت، کنترل و بازرسـی را نداشته باشد. چهارم، در همه نظارت‌ها، فـرض بـر ایـن اسـت کـه عامـل برحسـب برنامه‌ای عمل کند و ازاین‌رو بر او نظارت می‌شود تا حرکت صواب یا ناصواب او ثبـت و درج شود و چون برنامه‌ها برحسب اینکه آسمانی باشند یا زمینـی، مسـتبدان آن را تدوین کنند یا مردم‌گرایان و ... غایات متنوّعی دارند. چارچوب و شیوه نظارت‌هـا نیـز همسان نبوده و ازاین‌رو فلسفه نظارت نیز در هر مـورد، بـا دیگـر مـوارد تفـاوت‌هـای اساسی داشته، ضمن اینکه وجوه مشـترکی نیـز دارنـد. پـنجم، ویژگـی دیگـر اقسـام

---

۱. معادل واژه نظارت در زبان انگلیسی، ازجمله واژه‌های زیر پیشنهاد شده‌اند:
upevision..., stewardship, control, overseeing, in spection, monitoring

نظارت‌ها آن است که نظارت در جاهایی مطرح است کـه حرکتـی علمـی یـا عملـی، کمّی یا کیفی، گسترده یا محدود، مخفی یا آشکار و ... متناسب بـا اهـداف مقـرر، در جریان باشد. ازآنجاکه حین عمل احتمال خطا یا انحـراف از مسـیر مـی‌رود، ازایـن‌رو مورد کنترل و نظارت قرار می‌گیرد.

دهه‌ی اخیر درصحنه جهانی، شاهد رشد فـوق‌العـاده‌ای در زمینـه فنـاوری اطلاعـات است و امروزه فناوری اطلاعات و ارتباطات به‌گونه‌ای توسعه و اهمیت یافتـه کـه ایـن دوره را عصر اطلاعات و ارتباط و رایانه نامیده‌اند. اسـتفاده از رایانـه در خانـه بـه یـک حقیقت تبدیل‌شده و استفاده از آن در محل کار بسیار متداول شده و اکنون خواسته هر سازمانی است که در دنیای مجازی و الکترونیـک حضـور فعـال داشـته باشـد. در فضای سایبری کنترل و نظارت، مستلزم انجام نظارت بر فعالیت شبکه‌های ارتبـاطی، وب‌سایت‌ها و ارائه‌دهندگان خدمات اینترنت است. فعالیـت‌هـای انجـام‌شـده در طـی کنترل و نظارت عبارت‌اند از:

مراجعه به مراکز وب‌سایت‌ها، شبکه‌های ارتباطی و مراکز ارائه‌دهنده خدمات اینترنـت و میزبانی و کافی‌نت‌ها.

بازرسی محتوای موجود در سامانه‌هـا، شـبکه‌هـا و وب‌سـایت‌هـا و بررسـی و تحلیـل داده‌های ترافیکی جمع‌آوری‌شده توسط ارائه‌دهندگان خـدمات اینترنـت و همچنـین استفاده از نرم‌افزارهای مرتبط. در صورت لزوم شنود با مجوز موبایل یـا تلفـن عوامـل مرتبط با شبکه‌ها، وب‌سایت‌ها یا ارائه‌دهندگان دارای ادله مجرمانه. در صورت مواجهه با مصادیق مجرمانه، انعکاس مصادیق جرم به مبادی ذی‌ربط.

پلیس سایبر در ایران و آمریکا

در آخر لازم است به این نکته پرداخته شود که پلیسی که وظیفه نظـارت بـر فضـای سایبری را دارد، کدام پلیس است؟ آیا در این سه کشور هـر پلیسـی مـی‌توانـد ایـن وظیفه را عهده‌دار شود؟ مسلماً خیر؛ مانند هر امر دیگری که نهادهای خاص خـود را در پلیس دارد؛ نظارت بر فضـای مجـازی در پلـیس ایـن سـه کشـور نیـز بـه عهـده گروه‌های خاصی است.

ایران

در ایران، پلیس فتا از سوم بهمن ۱۳۸۹ به دستور فرمانده وقت نیروی انتظامی ایـران شروع به کارکرد و تنها نهاد پلیسی در ایران است که وظیفه نظارت بر فضای سایبری را بر عهده دارد، خود پلیس فتا به دودسته تقسیم می‌شود:

نخست، پلیس ستادی و دوم پلیس عملیاتی. پلیس‌های سـتادی بـر اسـاس دسـتور مقام قضایی به رصد سایت‌هـا یـا درگـاه‌هـای الکترونیکـی مـی‌پردازنـد و در صـورت مجرمانه بودن محتوای این سایت‌ها یا وقوع یکی از جرائم منـدرج در قـانون در ایـن فضا، این امر را به مراجع قضایی اطلاع مـی‌دهنـد. ایـن دسـته از پلـیس‌هـا هرچنـد فی‌نفسه ماهیت کارشان پیشگیری از وقوع جرائم است و با گشت‌زنی در فضای سایبر تلاش می‌کنند شهروندان یا مقامات قضایی را از تهدیدات موجود در ایـن فضـا آگـاه کنند، اما هیچ تدبیر فنی جهت حفاظت از اطلاعـات مـالی اتخـاذ نکـرده و تنهـا بـه هشدار و آگاه‌سازی عمومی از فواید و مضرات فضای سایبر بسنده کرده کـه بـیش‌تـر این هشدارها در خصوص حفظ حریم خصوصی اسـت. دسـته دوم پلـیس‌هـای فتـا، پلیس‌های عملیـاتی هسـتند کـه ماهیـت عملکردشـان اساسـاً پیگیـری اسـت و نـه پیشگیری در معنای خاص. این گروه از پلیس‌ها بنا به دستور مقام قضایی در صـورت وقوع جرم سعی در اعمال تدابیر واکنشی ازجمله فیلتر نمودن سایت‌هـا مـی‌کننـد و اقداماتشان بیشتر واکنشی است»[1].

آمریکا

در ایالات‌متحده‌ی آمریکا وظیفه‌ی نظارت بر فضای سایبر بـر عهـده‌ی اداره‌ی پلـیس فدرال[2] است. همچنین مرکزی به نام مرکز شکایت جرایم اینترنتی[3] وجود دارد که به دریافت شکایت مرتبط با جرایم سایبری، تحقیقات درباره‌ی آن و سپس ارجاع پرونده به دفترهـای فـدرال ایـالتی محلـی یـا دفترهـای اجـرای قـوانین بـین‌المللـی بـرای

---

۱ وطنی، امیر؛ اسدی، حمید، پیشین، ص ۱۱۸

2 Federal Bureau of Investigation (FBI)
3 the Internet Crime Complaint Center

رسیدگی‌های لازم می‌پردازد.[1] در کنار وجود متخصصین جرایم سایبر در این اداره و تیم‌های اقدام سایبر[2] جدید التاسیس، این اداره یک بخش سایبر[3] دارد که وظیفه‌ی مقابله با جرایم سایبری را دارد.[4]

نظارت بر فضای سایبر از طریق پیشگیری از جرم در ایران و آمریکا

پیشگیری انتظامی بر پایه اقدامات پلیسی در جهت حمایت از شهروندان آسیب‌پذیر، افزایش آگاهی‌های عمومی، نظارت بر اماکن عمومی و افزایش هزینه‌های ارتکاب جرم مبتنی است. متولی اصلی این نوع پیشگیری، نیروی انتظامی است که جهت تحقق آن، بایستی رویکرد جدیدی نسبت به وظایف سنتی خود اتخاذ کند؛ زیرا پیشگیری انتظامی عمدتاً مبتنی بر تدابیر و اقدامات کنشی-پیش‌جنایی توسط پلیس است و حال‌آنکه وظایف سنتی پلیس عمدتاً دربرگیرنده اقدامات واکنشی-پس جنایی در جهت کشف و تعقیب مجرمین است. با توجه به آنچه بیان شد می‌توان پیشگیری انتظامی را این‌گونه تعریف نمود؛ مجموعه تدابیر و اقدامات کنشی و واکنشی نیروی پلیس که با حمایت از افراد در معرض خطر، افزایش آگاهی‌های عمومی، نظارت بر اماکن عمومی، افزایش هزینه‌های ارتکاب جرم و مداخله پس از وقوع جرم و مداخله پس از وقوع جرم درصدد پیشگیری از ارتکاب جرم در جامعه است.

ایران

در خصوص جایگاه پیشگیری از جرم در پلیس ایران باید گفت بند هشت ماده چهار[5] قانون تأسیس نیروی انتظامی مصوب ۱۳۶۹ به پیشگیری از جرم به‌عنوان یکی از وظایف نیروی انتظامی اشاره نموده؛ بنابراین قانون‌گذار یکی از وظایف مهمی که به

---

۱ فریبرزی، الهام، سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و جهان، فقه و تاریخ تمدن ملل اسلامی، بهار ۱۳۹۰، شماره ۲۷، صص ۱۷۴ و ۱۷۵

2 Cyber Action Teams
3 Cyber Division
4 https://www.fbi.gov/investigate/cyber

۵ ماده‌ی ۴ قانون نیروی انتظامی مصوب ۱۳۶۹: انجام وظایفی که بر طبق قانون به‌عنوان ضابط قوه قضائیه به عهده نیروی انتظامی محول است از قبیل:الف- مبارزه با مواد مخدر. ب- مبارزه با قاچاق. ج- مبارزه با منکرات و فساد. د- پیشگیری از وقوع جرم. ه- کشف جرایم و- بازرسی و تحقیق. ز- حفظ آثار و دلایل جرم. ح- دستگیری متهمین و مجرمین و جلوگیری از فرار و اختفاء آن‌ها. ط- اجرا و ابلاغ احکام قضایی.

عهده ناجا (در بند د) واگذار کرده، پیشگیری از وقوع جرم است. با توجه به شرح وظایف و مأموریت‌های نیروی انتظامی آنچه تداعی می‌شود آنکه حوزه اقدامات نیروی انتظامی به‌عنوان یکی از نیروهای مسلح کشور جهت تأمین و حفظ امنیت بسیار گسترده است. به‌نحوی‌که کارکنان آن با بسیاری از اقشار جامعه از مسئولان کشوری و فرهنگی تا باندهای قاچاق مواد مخدر، قاچاق ارز و کالا، سارقان، جنایتکاران و ... ارتباط داشته و در این میان تأثیراتی نیز از محیط و شرایط اطراف خود به‌صورت مثبت و منفی دریافت می‌نمایند. در راستای پیشگیری فعالیت خوبی خصوصاً در سال‌های پس از ادغام نیروهای سه‌گانه صورت گرفت؛ تشکیل پلیس پیشگیری ناجا را می‌توان از عمده‌ترین و بارزترین فعالیت برشمرد. همین‌طور اهتمام جدی نسبت به پیشگیری از جرم تنها در سال‌های اخیر صورت گرفته و ازنظر ساختاری، اداره کل پیشگیری از جرم که یکی از ادارات معاونت انتظامی نیروی انتظامی بود؛ اخیراً تبدیل به معاونت مستقلی گردیده که موفقیت این معاونت منوط به استفاده از راهکارهای پیشگیری انتظامی است.

افزون بر این معاونت اجتماعی نیروی انتظامی نیز اقداماتی که ماهیتاً پیشگیرانه بوده را در دستور کار خود قرار داده بااین‌حال اقدامات مذکور مبتنی بر شیوه‌های علمی پیشگیری از جرم نبوده و بیشتر جنبه ابتکاری و ابداعی داشته است. پیشگیری انتظامی مبتنی بر قابلیت‌های نیروی پلیس در تحقق اهداف پیشگیری از جرم است؛ به‌عبارت‌دیگر مبنای پیشگیری انتظامی، اختیارات و توانایی‌های نیروی پلیس در پیشگیری از جرم در جامعه است؛ زیرا نیروی پلیس به لحاظ داشتن اختیارات و ابزار ویژه می‌تواند نقش به‌سزایی در کاهش نرخ جرایم- پیش از وقوع جرم و پس از آن- داشته باشد. ازآنجاکه پیشگیری از جرم اصولاً مبتنی بر دو شیوه است؛ یکی پیشگیری کیفری و دیگری پیشگیری غیر کیفری؛ بررسی مبانی پیشگیری انتظامی مستلزم تبیین این مطلب است که پیشگیری انتظامی چگونه و تا چه میزان می‌تواند در جهت تحقق اهداف پیشگیری کیفری و غیر کیفری مؤثر باشد. افزون بر این، تحقق اهداف پیشگیری کیفری و غیر کیفری توسط پلیس و درنهایت تحقق اهداف پیشگیری انتظامی منوط به تبیین و استفاده از رویکردهای جدیدی در نیروی پلیس

است که بسترهای لازم برای شکل‌گیری یک راهبرد مبتنی بر پیشگیری انتظامی را در نیروی پلیس فراهم سازد.[1]

در پلیس فتا واحدی تحت عنوان دایره پیشگیری سازمان‌دهی و با به‌کارگیری کارآگاهان خبره در علوم جنایی و رایانه مشغول انجام‌وظیفه می‌باشند. مسئولیت این افراد رصد سایت‌های اینترنتی و مطالب مندرج در آن‌ها است، درحالی‌که سایت ازلحاظ فنی باید فاکتورهای لازم را دارا باشد، پلیس با موارد جرایم مشهود مانند تبلیغ قرص‌های روان‌گردان، غیرمجاز جنسی، تبلیغات استفاده از مواد مخدر، سایت‌های ضد دینی و شیطان‌پرستی و نیز آن‌هایی که علیه حاکمیت نظام سیاسی کشور تبلیغ می‌کنند، اقدام قانونی لازم را انجام و ضمن گزارش به مقام قضایی با همکاری کارگروه مشخص‌شده در قانون نسبت به مسدود نمودن و پالایش سایت اقدام خواهد شد.[2]

آمریکا

کشور آمریکا از سال‌ها پیش با توجه به تعریف فضای سایبری و تهدیدات آن اقدام به تشکیل واحدهای مختلفی برای دفاع در برابر حملات سایبری نموده است. طی تحقیقات به‌عمل‌آمده، در کشور آمریکا مسئولیت دفاع سایبری در بخش نظامی بر عهده سازمان فرماندهی سایبری ایالات‌متحده[3] است. مأموریت این سازمان برقراری امنیت فضای سایبر برای ارتش آمریکا، وزارت دفاع و همچنین برقراری امنیت و آزادی ایالات‌متحده و هم‌پیمانانش در فضای سایبر است.

علاوه بر این سازمان، دو سازمان از جامعه‌ی اطلاعاتی آمریکا (آژانس امنیت ملی[4] و پلیس فدرال[5]) و یک اداره از وزارت امنیت داخلی نیز در زمینه‌ی دفاع و امنیت فضای سایبر فعالیت دارند. همچنین رئیس فرماندهی اطلاعات ملی به‌عنوان

---

1 https://www.isna.ir/news/8910-02927/

۲. عالی پور هفشجانی، خداداد، نقش پلیس در ارتباط با جرایم سایبری (تعقیب، کشف، پیشگیری)، ۱۳۹۰، دانشکده علوم انسانی، دانشگاه پیام نور مرکز تهران، ص ۹۹.

3 United State cyber command

4 NSA-National Security Agency

آژانس امنیت ملی (مسئولیت شنود سیگنال و حفاظت از سیگنال را در کشور ایالت متحده بر عهده دارد.)

5 FBI-Federal Bareau of investigation

پلیس فدرال آمریکا، مسئولیت مبارزه با جرایم سازمان‌یافته و تروریسم را بر عهده دارد.

هماهنگ‌کننده و مشاور رئیس‌جمهور در حوزه دفاع سایبری ایفاء نقش می‌نماید. در این زمینه در آمریکا دو قانون اهمیت دارد: یکی قانون اصلاح قانون نظارت اطلاعاتی بر خارجیان و دیگری قانون تجاوز به اطلاعات امنیتی.

بخش ۷۰۲ از قانون اصلاح قانون نظارت اطلاعاتی بر خارجیان مصوب ۲۰۰۸ میلادی[1] از دو جهت در بحث فعلی شایان توجه است: یکی اینکه به دادستان کل و اداره‌کننده اطلاعات ملی اجازه می‌دهد متفقاً مجوز نظارت الکترونیک بر اشخاص غیر آمریکایی که در خارج از آمریکا ساکن هستند را برای به دست آوردن اطلاعات جاسوسی خارجی صادر کند. نکته‌ی مهم درباره‌ی این ماده این است که در صدور این مجوز نیازی نیست فرد خاصی هدف قرار داده شود و با صدور این مجوز امکان نظارت بر اشخاص خارجی در خارج از خاک آمریکا به‌طورکلی وجود دارد. مدت این مجوز برای یک دوره‌ی یک‌ساله است.

مورد دیگر این است که این بخش از قانون مجوزی برای ایجاد برنامه‌ی منشور[2] شد. منشور اسم رمز یک برنامه‌ی جاسوسی است که آژانس امنیت ملی ایالات‌متحده آمریکا آن را پیش می‌برد و آرمان آن گردآوری داده ارتباط اینترنتی از چندین شرکت فراهم‌آورنده خدمات اینترنت در آمریکا است. این برنامه با نمادگر کنش شنود الکترونیک US-984XN نیز شناخته می‌شود. بر پایه بخش ۷۰۲ متمم‌های لایحه ۲۰۰۸ لایحه نظارت بر اطلاعات خارجی ۱۹۷۸ منشور، ارتباطات اینترنتی نگهداری‌شده را با درخواست از شرکت‌های اینترنتی مانند گوگل گردآوری می‌کند تا هرگونه داده را که با شرایط داوری مورد تأیید دادگاه نظارت بر اطلاعات خارجی ایالات‌متحده آمریکا سازگار باشد، واگردانی کند. آژانس امنیت ملی می‌تواند از این درخواست‌های منشور برای هدف‌گیری ارتباطاتی استفاده کند که هنگام جابجایی در ستون فقرات اینترنت رمزنگاری‌شده‌اند تا بدین‌وسیله بر داده نگهداری‌شده‌ای تمرکز کند که سامانه‌های فیلتر اینترنتی، مدت کوتاهی پیش از آن از رده خارج کرده بودند و داده‌ای را به دست آورد که می‌تواند از میان دیگر چیزها راحت‌تر مدیریت کند.

---

1 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008
2 PRISM

وجود این برنامه ازاین‌جهت مهم است که نشان می‌دهد امکان گردآوری و نظارت بر حجم وسیعی از داده‌های سایبری را فراهم می‌کند که از سرورهای موجود در آمریکا می‌گذرد.

از سوی دیگری قانون تجاوز به اطلاعات امنیتی (قانون ایالتی که در جولای ۲۰۰۳ قابل‌اجرا شد)، مستلزم این است که هر تجارت جهانی (و برخی از آژانس‌های ایالت کالیفرنیا) تمام اطلاعات شخصی ذخیره‌شده را رمزدار کند یا هر شهروند کالیفرنیایی که اطلاعات شخصیش توسط شخص دیگری احتمالاً یک هکر با سوءنیت به خطر افتاده است را گزارش دهد. این قانون اولین نمونه از نوع خودش در جهان به‌حساب می‌آید. یک سناتور از کالیفرنیا اخیراً پیشنهاد یک لایحه ملی را مطرح نموده که می‌تواند قانون ملی مشابهی ایجاد کند.[۱]

سازوکارهای کشف جرایم سایبری در ایران و آمریکا توسط پلیس

کشف جرائم سایبری مترادف است با بررسی صحنه وقوع جرم یا کالبدشکافی هدفی که جرم بر روی آن انجام‌شده است. بررسی مستندات الکترونیکی مهم و جستجو و دریافت داده‌ها از کامپیوترها از مهم‌ترین نیازهای کشف جرائم سایبری هستند. در این نیازها قطعاً مسئله مهم صحت داده‌ها است، درصورتی‌که در نگهداری اثرات یا ساده‌تر بگوییم فایل‌های دیجیتال سهل‌انگاری شود، به‌راحتی قابل‌تخریب هستند. در فرآیند کشف جرائم سایبری برای بازگردانی اثرات جرم معمولاً با استفاده از روش‌های خاص فایل‌های حذف‌شده، فایل‌های رمزنگاری‌شده و همچنین فایل‌های تخریب‌شده را برای بررسی‌های بیشتر بازگردانی می‌کنند. علاوه بر این نمی‌توان نقش و مسئولیت ارائه‌دهندگان اطلاعات و داده‌ها را انکار کرد که در این فصل، در مباحث پیش رو این موارد را بررسی خواهیم کرد.

نکته قابل‌توجه دیگر اینکه، قبل از پیدا کردن عامل جرم سایبری، نحوه گزارش و تشخیص نوع جرائم مهم است؛ زیرا ابتدا باید پی برد که جرمی به وقوع پیوسته و سپس باید به دنبال عامل یا عوامل آن بود که مرحله کشف جرم معمولاً توسط

---

۱. مراغی، علی‌اصغر، فرج دنیوی، حسن، اقدامات قانونی جهانی فعلی در برابر جرایم سایبری بامطالعه تطبیقی در حقوق ایران و آمریکا، مرکز همایش‌های پژوهشگاه نیرو، تیرماه ۱۳۹۵، ص ۱۰-۸

پلیس با همکاری نهادهای مردمی و رسمی صورت می‌گیرد.

ایران

ماده‌ی ۶۸۳ قانون آیین دادرسی کیفری بیان می‌دارد: «کنترل محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به کنترل ارتباطات مخابراتی مقرر در آیین دادرسی کیفری است». مقصود از مقررات راجع به کنترل ارتباطات مخابراتی در این ماده بیشتر از هر چه، اشاره به ماده‌ی ۱۵۰ از همین قانون است که برای کنترل ارتباطات مخابراتی وجود یکی از دو شرط زیر را لازم می‌داند:

۱. مربوط به امنیت داخلی و خارجی کشور باشد؛

۲. برای کشف جرایم موضوع بندهای (الف)، (ب)، (پ) و (ت) ماده‌ی ۳۰۲ لازم باشد.

از این میان مورد دوم که به‌طور مستقیم با موضوع موردبحث در این نوشتار مرتبط است، تقریباً تمامی جرایم موجود در ماده‌ی ۳۰۲ را در برمی‌گیرد و تنها جرایم ذکر شده در بند (ث) یعنی جرایم سیاسی و مطبوعاتی را از موضوع کنترل الکترونیک خارج کرده، در حقیقت قانون‌گذار به ضابط قضایی اجازه داده به‌جز استثنای مذکور به‌منظور کشف تمامی جرایمی که به لحاظ اهمیت و شدت جرم در صلاحیت رسیدگی دادگاه کیفری یک قرار دارند و در یک طبقه‌بندی عمومی در حوزه جنایات قرار می‌گیرند ارتباطات الکترونیک فرد خاصی را تحت نظارت و کنترل داشته باشند. در چنین مواردی نیز ضابط قضایی نمی‌تواند به‌صورت سرخود و به نیت کشف این دسته جرایم، اقدام به کنترل ارتباطات الکترونیکی افراد کند، بلکه موافقت رئیس‌کل دادگستری استان و با تعیین مدت و دفعات کنترل، شرط ضروری برای این اقدام است.

امریکا

قانون حریم ارتباطات الکترونیکی[1] نحوه دستیابی مأموران به اطلاعات ذخیره‌شده در اعتبار ارائه‌دهندگان خدمات شبکه‌ای (نظیر ISPها) را مقرر می‌کند. هر جا که مأموران یا مقام‌های تعقیب به دنبال رایانامهٔ ذخیره‌شده، سوابق مربوط به اعتبار یا

1 Electronic Communications Privacy Act(ECPA)

اطلاعات مربوط به مشترک شبکه‌ی ارائه‌دهنده خدمات هستند، باید این قانون را رعایت کنند.

بخش ارتباطات ذخیره‌شده در قانون ECPA (مواد ۲۷۰۱ تا ۲۷۱۲ عنوان ۱۸)، حقوق قانونی را برای حمایت از حریم خصوصی مشتریان و مشترکان ارائه‌دهندگان خدمات شبکه‌های رایانه‌ای مقرر می‌کند.

ازآنجاکه این قانون به‌طور غیرمعمول یک قانون مکمل محسوب می‌شود، آشنایی باهدف تدوین‌کنندگان آن می‌تواند در درک خود آن کمک بزرگی کند. ساختار این قانون طبقه‌بندی‌هایی را بازتاب می‌دهد که نشان می‌دهد تدوین‌کنندگان کدام نوع اطلاعاتی را دارای منافع حریم خصوصی کمتر و کدام نوع را دارای منافع حریم خصوصی بیشتر قلمداد می‌کرده‌اند. برای مثال، آن‌ها در رایانامه‌های ذخیره‌شده، در مورد اطلاعات مربوط به اعتبار مشترک منافع مهم‌تری را احراز کرده‌اند. همچنین، باور داشتند خدمات رایانه‌ای در دسترس «عموم جامعه»،[1] مستلزم محدودیت کمتری در اعمال مقررات نسبت به خدماتی است که در دسترس عموم نیست (شاید قضاوت مذکور این دیدگاه را بازتاب دهد که ارائه‌دهندگان خدمات در دسترس عموم جامعه، احتمالاً روابط بسته‌ای با سایر مشتریان‌شان ندارند و به‌این‌ترتیب، ممکن است کمتر تمایل داشته باشند از حریم خصوصی مشتریانشان حمایت شود). جهت حمایت از مفهوم منافع حریم خصوصی که تدوین‌کنندگان به رسمیت شناخته‌اند، قانون ECPA درجه‌های گوناگونی از حمایت‌های قانونی را مقرر می‌کند که مبنای آن‌ها میزان اهمیت متصور نسبت به منافع حریم خصوصی موردنظر است. بعضی اطلاعات را می‌توان به‌صرف صدور یک احضاریه از ارائه‌دهنده خدمات دریافت کرد؛ گروه دیگر مستلزم صدور دستور ویژه دادگاه است و بقیه هم مستلزم صدور قرار تفتیش است. به‌طورکلی، هرچه منافع حریم خصوصی اشخاص اهمیت بیشتری داشته باشد، حمایت از آن نیز قوی‌تر خواهد بود. لازم است مأموران و مقام‌های تعقیب، درجه‌های گوناگونی که تدوین‌کنندگان درنظرگرفته‌اند را بر روی حقایق هر یک از پرونده‌ها پیاده کنند تا بتوانند رویه مناسبی جهت کسب اطلاعاتی که دنبال

---

1. To the Public

می‌کنند به دست آورند. ابتدا آن‌ها باید ارائه‌دهندگان خدمات شبکه‌ای را طبقه‌بندی کنند (برای مثال، آیا ارائه‌دهنده خدمات، خدمات ارتباطی الکترونیکی، خدمات رایانه‌ای دوردست یا فعالیت دیگری را ارائه می‌دهد). سپس باید اطلاعاتی که دنبال می‌کنند را طبقه‌بندی کنند (مثلاً آیا محتوای اطلاعات در یک ذخیره الکترونیکی قرار دارد یا توسط خدمات رایانه‌ای دوردست نگهداری می‌شود، سابقه ... متعلق به یک مشترک یا سایر اطلاعاتی که در این قانون برشمرده شده است). سوم، مأموران باید توجه کنند که به دنبال تحمیل افشای اطلاعات هستند یا اینکه ارائه‌دهنده داوطلبانه می‌پذیرد اطلاعات را افشا کند. در حالت نخست باید مشخص کنند که به‌قرار تفتیش نیاز دارند یا دستور دادگاه مطابق بند «ت» ماده ۲۷۰۳ یا احضاریه. اگر به دنبال پذیرش داوطلبانه افشای اطلاعات هستند، باید مشخص کنند آیا قانون چنین اجازه‌ای را به آن‌ها می‌دهد یا خیر.

اصلاحات این قانون به‌موجب تصویب قانون پاتریوت مصوب ۲۰۰۱ اعمال شده است. قانون پاتریوت، این قانون را بر اساس فناوری‌های روز شفاف و اصلاح‌کرده و در بسیاری موارد، محدودیت‌هایی را رفع کرده که بر مجریان قانون در دسترسی به ارتباطات ذخیره‌شده وجود داشته. کارکنان مجریان قانون که با این مقررات قانونی سروکار دارند، قویاً تشویق می‌شوند تا گزارش‌های خود در باب تجربیاتشان را به مرکز CCIPS ارسال نمایند تا امکان طرح آن‌ها نزد کنگره میسر شود. به‌این‌ترتیب، کنگره تصمیم خواهد گرفت که تغییرهای اعمال شده در قانون پاتریوت همچنان برقرار بماند یا اینکه خودشان اصلاح شوند.

قانون ECPA ارائه‌دهندگان مشمول خود را به دودسته تقسیم می‌کند: ۱. ارائه‌دهندگان خدمات ارتباطی الکترونیکی و ۲. ارائه‌دهندگان خدمات رایانه‌ای دوردست. زمانی که مأموران و مقام‌های تعقیب خواهان دستیابی به سوابق هستند، باید بتوانند انواع اطلاعات مندرج در قانون ECPA را طبقه‌بندی کنند. این قانون اطلاعات را به سه بخش تقسیم می‌کند: ۱. اطلاعات اصلی[1] راجع به مشترک که در شماره (۲) بند «پ» ماده ۲۷۰۳ آمده است؛ ۲. سوابق یا سایر اطلاعات راجع به

---

1. Basic Information

مشتری یا مشترک خدمات؛ و ۳. محتوی (ر.ک: بند (۸) ماده ۲۵۱۰ و شماره (۱) بند «پ» ماده ۲۷۰۳).

شماره (۲) بند «پ» ماده ۲۷۰۳، اطلاعات اصلی مشترک را فهرست‌وار بیان کرده است: ۱. نام؛ ۲. آدرس؛ ۳. سوابق تلفن محلی و راه دور یا سوابق تعداد دفعات و مدت مکالمات؛ ۴. مدت‌زمان استفاده از خدمات (که شامل قید روز شروع آن‌هم می‌شود) و نوع خدمات بهره‌برداری شده؛ ۵. شماره تلفن یا وسیله یا سایر شماره یا شناسایی اگر هویت مشترک که شامل آدرس شبکه‌هایی که به‌طور موقت تخصیص‌یافته‌اند نیز می‌شود؛ و ۶. ابزار و منابع پرداخت استفاده ازاین‌گونه خدمات (که شامل کارت‌های اعتباری یا شماره‌حساب بانکی نیز می‌شود).

به‌طورکلی، مواردی که در این فهرست آمده، به هویت مشترک، رابطه‌اش با ارائه‌دهنده خدمات و سوابق اصلی تماس‌هایش مربوط می‌شود. این فهرست شامل موارد دیگری نمی‌شود و سوابق تراکنش‌های گسترده‌تر را دربرنمی‌گیرد، مانند اطلاعات مندرج در لوگ که آدرس‌های رایانامهٔ اشخاصی را نشان می‌دهد که مشتری در جلسه پیشین با آن‌ها مکاتبه کرده بود. ماده ۲۱۰ قانون پاتریوت، طبقه‌بندی‌های اطلاعات اصلی مشترک را از سه لحاظ گسترش داده است. این قانون عبارت‌های «سوابق تعداد دفعات و مدت جلسات» و «هرگونه آدرس شبکه‌ای تخصیص‌یافته موقت» را به شماره (۲) بند «پ» ماده ۲۷۰۳ اضافه کرده است. در چارچوب اینترنت، این سوابق شامل آدرس‌های IP تخصیص‌یافته توسط ارائه‌دهنده خدمات اینترنتی به مشتری برای یک جلسه می‌شود. همچنین، این سوابق شامل سایر اطلاعات مربوط به دسترسی به اعتبار، مانند شماره تلفن مبدأ جهت اتصال به اینترنت یا آدرس IP کاربر که از طریق اعتبار خود به اینترنت دسترسی می‌یابد نیز می‌شود. علاوه بر این، قانون پاتریوت به فهرست اطلاعات مربوط به مشترک، عبارت «ابزار و منابع پرداخت» را هم اضافه کرده که مشتری برای پرداخت هزینه اعتبار خود استفاده می‌کند و شامل «کارت اعتباری یا شماره‌حساب بانکی» می‌شود.

سوابق یا سایر اطلاعات راجع به مشتری یا مشترک؛ شماره (۱) بند «پ» ماده ۲۷۰۳، نوع دوم اطلاعات را بیان می‌کند: «هر نوع سابقه یا سایر اطلاعات راجع به

مشترک یا مشتری این‌گونه خدمات (شامل محتوای ارتباطات نمی‌شود)». این طبقه، هفت‌رنگ و هزارجور است و تمامی سوابقی را در برمی‌گیرد که در حوزه محتوی نمی‌گنجند، ولی شامل اطلاعات اصلی راجع به مشترک می‌شوند.

مثال‌های معمولی که در زمینهٔ «سوابق راجع به مشترک» می‌توان بیان کرد، سوابق تراکنش است، مانند لوگ‌های اعتبار که استفاده از آن را ثبت می‌کنند؛ داده‌های راجع به تعیین موقعیت تلفن همراه[1] به هنگام برقراری تماس‌ها و آدرس‌های رایانامهٔ سایر اشخاص که دارنده اعتبار با آن‌ها مکاتبه کرده است (در دعوای ایالات‌متحده علیه آلن،[2] دادگاه نتیجه‌گیری کرد که لوگ شناساگر تاریخ، زمان، نام کاربر و جزئیات آدرس اینترنتی سایت‌هایی که کاربر به آن‌ها دسترسی یافته، سابقه یا سایر اطلاعات راجع به مشترک یا مشتری این‌گونه خدمات را مطابق قانون ECPA به وجود آورده است. یا در دعوای هیل[3] علیه ام.سی. آی. ورلدکام، دادگاه نتیجه‌گیری کرد که نام‌ها، آدرس‌ها و شماره تلفن اشخاصی که با آن‌ها تماس برقرارشده، سابقه یا سایر اطلاعات راجع به مشترک یا مشتری چنین خدماتی نسبت به اعتبار استفاده از تلفن را ایجاد کرده است). مطابق اصلاحات قانونی که در سال ۱۹۹۴ نسبت به بند «پ» ماده ۲۷۰۳ صورت گرفت، هدف از جداسازی اطلاعات اصلی مشترک از سایر سوابق، که البته شامل محتوا نمی‌شود، بدین دلیل بوده که میان اطلاعات اصلی راجع به مشترک و اطلاعاتی که از تبادل انجام‌شده افشاگری بیشتری می‌کنند و می‌توانند حاوی «کل پیشینه فعالیت‌های برخط شخص» باشند، تمایز صورت گیرد.

محتوی[4]؛ محتوای اعتبار شبکه و فایل‌های واقعی ذخیره‌شده در آن است. بند هشت ماده ۲۵۱۰: «محتوی نسبت به هر نوع ارتباطات سیمی، شفاهی یا الکترونیکی مصداق می‌یابد و شامل هر نوع اطلاعاتی می‌شود که شالودهٔ اصلی، فحوا یا معنای آن ارتباط را دربردارد». برای مثال، پیام‌های پستی ذخیره شدهٔ الکترونیکی یا صوتی «محتوا» محسوب می‌شوند، درست مانند فایل‌های پردازشگر متنی ذخیره‌شده در

---

1. Cell-Site Data
2. U.S. v. Allen, 2000
3. Hill v. MCI Worldcom, 2000
4. Content

اعتبارهای شبکه‌ای کارمند. حتی سرصفحه‌های موضوعی[1] پیام‌ها نیز محتوا محسوب می‌شوند (در دعوای براون علیه وادل،[2] شعبهٔ چهارم دادگاه سیار یادآور شد پیام‌های رقمی پیجر، طیف نامحدودی از پیام‌های اصلی شماره‌ای رمزدار را دربرمی‌گیرد که لازم است به هنگام صدور رأی در باب شنود پیام‌های پیجر، مقررات «عنوان سوم»[3] رعایت شود).

می‌توان محتوا را به سه زیرطبقهٔ دیگر نیز تقسیم کرد: ۱. محتوای ذخیره‌شده در «ذخیرهٔ الکترونیکی» توسط ارائه‌دهنده ECS؛ ۲. محتوای ذخیره‌شده توسط ارائه‌دهنده RCS؛ و ۳. محتوای نگهداری‌شده توسط دیگری.

در زمینه جمع‌آوری اطلاعات، مأموران تحقیق می‌توانند جهت تحصیل اطلاعات اصلی مشترک احضاریه صادر کنند .مجریان قانون می‌توانند برای دستیابی به دو نوع اطلاعات از احضاریه استفاده کنند: نخست اجبار به افشای اطلاعات اصلی راجع به مشترک: ۱. نام؛ ۲. آدرس؛ ۳. سوابق مربوط به تماس تلفنی محلی و راه دور، یا سوابق تعداد دفعات و مدت هر یک از این تماس‌ها؛ ۴. مدت‌زمان استفاده از خدمات (شامل زمان شروع آن نیز می‌شود) و نوع خدماتی که بهره‌برداری شده است؛ ۵. شماره تلفن یا وسیله یا سایر شناساگرهای هویت مشترک که شامل آدرس شبکه‌هایی که به‌طور موقت بکار رفته نیز می‌شود؛ و ۶. ابزار و منابع پرداخت استفاده ازاین‌گونه خدمات (که شامل کارت‌های اعتباری و شماره‌حساب بانکی نیز می‌شود).

همچنین، مأموران می‌توانند با صدور احضاریه، به اطلاعاتی نیز دست یابند که خارج از حوزه قانونی ECPA است. به‌این‌ترتیب، ماده ۲۷۰۳ هم هیچ شرطی را برای افشای محتوای آن تحمیل نمی‌کند و مأموران می‌توانند شرکت را با صدور یک احضاریه ملزم کنند ارتباطات را افشا کنند؛ چراکه قانون ECPA شامل آن نمی‌شود. هم‌چنین، اطلاعات مرتبط یا متعلق به شخصی که نه «مشترک»[4] است و نه «مشتری»،[5] از حمایت این قانون برخوردار نیستند و می‌توان با استفاده از احضاریه

---

1. Subject Headers
2. Brown v. Waddell, 1995

۳. قانون استراق سمع

4. Subscriber
5. Customer

به همان ترتیب عمل کرد.

مجاری قانونی صدور احضاریه محدود است.[1] البته دلایلی که در پاسخ به احضاریه صادره توسط هیئت عالی منصفه فدرال[2] به‌دست‌آمده، باید تحت حمایت مقررات افشای ماده شش قانون آئین دادرسی کیفری فدرال نیز قرار گیرد. هرگونه احضاریه هیئت عالی منصفه یا رسیدگی قضایی[3] فدرال یا ایالت، به همان اندازه احضاریه اداری[4] قانون ایالت یا فدرال اعتبار دارد. برای مثال، می‌توان از احضاریه‌ای که مطابق شماره (۴) بند «الف» ماده شش قانون بازرسی عمومی[5] صادر می‌شود استفاده کرد. بااین‌حال، حداقل یک دادگاه رأی داده که صدور احضاریه در مرحله کشف ادله دعاوی حقوقی مطابق ماده ۴۵ قانون آئین دادرسی مدنی فدرال[6] نامناسب است (در دعوای اف.تی. سی. علیه شرکت ارتباطاتی نت‌اسکیپ[7]، دادگاه رأی داد که صدور احضاریه در مرحله کشف ادله، شامل مفهوم «احضاریه در مرحله رسیدگی» نمی‌شود).

علاوه بر این مأموران تحقیق می‌توانند کلیهٔ محتوای موجود در اعتبار را با ارائه قرار تفتیش به دست آورند. قانون ECPA آن‌ها را ملزم نمی‌کند مشتری یا مشترک را درزمانی که اطلاعات را از ارائه‌دهنده خدمات با ارائه قرار تفتیش دریافت می‌کنند، آگاه سازند.

مأمورانی که مطابق ماده ۴۱ قانون آئین دادرسی کیفری فدرال قرار تفتیش یا معادل ایالتی آن را دریافت می‌کنند، می‌توانند موارد زیر را به دست آورند: ۱. کلیهٔ مواردی که می‌توان با دستور دادگاه با ابلاغ به دست آورد؛ ۲. محتوای ارتباطات الکترونیکی که در ذخیرهٔ الکترونیکی سیستم ارتباطات رایانه‌ای به مدت ۱۸۰ روز یا کمتر ذخیره‌شده است[8] و ۳. به‌عبارت‌دیگر، مأموران می‌توانند با تحصیل قرار تفتیشی که بر پایه سبب محتمل مطابق ماده ۴۱ صادرشده، هر نوع سابقه و کل محتوای اعتبار

---

1. U.S. v. Morton Salt Co. 1950
2. Federal Grand Jury Subpoena
3. Trial Subpoena
4. Administrate
5. Inspector General Act
6. Federal Rules of Civil Procedure
7. FTC v. Netscape Communication Corp. 2000
8. 2703(a)

را به دست آورند.[1] قرار تفتیش را می‌توان به ارائه‌دهنده خدمات، ارائـه و وی را ملـزم کرد برای مجریان قانون اطلاعات مندرج در آن را افشا کند.

قرارهای تفتیش صادره بر اساس ماده ۴۱ به «تفتیش اموال ... واقع در منطقـه تحـت صلاحیت قاضی» محدود می‌شوند،[2] درباره قرارهایی که نوعاً مطابق مـاده ۴۱ تنظـیم می‌شوند، اصولاً مأموران تحقیق موظف‌اند یـک سـوگندنامه و قـرار پیشـنهادی را بـا رعایت این ماده تنظیم کنند. بااین‌حال، زمانی که قاضی قرار را امضا می‌کنـد، عمومـاً مأموران تحقیق شخصاً رایانه‌های ارائه‌دهنده خدمات را جهت کشف مـواردی کـه در قرار آمده تفتیش نمی‌کنند، بلکه آن را همانند یک احضاریه به اطلاع وی می‌رسـانند تا به مفاد اشاره‌شده عمل کند؛ بنابراین به‌طورکلی در ایـالات‌متحـده پـس از ضـابطه دریافت احضاریه جهت دسترسی به داده‌هایی که ماهیت شکلی دارند، بـرای دریافـت داده‌های رایانه‌ای محتوایی و شکلی نیز چهار دستور پیش‌بینی‌شده است:[3]

الف) احضاریه با ابلاغ پیشین به مشترک یا مشتری موردنظر

مأمورانی که احضاریه تحصیل می‌کنند، چه بـه مشـترک پیشـاپیش ابـلاغ کننـد یـا مقررات ابلاغ با تأخیر مندرج در قسمت الف بخش ۲۷۰۵ را رعایت کنند، مـی‌تواننـد موارد زیر را تحصیل کنند ۱. همه مواردی کـه بـا اسـتفاده از احضـاریه بـدون ابـلاغ می‌توان به دست آورد؛ ۲. محتوای ارتباطات الکترونیکـی یـا کـابلی کـه ارائـه‌دهنـده خدمات رایانه‌ای راه دور[4] بـه‌جـای مشـترک یـا مشـتری خـود نگهـداری مـی‌کنـد؛ ۳. محتـوای ارتباطـات الکترونیکـی یـا کـابلی کـه بـر روی سیسـتم‌هـای ارتباطـات الکترونیکی، در ذخیره الکترونیکی[5] به مدت بیش از ۱۸۰ روز نگهـداری شـده باشـد (قسمت الف بخش ۲۷۰۳).

---

[1] – گنجانیدن ارتباطات سیمی (مانند پست صوتی) در این طبقه تا ۳۱ دسامبر ۲۰۰۵ اعتبار خواهد داشت، مگر اینکه کنگره آن را تمدید کند. ر.ک PATRIOT Act §§ 209, 224, 115 Stat. 272, 283, 295 (2001) :

۲– اصلاحیهٔ صورت گرفته در قانون ECPA که صدور قرارهای تفتیش خارج از قلمرو صلاحیتی را مجاز می‌شمرد، در صورت عدم تمدید کنگره تا پایان روز ۳۱ دسامبر ۲۰۰۵ اعتبار خواهد داشت. ر.ک:

PATRIOT Act §§ 220, 224, 115 Stat. 272, 291-92, 295 (2001)

3 Department of Justice of the United States, 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.p63

4 remote computing service

5 electronic storage

ب) دستور دادگاه مطابق قسمت «د» بخش ۲۷۰۳

این دستور توسط قاضی فدرال، قاضی دادگاه ناحیه یا قاضی دادگاه معادل ایالتی صادر می‌شود و به‌موجب آن این موارد را می‌توان به دست آورد: ۱. تمام مواردی که با صدور احضاریه بدون ابلاغ می‌توان اخذ کرد؛ ۲. تمام سوابق یا اطلاعات راجع به مشترک یا مشتری اینگونه خدمات که البته محتوای ارتباطات نگهداری شده توسط ارائه‌دهندگان خدمات ارتباطات الکترونیکی و رایانه‌ای راه دور را شامل نمی‌شود. برای اخذ این دستور که به دستور قضایی مبتنی بر حقایق قابل تشریح[1] نیز معروف است یا به‌طور خلاصه دستور d نامیده می‌شود، مجریان قانون باید دلایل مشخص و قابل تشریح خود را که نشان‌دهنده زمینه‌های متعارف است و این اعتقاد را ایجاد می‌کند که محتوای ارتباطات کابلی یا الکترونیکی یا سوابق دیگر اطلاعاتی که دنبال می‌کنند، جزئی از جرم یا در ارتباط با جرمی هستند که آن‌ها قصد تحقیق آن را دارند، ارائه دهند. به‌این‌ترتیب، این معیار به مجریان قانون اجازه نمی‌دهد که صرفاً گواهی کنند، یک سری حقایق مشخص و قابل تشریح وجود دارد، بلکه باید مدارک واقعی ارائه دهند تا بتوانند چنین دستوری را اخذ کنند.

۳. دستور دادگاه مطابق بخش ۲۷۰۳، با ابلاغ پیشین به مشتری یا مشترک موردنظر

چنانچه مجریان قانون بتوانند این دستور را اخذ کنند، موارد زیر به دست می‌آید: ۱. تمام مواردی که با استفاده از دستور بدون ابلاغ قسمت «د» بخش ۲۷۰۳ می‌توان به دست آورد؛ ۲. محتوای هرگونه ارتباطات الکترونیکی یا کابلی که ارائه‌دهنده خدمات رایانه‌ای راه دور به‌جای مشترک یا مشتری خود نگهداری می‌کند؛ ۳. محتوای ارتباطات الکترونیکی یا کابلی که در ذخیرهٔ الکترونیکی سیستم ارتباطات الکترونیکی بیش از ۱۸۰ روز موجود بوده است. البته مأموران در اینجا نیز با رعایت مقررات ابلاغ با تأخیر، بازهم می‌توانند این موارد را به دست آورند.

---

1 articulable facts court order

۴. قرار تفتیش[1]

مأمورانی که مطابق ماده ۴۱ آئین دادرسی کیفری فدرال[2] قرار تفتیش یا معادل ایالتی آن را دریافت می‌کنند، به موارد زیر می‌توانند دست یابند: ۱. تمام مواردی که می‌توان با استناد به دستور دادگاه با ابلاغ پیشین به دست آورد؛ ۲. محتوای ارتباطات الکترونیکی یا کابلی که در ذخیرهٔ الکترونیکی سیستم ارتباطات رایانه‌ای به مدت ۱۸۰ روز یا کمتر، ذخیره‌شده است؛ ۳. به‌طور خلاصه، مأموران با تحصیل قرار تفتیشی که بر پایه سبب محتمل[3] و مطابق ماده ۴۱ صادرشده است، هرگونه سابقه و همه محتویات اعتبار مشترک یا مشتری موردنظر را می‌توانند به دست آورند که به‌این‌ترتیب، شنود ارتباطات الکترونیکی و کابلی نیز تحت شمول این مقررات قرار می‌گیرد، اما نکته مهم این است که اثبات سبب محتملی که در اصلاحیهٔ چهارم قانون اساسی[4] آمده و از مجریان قانون خواسته برای اثبات آن سوگندنامه[5] ارائه دهند و گواهی خود را به آن ضمیمه کنند، به مراتب از ارائه حقایق قابل تشریح، برای اخذ دستور دادگاه مشکل‌تر است.

سازوکارهای تحقیق جرایم سایبری توسط پلیس در ایران و آمریکا

تحقیق در لغت به معنی بررسی و پژوهش برای رسیدن به واقعیت است[6] و تحقیقات مقدماتی عبارت است از مجموعه اقدامات و تحقیقاتی که از سوی ضابطان دادگستری رأساً یا به دستور و حسب ارجاع مقامات قضایی یا از سوی قضات تحقیق و نیز سایر مقامات صالح قضایی به‌منظور تسهیل و تمهید دلایل، اعم از دلایل اثبات جرم و دلایل مفید به حال متهم با توجه به اصل برائت صورت می‌پذیرد و هدف اصلی آن آماده‌سازی پرونده و تسهیل و تسریع رسیدگی در دادگاه است.[7]

در بین ضوابط و اصول قانونی حاکم بر تحقیقات مقدماتی در خصوص جرایم سایبری، موضوع احراز صلاحیت، تفتیش، توقیف و شنود در محیط سایبر را می‌توان

---

1 warrant
2 federal rules of criminal procedure
3 probable cause
4 fourth amendment
5 affidavit

۶. معین، محمد، فرهنگ فارسی (ج ۱)، چ ۲۲، تهران، انتشارات امیرکبیر، ۱۳۷۵، ص ۱۰۴۰

۷. آشوری، محمد، مقدمه‌ای بر کتاب جرایم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزهکاری، چ ۲، تهران، انتشارات بهنام،۱۳۸۶، ص ۱۰

ازجمله موضوعات چالشی تحقیقات مقدماتی جرایم سایبری دانست که به بررسی آن خواهیم پرداخت.

منظور از پی‌جویی در این پژوهش بررسی و جستجوی اطلاعات مرتبط با جرم یا اشراف و تکمیل اطلاعات افعال مجرمانه در فضای سایبر است که به‌طور مستقیم یا غیرمستقیم در رصد، تشخیص، شناسایی، کشف و مقابله با جرایم مؤثر واقع می‌شود و از آنجاکه هدف از تحقیقات مقدماتی در نهایت کشف جرم است؛ کلیهٔ اقداماتی که قبل، حین یا پس از وقوع جرم به‌منظور شناسایی، جمع‌آوری، بررسی، تجزیه وتحلیل آثار و دلایل جرم و همچنین شناسایی، دستگیری و بازجویی متهم در جهت روشن شدن حقیقت و انتساب و عدم انتساب جرم به فهم و در نهایت صدور حکم توسط مقامات قضایی انجام می‌شود را می‌توان کشف جرم تلقی کرد.

ایران

قانون آیین دادرسی کیفری در ماده ۹۰ تحقیقات مقدماتی را مجموعه اقداماتی دانسته که از سوی بازپرس یا دیگر مقامات قضایی به‌موجب قانون برای حفظ آثار و علایم و جمع‌آوری ادله وقوع جرم، شناسایی، یافتن و جلوگیری از فرار یا مخفی شدن متهم انجام می‌شود.

تحقیقات و پی‌جویی جرایم سایبری را باید به سه مرحله حین، قبل و بعد از وقوع جرم سایبری تقسیم نمود که در هر یک از مراحل اشاره‌شده پلیس وظایفی را به شرح زیر انجام می‌دهد که ضمن اشاره به هرکدام در ادامه به تفضیل به آن‌ها خواهیم پرداخت :۱- قبل از وقوع جرم: وفق بند هشت از ماده چهار قانون نیروی انتظامی جمهوری اسلامی ایران پیشگیری از وقوع جرم یکی از وظایفی است که بر طبق قانون به‌عنوان ضابط قوه قضاییه به عهده نیروی انتظامی گذاشته‌شده است، لذا در این مرحله مأموریت با رصد، پایش و تشخیص تهدیدها، آسیب‌ها و جرایم احتمالی عملیاتی می‌شود. لازم به ذکر است پیشگیری از وقوع جرم به‌نوعی پی‌جویی و مقابله است. موضوع پیشگیری که پیشتر به آن پرداختیم.

۲- حین وقوع: در این مرحله تأثیر جرم کامل نشده و پلیس با درخواست بزه دیده یا سازمان آسیب‌دیده وارد عمل می‌شود و برای ممانعت از ادامه فعالیت مجرمانه تلاش

می‌کند.

۳- بعد از وقوع جرم: در این مرحله پلیس و دستگاه قضایی با تجسس و پاسخگویی عمل نموده و به‌منظور تکمیل تحقیقات و پرونده وارد مرحله تعقیب مجرمین بر اساس مراحل ذیل می‌گردد: الف) اخذ مجوز قضایی؛ ب) تشکیل تیم تحقیق؛ ج) تحقیق در مورد جرم سایبری (بازرسی صحنه جرم، شناسایی هویت در فضای سایبر، ادله الکترونیک، بازجویی از مظنونین)؛ د) استفاده از کارشناسان فنی رایانه به‌عنوان مشاور؛ ه) بازسازی صحنه جرم[1].

در ایران مواد ۶۷۰ الی ۶۷۸ قانون آیین دادرسی کیفری به موضوع تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای پرداخته و در هر مورد راهکارهایی را پیش‌بینی نموده است. در این میان ماده‌ی ۶۷۰ امکان ارائه داده‌های حفاظت‌شده به ضابطان به دستور مقام قضایی را در صورت ضرورت پیش‌بینی نموده است. ماده‌ی ۶۷۱ نیز دستور تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای را به‌موجب دستور مقام قضایی و در مواردی دانسته که «ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد». این یعنی به‌قصد کشف جرم نیز امکان تفتیش و توقیف داده‌های ذخیره‌شده وجود دارد، هرچند کاربرد اصلی آن را می‌توان در مرحله‌ی تعقیب و به‌منظور شناسایی متهم یا ادله جرم متصور شد.

در توقیف داده‌ها ماده ۶۷۵ مقرر می‌دارد: در خصوص توقیف داده‌ها با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، کپی‌برداری یا تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل‌دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود. به‌تصریح ماده مذکور داده‌های رایانه‌ای با رعایت ضوابط مقرر ازجمله: تناسب، نوع، اهمیت و نقش داده‌ها در ارتکاب جرم که تشخیص آن با مقام قضایی است، امکان‌پذیر است.

در مورد شیوه‌های توقیف سامانه‌های رایانه‌ای ماده ۶۷۷ قانون مذکور با رعایت

---

۱. بابایی، محسن، شیروی، مهسا، حدود اختیارات در فرآیند پی‌جویی جرایم سایبری در حقوق ایران و انگلستان، مجموعه مقالات همایش ملی رویارویی با جرایم سایبری، ج ۱،۱۰ اسفند ۱۳۹۵، صص ۳۵۰-۲۴۹.

تناسب بین توقیف سامانه‌های رایانه‌ای با نوع و اهمیت و نقش آن‌ها در ارتکاب جرم آن را با روش‌هایی از قبیل: پلمپ سامانه در محل استقرار، ضبط سامانه و غیرقابل‌دسترس کردن سامانه با تغییر گذرواژه امکان‌پذیر دانسته است. در توقیف داده‌ها و سامانه‌های رایانه‌ای ممکن است مکان تحت تفتیش و توقیف دارای سیستم رایانه‌ای باشد که از آن فقط جهت تأمین دسترسی به داده‌های ذخیره‌شده در یک سیستم متفاوت مستقر در مکانی دوردست استفاده شود. در چنین شرایطی لازم است مأموران تفتیش حکم تفتیشی در اختیار داشته باشند که به حد کافی موسع باشد و سیستم رایانه‌ای دوردست را نیز در برگیرد. در این مورد قانون جرایم رایانه‌ای در ماده‌ی ۶۷۸ به ضابطان این اجازه را داده که در صورت ضرورت در برخورد با سیستم‌های رایانه‌ای که در قرار تفتیش و بازرسی ذکر نشده، حیطه تحقیق خود را گسترش دهند مشروط بر اینکه به دستور مقام قضایی باشد.[۱]

بنابراین برای اینکه پلیس بتواند داده‌ها یا سیستم‌های رایانه‌ای را تفتیش و توقیف نماید، به دستور مقام قضایی نیاز دارد؛ مگر کسی که داده‌ها یا سیستم‌های مذکور را در اختیار دارد، رضایت کتبی به‌منظور تفتیش آن بدهد. درعین‌حال، در صورت وجود ظن منطقی مبنی بر وجود ادله و فوریت امر، پلیس می‌تواند بدون دستور قضایی اقدام به تفتیش یا توقیف داده‌ها نماید که این مهم درجایی مطرح می‌شود که منافع عمومی علت امر باشد. در حقیقت، در موارد کلی هنگام بررسی دلایل وقوع جرم، پلیس باید اطمینان یابد که حقوق شخصی افراد را کاملاً رعایت کرده است.[۲]

این کار باید به طریقی انجام شود که دلایل موردنظر، از هرگونه تغییر، تحریف یا آسیب مصون بماند. در مرحله‌ی تجزیه‌وتحلیل، به ارزش اثباتی و اهمیت دلیل پرداخته می‌شود و درنهایت در مرحله‌ی ارائه گزارش، پلیس باید گزارش مکتوبی که

---

۱. موذن زادگان، حسنعلی، شایگان، محمد رسول، استنادپذیری و تحصیل ادله الکترونیکی درحقوق کیفری ایران، فصلنامه دیدگاه‌های دیدگاه‌های حقوقی، ش ۴۸، زمستان ۱۳۸۸، ص ۹۲-۹۴.

پی‌نوشت: توضیح اینکه نویسندگان مقاله‌ی مذکور این توضیحات را درباره‌ی ماده‌ی ۴۳ قانون جرایم رایانه‌ای نگاشته‌اند اما ماده‌ی ۴۳ عیناً در ماده‌ی ۶۷۸ قانون آیین دادرسی کیفری به‌عنوان قانون لاحق تکرار شده است.

۲- آیکاو، دیوید جی؛ راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای؛ ترجمه‌ی اکبر استرکی، محمد صادق روزبهانی، تورج ریحانی و راحله الیاسی، تهران، معاونت پژوهش دانشگاه علوم انتظامی، سال ۱۳۸۸، ص ۷۶.

کلیات مربوط به فرایند بررسی و اطلاعات به‌دست‌آمده را دارا باشد، بـه مقـام قضـایی ارائه دهد. دلایل ارائه‌شـده تنهـا در صـورتی قابلیـت شناسـایی، کشـف، جمـع‌آوری، مستندسازی، تجزیه‌وتحلیل، حفظ و مراقبت از دلایـل الکترونیکـی و ارائـه آن‌هـا بـه دادگاه را دارند که به نحو صحیحی به کار گرفته‌شده باشند.

در مرحله شناسایی منابع حاوی ادله اهمیت بسیار زیادی در کشف جـرایم سـایبری دارد. هم‌اکنون بسیاری از تولیدات کامپیوتری هستند که می‌توانند ادله الکترونیک را نگهداری کنند، ازجمله ادله دیجیتالی مانند تلفن‌های دیجیتال، دستگاه‌های دستی[1]، کامپیوترهـای قابـل‌حمـل، کـامپیوتر رومیـزی، سـرورهای بـزرگ و ابرکامپیوترهـا. همچنین، اشکال متنوعی از رسانه‌های ذخیـره‌سـاز وجـود دارنـد کـه ازجملـه آن‌هـا می‌توان به لوح‌های فشرده، دیسک‌های نرم[2]، نوارهای مغناطیسی و دیسک‌های زیپ[3] زیپ[3] اشاره کرد. علاوه بر این، سیم‌ها، کابل‌ها و هوا نیز می‌توانند حامل ادله دیجیتال باشند که با استفاده مناسب می‌توان آن‌ها را جمع‌آوری و بـرای بررسـی‌هـای بعـدی ذخیره کرد.

پلیس پس از شناسایی ادله دیجیتال، بایـد آن‌هـا را در همـان وضـعیت اصـلی خـود محافظت کند، این کار دقیقاً بر اساس الزامات قانونی است و در راستای استنادپذیری ادله الکترونیک ارائه‌شده از سوی مجریان قانون مقررشده و بر اسـاس آن در صـورتی ادله الکترونیک جمع‌آوری‌شده معتبر قلمداد می‌شود که هیچ‌گونه تغییـری در آن‌هـا به وجود نیامده باشد. عمده اقدامی که لازم است در راستای محافظت ادله انجـام داد این است که از هرگونه تغییری در آن‌ها جلوگیری شود.[4]

طبقه‌بندی ادله فرایندی است که بر اساس آن ویژگی‌هایی کشف می‌شود و می‌تـوان از آن‌ها جهت بیان موضوعات کلی استفاده کرد و آن را از میان نمونه‌های مشابه تمیز داد. زمانی یک موضوع طبقه‌بندی‌شده محسوب می‌شود که بتـوان آن را در طبقـه‌ای

1.handhelds
2.Floppy Disks
3.Zip
۴- کیسی، اوئن؛ دلایل دیجیتال و جرم رایانه‌ای (علم قانونی، رایانه‌ها و اینترنت)، ۹۱۴۱، مترجمـان امیرحسـین جلالـی فراهـانی و علـی شایان، تهران، نشر سلسبیل، ص ۷۰

از موضوعات با ویژگی‌های مشابه قرار داد[1]. در حوزه ادله الکترونیک، به‌عنوان‌مثال اکثر افراد با پست الکترونیک آشنایی دارند و می‌توانند به‌راحتی آن را شناسایی کنند؛ اما مجریان قانون و بخصوص پلیس باید قدری فراتر روند و بتوانند پس از کسب آموزش‌های لازم، پست‌های الکترونیک را بر اساس موضوعات دقیق‌تری طبقه‌بندی و حتی مشخص کنند که با کدام برنامه ایجادشده است.

یکی از مزایای بزرگ طبقه‌بندی ادله الکترونیک، احراز هویت پدیدآورندگان آن است. بااینکه این کار مشکل است، اما می‌تواند بسیار مفید واقع شود. همچنین برای بازسازی جرم نیز کارساز واقع می‌شوند؛ زیرا جزئیات قابل‌اعتماد بیشتری را فراهم می‌کند. بااینکه فرایند طبقه‌بندی، مقایسه و ماهیت‌انگاری ادله الکترونیک طاقت فرساست، اما در ارزیابی دقیق و مفصل آن‌ها از اهمیت خاصی برخوردار است. چنانچه این اقدامات به شایستگی اجرا شود، با احتمال بیشتر به کشف نشانه‌هایی هرچند جزئی از پیوند اساسی با موضوع موردنظر منتهی می‌شود. همچنین، این فرایندها می‌توانند در تبیین هر چه‌بهتر ادله در محضر دادگاه نقش حساسی ایفا کنند.[2]

نکته دیگر اینکه در قوانین اکثر کشورها برای توقیف داده‌ها و سیستم‌های رایانه‌ای سقف زمانی تعیین‌شده است. در این راستا ماده‌ی ۶۸۱ قانون آیین دادرسی کیفری به این موضوع اختصاص‌یافته که مطابق آن قاضی موظف شده: در مهلت متناسب و متعارف نسبت به موارد توقیف تعیین تکلیف کند. گرچه به نظر می‌رسد اگر قانون‌گذار به‌جای عبارت مذکور که ضابطه و معیار مشخصی ندارد، یک مهلت قانونی تعیین می‌کرد، با اختیار تمدید مهلت در صورت ضرورت از سوی قاضی با در نظر گرفتن حق اعتراض از سوی متضرر نسبت به اقدام قاضی حقوق متهم بهتر تضمین می‌شد.

مواد ۶۶۴ و ۶۶۵ آ.د.ک به صلاحیت دادگاه‌های ایران در رسیدگی به جرایم سایبری با توجه به اصول صلاحیت حمایتی، شخصی، سرزمینی و جهانی پرداخته که بزه

---

۱. همان، ص ۸۷

۲. جلالی فراهانی، امیرحسین؛ درآمدی بر آیین دادرسی کیفری جرایم سایبری، ص ۲۴۵

دیدگان مصرح در بندهای الف، ب، پ، ت ماده ۶۶۴ می‌توانند به دادگاه‌های ایران جهت رسیدگی به جرایم وقوع پیوسته مراجعه نمایند، لذا صرف‌نظر از ایرادات و اشکالاتی که به این بخش از آیین دادرسی جرایم رایانه‌ای مطرح است، آنکه مقنن در بند «ت» ماده ۶۶۴ صرفاً به جرایم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از ۱۸ سال، اعم از اینکه بزه‌دیده یا مرتکب ایرانی یا غیر ایرانی در ایران یافت شود، پرداخته است. درحالی‌که جا داشت با توجه به موارد صلاحیت جهانی محاکم در رسیدگی جرایم بین‌المللی مانند جرایم علیه بشریت، جنایات جنگی، نسل‌کشی و ... چنانچه جرایم رایانه‌ای منتهی به جرایم بین‌المللی مذکور شود، موردتوجه قرار می‌گرفت و صرفاً به یکی از موارد صلاحیت جهانی که اشخاص زیر ۱۸ سال است موردتوجه قرار نگیرد تا از این حیث امکان حمایت از بزه دیدگان سایبری در صورت تحقق جرایم بین‌المللی نیز فراهم شود و آنچه راجع به صلاحیت دادگاه‌های ایران در رسیدگی به جرایم حاصل از بند «ب» ماده ۶۶۴ مطرح می‌شود هم خالی از ایراد و سؤال نیست. لذا چنانچه بزه دیدگان جرم ارتکابی از طریق تارنماهای دارای دامنه مرتبه بالای کد کشور ایران (.ir) ارتکاب یابد تبعه‌های کشورهای خارجی باشند، مشخص نیست رویکرد مقنن و دادگاه‌های ایران در رسیدگی به شکایات بزه دیدگان سایبری ساکن در کشورهای دیگر چگونه است. برفرض اینکه از طریق تارنماهای ایران جرمی انجام شود که بزه دیدگان آن هزاران نفر خارجی باشند. آیا مقنن ایران تمایلی به رسیدگی به این جرایم دارد یا خیر؟ که پاسخ این سؤال با توجه به رویه قضایی کشورمان از این حیث منفی است.

اقدام حمایتی دیگر این قانون را می‌توان حفظ داده‌ای رایانه‌ای یا سامانه‌های رایانه‌ای و مخابراتی دانست که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد که این حمایت از حمایت‌های تبعی از بزه دیدگان مطرح است و برای تحقیق و دادرسی، لازم و ضروری است، از سوی مقام قضایی دستور حفاظت یا توقیف و تفتیش آن‌ها صادر شود و چنانچه ضابطان قضایی، کارکنان دولت یا اشخاصی که وظیفه حفاظت داده‌ها بر آن‌ها سپرده‌شده خودداری یا آن‌ها را افشا نماید، مطابق مواد ۶۶۹و ۶۷۰ و ۶۷۱ مستوجب مجازات خواهد بود. این امر مبین آن است که

مقنن در حفظ حقوق بزه دیده سایبری از حیث جمع‌آوری و نگهداری ادله جرم و شناسایی مجرمین اهمیت به‌سزایی قائل است.

در پایان باید به ماده‌ی ۶۸۷ قانون آیین دادرسی کیفری اشاره کرد که مقرر داشته، در رسیدگی به جرایم رایانه‌ای درجایی که در این بخش (بخش دهم- آیین دادرسی جرایم رایانه‌ای) مقررات خاصی از جهت آیین دادرسی پیش‌بینی‌نشده باشد، مطابق مقررات عمومی آیین دادرسی کیفری عمل خواهد شد. درواقع این ماده در موارد سکوت بخش دهم، سایر مواد قانون آیین دادرسی کیفری را حاکم دانسته است.

می‌توان گفت سایر مقررات آ.د.ک در بسیاری از موارد از جرایم رایانه‌ای که مقرره‌ای ندارند، مثل کشف جرم و تحقیقات مقدماتی، قابل‌اجرا و لازم الرعایه است که بدین ترتیب ملاحظه می‌شود که مقنن کشورمان در تدوین قانون جرایم رایانه‌ای توجه چندانی به بزه دیدگان جرایم سایبری نداشته است.[1]

امریکا

دو قانون مصوب فدرال، بر نظارت زندهٔ الکترونیکی[2] در تحقیق‌های کیفری فدرال حکومت دارند. نخستین و مهمترین قانون، قانون استراق سمع[3] است (مواد ۲۵۱۰ تا ۲۵۲۲ عنوان ۱۸) که در ابتدا با عنوان «عنوان سوم» از مجموعه قوانین کنترل جرایم و خیابان‌های بی‌خطر[4] (که عموماً با «عنوان سوم» شناخته می‌شود) مطرح شد. دومین قانون، قانون نحوهٔ استفادهٔ از ابزار ثبت‌کننده، تله‌گذار و ردیاب است که در مواد ۳۱۲۱ تا ۳۱۲۷ عنوان ۱۸ آمده که بر نحوهٔ استفاده ازاین‌گونه ابزارها حکومت دارد. قصور در رعایت این‌گونه قوانین می‌تواند به ایجاد مسئولیت‌های کیفری و حقوقی و حتی مطابق عنوان سوم به عدم پذیرش ادله به دست آمده هم منجر شود. در ادامه به بررسی هریک از این قوانین به‌طور جداگانه می‌پردازیم.

قانون نحوهٔ استفاده از ابزار ثبت‌کننده، تله‌گذار و ردیاب

قانون نحوهٔ استفاده از ابزار ثبت‌کننده، تله‌گذار و ردیاب، درباره مجموعه اطلاعات

---

۱. اسلامی، ابراهیم، جایگاه حمایت از بزه دیدگان جرایم سایبری در مقررات کیفری حقوق داخلی و بین‌المللی، پژوهشنامه حقوق اسلامی، سال هفدهم، ش ۱، بهار و تابستان ۱۳۹۵، ص ۱۷۷ و ۱۷۸

2. Real-Time Electronic Surveillance
3. Wiretap Statute
4. The Omnibus Crime Control and Safe Streets Act of 1968

آدرس‌ده و سایر اطلاعات غیر از محتوای ارتباطات الکترونیکی و سیمی است. قانون نحوهٔ استفاده از ابزارهای ثبت‌کننده، تله‌گذار و ردیاب بر مجموعهٔ زندهٔ اطلاعات آدرس‌ده و غیر از محتوای این‌گونه ارتباطات حکومت دارد. شماره (۱) بند «ح» ماده ۲۵۱۱ عنوان ۱۸ مقرر می‌دارد استفاده از ابزار ثبت‌کننده، تله‌گذار و ردیاب نقض عنوان سوم (قانون استراق سمع) محسوب نمی‌شود.

این قانون به دادستان[1] اجازه می‌دهد از دادگاه درخواست کند جهت نصب ابزار ثبت‌کننده یا تله‌گذار دستور لازم را صادر کند تا اطلاعاتی که احتمال می‌رود با تحقیق کیفری آتی مرتبطند، به دست آیند.[2] به عبارت دقیق‌تر، ابزار ثبت‌کننده اطلاعات خروجی آدرس‌ده را (مانند شماره‌ای که با تلفن تحت نظارت گرفته می‌شود) ثبت می‌کند و ابزار تله‌گذار و ردیاب، سوابق مربوط به اطلاعات آدرس‌ده ورودی را ثبت می‌کند (مانند اطلاعات هویت تماس‌گیرنده). در سال ۲۰۰۱، قانون پاتریوت تصریح کرد این قانون سطح وسیعی از فناوری‌های ارتباطات را دربرمی‌گیرد. قانون نحوهٔ استفاده از ابزارهای ثبت‌کننده، تله‌گذار و ردیاب، از این ابزارها تعریف گسترده‌ای ارائه داده است. همانگونه در بند سه ماده ۳۱۲۷ آمده، «ابزار ثبت‌کننده»[3] عبارت است از «دستگاه یا فرایندی که اطلاعات مربوط به شماره‌گیری، مسیریابی، آدرس‌دهی یا نشانه‌گذاری اطلاعات جابه‌جاشده بوسیلهٔ ابزار یا امکاناتی که از طریق آن ارتباطات سیمی یا الکترونیکی جابه‌جا می‌شود یا برای جابه‌جایی فراهم آمده است را ثبت یا رمزگشایی می‌کند. بااین‌حال، این‌گونه اطلاعات شامل محتوای آن ارتباطات نخواهد بود».

این تعریف، دستگاه‌ها یا فرایندهای بکار رفته در تهیهٔ صورت‌حساب یا محاسبهٔ هزینه‌ها را از شمول آن خارج می‌کند.[4] این قانون «ابزارهای تله‌گذار و ردیاب»[5] را این‌گونه تعریف می‌کند: «ابزار یا فرایندی که ارتعاش‌های الکترونیکی یا سایر ارتعاش‌های ورودی را دریافت و از طریق آن اطلاعات مربوط به شماره مبدأ یا سایر

---

1. Government Attorney
2. 18U.S.C.3122(b)(2)
3. Pen Register
4. 18U.S.C.3127(3)
5. Trap and Trace Devices

شماره تماس‌ها، مسیریابی، آدرس‌دهی یا نشانه‌گذاری را شناسایی می‌کند، به گونه‌ای که احتمال متعارف وجود دارد که آن اطلاعات منبع ارتباطات الکترونیکی یا سیمی را شناسایی می‌کنند. بااین‌حال، این اطلاعات شامل محتوای ارتباطات نمی‌شوند».[1]
ازآنجاکه سرصفحه‌های اینترنت هر دو نوع اطلاعات «به» و «از طرف» را دارند، دستگاهی که تمامی سرصفحه را می‌خواند (به جز موضوع ارتباط که در سرصفحه‌های رایانامه درج شده است) به راحتی به‌عنوان یک ابزار ثبت‌کننده، تله‌گذار و ردیاب شناخته می‌شود.

دستورهای ابزارهای ثبت‌کننده و ردیاب: درخواست، صدور، اجرا و گزارش

برای اخذ دستور استفاده از ابزار ثبت‌کننده و ردیاب، درخواست‌کنندگان باید خودشان و مجریان قانون اِجراکنندهٔ تحقیق را معرفی کنند و سپس اطمینان دهند که معتقدند اطلاعاتی که احتمالاً به دست می‌آید، با تحقیق کیفری آتی مأموران مرتبط خواهد بود[2]. دادگاه صادرکنندهٔ دستور نیز باید نسبت به جرم تحت تحقیق صلاحیت داشته باشد[3]؛ بنابراین تا جایی که این درخواست شامل این عناصر شود، دادگاه اجازه خواهد داد آن ابزارها در هر جایی از ایالات‌متحده نصب و بکار گرفته شوند[4]. دادگاه هیچگونه بررسی قضایی مستقلی را جهت تأیید مدارک گواهی‌شده انجام نخواهد داد.
دستور قضایی فدرال مبنی بر استفاده از ابزار ثبت‌کننده و ردیاب، می‌تواند بر خارج از حوزه تحت اختیار دادگاه صادرکننده اثر بگذارد. درجایی که درخواست‌کننده مأمور فدرال است، این دستور «نسبت به هر شخص حقیقی یا حقوقی ارائه‌دهنده خدمات ارتباطی الکترونیکی یا سیمی واقع در ایالات‌متحده که معاضدت آن می‌تواند اجرای دستور را تسهیل کند، قابلیت اجرا دارد».[5] برای مثال، مقام تعقیب فدرال می‌تواند برای ردیابی مکالمه‌های تلفنی انجام‌شده با یک تلفن ویژه دستوری اخذ کند. این دستور صرفاً حامل[6] محلی آن خط را مخاطب قرار نمی‌دهد، بلکه سایر ارائه‌دهندگانی

---

1. 18U.S.C.3127(4)
2. 18U.S.C.3122(b)(1)-(2)
3. 18U.S.C.3127(2)(a)
4. 18U.S.C.3123(a)(1)
5. 18U.S.C.3123(a)(1)
6. Carrier

ارائه‌دهندگانی را هم دربرمی‌گیرد که مکالمه‌ها از آن‌ها عبور می‌کند تا به تلفن موردنظر برسند (مانند حامل‌های محلی و راه‌دور بخشی از کشور). به‌طور مشابه، در چارچوب اینترنت نیز مقام تعقیب فدرال می‌تواند دستور ردیابی اطلاعات به رایانه قربانی موردنظر یا آدرس IP وی را اخذ کند. اگر هکری ارتباطات را از طریق زنجیره‌ای از رایانه‌های واسطه مسیریابی می‌کند، دستور صادره درباره تک‌تک رایانه‌های این زنجیره، از رایانه قربانی تا منبع ارتباطات، لازم‌الاجرا خواهد بود.

قانون ابزارهای ثبت‌کننده و ردیاب مقرر نکرده که در درخواست تنظیمی یا دستور صادره باید کلیه ارائه‌دهندگان مخاطب دستور مشخص شوند، اگرچه لازم است ارائه‌دهنده نخست مشخص شود.[1] برای جلب معاضدت ارائه‌دهنده، مأمور تحقیق فقط موظف است دستور را ابلاغ کند. همچنین، طبق درخواست ارائه‌دهنده، مجریان قانون باید «گواهی کتبی یا الکترونیکی» تهیه کنند که نشان دهد آن دستور نسبت به آن ارائه‌دهنده اجرا می‌شود.[2] برای اجرای این فرایند نسبتاً غیررسمی، انگیزه‌های عملی راسخی وجود دارد. زمانی که مقام‌های تعقیب درخواست صدوردستور نصب ابزارهای ثبت‌کننده، تله‌گذار و ردیاب را مطرح می‌کنند، معمولاً از هویت ارائه‌دهندگانی که در زنجیرهٔ ارتباطات قرار می‌گیرند و مشمول دستور می‌شوند، بی‌اطلاعند. اگر قرار باشد پس از شناسایی هر یک از آن‌ها به دادگاه مراجعه کنند و دستور جدیدی اخذ کنند، با تأخیر زیادی در تحقیق مواجه خواهند شد.

دستور صادره می‌تواند استفاده از این ابزارها را تا ۶۰ روز تجویز کند و می‌توان آن را برای دوره‌های شصت روزه تمدید کرد.[3] همچنین، دادگاه به ارائه‌دهنده دستور می‌دهد که وجود ابزار ثبت‌کننده، تله‌گذار و ردیاب را برای هیچکس فاش نکند، تا وقتی که دستور دیگری از جانب دادگاه صادر شود.[4] ممکن است به ارائه‌دهندگان خدمات ارتباطات الکترونیکی یا سیمی، صاحبان املاک، نگهبانان یا سایر اشخاص دستور داده شود که بی‌درنگ تمامی اطلاعات، امکانات و معاضدت فنی ضروری را

---

1. 18U.S.C.3123(b)(1)(A)
2. 3123(a)(1)
3. 18U.S.C.3123(c)
4. 18U.S.C.3123(d)(2)

برای مأموران فراهم آورند تا جهت نصب این‌گونه ابزارها به کار برند.[1] ارائه‌دهندگانی که مخاطب دستور قرار می‌گیرند و ملزم می‌شوند جهت نصب ابزارهای ثبت‌کننده و ردیاب معاضدت کنند، مطابق ماده ۳۱۲۴ می‌توانند میزان متعارفی از هزینه‌هایی که در جهت فراهم آوردن تسهیلات یا معاضدت فنی متحمل شده‌اند را از مجریان قانون مطالبه کنند.[2] حسن نیت ارائه‌دهنده نسبت به دستور دادگاه می‌تواند در برابر هرگونه دعوای کیفری یا حقوقی اقامه شده به دلیل معاضدتش بر اساس دستور صادره، دفاع تمام عیاری محسوب شود.[3]

همچنین، قانون ابزار ثبت‌کننده و ردیاب به ارائه‌دهندگان خدمات ارتباطی الکترونیکی یا سیمی این صلاحیت وسیع را می‌دهد که از ابزارهای مزبور در شبکهٔ خودشان بدون اخذ دستور دادگاه استفاده کنند. بند «ب» ماده ۳۱۲۱ مقرر می‌کند در موارد ذیل ارائه‌دهندگان می‌توانند از ابزارهای مزبور بدون دستور دادگاه استفاده کنند:

۱. استفاده ازاین‌گونه ابزارها با کارکرد، نگهداری و ارزیابی خدمات ارتباط الکترونیکی یا سیمی مرتبط یا برای حفظ حقوق یا اموال ارائه‌دهنده یا جهت حفظ کاربران از سوءاستفاده یا استفادهٔ غیرقانونی از خدمات لازم باشد؛ یا

۲. ضبط رویدادهای مربوط به آغاز یا پایان ارتباطات الکترونیکی یا سیمی جهت حفاظت از ارائه‌دهنده خدمات، سایر ارائه‌دهندگانی که در راستای تکمیل ارتباطات سیمی عمل می‌کنند یا کاربران آن خدمات، در برابر فعالیت‌های متقلبانه، سوءاستفاده یا استفاده‌های غیرقانونی از آن خدمات لازم باشد؛ یا

۳. زمانی که از کاربر آن خدمات رضایت اخذ شده باشد.[4]

قانون استراق سمع

از زمان تصویب عنوان سوم در سال ۱۹۶۸ و اصلاح آن در سال ۱۹۸۶، چارچوب قانونی فراهم آمده که بر نظارت زندهٔ الکترونیکی محتوای ارتباطات حکومت دارد.

---

1. 18U.S.C.3124(a), (b)
2. 3124(c)
3. 18U.S.C.3124(d), (e)
4. 3121(b)

زمانی که مأموران قصد استراق سمع تلفن متهم را دارند، «ضربه به صفحه کلید رایانه»[1] توسط هکری که به سیستم رایانه‌ای نفوذ کرده را کنترل می‌کنند، یا اینکه پیامدهای شنود شهروندی که دلایل ارتکاب جرم را کشف کرده می‌پذیرند، باید ابتدا به مضامین عنوان سوم توجه کنند.

چارچوب عنوان سوم به‌طور شگفت‌انگیزی ساده است. تدوین‌کنندگان قانون تصور می‌کردند هر ارتباط خصوصی را می‌توان بر مبنای مدل تماس دوطرفه بین دو شرکت‌کنندهٔ در آن درنظرگرفت، مانند ارتباط تلفنی بین «الف» و «ب»؛ اما اساساً این قانون اشخاص ثالثی که عضوی از ارتباط خصوصی محسوب نمی‌شوند (مانند مجریان قانون) را از شنود آنچه میان کاربران ابزارهای «الکترونیکی، مکانیکی یا سایر ابزارها»، برقرار است منع می‌کند، مگر اینکه یکی از چند استثنای قانونی قابلیت اجرا داشته باشد.[2] این ممنوعیت کاملاً گسترده است. برخلاف بعضی قوانین حریم خصوصی که تنها مقررات خود را به برخی موارد یا مکان‌های ویژه محدود می‌کنند، عنوان سوم به‌طور گسترده این‌گونه استراق سمع‌ها را (با توجه به برخی استثناها و شرایط داخلی) برای هر شخصی در هر نقطه از ایالات‌متحده منع می‌کند. مأموران تحقیق که قصد نظارت بر منزل، محل کار، ادارات دولتی، زندان یا اینترنت را دارند، باید اطمینان دهند که نظارتشان با رعایت ممنوعیت‌های عنوان سوم است.

عنوان سوم به‌طور گسترده «شنود»،[3] «ارتباطات شفاهی»،[4] «ارتباطات سیمی»[5] و «ارتباطات الکترونیکی»[6] را منع می‌کند. تعاریف این واژگان در قانون آمده است.[7] در در پرونده‌های جرایم رایانه‌ای، مأموران ومقام های تعقیبی که طرح نظارت الکترونیکی را می‌ریزند، باید تعاریف «ارتباطات سیمی»، «ارتباطات الکترونیکی» و «شنود» را کاملاً درک کنند.

---

1. Key Stroke
2. 2511(1)
3. Interception
4. Oral Communication
5. Wire Communication
6. Electronic Communication
7. 18U.S.C.2510

الف) ارتباطات سیمی

به‌طورکلی، مکالمه‌های تلفنی، ارتباطات سیمی محسوب می‌شوند.

مطابق قسم نخست ماده ۲۵۱۰، واژهٔ «ارتباطات سیمی» این‌گونه تعریف شده است: «هرگونه جابه‌جایی شنیداری که تمام یا قسمتی از آن با امکانات جابه‌جایی ارتباطات سیمی، سیمی یا سایر تماس‌های مشابه بین مبدأ و مقصد موردنظر صورت می‌گیرد (و شامل استفاده ازاین‌گونه تماس‌ها در ایستگاه سوئیچینگ هم می‌شود) و توسط ارائه‌دهنده یا متصدی این‌گونه امکانات برای جابه‌جایی ارتباطات داخلی یا خارجی یا برای ارتباطات مؤثر بر تجارت داخلی یا خارجی فراهم‌شده یا به اجرا درآمده است».

ب) ارتباط الکترونیکی

بیشتر ارتباطات اینترنتی (مانند رایانامه)، ارتباطات الکترونیکی محسوب می‌شوند.

بند (۱۲) ماده ۲۵۱۰، ارتباطات الکترونیکی را این‌گونه تعریف می‌کند: «هر نوع نشانه، سیگنال، نوشته، تصویر، صوت، داده یا اطلاعات محرمانه با هر ماهیتی که تمام یا قسمتی از آن‌ها از طریق سیم، سیستم رادیویی، الکترومغناطیسی، نوری- الکترونیکی، نوری- سنتزی جابه‌جا می‌شود و بر تجارت داخلی یا خارجی تأثیر دارد، اما شامل موارد زیر نمی‌شود: ۱. هرگونه ارتباطات سیمی یا شفاهی؛ ۲. هرگونه ارتباطاتی که در دستگاه پیج[1] صرفاً صوتی به وجود آمده باشد؛ ۳. هرگونه ارتباطی که در دستگاه ردیاب ایجاد شده باشد؛ یا ۴. جابه‌جایی وجوه ذخیره‌شده توسط موسسهٔ مالی در سیستم ارتباطی که برای ذخیرهٔ الکترونیکی و جابه‌جایی وجوه بکار می‌رود».

پ) شنود

بند چهار ماده ۲۵۱۰ «شنود» را چنین تعریف کرده است: «هرگونه دستیابی شنیداری یا غیر آن به محتوای ارتباطات شفاهی، الکترونیکی یا سیمی از طریق استفاده از هرگونه ابزار الکترونیکی، مکانیکی یا غیر آن را می‌گویند». عنوان سوم در سطح گسترده‌ای هرگونه شنود، استفاده یا افشای عمدی ارتباطات سیمی و

---

1. Tone-Only Paging Device

الکترونیکی را منع کرده است، مگر اینکه استثنای قانونی وجود داشته باشد.[1] به‌طورکلی، این‌گونه ممنوعیت‌ها اشخاص ثالث (که شامل دولت نیز می‌شود) را از استراق سمع تلفن‌ها و نصب «اسنیفر» های الکترونیکی که ترافیک اینترنتی را می‌خوانند، بازمی‌دارد.

در جرایم رایانه‌ای، غالباً هفت استثنا قابلیت اجرا دارد:

۱. شنود مطابق دستور دادگاه؛[2]
۲. استثنای «رضایت»؛[3]
۳. استثنای «ارائه‌دهنده خدمات»؛[4]
۴. استثنای «ورود به عنف به رایانه»[5]؛[6]
۵. استثنای «تلفن داخلی»[7]؛[8]
۶. استثنای «تحصیل غیرارادی ادله جرم»؛[9] و
۷. استثنای «در دسترس عموم بودن».[10]

عنوان سوم به مجریان قانون اجازه می‌دهد متعاقب دستور دادگاه که مطابق ماده ۲۵۱۸ صادرشده، ارتباطات سیمی و الکترونیکی را شنود کنند (دستور عنوان سوم). جهت درخواست شنود ارتباطات سیمی در سطح فدرال مطابق عنوان سوم، به تاییدیه مقام عالی وزارت دادگستری نیاز است و درباره ارتباطات الکترونیکی (به‌جز پیجرهای رقمی) به‌موجب رویه‌ی وزارت دادگستری عمل می‌شود. چنانچه شنود توسط وزارت دادگستری تأیید شد و به امضای دادگاه ناحیه یا دادگاه تجدیدنظر ایالات‌متحده رسید، دستور صادره مطابق عنوان سوم به مجریان قانون اجازه شنود ارتباطات را تا سی روز می‌دهد.

مواد ۲۵۱۶ تا ۲۵۱۸ چندین شرط لازم‌الاجرا را تحمیل می‌کنند تا مأموران تحقیق

---

1. 18U.S.C.2511(1)
2. 18U.S.C. 2518
3. 18U.S.C.2511(2)(c)-(d)
4. 18U.S.C.2511(2)(a)(i)
5. Computer Trespass
6. 18U.S.C.2511(2)(i)
7. Extension Telephone
8. 18U.S.C.2510(5)(a)
9. 18U.S.C.2511(3)(b)(iv)
10. 18U.S.C.2511(2)(g)(i)

پیش از اخذ دستور عنوان سوم آن را رعایت کنند. به لحاظ اهمیت فوق‌العاده موضوع، در درخواست صدور این دستور باید سبب محتملی ارائه شود که شنود، دلایل مربوط به جرم جنایی سابق[1] را که فهرست آن در ماده ۲۵۱۶ آمده آشکار می‌کند.[2]

نتیجه‌گیری

جرم سایبری ماهیت جرایم کلاسیک را متحول کرده است. این جرایم دارای ماهیت فنی یا به‌عبارت‌دیگر دارای ماهیتی ناشی از پیشرفت فنّاوری مدرن هستند. همین ماهیت فنی بر تفسیر برخورد با جرم تأثیر می‌گذارد. جرایم کلاسیک در حالت رایانه‌ای از سویی به‌واسطه تغییر در توصیف حالت کلاسیک دچار تحول شده‌اند و از سوی دیگر برخی اشکال ارتکابی به دلیل عدم انطباق با توصیف‌های کلاسیک مجرمانه، اعمال مجرمانه جدیدی را ایجاد کرده‌اند. از طرفی این‌یک واقعیت گریزناپذیر است که بزهکاری در حال پیشرفت است و ما هرروز با گونه‌های جدید آن مواجه می‌شویم و از بارزترین این جرایم، جرایم سایبری (رایانه‌ای) است.

وجود قوانین آیین دادرسی کیفری در زمینه جرایم رایانه‌ای در دنیای امروز بسیار ضروری است چراکه قوانین دادرسی کیفری هر کشور، معرّف میزان رشد و پیشرفت آن جامعه درراه تحقق بخشیدن به حقوق و ارزش‌های انسانی و حمایت از آن‌هاست.

از منظر جرم‌انگاری، پاسخ جدی به جرایم سایبری را می‌توان در قانون کنترل فراگیر مصوب ۱۹۸۴ در ایالت متحده نام برد. اصلاحاتی که در قانون آیین دادرسی این کشور در همین سال‌ها صورت گرفت گام رو به جلویی در جهت جرم‌انگاری جرایم سایبری بود. همچنین، جرایم سایبری در آمریکا به‌طور جداگانه در قوانین مختلف با عناوین مختلف تصویب‌شده است. ازجمله قانون استراق سمع، قانون حریم ارتباطات الکترونیکی و قانون حریم خصوصی در مرحله کشف این جرایم، قانون نحوه‌ی استفاده از ابزار ثبت کننده، تله‌گذار و ردیاب که در مرحله تحقیق از انواع مختلف جرایم مورداستفاده قرار می‌گیرد.

---

1. Predicate Felony Offense
2. 2518(3)(a)-(b)

رجوع به موادِ قانون آیین دادرسی کیفری در راستای پـر کـردنِ خـلأِ ناشـی از مـواد شکلیِ قانون جرایم رایانه‌ای نیز نتوانسته راهگشایِ تمامیِ مسائلِ مربوطه باشد. البتـه در کنار مواد قانون آیین دادرسی کیفری مصوب ۱۳۹۲ فصلی به آیین دادرسی ویـژه جرایم رایانه‌ای اختصاص داده‌شده که گام تأثیرگذاری در این زمینـه اسـت و ایـن در حالی است که با ماهیت و ویژگی‌های این‌گونـه جـرایم، تشـریفاتِ خاصـی در جهـتِ شناسایی، کشف، پیگیری، تحقیقات مقدماتی و رسیدگی به آن‌ها را می‌طلبد.

آیین دادرسی کیفری به‌عنوان یکی از شاخه‌های حقوق جزا در اثر پیـدایش فنـاوری اطلاعات دچار چالش‌های شدیدی شده است. یکی از مسائل آیین دادرسـی کیفـری در ارتباط با جرایم مرتبط با فنـاوری اطلاعـات در زمینـه تحقیقـات مقـدماتی بـروز می‌کند، زیرا مقامات تعقیب و تحقیق ناچارند برای کشف جرم و تحقیق در خصـوص جرایم مرتبط با فناوری اطلاعات به جمع‌آوری داده‌های ذخیره‌شده یا پـردازش‌شـده در سیستم‌های رایانه‌ای و محیط‌های مجـازی بپردازنـد. ایـن کـار مسـتلزم ورود بـه سیستم‌های رایانه‌ای، بازرسی در محیط مجازی، توقیف داده‌ها و برنامه‌هـای رایانـه‌ای است. البته تفتیش و توقیف و جمع‌آوری داده‌های رایانه‌ای که به‌طـور دایـم در یـک محیط مادی حامل داده مانند CD و دیسکت ذخیـره مـی‌شـوند، در اکثـر کشـورها مسائل جدیدی به وجود نمی‌آورد، اما اعمال مقررات مربوط به ضبط و بازرسی اشـیاء و موضوعات ملموس و قابل‌رؤیت، نسبت به مواردی که داده‌ها برای همیشـه در یـک محیط مادی حامل داده، ذخیره نشده و نسبت به داده‌های آنلاین مشکلاتی را ایجـاد نموده است؛ زیرا داده‌ها یا اطلاعات رایانه‌ای محض در محیط مجازی یا سـایبر، دارای خصایص و ویژگی‌هایی هستند که با خصایص و ویژگـی‌هـای یـک شـیء ملمـوس و مادی، متفاوت است.

به‌کارگیری فناوری رایانه، نه‌تنها راه‌های نوینی برای ارتکاب جـرم و سـوء اسـتفاده از فضای سایبر به روی مجرمین گشوده، بلکه مشکلات جدیدی درزمینه آیین رسیدگی کیفری و به‌کارگیری مدارک و دلایل الکترونیکی ناشی از آن‌ها در فرایند کیفـری بـه وجود آورده است؛ زیرا با تولید و جـایگزینی مـدارک و دلایـل الکترونیکـی بـه‌جـای مدارک و دلایل سنتی که از ویژگی‌هایی نظیـر غیرقابـل رؤیـت و غیرملمـوس بـودن

برخوردار هستند، مشکلات زیادی برای مقامات پلیسی و قضایی از حیث کشف، شناسایی، تفتیش و بازرسی، توقیف، گردآوری، حفظ و نگهداری ادله الکترونیکی در فرایند کیفری به وجود آورده است؛ بنابراین ویژگی‌های ادله ناشی از فناوری اطلاعات و مشکلات ناشی از آن سبب شده که موانعی برابر استناد پذیری ادله الکترونیکی به وجود آید.

برای کشف این‌گونه جرایم و جمع‌آوری دلایل راجع به آن‌ها، بازرسی و تفتیش رایانه‌ها و توقیف محتویات آن‌ها ضرورت می‌یابد و نهایتاً مقامات قضایی ناچارند در خصوص صحت‌وسقم و قابلیت یا عدم قابلیت استناد پذیری محتویات رایانه‌ای که ادله الکترونیک نامیده می‌شوند، اظهارنظر نمایند. ادله دیجیتال ارائه‌شده از سوی ضابطین و مقامات تعقیب در صورتی قابل استناد است که علاوه بر مقررات مندرج در قوانین، زنجیره حفاظتی نیز در مورد آن‌ها رعایت شده باشد و همان‌طور که گفتیم منظور از زنجیره حفاظتی، ثبت کلیه اقداماتی است که ضابطین دادگستری و سایر اشخاص دست‌اندرکار، به‌موجب قانون و با به‌کارگیری ابزارها و روش‌های استاندارد در مراحل شناسایی، کشف، جمع‌آوری، مستندسازی، تجزیه‌وتحلیل، حفظ و مراقبت از ادله دیجیتال و ارائه آن‌ها به دادگاه اجرا می‌شوند.

بنابراین، مجریان قانون باید امکان‌سنجی و نیازسنجی ارکان مختلف نظام حقوق کیفری برای مواجهه با انواع تهدیدهای سایبری را جزء برنامه‌های اصلی خود قرار دهند. تردیدی نیست که آن‌ها تنها مرجع مجری قوانین و احکام کیفری هستند، لذا باید در امر جرم‌انگاری سایبری یا اصلاح قوانین فعلی، حضور فعالی داشته باشند تا از بروز خلأها و نارسایی‌هایی که آشکارا لمس می‌کنند، جلوگیری کنند و فرصت مغتنمی برای مجریان قانون فراهم شود تا مشارکت جدی‌شان را به نمایش بگذارند؛ زیرا هرگونه تحدید یا توسیع در ضوابط حمایتی این حوزه، تأثیر مستقیمی بر نحوه عملکردشان خواهد داشت.

نظام کشف علمی جرایم سایبری نیز جزء وظایف ذاتی مجریان قانون است و اساساً از هیچ مرجع حاکمیتی دیگری انتظار ورود و دخالت در آن نمی‌رود. با توجه به توضیحاتی که داده شد، این مجموعه چاره‌ای جز سرمایه‌گذاری زیربنایی در این

حوزه ندارد و باید تمامی ملزومات آن را از بنیان فراهم آورد؛ زیرا بـه نظـر نمـی‌رسـد امکان بهره‌گیری از امکانات و نیروهای سایر حوزه‌ها وجود داشته باشد. درعـین‌حـال، باید برای زیرشاخه‌های گوناگون فناوری‌های اطلاعاتی و ارتباطاتی چاره‌جویی اساسی شود. برای مثال، عملیات تحقیق در فضای شبکه‌ای با سیستم‌های رایانه‌ای مسـتقل، متفاوت و به نیروهای تخصصی ویـژه‌ای نیـاز دارد. در ایـن مرحلـه در حقـوق ایـران خلأهای قانونی فراوانی وجود دارد، اما الگـوبرداری از راهکارهـای موجـود در قـوانین فرانسه و آمریکا می‌تواند راهگشا باشد. برای نمونه در ایران نیز مانند فرانسه مـی‌تـوان گشت‌های اینترنتی با تصویب قانون مربوطـه بـه راه انـداخت، همچنـین مـی‌تـوان از سازوکاری که در قانون آیین دادرسی و قانون حمایت الکترونیک آمریکا بـرای صـدور قرار تفتیش و دستور دادگاه صورت می‌گیرد استفاده کـرد. از سـوی دیگـر گـردآوری اطلاعات الکترونیکی موردنیاز از سیستم‌های ارتباطات الکترونیکی گوناگون، مسـتلزم کسب مهارت‌های ویژه‌ای است. هرگونه کوتاهی در این امر موجب مـی‌شـود محـاکم کیفری در رسیدگی به جرایم مربوطه با مشـکل مواجـه شـوند. در ایـن مرحلـه نیـز استفاده از ابتکارهای موجود در قانون استراق سـمع و قـانون نحـوه اسـتفاده از ابـزار ثبت‌کننده، تله‌گذار و ردیاب آمریکا می‌تواند اثرات مطلوبی به‌جا بگذارد.

تمامی این اقدامات زمانی در رابطه با نظام حقوق کیفری سایبری کارایی و اثربخشـی لازم را خواهند داشت که در پرتو بین‌المللی و فرامرزی بودن این فضا، مورد ملاحظـه قرار گیرند. مجریان قانون باید به این باور برسـند کـه ازایـن‌پـس بخـش عمـده‌ای از عملیات اجرایی سایبری‌شان، خواسته یا ناخواسته، در تعامل با مجریـان قـانون سـایر کشورها سپری خواهد شد. نتیجه حتمی ایـن وضـعیت نـوین، رویـارویی نظـام‌هـای حقوقی مختلف خواهد بود که در این میان مجریان قانون وظیفه خطیر سازگارسـازی آن‌هـا بـا یکـدیگر و ایجـاد زمینـه مسـاعد بـرای توسـعه هرچـه بیشـتر همکـاری و معاضدت‌های دوجانبه یا چندجانبه را به عهده دارند. هرگونه قصور یـا تقصـیر و بـروز اختلافات و تعارض‌های گوناگون، تنها به نفع مجرمان سایبری تمام خواهد شد.

بااین‌حال، مقابله با این‌گونه ناهنجاری‌ها، به‌ویژه با توسل به ابزار کیفر، با دشواری‌هایی همراه است که عملاً نظام‌های حقوق کیفری را با بن‌بست مصیبت‌باری مواجـه کـرده

است. اگرچه حسب مورد، قوانین کیفری موردنیاز به تصویب رسیده، اما این نظام‌ها بهتر از هر کس می‌دانند تا چه اندازه قوانین‌شان جنبه بازدارندگی می‌یابند. لذا با توجه به وضعیت گریزناپذیر جامعه جهانی کنونی، چاره‌ای جز برنامه‌ریزی برای پیشگیری از وقوع هنجارشکنی‌های مجرمانه سایبری باقی نمی‌ماند. به‌ویژه آن‌که جهانیان آماج حملات جهانی قرارگرفته‌اند و هرگونه محدودیتی از پیش روی مجرمان و تحقق اهداف شومشان برداشته‌شده است.

با تشکیل و راه‌اندازی پلیس فتا، اقداماتی جدی در جهت رفع آسیب‌های سایبری و جرایم فضای مجازی صورت گرفته است. با توجه به نو پا بودن این پلیس، راهی بس طولانی و دشوار در پیش است تا این نهاد تازه تأسیس بتواند با توانمندی‌های اکتسابی، خود را آماده‌ی مبارزه و تقابل با جرایم سایبری کند. برای جلوگیری از بروز هرگونه جرایم سایبری، پلیس فتا باید راهکار پیشگیرانه را مدنظر قرار دهد.

پیشنهادها

۱. تصویب قانون برای تعریف و حمایت از برخی رایانه‌های دولتی، راهبردی و حائز اهمیت به‌عنوان رایانه محافظت‌شده و جرم‌انگاری هرگونه تعدی و تجاوز به آن؛

۲. بازنگری وضع قوانین موجود و ارزیابی کفایت قوانین ماهوی و شکلی زیربنای حقوقی و اداری و ارائه راه‌حل‌های مناسب؛

۳. تصویب قوانینی ساختارمند و منسجم جهت تعیین تکالیف و اختیارات قانونی پلیس فتا در مرحله‌ی پیشگیری؛

۴. ارتقای سطح همکاری سازمان‌ها در زمینه مبادله تجربیات و اطلاعات مربوط به تجارب قضایی و اجرایی قابل‌اعمال در پیشگیری و مبارزه با جرایم رایانه‌ای و سایبری؛

۵. تضمین بازنگری و اصلاح ادواری قوانین، سیاست‌ها و روش‌ها به‌منظور ملحوظ شدن تغییرات ناشی از توسعه و تحولات فنّاورانه در جرایم رایانه‌ای؛

۶. تصویب قوانینی برای مشروعیت‌بخشی جهت استفاده‌ی پلیس فتا از نرم‌افزارها و برنامه‌های آنالیز داده‌های الکترونیک به‌منظور نظارت بر فضای

سایبر؛

۷. ایجاد قرارهای احضاریه و تفتیش در کنار حکم دادگاه در قوانین ایران مشابه شیوه‌ای که در ایالات‌متحده‌ی آمریکا موجود است؛

۸. ایجاد مکانیسمی برای آموزش بزه دیدگان بالقوه جرایم رایانه‌ای؛

۹. به‌کارگیری تدابیر امنیتی اختیاری به‌وسیله کاربران در بخش خصوصی؛

۱۰. تصویب مجموعه موادی که استثنائات قانونی نظارت و شنود در فضای سایبر (مانند استثنائات مربوط به ارائه‌دهندگان خدمات دسترسی) را تعیین کند و موارد غیرازآن را جرم بداند.

منابع

- آشوری، محمد (۱۳۸۶)، مقدمه‌ای بر کتاب جرایم رایانه‌ای و اینترنتی جلوه‌ای نوین از بزهکاری، چ ۲، تهران، انتشارات بهنام.

- آیکاو، دیوید جی (۱۳۸۸)، راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای؛ ترجمه‌ی اکبر استرکی، محمد صادق روزبهانی، تورج ریحانی و راحله الیاسی، تهران، معاونت پژوهش دانشگاه علوم انتظامی.

- اسلامی، ابراهیم (۱۳۹۵)، جایگاه حمایت از بزه دیدگان جرایم سایبری در مقررات کیفری حقوق داخلی و بین‌المللی، پژوهشنامه حقوق اسلامی، سال هفدهم، ش ۱، بهار و تابستان.

- بابایی، محسن، شیروی، مهسا (۱۳۹۵)، حدود اختیارات در فرآیند پی‌جویی جرایم سایبری در حقوق ایران و انگلستان، مجموعه مقالات همایش ملی رویارویی با جرایم سایبری، ج ۱.

- صبح خیز، رضا (۱۳۹۴)، چالش‌های حقوقی جرایم سایبری در نظام حقوق بین‌الملل و نظام حقوقی ایران، فصلنامه‌ی پژوهش‌های اطلاعاتی و جنایی، سال دهم، شماره‌ی سوم، پاییز.

- عالی پور هفشجانی، خداداد (۱۳۹۰)، نقش پلیس در ارتباط با جرایم سایبری (تعقیب، کشف، پیشگیری)، دانشکده علوم انسانی، دانشگاه پیام نور مرکز تهران

- فریبرزی، الهام (۱۳۹۰)، سیر تحول قوانین مرتبط با جرایم رایانه‌ای در ایران و

جهان، فقه و تاریخ تمدن ملل اسلامی، بهار، شماره ۲۷
- کیسی، اوئن، دلایل دیجیتال و جرم رایانه‌ای (علم قانونی، رایانه‌ها و اینترنت)، مترجمان امیرحسین جلالی فراهانی و علی شایان، تهران، نشر سلسبیل.
- مارکو، گرکی (۱۳۸۹)، ترجمه‌ی اکبری، مرتضی، جرایم سایبری: راهنمایی برای کشورهای درحال‌توسعه، تهران، پلیس امنیت فضای تولید و تبادل اطلاعات (فتا)، چاپ اول.
- مراغی، علی‌اصغر، فرج دنیوی، حسن (۱۳۹۵)، اقدامات قانونی جهانی فعلی در برابر جرایم سایبری بامطالعه تطبیقی در حقوق ایران و آمریکا، مرکز همایش‌های پژوهشگاه نیرو، تیرماه.
- معین، محمد (۱۳۷۵)، فرهنگ فارسی (ج ۱)، چ ۲۲، تهران، انتشارات امیرکبیر.
- موذن زادگان، حسنعلی، شایگان، محمد رسول (۱۳۸۸)، استناد پذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران، فصلنامه دیدگاه‌های حقوقی، ش ۴۸، زمستان.
- وطنی، امیر؛ اسدی، حمید (۱۳۹۵)، سیاست جنایی جمهوری اسلامی ایران در جرایم سایبری با تأکید بر ویژگی‌های خاص این جرایم، پژوهشنامه حقوق اسلامی، سال هفدهم، شماره اول (پیاپی ۴۳)، بهار و تابستان.
-Department of Justice of the United States, 2002. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.*
-Electronic Communications Privacy Act (ECPA)
-Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008
-PATRIOT Act
-The Omnibus Crime Control and Safe Streets Act of 1968
-Wiretap Statute

تارنماها

-https://dictionary.cambridge.org/dictionary/english/cyberspace
-https://www.fbi.gov/investigate/cyber