توقیف داده و سامانه در جرایم امنیتی؛ چالش ها و معیارها

صادق تبریزی[1]، محمدرضا الهی منش[2]، حسن عالی پور[3]، جواد طهماسبی[4]

چکیده

جرایم امنیتی ماهیتی ترکیبی از منظر زمان تحقق رفتار جرم دارند. فرآیند سه مرحله‌ای اقدام اطلاعاتی، اقدام پلیسی و اقدام قضایی به نوبت، رفتارهای مجرمانه در آستانه وقوع، در حال وقوع و پس از وقوع را در بر می‌گیرد. با رایانه‌ای شدن جرایم ضد امنیت ملی خواه رایانه موضوع بزه باشد یا بستری برای تحقق جرایم امنیتی سنتی، اهمیت توقیف داده و سامانه برای اقدام‌های سه‌گانه اطلاعاتی، پلیسی و قضایی آشکار است؛ با این حال سه چالش عمده پیش‌روی توقیف داده و سامانه است؛ نخست اینکه توقیف داده و سامانه برای اقدام اطلاعاتی تا چه اندازه می‌تواند برای اقدام‌های پلیسی و قضایی کاربرد داشته باشد. دوم اینکه توقیف داده و سامانه تا چه اندازه از اصول مقرر در قانون آیین دادرسی کیفری تبعیت می‌کند. سوم اینکه، توقیف داده و سامانه در مرحله‌ای که جرم هنوز واقع نشده یا در آستانه وقوع یا در حال وقوع است تا چه اندازه با اصول حقوق کیفری و رعایت حقوق شهروندان منطبق است. مقاله حاضر به روش توصیف و تحلیل می‌کوشد تا چالش-های توقیف داده و سامانه در جرایم امنیتی را بازگو کند و معیارهای درست توقیف را ارایه دهد. یافته‌های این پژوهش نشان می‌دهد که چالش توقیف داده و سامانه تابعی از ویژگی‌های فضای سایبر، نگرش‌های امنیتی نسبت به فضای سایبر، ماهیت جرایم سایبری و نقش جهت‌دهی ضابطان دادگستری نسبت به مقامات قضایی در تعقیب جرایم امنیتی است و راهکار نوشته نیز در راستای انطباق هر چه بیشتر اصول و معیارهای توقیف داده بر قانونمندی، تناسب و مستند بودن است.

چکیده: جرایم امنیتی، فضای سایبر، توقیف داده و سامانه، اقدام اطلاعاتی و قضایی

[1] قاضی دادگستری تهران و استادیار مدعو، دانشگاه آزاد اسلامی، تهران شمال؛ ایران

[2] استادیارگروه حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی، تهران شمال، ایران(نویسنده مسئول) M.elahimanesh92@yahoo.com

[3] استادیار گروه حقوق جزا و جرم شناسی پردیس فارابی دانشگاه تهران ، ایران

[4] استادیارگروه حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی تهران و قاضی دیوانعالی کشور، تهران شمال، ایران

مقدمه

در فضای سایبر، مفاهیم فضا، جامعه و کنترل، ابعاد جدید و متفاوتی می‌یابند. در فضای سایبر، جامعه تبدیل به مفهومی بدون جغرافیا می‌شود. جامعه در فضای سایبر از افرادی شکل می‌گیرد که هیچکدام یکدیگر را نمی‌شناسند. روابط اجتماعی در این فضا از سطح متفاوتی از فضای واقعی برخوردار است.در نتیجه می‌توان از شکل‌گیری جامعه‌ای مجازی و شبکه‌ای در کنار جامعه واقعی صحبت کرد که بستر وقوع رویدادهای متفاوت است. شهروندان این جامعه‌ی مجازی در فضای فرهنگی متکثر و بدون مرز و با هویت پیوندی، اجتماعی می‌شوند.(عاملی، ۱۳۸۲: ۲۸). هرچند که رایانه برای جامعه بشری دستاوردهای بسیاری داشته است، اما فضای سایبر نیز همانند دیگر عرصه‌های زندگی اجتماعی نتوانسته است از آسیب وگزند سوءاستفاده‌گران در امان باشد. از جمله آسیب‌ها و تهدیداتی که در این فضا ممکن است مورد توجه بزهکاران قرار بگیرد، ارتکاب جرایم علیه امنیت است. با توجه به نفوذ همه جانبه فناوری اطلاعات و ارتباطات الکترونیکی در کشورها و گره خوردن امنیت ملی کشورها با این فضا و افزایش احتمال آسیب‌پذیری، این امر مورد توجیه مقنن قرار گرفته و مصادیقی از جرایم به صورت خاص (در قانون جرایم رایانه‌ای) و یا با ارجاع به قوانین عام مورد جرم‌انگاری قرار گرفته است. از جمله این مصادیق عبارتند از: ۱- تشکیل جمعیت، دسته، گروه در فضای مجازی با هدف برهم زدن امنیت کشور، ۲- هر گونه تهدید به بمب‌گذاری، ۳- تبلیغ علیه نظام جمهوری اسلامی ایران، ٤- تبلیغ به نفع گروه‌ها و سازمان‌های مخالف نظام جمهوری اسلامی ایران، ٥- تحریک نیروهای رزمنده، ٦- تحریک یا اغوای مردم به جنگ و کشتار یکدیگر، ۷- فاش نمودن محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند، ۸- انتشار محتوا علیه اصول قانون اساسی، ۹- اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی، ۱۰- تحریص و تشویق افراد و گروه ها به ارتکاب اعمالی علیه امنیت، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور، ۱۱- فاش نمودن و انتشار غیر مجاز اسرار نیروهای مسلح، ۱۲- فاش نمودن و انتشار غیر مجاز نقشه و استحکامات نظامی، ۱۳- انتشار غیر مجاز مذاکرات غیرعلنی مجلس شورای اسلامی، ١٤- انتشار بدون مجوز مذاکرات محاکم غیر علنی دادگستری و تحقیقات مراجع قضایی، ۱۵- انتشار محتوایی که از سوی شورای عالی امنیت ملی منع شده باشد. ارتکاب هر یک از جرایم یاد شده، بدلیل اخلال در امنیت ملی و صدمه به آن می‌تواند با آثار جبران‌ناپذیری همراه باشد، از همین‌رو، یکسری اقداماتی توسط مراجع قانونی تعریف شده که این مراجع باید نسبت به انجام هر یک از اقدامات یاد شده با حساسیت وارد شوند. از جمله این اقدامات توقیف داده و سامانه است. در کنوانسیون جرایم سایبر، منظور از «داده» هر گونه نمایش حقایق، اطلاعات یا مفاهیم به شکلی مناسب که برای پردازش در یک سیستم رایانه‌ای که شامل برنامه‌ای مناسب است. منظور از سامانه نیز؛ «به مجموعه عناصر و اجزای مرتبط با هم که برای رسیدن به یک هدف خاص با یکدیگر کار می‌کنند، سیستم یا سامانه یا نظام می‌گویند». توقیف داده و سامانه به معنای این است که شخص دارای صلاحیت، داده

یا سامانه را در موارد پیش‌بینی شده در قانون توقیف نماید و این اجازه را به مالک یا متصرف ندهد که در داده و سامانه توقیف شده دخل و تصرفی نماید.

امروزه داده‌ها و سامانه‌های الکترونیکی به عنوان ابزاری در خدمت دستگاه عدالت، کارکردهای دیگری نیز دارند که در صورت ارتکاب جرایم و به ویژه در جرایم امنیتی، تحت شرایطی ممکن است مورد توقیف یا تفتیش قرار بگیرند. قانون گذار برای توقیف ابزارهای الکترونیکی، معیارها و شرایطی را پیش‌بینی کرده است که این معیارها و شرایط، در ارتباط با جرایم علیه امنیت، با چالش‌هایی همراه است که در این مقاله، هدف آشنایی با معیارها و چالش‌های پیش‌روی توقیف داده و سامانه‌های الکترونیکی در جرایم علیه امنیت می‌باشد.

بند اول: بیان مسئله

از جمله مراجع قانونی که در قوانین جاری برای آنها وظایفی در ارتباط با پیشگیری از ارتکاب جرایم امنیتی در فضای سایبر و در صورت ارتکاب آنها؛ کشف، تعقیب، تفتیش و توقیف، تحقیقات مقدماتی، رسیدگی و اجرای احکام پیش‌بینی شده است، مراجع اطلاعاتی، مراجع پلیسی و مراجع قضایی هستند. منظور از مراجع اطلاعاتی، مراجعی هستند که وظایف گردآوری یا دیده‌بانی افراد، گروه‌ها یا اعمال خطرناک که هنوز مرتکبین اقدامی نکرده‌اند ولی در آستانه ارتکاب آن هستند، انجام می‌دهند. وزارت اطلاعات به صورت خاص و سایر نهادها از جمله نهادهای نظامی و انتظامی در راستای دستورات قضایی یا کمک به وزارت اطلاعات از مرجع اطلاعاتی محسوب می‌شوند که قانون‌گذار برای آنها وظایفی تعیین کرده و باید اقدامات اطلاعاتی را در مراحل مختلف (قبل، حین و بعد) ارتکاب جرایم علیه امنیت در محیط سایبری انجام دهند. منظور از مراجع پلیسی، مراجعی هستند که در راستای ماموریت‌های محوله وظیفه حفظ نظم و امنیت را بر عهده دارند یا در مقام ضابط و تحت نظارت و تعلیمات دادستان در کشف جرم، حفظ آثار و علائم و جمع‌آوری ادله وقوع جرم، شناسایی، یافتن و جلوگیری از فرار و مخفی شدن متهم، تحقیقات مقدماتی، ابلاغ اوراق و اجرای تصمیمات قضایی، به موجب قانون اقدام می‌کنند. با توجه به تشکیل پلیس فتا در نظام حقوقی ایران، انجام اقدامات پلیسی در فضای سایبری بر عهده این پلیس می‌باشد. منظور از مراجع قضایی نیز، مراجعی هستند که تعقیب، تحقیقات مقدماتی، رسیدگی و اجرای احکام محکومین را بر عهده دارند و در معیت آنها ضابطین دادگستری قرار دارند. این مقامات در فرایند توقیف داده‌ها و سامانه‌ها در هر نوع جرم ارتکابی حتی جرایم امنیتی، دارای اختیارات مطلق نبوده و ملزم به رعایت شرایط و معیارهای قانونی مشخصی هستند. منظور از فرایند توقیف داده و سامانه، فرایندهای تعریف شده در مقررات شکلی هستند که تا قبل از تصویب قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۲ تنها در بخش دوم قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ذکر شده بودند که به همین دلیل مقنن در همین بخش و در راستای پر کردن خلاهای دادرسی در این جرایم، به قانون آیین دادرسی کیفری ارجاع داده بود. ولی با توجه به ماهیت و ویژگی‌های جرایم رایانه‌ای که آیین‌نامه و تشریفات خاصی را در جهت شناسایی، کشف، پیگیری، تحقیقات و رسیدگی به آنها می‌طلبید، ارجاع قانونگذار به مواد قانون آیین دادرسی کیفری در راستای پر کردن خلأ ناشی از مواد شکلی قانون جرایم رایانه‌ای نیز به تنهایی نمی‌توانست راهگشای تمامی مسایل

مربوط به فرایندهای دادرسی در جرایم رایانه‌ای باشد. بعد از تصویب قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ فرایند دادرسی جرایم رایانه‌ای و به تبع آن فرایندهای پیرامون توقیف داده و سامانه در این قانون به صورت خاص مورد پیش‌بینی قرار گرفتند. این فرایندها که مشتمل بر ضوابط و اصول قانونی حاکم بر آیین دادرسی کیفری جرایم سایبر (بخصوص در مرحله تحقیقات مقدماتی) ضمن اینکه از ضوابط عمومی حاکم بر فضای سنتی پیروی می‌کند، دارای قواعد خاصی است که در فرآیند دادرسی (به مفهوم عام) باید رعایت شود. مطابق این قواعد اصول و شرایط عام و خاصی برای توقیف داده‌ها و سامانه‌ای رایانه‌ای بیان شده که برخی از آنها مشترک بوده و این اصول و شرایط در توقیف سایر ادله نیز باید رعایت می‌شود.

مسئله اصلی پژوهش حاضر بررسی چالش‌ها و معیارهای توقیف داده و سامانه در جرایم امنیتی سایبری است. با این سوال که مراجع اطلاعاتی، پلیسی و قضایی در فرایند توقیف داده و سامانه در جرایم علیه امنیت با چه معیارها و چالش‌هایی مواجه می‌باشند. در راستای پاسخ به مسئله اصلی و دیگر مسائل فرعی مرتبط، اقدامات پلیسی، اطلاعاتی و قضایی جهت توقیف داده و سامانه در جرایم امنیتی و چالش‌های مرتبط با هر یک از این اقدامات مورد مطالعه قرار گرفته و در نهایت معیارهای درست توقیف داده و سامانه در جرایم امنیتی سایبری تبیین می‌شود.

الف: اهمیت و ضرورت

توقیف داده و سامانه به‌عنوان ادله الکترونیکی، نقش حیاتی در اثبات جرایم در محیط سایبری دارد. در واقع بدون تحصیل ادله الکترونیکی اثبات جرایم سایبری غیرممکن است. بنابراین، از اولین اقدامات قضایی و انتظامی در صورت وقوع جرم در فضای سایبری، توقیف و تفتیش داده‌ها و سامانه‌های مشکوک است. اما، توقیف داده‌ها و سامانه‌ها همیشه به سهولت انجام نمی‌پذیرد و مرتکبین به ویژه در جرایم امنیتی سایبری، سعی می‌کنند با ایجاد موانع یا استفاده از بدافزارهایی مانع دسترسی به آنها شوند. بنابراین، توقیف ادله و سامانه‌های مرتبط با جرایم امنیتی سایبری با چالش‌هایی همراه است که شناخت آنها و ارائه معیارهایی برای توقیف چنین داده‌هایی از اهمیت مطالعاتی برخوردار بوده و مزایای غیرقابل انکاری را در بازشناسی ادله الکترونیکی در جرایم امنیتی سایبری از ادله الکترونیکی در سایر جرایم سایبری دارد. در مورد ضرورت پژوهش هم می‌توان بیان داشت که عدم آشنایی با چالش‌های پیش‌روی توقیف داده و سامانه در جرایم امنیتی و معیارهایی که مقنن برای توقیف آنها در چنین جرایمی پیش‌بینی نموده می‌تواند منجر به از بین رفتن و یا آسیب داده‌ها، غیرقابل استناد بودن آنها، انتقال و ... در این جرایم شود. بنابرین ضرورت دارد، مراجع قضایی و انتظامی با شناخت چالش‌ها و معیارهای پیش‌روی توقیف داده‌ها و سامانه‌های جرایم امنیتی سایبری، بین داده‌ها و سامانه‌های مرتبط با این جرایم و سایر ادله الکترونیکی تمایز قائل شوند.

ب: اهداف تحقیق و سوالات

هدف اصلی این پژوهش «تبیین چالش‌های توقیف داده و سامانه در جرایم امنیتی» است. اهداف فرعی آن نیز عبارت‌اند از:

۱. شناسایی پیوندهای منفی بین داده و سامانه و امنیت ملی
۲. تبیین انواع بدافزارهای در قالب داده و سامانه‌های الکترونیکی
۳. شناخت انواع اقدامات اطلاعاتی، انتظامی و قضایی در فرایند توقیف داده و سامانه
٤. تبیین معیارهای و چالش‌های توقیف داده‌ها و سامانه‌های الکترونیکی در جرایم امنیتی
٥. ارائه راهکارهای لازم برای رفع چالش‌های مرتبط با توقیف داده‌ها و سامانه‌های الکترونیکی در جرایم امنیتی

در همین راستا و متناظر با اهداف یاد شده، سوالات اصلی و فرعی بدین شرح تدوین می‌گردد:

سوال اصلی: مراجع اطلاعاتی، پلیسی و قضایی در فرایند توقیف داده و سامانه در جرایم علیه امنیت با چه معیارها و چالش‌هایی مواجه می‌باشند؟

سوال‌های فرعی

۱. منظور از اقدامات اطلاعاتی، پلیسی و قضایی در توقیف داده‌ها و سامانه‌های الکترونیکی در جرایم امنیتی، چه نوع اقداماتی هستند؟
۲. چه راهکارهایی برای رفع چالش‌های پیش‌روی مراجع قضایی، انتظامی و امنیتی در توقیف داده و سامانه‌های الکترونیکی متصور می‌باشد؟

در راستای پاسخ به سوال‌های یاد شده و برخی مسائل دیگر، در ادامه ابتدا به تبیین ادبیات و مبانی نظری پرداخته و منظور از اقدامات اطلاعاتی، پلیسی و قضایی را مورد بررسی قرار می‌دهیم و سپس چالش‌های توقیف داده‌ها و سامانه‌های الکترونیکی در جرایم امنیتی را احصاء کرده و راهکارهای رفع آنها را مورد مطالعه قرار می‌دهیم.

بند دوم: ادبیات و مبانی نظری

الف: پیشینه پژوهش

۱. مقاله‌ای تحت عنوان «تهدیدات و جرایم سایبری علیه امنیت و چالش های پیش رو» توسط صادق مرادی و همکاران در شماره ۱ فصلنامه فقه جزایی تطبیقی در سال ۱٤۰۱ به چاپ رسیده و محقین به این نتیجه رسیده‌اند: «جرایم سایبری مانند جاسوسی و دسترسی غیر مجاز سایبری از جمله جرایم علیه امنیت است که جرم‌انگاری شده است. اما امنیت در معرض تهدیدهای سایبری مهم دیگری نیز قرار دارد که چالش ای آینده امنیت محسوب می‌شود. تروریسم سایبری، جنگ سایبری، اخلال و هک سایبری، فشینگ، فارمینگ، اسمیشینگ از جمله تهدیدهای امنیتی است که به دلیل ماهیت نامشخص چالش های امنیتی موجود در فضای سایبر از چالش های آینده محسوب شده و مقابله با آن نیازمند پیشگیری کیفری و غیرکیفری است». در مورد

تفاوت پژوهش اینجانب در این مقاله و پژوهش یاد شده می‌توان بیان داشت که اینجانب در مقاله خود بدنبال احصاء چالش‌های شکلی پیش‌روی توقیف داده‌ها و سامانه‌های الکترونیکی در جرایم امنیتی سایبری و ارائه راهکارهای رفع آنها است در حالی که در این مقاله مصادیق جرایم امنیتی سایبری احصاء شده و مباحث ماهوی پیرامون آنها مورد تحقیق قرار گرفته است.

۲. مقاله‌ای تحت عنوان «پیشگیری اجتماعی از جرایم امنیتی ــ سایبری» توسط دکتر حمید بهره‌مند و ذولفقار داودی در شماره ۱ فصلنامه مطالعات حقوق کیفری و جرم‌شناسی دانشگاه تهران در سال ۱۳۹۷ به چاپ رسیده و محقین به این نتیجه رسیده‌اند: «برنامه‌های خانواده‌مدار، تدابیر آموزشی ـ سایبری، بالا بردن سواد رسانه‌ای، تنظیم کدهای رفتاری، اطلاع‌رسانی و اطلاع‌گیری، توجه به حکمرانی خوب و شاخص‌های آن، مشارکت و اجماع‌گری، ارتقای پاسخگویی و شفافیت، فرهنگ‌سازی و تولید رسانه‌ای می‌توانند به عنوان اقدامات پیشگیرانه اجتماعی در پیشگیری از ارتکاب جرایم امنیتی سایبری بکار گرفته شوند». همانگونه که مشخص این تحقیق در ارتباط با مصادیق روش‌های پیشگیرانه اجتماعی از جرایم امنیتی سایبری به نگارش درآمده در حالی که اینجانب در پژوهش حاضر به دنبال احصاء چالش‌های پیش‌روی مراجع انتظامی، اطلاعاتی و امنیتی در توقیف داده و سامانه‌های در ارتکاب جرایم امنیتی سایبری می‌باشد.

۳. مقاله‌ای تحت عنوان «اصل تناسب در توقیف داده و سامانه در فرایند کیفری» توسط دکتر عالی‌پور و همکاران در شماره ۱۱۷ مجله حقوقی دادگستری در سال ۱۴۰۱ به چاپ رسیده و محققین به این نتیجه رسیده‌اند: «تناسب در توقیف داده‌ها و سامانه‌های رایانه‌ای علاوه بر اتکا به رویکردهای مبتنی بر بایستگی‌های فضای سنتی مانند اعمال اقدامات احتیاطی برای رعایت حقوق جامعه و بزه‌دیده و اقتضائات فضای سایبر مانند درک جایگاه فضای مبادلات رایانه‌ای در فعالیت‌های امروزین، به پاسداشت حقوق متهم نیز توجه داشته است». این تحقیق نیز در ارتباط با یکی از اصول حاکم بر دادرسی جرایم سایبری بوده و لزوم تناسب داده و سامانه با داده و سامانه‌های وسیله ارتکاب جرایم سایبری که می‌بایست توسط مراجع قضایی و انتظامی مورد توجه قرار بگیرند می‌باشد. در حالی که اینجانب در پژوهش حاضر به دنبال احصاء چالش‌های پیش‌روی مراجع انتظامی، اطلاعاتی و امنیتی در توقیف داده و سامانه‌های در ارتکاب جرایم امنیتی سایبری می‌باشد و از منظر موضوعی متفاوت از پژوهش فوق می‌باشد.

با عنایت به پیشینه یاد شده و بررسی جامع سامانه‌های پژوهشی می‌توان به این نتیجه رسید که تحقیق پیرامون «توقیف داده و سامانه در جرایم امنیتی؛ چالش ها و معیارها» پژوهش جدیدی بوده و با نوآوری‌های متعددی به ویژه در خصوص معیارها و شرایط توقیف داده‌ها و سامانه‌ها و چالش‌های توقیف داده‌ها و سامانه‌های مرتبط با جرایم امنیتی سایبری همراه است.

ب: پیوند امنیت سایبری و امنیت ملی

یکی از مسائل جدید در زمینهٔ جرایم و علوم قضایی دیجیتال، آمادگی گروهی برای مقابله با حملات در امنیت شبکه‌های رایانه‌ای است، منظور از «امنیت شبکه»[5]، مجموعه اقداماتی است که برای محافظت از داده‌ها و سامانه‌ها و جلوگیری از بروز مشکلات امنیتی در بستر شبکه صورت می‌گیرد. از همین‌رو، امینت شبکه‌ها همواره مورد توجه کاربران به ویژه سازمان‌هایی که خدمات امنیتی و عمومی ارائه می‌دهند قرار دارد. «حملات امنیتی و رخنه به شبکه‌های رایانه‌ای سازمان‌ها ممکن است داده‌های محرمانه را به خطر انداخته، اعتماد مشتریان را کاهش داده، روابط عمومی را ضعیف ساخته و منجر به اختلال در کارها و تحمیل خسارات مالی شود؛ به‌علاوه، از دست‌رفتن داده‌های سازمانی، باعث بروز تهدیداتی از قبیل تحریف، باج‌خواهی، سرقت هویت، سرقت فناوری و حتی خطراتی علیه امنیت ملی شود» (لودر و کاسپرسون، ۲۰۰۲: ۵۷-۵۶). بنابراین تهدیدات امنیتی موجب شده تا اقداماتی به منظور بالابردن ضریب امنیتی داده‌های محرمانه و داده‌هایی که توسط ارائه‌دهندگان خدمات عمومی در ارتباط با خدمات سازمان‌های دولتی یا نیمه دولتی تبادل می‌شود، انجام بگیرد. در ایران نیز توسط پلیس فتا اقداماتی در این خصوص صورت گرفته است که ایجاد برخی محدودیت‌های دسترسی به همین منظور طراحی شده‌اند.

منظور از امنیت اطلاعات در محیط سایبر، مفهوم خاص خود، حفاظت داده‌ها در مقابل افراد غیرمجاز و کنترل سطوح دسترسی کاربران است. از آنجا که فن‌آوری‌های وب، زیرساخت‌های نرم‌افزاری پیچیده‌اند، موقعیت برای نقض امنیت اطلاعات سایبری نیز فراهم است و زمانی که فن‌آوری‌های وب مختل شوند، می‌توانند به عنوان عامل‌های حمله استفاده شوند (نوری، ۱۳۸۲: ٤٦). اما امنیت در مفهوم عام مسائل متعددی را در بر می‌گیرد و اهداف گوناگونی یعنی کنترل دسترسی، تأیید هویت کاربران، محرمانگی اطلاعات، صحت داده‌ها و غیرقابل انکار بودن ارسال و دریافت اطلاعات را برآورده می‌سازد. امنیت اطلاعات در محیط سایبر نیز عبارت است از حفظ منافع افراد یا نهادهای وابسته به اطلاعات، سیستم‌ها و ارتباطات ارائه دهنده اطلاعات در قبال آسیب‌های ناشی از فقدان، از دست رفتن محرمانه بدون انسجام (امنیت اطلاعات؛ راهنمایی برای هیئت مدیران و مدیران اجرایی، ۲۰۰۱).

امنیت اطلاعات از دیرباز مورد توجه بوده و از قدیم همواره تلاش بر آن بوده که اطلاعات حساس و مهم را به دقت حفظ نمایند. این تلاش بیشتر در راستای عدم افشای اطلاعات بوده که می‌باید محرمانه می‌مانده و خصوصاً در مواقعی مثل جنگ‌ها اهمیت حفظ آنها چند برابر می‌شده است، لکن بقاء (تمامیت) اطلاعات شاید چندان مورد توجه نبوده است. اهمیت خود اطلاعات و مصون ماندن آنها از تخریب و امحاء رفته رفته در جوامع و خصوصاً جوامع اطلاعاتی کنونی بیش از پیش شده است.

[5] Network security

جوامع اطلاعاتی مبتنی بر اطلاعات سودمند بوده و بقاء اطلاعات نیز در گرو سلامت و حفظ امنیت آن‌هاست. از این‌رو تمامیت اطلاعات صرف‌نظر از محتوایی که انتقال می‌دهند دارای اهمیت فراوانی هستند و داده‌های دیجیتالی که به مدد فناوری رایانه‌ای ایجاد شده و تکثیر می‌یابند اهمیت بسزایی را در جوامع اطلاعاتی یافته‌اند. آنچه که به امنیت اطلاعات و سیستم‌های رایانه‌ای اهمیت فراوان بخشیده همانا گسترش فضای سایبر است. به اشتراک‌گذاری اطلاعات در اینترنت و اهمیت فوق‌العاده که استفاده از بانک‌های اطلاعاتی و پایگاه‌های داده اینترنت در حوزه‌های مختلف اطلاع‌رسانی، ارتباطات، تجارت الکترونیک، آموزش الکترونیک و مواردی از این قبیل دارند. در نگاهی کلان، اهمیت اطلاعات داده‌ها را روشن می‌سازد. «در چند دهه ظهور اول شبکه، پژوهش‌گران دانشگاه‌ها از آن برای ارسال پست الکترونیکی استفاده می‌کردند و کارمندان شرکت از آن برای (به اشتراک‌گذاری) چاپ‌گراستفاده می‌نمودند. تحت این شرایط، امنیت چندان مورد توجه نبود. اما اکنون که میلیون‌ها نفر از شهروندان از شبکه برای بانکداری، فروش و پرداخت مالیات‌ها استفاده می‌کنند امنیت یک مسئله جدی است.

«اکنون نرم‌افزارهایی که حاصل تلاش فکری دانشمندان بسیار در حوزه رایانه است به زحمت و با صرف هزینه‌های مالی و زمانی تولید می‌شود و بعضاً به بهانه زیادی توسط کاربران خریداری می‌شود. همین‌طور فایل‌های محتوایی همچون فایل‌های صوتی، تصویری و نوشتاری افراد ممکن است برآیند زحمت و رنج بردن آنها طی سالیان متمادی باشد. اهمیت اطلاعات همچنین بستگی به میزان وابستگی جوامع به اطلاعات دارد؛ در واقع هرقدر جامعه‌ای اطلاعاتی‌تر باشد همان قدر اطلاعات در آن جامعه بیشتر اهمیت می‌یابد. این اهمیت اطلاعات را در هر کشور می‌توان از میزان تصویب قوانین آن کشور در این حوزه دریافت؛ قوانین مترقی کپی رایت در یک کشور نمونه‌ای از این قوانین می‌تواند باشد؛ برای مثال یک نسخه از نرم افزار سیستم عامل ویندوز در کشورهای پیشرفته که از مالکیت فکری اشخاص به شدت حمایت می‌شود- به بهای گزافی قابل خریداری است و قوانین نیز به شدت با نقض حقوق مؤلف از آن حمایت می‌کنند. اما همین نرم‌افزار در کشورهایی که حمایت از مالکیت معنوی در آنها چندان دقیق نیست یا اصلا مالکیت معنوی مورد حمایت قرار نمی‌گیرد به ثمن بخس و حتی به صورت رایگان قابل خریداری یا تهیه است؛ نه قانونی در این باره هست و نه اینکه نیروهای انتظامی و قضایی به این مسئله چندان اهمیتی می‌دهند.

علاوه‌بر داده‌ها، اطلاعات و برنامه‌های رایانه‌ای حاصل از تلاش فکری افراد، باید به اهمیت عمده داده‌های مالی افراد نیز در چرخه دریافت‌ها و پرداخت‌های الکترونیک و نقش این داده‌ها در تجارت الکترونیک توجه داشت. هر روزه میلیون‌ها پرداخت و دریافت داده‌های مالی در سطح جهان صورت می‌گیرد که حفظ آنها از تعرض و حملات الکترونیکی دارای اهمیت ویژه‌ای است و دولت‌ها توجه خاصی نسبت به این مسئله دارند. در کنار داده‌ها و اطلاعات البته سیستم‌های رایانه‌ای نیز اهمیت مشابهی دارند چرا که داده‌ها و سیستم‌ها در یک درجه از اهمیت قرار می‌گیرند. آماری که هر ساله کشورهای مختلف از حملات به اطلاعات و سیستم‌های رایانه‌ای ارائه می‌کنند و میزان خسارات هنگفت ناشی از آنها که بر دوش دولت، کاربران و ارائه‌کنندگان خدمات رایانه‌ای تحمیل می‌شود نشان‌گر ابعاد وخیم تعرض به امنیت به اطلاعات، سیستم‌ها و شبکه‌های رایانه‌ای است.

افرادی که در فضای سایبر و رایانه در پی انجام جرم و بالاخص خرابکاری و جرایم علیه امنیت هستند، عموماً از ابزارهای متعددی برای این کار استفاده می‌کنند. از جمله مهمترین این ابزارها می‌توان به موارد ذیل اشاره کرد:

بدافزار: اصطلاح «نرم افزار بدافزار» می‌تواند به معنی هر تکه‌ای از کد رایانه باشد که تأثیری مغرضانه یا ناخواسته بر روی یک سیستم IT یا شبکه دارد. در حالی که بدون اغراق، هزاران مثال منحصر به فرد از نرم افزار بدافزار وجود دارد، دسته بندی کلیدی اساساً به صورت زیر در نظر گرفته می‌شود:

ویروس: یک برنامه تکثیر که توسط آلوده کردن اجسام «حامل» مانند دیسک‌ها، فایل‌ها یا اسناد وارد یک سیستم می‌شود. یک ویروس ممکن است بار مفیدی را حمل کند که در نقاطی بعد از آلودگی فعال خواهند شد و موجب اثرات ناخواسته و اغلب آسیب‌زا می‌گردد. این که لغت «ویروس» اغلب به غلط به عنوان یک برچسب عمومی برای همه اشکال نرم افزار بدافزار مورد استفاده قرار می‌گیرد بی‌ارزش است. این موضوع اغلب در متن گزارشات رسانه‌ای اتفاق می‌افتد و این حقیقت که کاربرهای پایانی بسیاری همه اشکال نرم افزار بدافزار را مترادف با مفهوم یک ویروس در نظر می‌گیرند را بازتاب و توضیح می‌دهد.

ویروس رایانه‌ای کد مخرب رایانه‌ای است که توانایی کپی‌سازی از خود و گسترش نمونه‌های مختلف از خود را به داخل کدهای قابل اجرای دیگر یا اسناد رایانه‌ای، شبکه و برنامه‌های نرم افزاری داراست (ویلیامز، ۲۰۱۰: ۱۹۵).

فضا و حافظه رایانه را با به کارگیری برنامه‌های مجاز اشغال می‌کنند، در نتیجه آنها عموما باعث بروز رفتارهای نامتعارف از سامانه و اختلال در آن می‌شوند. ویروس‌ها یکی از اعضای خانواده بدافزارها به نام مالور هستند. ویروس می‌تواند با استفاده از یک قطعه مجاز از نرم افزار آلوده به آن ویروس و با توسل به روش اسب تروا به سامانه داخل شود و سپس اقدامات تخریبی خود را آغاز کند. ویروس پس از فعال شدن «می‌تواند یکی از خود در حافظه کامپیوتر ایجاد کند، این کپی مقیم به دنبال میزبان‌های آلوده نشده می‌گردد، وقتی یکی را پیدا کند یک کپی از خود به درون میزبان تزریق می‌کند». همچنین ویروس ممکن است اقدام به «پی لود[6]» کند، یعنی هر کاری انجام دهد از جمله نشان دادن یک پیام جالب توجه سیاسی یا پاک کردن فایل‌های موجود بر روی هارد درایو» (ضیایی‌پور، ۱۳۸۳: ۱۹۸).

این قسم از بدافزارها مهمترین حربه در دست مخربان رایانه‌ای محسوب می‌گردند. ویروس‌های رایانه‌ای نظیر ویروس بیولوژیکی عمل می‌نمایند. حیات و فعالیت ویروس بیولوژیکی متکی به خود نیست و در بدن میزبان مفهوم می‌یابد؛ ویروس به سلول‌های زنده موجودات نفوذ کرده و در محیط سلولی تکثیر می‌یابد. بدین ترتیب ویروس به سایر سلول‌ها نیز گسترش یافته و بقاء و حیاتش بدون سلول زنده مسیر نیست. «برنامه اصلی در رایانه نقش سلول زنده را داشته و ویروس بر نحوه عملکرد آن تأثیر می‌گذارد به صورتی که به محض اجرا ء برنامه، نسخه‌ای از آن تهیه می‌شود. به هر حال

[6] Pay load

چنانچه از برنامه ویروسی نسخه‌ای روی دیسک تهیه شود و بر روی رایانه دیگر اجرا گردد، باعث انتقال ویروس خواهد شد (آیکاو، ۱۳۸۳: ۹٤).

ویروس‌ها به طرق مختلف کار خود را انجام می‌دهند. یکی از روش‌های آنها قرار گرفتن در حافظه جانبی رایانه است، لذا تا زمانی که رایانه مشغول به کار باشد، آنها هم به کار خود ادامه داده و در سراسر رایانه منتشر می‌شوند و در صورت متصل بودن حامل‌های داده، بدان‌ها نفوذ می‌کنند. طریق دیگر این است که ویروس‌ها را در سکتور بوت دیسک سخت یا حامل‌های داده مانند سی دی خود را مخفی می‌نمایند و با شروع کار رایانه، به طور خود کار خود را در حافظه رایانه جای داده و به‌عنوان یک برنامه کامپیوتری عملیات خود را انجام می‌دهند و سیستم عامل رایانه نیز، به نوعی گمراه شده و تصور می‌کند این ویروس همانند سایر برنامه‌های مجاز رایانه‌ای است، اما غافل از آنکه ویروس با اشغال حافظه اصلی و فضای پردازش‌گر مرکزی به تدریج سعی در مختل کردن سامانه دارد. ویروس‌های رایانه‌ای با آلوده نمودن سامانه رایانه‌ای هدف، می‌توانند آثار و پیامدهای مخربی را به همراه داشته باشند، به طور کلی انواع آثار تخریبی ویروس‌ها و بدافزارهای رایانه‌ای عبارتند از:

۱. ایجاد اختلال در سامانه
۲. شبیه‌سازی خطا
۳. تخریب سخت افزار (نادرخانی، ۱۳۹۰: ٤٦-٤٤).

کرم: «گروه دیگر از کدهای مخرب، کرم‌ها هستند، کرم‌ها برخلاف ویروس‌ها توانایی تکثیر خود را بدون شناسایی کد مستقر روی رایانه میزبان ندارند. کرم‌ها معمولاً از انتقال فایل‌ها بر روی شبکه یا خود رایانه استفاده کرده و در نتیجه به شبکه‌های رایانه‌ای آسیب رسانده و پهنای باند آنها را محدود می‌نمایند» (ویلیامز، ۲۰۱۰: ۱۹۵).

کرم‌ها با اشتراک یک شباهت ظاهری با ویروس در مورد تکثیر میان سیستم‌های شبکه شده، از این نظر متفاوتند که آنها قادر به انتشار به صورت مستقل، بدون نیاز به آلوده کردن یک حامل به روش یک ویروس هستند. کرم‌ها از اتصال شبکه‌ای میان سیستم‌ها سود می‌برند (ویور[۷]، پاکسون[۸]، استانیفورد[۹] و کانینگهام[۱۰]، ۲۰۰۳) و می‌تواند به عنوان نتیجه‌ای از فعالیت کاملاً اتوماتیک شده (مثلاً اسکن آدرس‌های IP تصادفی و بهره برداری از آسیب‌پذیری‌ها جهت وارد شدن به سیستم‌های دور دست) یا اقدامات به اجرا در آمده توسط کاربر (مثلاً باز کردن مضامین جعلی از ضمیمه ایمیل یا اشتراک فایل‌های جفت جفت) انتشار یابد.

کرم‌ها بر خلاف ویروس‌ها برنامه‌های متکی به خود هستند و بدون نیاز به سایر برنامه‌ها فعالیت دارند، کرم ها به راحتی تکثیر یافته و رایانه‌های متصل به شبکه را آلوده می‌نمایند. لذا کرم‌ها روی شبکه فعالیت دارند؛ اما فعالیت ویروس‌ها

[7] - Weaver
[8] - Paxson
[9] - Staniford
[10] - Conningham

وابسته به تکثیر یا نسخه‌برداری است. این نوع از بدافزارها می‌تواند به یک سامانه دسترسی پیدا کند، اما نمی‌تواند در خارج از شبکه برای مثال از طریق یک دیسکت گسترش پیدا کند. آنها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آنکه رایانه کند شود و یا از کار بیافتد (آنجلیز، ۱۳۸۳: ۳٦).

بنابراین کرم یک عامل خود مختار است که از طریق خودش تکثیر می‌شود در حالی که ویروس خود رابه نرمافزارها می‌چسباند و با اجرای آن نرم افزار تکثیر می‌شود» (ضیایی پرور، ۱۳۸۳: ۱۹۷). غالبا کرم‌ها را به دو دسته تقسیم می‌کنند:

الف- کرم‌های میزبان: در حافظه کامپیوتری که روشن است قرار گرفته و از شبکه برای ایجاد کپی‌هایی از خود در کامپیوتر های دیگر استفاده می‌کنند و منبع اصلی پس از استقرار یک کپی بر روی کامپیوتر میزبان، خود از بین می‌رود.

ب- کرم‌های شبکه: این کرم‌ها از قطعات متعددی تشکیل شده‌اند که هر یک از این قطعات در سامانه‌های مختلفی اجرا می‌شوند و ممکن است هر یک عملکرد خاصی داشته باشند؛ از این کرم‌ها از شبکه برای اهداف ارتباطی بهره می‌گیرند؛ قطعات کرم‌های شبکه معمولاً طریق شبکه با یکدیگر ارتباط برقرار می‌کنند.

کرم‌های رایانه‌ای در کشورهای که از نسبت به فناوری رایانه و سیستم‌های امنیتی کمتر پیش رفته‌اند، تهدیدی به مراتب شدیدتر محسوب می‌گردد. به عنوان مثال در سال ۱۳۸۹ رایانه‌های ایران مورد هجوم شدید کرم خطرناک رایانه‌ای به نام «ستاکس نت» قرار گرفته‌اند که تلاش می‌کند اطلاعات سیستم‌های کنترل صنعتی را به سرقت ببرد. این کرم به دنبال سیستم مدیریتی «اس.سی.ای.دی.ای» زیمنس که معمولاً در کارخانه‌های بزرگ تولیدی و صنعتی مورد استفاده قرار می‌گیرد، بوده و تلاش می‌کند اسرار صنعتی رایانه‌های این کارخانه‌ها را بر روی اینترنت بارگذاری کند (نادرخانی، ۱۳۹۰: ٤٦-٤٩-٤٨).

اسب تروجان: این دسته از بدافزارها که نام خود را از اسب چوبی میان تهی مورد استفاده یونانیان جهت هجوم به تروا گرفته است. به برنامه‌هایی اشاره دارد که کاربر را برای به اجرا در آوردن خود توسط تظاهر به انجام یک دستورالعمل مشخص فریب می‌دهد اما در نهایت مشخص می‌شود که در حال انجام کاری دیگر (در عوض دستورالعمل مورد ادعا یا علاوه بر آن) می‌باشد که منجر به تأثیرات غیر منتظره و اساساً ناخواسته می‌شود.

نرم‌افزارهای جاسوسی: اینها نه ویروس‌اند و نه کرم، اما نرم‌افزارهایی هستند که در بسیاری از اوقات مورد سوء استفاده توسط شرکت‌های تبلیغاتی می‌باشند؛ «ادورها[11]» و «اسپای‌ورها[12]» جاسوسانی هستند که نه تنها تبلیغات بنر را بر روی صفحات رایانه نشان می‌دهند بلکه عادات وب گردی کاربران را نیز جمع‌آوری و پیگیری می‌کنند و سپس به شرکت-های تبلیغاتی گزارش می‌دهند. این شرکت‌ها هم وقتی می‌بینند که به عنوان مثال شما بیشترین مراجعه‌تان به سایت‌های گردشگری بوده است، تبلیغاتی را با مضمون‌های مشابه به صورت نواری در بالا یا پایین صفحه کامپوتر هنگامی که کاربر

[11] Ad ware
[12] Spyware

در حال گشت‌زنی در اینترنت است، به نمایش می‌گذارند. این برنامه‌ها به طور رایگان قابل دسترس‌اند و می‌توان آنها را بر روی سیستم عامل خود نصب نمود؛ هر چند گاهی اوقات این نرم‌افزارها با نیات و مقاصد منفی توسط شرکت‌های تبلیغاتی استفاده نمی‌شوند، اما در اکثر مواقع کاری جز جاسوسی و خرابکاری ندارند. یکی از مشکلات رایجی که آنها بوجود می‌آورند کاهش سرعت سیستم عامل نصب شده می‌باشد و در پاره‌ای اوقات آن قدر حجم فعالیت‌شان زیاد می‌شود که می‌توانند سیستم عامل را مختل و غیرقابل کاربری نمایند (نادرخانی، ۱۳۹۰: ۵۰).

در یک جمع‌بندی کلی می‌توان ابزارهای مورد استفاده برای ارتکاب جرایم امنیتی سایبری را شامل مصادیق ذیل با تعاریف یاد شده در مقابل هر یک خلاصه کرد:

واژه ها	تعریف
بدافزار	بدافزار به اخلال در رایانه و سیستم‌ها می‌پردازد؛ از جمله ویروس و اسب تراوا (ویکی پدیا)
ویروس	برنامه‌ای قابل بازتولید که به سرعت در شبکه‌ها شیوع می‌یابد. ویروس به شکل برنامه‌های مجاز یا در پوشش آن ظاهر می‌شود. ویروس به سرعت تکثیر شده و باعث کندی یا توقف کارکرد سیستم می‌شود. (ویکی‌پدیا)
اسب تروا	برنامه‌ای به‌شکل برنامه‌های مجاز که‌سپری برای ویروس‌ها یا دیگر بدافزارهاست (ویکی پدیا)
اسپای ویو[۱۳]	برنامه‌ای پنهان در سیستم که فعالیت‌های کاربر نظیر ایمیل یا شماره کارت اعتباری را برداشته و از وب‌سایت‌ها لاگ می‌گیرد؛ سپس این اطلاعات را به فرد غیر مجازی ارسال می‌کند. (ویکی پدیا)
اد ویو[۱۴]	این برنامه، تبلیغات و آگهی‌ها را بر اساس وب‌گردی کاربر نمایش می‌دهد
اسکریپ کیدیز[۱۵]	فردی بدون تخصص خاص در فناوری مانند کودکی که اتفاقی به نقطه ضعفی در اینترنت بر می‌خورد (ویکی پدیا)
مهندسی اجتماعی	جمع‌آوری اطلاعات خصوصی با فریبکاری به منظور جلب اعتماد قربانی مثلاً درخواست تأیید شماره تامین اجتماعی برای رفع مشکلات به وجود آمده در حساب کاربری (ویکی پدیا)
اسپم	ارسال پیام‌های سرکاری گروه خبری یا پست‌های سرکاری (ویکی پدیا)
هک کردن	دسترسی غیر مجاز یا استفاده از داده‌ها، سیستم‌ها، سرور یا شبکه از جمله سعی در جست‌وجو، یا آزمایش آسیب‌پذیری سیستم، سرور یا شبکه یا اخلال در امنیت یا تأیید خواهی بدون اجازه مالک سیستم، سرور یا شبکه

اصطلاحات گوناگون دیگری نیز وجود دارند که ممکن است در مبحث کُد خطرناک یا آسیب‌زا با آنها مواجه شویم نظیر درهای عقب[۱۶] (مسیرهای گشوده شده توسط مهاجمین جهت اجازه دسترسی غیر قانونی به یک سیستم)، درهای دام

[13] Spywave
[14] Adwave
[15] Script Kiddies
[16] Backdoors

(نقاط ورودی که به صورت مشابه غیر قانونی هستند اما توسط توسعه دهندگان اصلی رها شده‌اند)، بمب‌های زمانی (مجموعه کد جهت داده اندازی بعد از سپری شدن یک مدت زمانی یا هنگامی که تاریخ یا زمان خاصی سر رسید) و بمب‌های استدلالی (توسط یک رویداد خاص یا مجموعه‌ای از رویدادهای رخ داده درون یک شبکه راه اندازی می‌شود).

ب: ویژگی‌های جرایم امنیتی

مطابق یک تعریف عینی و بر پایه ضـــرر حاصـــل از جرم، جرم علیه امنیت جرمی اســـت که مســـتقیماً علیه موجودیت حکومت واقع شود؛ اما اولین استثناء در همین‌جا اتفاق می‌افتد که حکومت‌ها نمی‌توانند به یک تعریف کاملاً عینی بسنده کنند و گفته می‌شـود حفظ حکومت مسـتلزم توسـعه این تعریف با توسـل به یک مفهوم ذهنی اسـت. مطابق این گسـترش مفهومی نه‌تنها جرمی که ضـررش مسـتقیماً متوجه حکومت باشـد جرم علیه امنیت اسـت، بلکه هر جرمی که با این هدف یعنی انگیزه آسیب رساندن به موجودیت حکومت واقع شود نیز جرم علیه امنیت محسوب می‌شود ولو زیاندیده مستقیم آن حکومت نباشـد. به‌عنوان مثال جرمی چون جاسـوسـی بنا بر دیدگاه عینی (نتیجه جرم) یک جرم علیه امنیت اسـت، اما جعل اسـکناس ابتدائاً جرمی علیه ملت و شـهروندان اسـت که اگر هدف آن آسـیب به حکومت باشـد (دیدگاه ذهنی) در زمرهٔ جرائم علیه امنیت قرار می‌گیرد. همانگونه که در جرائم دسـته اول فقط نتیجه مهم اسـت و انگیزه اهمیتی ندارد، در دسته دوم تنها انگیزه مهم است ولو نتیجه علیه حکومت نباشد؛ بنابراین و به طور خلا صه: جرم علیه امنیت جرمی است که مسـتقیماً علیه موجودیت حکومت یا باهدف آسـیب به موجودیت نظام حاکم علیه ملت واقع شـود (یزدیان جعفری، ۱۳۹۵: ٦٠). از همین‌رو؛ برخی حقوقدانان، برای یافتن جایگاه امنیت از زوایای مختلف به آن نگریسته‌اند، از تقسیم‌بندی امنیت چون هدف، امنیت چون ابزار برای حقوق کیفری و امنیت چون گفتمان بحث نموده‌لند، اما نهایتاً امنیت در حقوق کیفری را در حوزه‌ی امنیت ملی قرار داده‌لند و بیان کرده‌لند که امنیت ملی به‌مثابه معما می‌ملند (عالی پور،تبریزی، الهی منش، ١٤٠١ :٤٠).

امنیت ملی هر کشوری بخش مهمی از حکومت آن کشور را تشکیل می‌دهد و اساس ثبات یک حکومت را میزان امنیت ملی و داخلی آن تعیین می‌کند. با توجه به ارزشی که ملل گوناگون همیشه برای حاکمیت خود قائل بوده‌اند و با توجه به تلاش حکام در جهت حفظ قدرت و حاکمیت خود و خطرات که جرایم علیه امنیت می‌توانند برای حاکمیت و اسـتقلال آن‌ها ایجاد نمایند، از قدیم‌الایام مقررات سـخت راجع به جرایم علیه امنیت وجود داشـته اسـت. نگاهی به رویه قانونی و قضایی در کشور ایران در پیش‌بینی جرایم علیه امنیت داخلی و خارجی و رسیدگی به چنین جرایمی بیان‌گر این حقیقت اسـت که لزوم حراسـت و حفاظت از امنیت ملی از یک سـو و پاس داشـت کرامت انسـانی از سـوی دیگر بر آن داشـته تا رویکرد عدم تحمل و عدم مدارا و به بیان بهتر «تسـامح صـفر در مقابله با جرایم علیه امنیت» را به شـکل مقررات ملی در قوانین ماهوی و شکلی متبلور سازد.

علاوه بر این، جرایم علیه امنیت دارای ویژگی‌های خاصـی می‌باشـند که برخورداری از این ویژگی‌ها موجب شـده تا این جرایم از منظر حقوق کیفری متمایز از سـایر جرایم باشـد. از جمله ویزگی‌هایی که در مورد جرایم علیه امنیت می‌توان به

آن اشـاره کرد؛ وسـعت جرم‌انگاری در حوزه امنیت اسـت. در تبیین این ویژگی گفته شـده اسـت که حقوق جزا به‌عنوان ابزار رسـمی کنترل اجتماعی در جامعه ظرفیت فراوانی دارد تا به‌عنوان ضـمانت اجرای ارزش‌های جامعه و حکومت به کار گرفته شود، ابزاری که قاطع، سریع و مؤثر است، به شرطی که به‌صورت معتدل و در آخرین گام مورد رجوع قرار گیرد، اصلی که چنین تلقی‌ای از حقوق کیفری دارد به‌عنوان اصل «حداقلی بودن حقوق جزا» مشهور شده و موردپسند قاطبه‌ی علمای حقوق است. این اصل زمانی اجازه‌ی ورود به ضمانت اجرای کیفری را تجویز می‌کند که «قواعد حقوق خصـوصـی، اداری و ضـمانت اجراهای خاص آنها، توانایی لازم جهت تحقق اهداف مقنن را نداشـته باشـند» (غلامی، ۱۳۹۱: ٤٥). در حوزه‌ی امنیت، مقنن در تقابل بین آزادی و امنیت، دامان امنیت را گرفته و با جرم‌انگاری گسـترده و خارج از ضوابط جا افتاده‌ی حقوق کیفری سعی در حفظ و تداوم ارزش‌های مدنظر خویش دارد.

ویژگی دیگری که جرایم امنیتی را متمایز از سایر جرایم کرده است، توسعه‌ی جرم انگاری به رفتارهای غیرعمدی است. در میان حقوقدانان این دیدگاه مشهور است که اصل بر عمدی بودن جرایم است و در صورتی‌که عنوان شک نماییم که آیا برای عملی عنوان غیرعمدی نیز در نظر گرفته‌شده یا خیر بایستی قائل به عدم جرم‌انگاری شویم، چنانچه ما قتل عمد و غیر عمد داریم، ولی آیا تحریک غیرعمدی نیز داریم، بایسـتی حقوق افراد را در پرتو اصـل برائت رعایت نماییم، اما مسئله در جرایم امنیتی خارج از قاعده‌ی بالاست و مقنن در موارد بی‌شماری به گسترش مصادیق غیرعمدی پرداخته است.

جرم‌انگاری مقدمات جرم ویژگی دیگری است که در بررسی حقوق کیفری جرایم علیه امنیت می‌توان به آن دست یافت. در تکوین مراحل ارتکاب جرم، بزهکار مراحل زیر را طی می‌کند، ابتدا مجرم قصد ارتکاب جرم می‌کند، سپس به تهیه‌ی مقدمات جرم مبادرت می‌ورزد، بعد شروع به اجرای جرم می‌نماید و نهایتاً جرم را به مورد اجرا می‌گذارد. اما در جرایم امنیتی معمولاً شرایط ارتکاب جرم سهل‌تر است؛ مثلاً اگر کسی به قصد ارتکاب قتل یا سرقت طناب یا نردبان تهیه کند، وی را نمی‌توان به‌عنوان ارتکاب یک جرم خاص یا تحت عنوان شروع به جرم قتل یا سرقت مورد تعقیب قرار داد (میرمحمدصادقی، ۱۳۹٦: ۳٤). اما در جرایم امنیتی مواردی وارد سیطره‌ی حقوق کیفری شده که اصولاً محلی از اعراب در این قلمرو ندارند، ولی به دلیل طبع خاص حوزه‌ی امنیت، قالب کیفری گرفته‌اند.

رویکرد سخت‌گیرانه مقنن در مراحل مختلف دادرسی جرایم علیه امنیت از دیگر ویژگی‌های مربوط به این جرایم می‌باشند. نگاهی به قوانین ماهوی و عدم امکان تخفیف، تعلیق، تعویق، آزادی مشروط و بسیاری از نهادهای مخففه رویکرد سخت‌گیرانه قانون‌گذار را در سیاست تقنینی مشخص می‌کند چنین رویکردی در رسیدگی و در مراحل اجرایی نیز دیده می‌شود و عوام‌گرایی، شدت مجازات اتخاذی، رسیدگی در دادگاه خاص و ... رویه محاکم در رسیدگی به چنین جرایمی دیده می‌شود.

علاوه بر ویژگی‌های یاد شده، مطلق بودن جرایم امنیتی و عدم نیاز به اثبات نتیجه و فراسرزمینی بودن مقررات کشورها در خصوص مرتکبین این جرایم از دیگر مشخصه‌هایی هستند که موجب شده تا جرایم علیه امنیت از ماهیت متفاوتی باشند. ماهیت متفاوت جرایم علیه امنیت مختص ارتکاب جرم در دنیای واقعی نبوده، بلکه در جرایم علیه امنیت سایبری

نیز وضعیت به همین منوال می‌باشد. در واقع نوع فضایی که جرم علیه امنیت در آن ارتکاب یافته در جرم‌انگاری و نحوه برخورد با مرتکبین این جرایم موثر نبوده و ماهیت متفاوت جرایم علیه امنیت در هر دو فضای فیزیکی و سایبری موجب شده تا این جرایم ویژگی‌های خاصی برخوردار باشند.

پ: اقدامات مراجع قانونی در جرایم امنیتی

همانگونه که بیان شد، جرایم امنیتی اعم از اینکه در فضای واقعی یا سایبری ارتکاب یافته باشند، در مقایسه با سایر جرایم از ماهیت متفاوتی برخوردارند. به جز این ماهیت که محصول ویژگی‌های خاصی هست که مورد مطالعه قرار گرفت، جرایم علیه امنیت در فضای سایبر در ابعاد مختلف تفاوت‌های زیادی با ارتکاب این جرایم در فضای فیزیکی دارد. به همین دلیل اقداماتی هم که توسط مراجع قانونی در راستای پیشگیری از ارتکاب این جرایم و همچنین تحقیقات مقدماتی و رسیدگی به جرایم امنیتی در محیط سایبر از جمله در توقیف ادله انجام می‌گیرد، خاص بوده و متمایز از فضای فیزیکی می‌باشد. مراجع قانونی که در توقیف ادله در جرایم امنیتی نقش دارند، به مراجع اطلاعاتی، پلیسی و قضایی قابل تقسیم هستند. در این بخش اقداماتی که مراجع یاد شده در توقیف ادله الکترونیکی انجام می‌دهند، مطالعه و بررسی خواهد شد.

۱- اقدام اطلاعاتی

منظور از اقدام اطلاعاتی یعنی گردآوری یا دیده‌بانی افراد، گروه‌ها یا اعمال خطرناک که هنوز مرتکبین اقدامی نکرده‌اند ولی در آستانه ارتکاب آن هستند. ایجاد مشکلات و موانع در مسیر ارتکاب جرایم امنیتی یکی از اقدامات بسیار مهم در پیشگیری (وضعی) از ارتکاب این‌گونه از جرایم می‌باشد. متصدیان اقدامات اطلاعاتی که در نظام حقوقی – سیاسی ایران این وظیفه بر عهده وزارت اطلاعات و نهادهای نظامی و انتظامی قرار گرفته بخش عمده‌ای از اقدامات اطلاعاتی خود را باید معطوف به پیشگیری از ارتکاب جرایم امنیتی نمایند. ماده ۳۵ کنوانسیون جرایم سایبر مصوب ۲۰۰۱، در خصوص پیش‌بینی نهادی با وظایف امنیتی فوق قید گردیده است که «اعضا» موظفند یک مرکز تماس ۲٤ ساعته در دسترس در هفت روز را تاسیس کنند تا معاضدت فوری جهت تحقیقات یا رسیدگی‌های کیفری مرتبط با داده‌ها و سیستم‌های رایانه‌ای یا جمع‌آوری ادله الکترونیکی جرایم را تضمین کنند. چنانچه رویه قضایی با قوانین داخلی اجازه دهد، معاضدت مزبور باید به‌طور مستقیم شامل فراهم آوردن تسهیلات ذیل باشد: الف: مشاوره فنی، ب: حفظ داده با مطابقت مواد ۲۹ و ۳۰، ج: جمع‌آوری ادله، ارائه اطلاعات قانونی دست‌یابی متهمان.

از جمله اقدامات اطلاعاتی کاهش فرصت‌های ارتکاب جرم است که در جرم‌شناسی به پیش‌گیری وضعی معروف هستند. نقش کاربر این نوع پیشگیری در حوزه جرایم علیه امنیت بسیار مهم می‌باشد بسیاری از دولت‌ها با صرف هزینه‌های گزاف سعی در تجهیز خود از انواع وسایل و امکانات گوناگون جهت کشف و به ثمر نرسیدن این‌گونه جرایم می‌کنند از طرفی اجرای تدابیر پیشگیری وضعی در حوزه جرایم علیه امنیت در کشورهای غیر دموکراتیک یا قانون گریز، فی نفسه قابل دفاع نیست، زیرا خواه ناخواه منجر به تحدید یا سرکوب آزادی‌ها در فضای واقعی سایبر خواهد شد باعث از بین رفتن بخشی از آزادی می‌شود (نجفی‌ابرندآبادی، ۱۳۹۲: ۲۰۷٦) گرچه به نظر می‌رسد در حوزه جرایم علیه امنیت استفاده

از تدابیر پیشگیری وضعی ضروری می‌باشد حتی‌الامکان سعی گردد از رهگذر استفاده از این تدابیر کمترین خدشه به سایر حقوق اشخاص وارد گردد.

از جمله تدابیر ارزنده پیشگیری از جرایم علیه امنیت تدوین مجموع مقررات رفتاری و تقویت موانع درونی ارتکاب جرایم (اخلاق حرفه‌ای) می‌باشد مجموع مقررات رفتاری توصیف موازین رفتار مطلوب است که گاه‌گاهی در ارتباط با گروه‌هایی از افراد، سازمان‌ها و نهادهای حرفه‌ای مقرر می‌شود. محتوای این مجموع مقررات بسته به کار اهداف این گروهها، نهادها سازمان‌ها متفاوت است گرچه مجموع مقررات رفتاری در کل بیشتر جنبه غیر رسمی دارند برخی از آنها شکل قانونی دارند از این‌رو از نیروی اجرایی قوانین، از جمله اعمال مجازات‌های مدنی و کیفری برخوردارند در تدارک تدوین کدهای رفتاری اخلاق حرفه‌ای جایگاه ویژه‌ای دارد. قواعد رفتاری، لزوما مبتنی بر اخلاق‌گرایی نیست، از این رو اخلاق حرفه‌ای نیز لزوماً در معنای تدارک گزاره‌های اخلاقی نیست، زیرا اکثر قواعد رفتاری برای حراست از منافع شرکت یا حرفه مور نظر تدوین می‌گرد. بدیهی است که خودکنترلی تاثیرش بیشتر از کنترل خارجی است، اما به این منظور (تاثیر خو کنترلی) بازدارنده‌هایی در قالب تعقیب ضمانت اجراها می‌بایست آن را پشتیبانی کند (توسلی‌زاده، ۱۳۹۲: ۱٤۷). نکته مهم دیگر اینکه، اقدام‌های اطلاعاتی علاوه بر جنبه بیرونی، در مورد پرسنل اطلاعاتی نیز حائز اهمیت است.

از دیگر اقدام‌های اطلاعاتی، بکارگیری مخبرین در جهت گزارش‌دهی جرایم امنیتی است. این شیوه به ویژه در توقیف ادله بکارگرفته شده در ارتکاب جرایم امنیتی در فضای سایبر از اهمیت زیادی برخوردار می‌باشد. گزارش‌دهی صرفاً امری اختیاری نیست بلکه در جرایم علیه امنیت در خصوص برخی از مسئولین و مدیران اجباری نیز می‌باشد. هر چند در قوانین عمومی جزایی مقررات خاصی در ارتباط با جرم‌انگاری گزارش‌دهی اجباری به صورت خاص مقرراتی پیش‌بینی نشده است اما در ماده ۷۸ قانون مجازات جرایم نیروهای مسلح مورد جرم‌انگاری قرار گرفته است. مقنن با وضع این ماده که بسیار لازم و ضروری می‌باشد با هدف جلوگیری از ایجاد خسارت بیشتر به امنیت کشور اقدام به جرم‌انگاری عدم گزارش جرایم یا کتمان حقایق برای مسئولین فرماندهان نموده است. حتی مقنن این تکلیف را اگر چه براساس سهل‌انگاری باشد جرم‌انگاری نموده که با توجه به آثار زیانبار آن قابل توجیه می‌باشد.

برای پیکار با بزه‌های تروریستی و به ویژه به منظور جلوگیری از کمک مالی به تروریست‌ها و نظارت همه سویه به تراکنش‌های پولی و بانکی پیشگیری از پولشویی که برجسته‌ترین منبع تامین مالی تروریستی‌ها به شمار می‌رود. قانونگذار نه تنها رازداری بانکی را روا ندانسته که بانک‌ها را مکلف به شناسایی مشتریان خود و آگاهی دادن جابه‌جایی‌های پول گمان‌آور کرده است. البته افشای اطلاعات محدود به اطلاعات مالی بانکی نیست به هرگونه اطلاعات مرتبط با اقدامات تروریستی تسری داد. در ماده ۳ قانون مبارزه با تامین مالی تروریسم همه اشخاص را (اعم از کارمند و غیر کارمند) تکلیف نموده که جرایم علیه امنیت را گزارش نمایند به موجب این ماده: «کلیه اشخاص مطلع از جرائم موضوع این قانون موظفند مراتب را در اسرع وقت به مقامات اداری، انتظامی، امنیتی یا قضائی ذی‌صلاح اعلام کنند، در غیر این‌صورت به مجازات تعزیری درجه هفت محکوم می‌شوند». حمایت از این اشخاص و خانواده‌های گزارش‌دهندگان نیز از دیگر اقدامات اطلاعاتی

است که می‌تواند در پیشگیری از ارتکاب جرایم اطلاعاتی و استمرار این جرایم موثر باشد. در همین راستا، مقنن در ماده ۲۱٤ ق.آ.د.ک ۱۳۹۲ مقرراتی را پیش‌بینی کرده و آیین‌نامه‌ای نیز در همین خصوص در سال ۱۳۹٤ به تصویب رسیده است. عدم افشای هویت و اطلاعات آنها، عدم مواجهه حضوری این اشخاص در دادرسی‌های کیفری، استماع اظهارات شاهد و مطلع با وسایل ارتباط از راه دور، استقرار گشت‌های پلیسی و .... از جمله این حمایت‌ها می‌باشند.

۲- اقدام پلیسی

از دیگر اقداماتی که توسط مراجع قانونی و در راستای پیشگیری، کشف، توقیف ادله و تحقیقات مقدماتی جرایم امنیتی انجام می‌پذیرد، اقدامات پلیسی هستند. این اقدامات در دو دسته کلی قابل طبقه‌بندی می‌باشند: ۱- اقدام‌های مرتبط با پیشگیری از جرایم امنیتی سایبری، ۲- اقدام‌های مرتبط با کشف و توقیف ادله ارتکاب جرایم امنیتی سایبری. اقدامات یاد شده، به مانند اقداماتی که پلیس در فضای سنتی انجام می‌دهد نیست، بلکه پیچیده و فنی بوده و نیازمند، تشکیلات اختصاصی می‌باشد که زا ان تحت عنوان پلیس سایبر یاد می‌شود. پلیس سایبر به اشخاص متخصص و ذی‌صلاحی اطلاق می‌گردد که وظیفه‌ی تامین امنیت فضای سایبر و پاک‌سازی ارتباطات را در این فضا با رویکرد مقابله با جرایم سایبری از طریق پیش‌بینی، پیشگیری، کشف و تعقیب مجرمین سایبری را بر عهده دارد. پیش‌بینی پلیس تخصصی از جمله راهبردهایی است که در ایران نیز به تازگی تحت عنوان پلیس فتا در مجموعه نیروی انتظامی تشکیل شده است. ماهیت اصلی پلیس فتا، عملیاتی است. به این معنا که به صورت کاملاً تخصّصی و از طریق تجهیز به منابع ارزشمند نیروی انسانی، دانشی و تجهیزاتی با توان عملیاتی خوب، نسبت به تأمین امنیت فضای تولید و تبادل اطّلاعات با رویکرد مقابله با جرایم از طریق پیش‌بینی، پیش‌گیری و کشف جرم اقدام می‌نماید.

اقدامات پلیسی با توجه به اهمیتی که در حوزه امنیت سایبری دارد، همواره مورد توجه نهادهای بین‌المللی و منطقه‌ای نیز بوده و در راستای گسترش همکاری‌های بین‌المللی تفاهم‌نامه‌ای مشترک بین یوروپل، اتحادیه اروپا، آژانس دفاع از شبکه و اطلاعات، آژانس دفاع اروپا و تیم واکنش اضطراری رایانه‌ای در سال ۲۰۱۸ امضا شده است: این تفاهم‌نامه مشترک همکاری در حوزه‌هایی مانند عملیاتی کردن و اطمینان از مشارکت نیروی انتظامی و دستگاه قضایی در تمرینات شبیه‌سازی شده جرایم سایبری و درگیری زودهنگام در پاسخ به بحران‌های پیش‌رو می‌باشد (پلیس اتحادیه اروپا و دادگستری اروپا، ۲۰۱۹: ۳۱).

نقش پلیس در اتحادیه اروپا را باید در مرکز مبارزه با جرایم سایبری اروپا جستجو نمود. کمیسیون اروپا بر پایه مطالعات امکان‌سنجی انجام شده تصمیم به ایجاد مرکز مبارزه با جرایم سایبری در یوروپل گرفت. این مرکز نقطه کانونی و مهم در اتحادیه اروپا برای مبارزه با جرم های سایبری و حمایت از ۲۸ عضو این اتحادیه است و کمک می‌کند تا پلیس اروپا واکنش‌های سریع‌تر و دقیق‌تری را در این رابطه اتخاذ نموده و همچنین، در زمینه جرایم سایبری تحقیقات بهتر و همکاری‌های بین‌المللی صورت پذیرد (پلیس اتحادیه اروپا، ۲۰۲۰). یوروپل در سال ۲۰۱۳، مرکز مبارزه با جرایم سایبری اروپایی را برای تقویت اجرای قانون جهت مقابله با جرایم اینترنتی در اتحادیه اروپا و همچنین، کمک به محافظت از

شهروندان اروپایی، کسب و کار و دولت در قبال جرایم اینترنتی ایجاد کرد. همچنین، برای این مرکز سه وظیفه در نظر گرفته شد: اول، جرایم سایبری که توسط گروه‌های سازمان‌یافته انجام می‌شود، به‌ویژه افرادی که سودهای بزرگی از اقداماتی نظیر کلاهبرداری آنلاین به‌دست می‌آورند. دوم، جرایم سایبری که صدمات جدی به قربانیان خود وارد می‌کند، مانند سوءاستفاده جنسی آنلاین کودکان. سوم، جرایم سایبری که بر زیرساخت‌های مهم و سیستم‌های اطلاعاتی تأثیر می‌گذارد. با توجه به این سه حوزه فعالیت، انتظار می‌رود که این مرکز به‌عنوان قطب اصلی اطلاعات جنایی خدمت نموده و با تجزیه و تحلیل تخصصی، آموزش و ظرفیت‌سازی موجب هماهنگی عملیات و تحقیقات کشورهای عضو شود. این مرکز در سال ۲۰۱۳ علاوه بر همکاری با مقامات اجرایی قانون در مبارزه با جرایم سایبری، مشارکت‌های مهمی را با تیم‌های واکنش اضطراری رایانه، شرکت‌های مهم اینترنتی و خدمات مالی، صنعت ضدبدافزار، تولیدکنندگان نرم‌افزار و دانشگاه‌ها آغاز نموده (مرکز جرایم سایبری اروپا، ۲۰۱٤: ٤) و از زمان تأسیس، سهم قابل توجهی در مبارزه با جرایم اینترنتی داشته است. یوروپول دارای ابزارها و منابع لازم جهت ارزیابی و شناسایی تهدیدات مختلف تا فعالیت‌های جمع‌آوری هوشمند اطلاعات و فعالیت‌های عملیاتی خود، به‌منظور ایجاد امنیت در اروپا است. فعالیت‌های یوروپل عبارت است از: اتخاذ طیف گسترده‌ای از روش‌های مبارزه با جرایم اینترنتی، تجزیه و تحلیل استراتژیک، تجزیه و تحلیل اطلاعات از جمله اطلاعات جنایی و فعالیت‌های اطلاعاتی سایبری، ایجاد تیم‌های مشترک تحقیقاتی و همچنین، فعالیت‌های پیشرفته بررسی جرم و آموزش و ظرفیت‌سازی آن و اجرای قانون در کشورهای عضو.

در همین راستا؛ در انگلستان، دو نهاد اصلی جدید برای مسائل سایبری در سال ۲۰۱۰ ایجاد شد، دفتر امنیت سایبر[۱۷] و مرکز عملیات امنیت سایبری[۱۸]. دفتر امنیت سایبری در دفتر کابینه مستقر است و متولی امنیت سایبری راهبردی بریتانیا است و رهبری راهبردی امنیت سایبری در کل دولت و سراسر ادارات آن را به عهده دارد، و مرکز عملیات امنیت سایبری پایش و هماهنگی[۱۹] پاسخ به حادثه را فراهم می‌کند.[۲۰] وظایف اصلی این مرکز نظارت بر تحولات در فضای سایبر، (نهایتاً سطح آگاهی موقعیتی[۲۱] جمعی را فراهم می‌آورد). تجزیه و تحلیل روندها، و بهبود هماهنگی پاسخ های فنی به حوادث سایبری می‌باشد. علاوه بر این، تعدادی از سازمان‌ها در حال حاضر برای محافظت از تهدیدات سایبری انگلستان در حال فعالیت می‌باشند، از جمله گروه امنیت ارتباطات و الکترونیک[۲۲]، مرکز حفاظت از زیرساخت‌های ملی[۲۳] و دیگر سازمان‌های مرتبط نظیر دفتر کابینه، اداره رسیدگی به جرایم سازمان یافته[۲٤]، پلیس و ... (حسینی و ظریف منش، ۱۳۹۲: ٥٦).

[17] .OCS: Office of Cyber Security
[18]. CSOC: Cyber Security of operation Centre
[19] . Monitoring and Coordinating
[20] . Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space published by TSO
[21]. situational awareness
[22] . CESG -Communications-Electronics Security Group
[23] . CPNI -Centre for the Protection of National Infrastructure
[24] . SOCA: Serious Organised Crime Agency

گروه امنیت ارتباطات و الکترونیک قدرت و تصدی ملی امور فنی در تضمین اطلاعات را فراهم می‌آورد و تیم واکنش اضطراری رایانه‌ای[۲۵] را اداره می‌کند، و هشدارها، اعلام خطر و کمک رسانی در حل و فصل جدی حوادث فناوری اطلاعات برای بخش عمومی فراهم می‌آورد. سازمان مرکز حفاظت از زیر ساخت‌های ملی است که بر روی توصیه‌های امنیتی حفاظتی برای سازمان‌ها و کسب و کارهای مرتبط با زیرساخت‌های حیاتی ملی فعالیت می‌نماید و همکاری نزدیکی با گروه امنیت ارتباطات و الکترونیک دارد و نقش هماهنگی در پاسخ گوئی به حوادث امنیتی را برای حرفه‌ها و سازمان‌هایی که زیرساخت‌های حیاتی ملی بریتانیا را تشکیل می‌دهند، ایفا می‌نماید. این سازمان در ۱ فوریه ۲۰۰۷، از ادغام مرکز هماهنگی زیرساخت های امنیت ملی و بخشی از سرویس امنیتی بریتانیا، ایجاد گردید. واحد مرکز هماهنگی زیرساخت‌های امنیت‌ملی مسئولیت ارائه مرکز مشاوره امنیت ملی و مشاوره و اطلاعات مربوط به شبکه‌های رایانه‌ای دفاعی و مسائل مربوط به تضمین اطلاعات غیررایانه‌ای را عهده‌دار بود و مرکز مشاوره امنیت ملی مسئولیت ارائه مشاوره در مورد امنیت فیزیکی و مسائل امنیتی کارکنان را به عهده داشت. سازمان حفاظت از زیرساخت‌های ملی از نظر ساختاری یک سازمان بین اداره‌ای، با منابعی از تعدادی از ادارات و سازمان‌های دولتی، مانند سرویس امنیتی بریتانیا، گروه امنیت ارتباطات و الکترونیک و دیگر سازمان‌های مسئول زیر ساخت‌های حیاتی است. این سازمان به مدیر کل سرویس امنیتی بریتانیا پاسخگو است و تحت قانون سرویس امنیتی ۱۹۸۹ عمل می‌نماید (حسینی و ظریف‌منش، ۱۳۹۲: ۵۷).

برای اینکه پلیس بتواند داده‌ها یا سیستم‌های رایانه‌ای مرتبط با جرایم امنیتی را تفتیش و توقیف نماید به دستور مقام قضایی نیاز دارد مگر اینکه خود شخص رضایت کتبی برای تفتیش بدهد ولی در عین حال پلیس می‌تواند بنابر وجود دلایل و فوریت امر بدون دستور قضایی اقدام به تفتیش یا توقیف داده‌ها نماید. در تفتیش چند حالت به وجود می‌آید که قابل بررسی می‌باشند و باید علاوه بر قواعد صلاحیت برای دسترسی، حریم خصوصی را در کنار آن ها نیز مدنظر قرار داد. در تفتیش مرسوم و سنتی هیچ تمایزی بین حامل داده و داده ذخیره شده در آن وجود ندارد. بنابراین در صورتی که اماکن تفتیش می‌شدند فقط داده‌های موجود در حامل داده که در اماکن واقع شده بود، قابل تفتیش بودند. برای تفتیش داده موجود در حامل داده واقع در محل دیگر یک اخظاریه تفتیش جداگانه یا یک رویه قانونی تصریح شده برای تفتیش محل دیگر لازم بود (زندی، ۱۳۹۳: ۱۳۱).

با استفاده از تسهیلات ارتباطی شبکه، کاربر می‌تواند باعث شود که داده در سامانه‌های متصلی که در مکان‌هایی غیر از محل استقرار کاربر قرار دارند، ذخیره شوند. متهم می‌تواند داده‌ای را که ممکن است هدف تفتیش یا توقیف باشد، به جای دیگری منتقل کند، بدون اینکه برای مقامات تحقیق این امکان وجود داشته باشد که محل استقرار دیگر را حدس بزنند. همچنین تحت شرایط معین، تنظیم و اجرای جداگانه سامانه رایانه‌ای متصل، احتمال خطر ضایع شدن ادله را به‌وجود می‌آورد. بنابراین به نظر می‌رسد که لازمه منطقی جامعه اطلاعاتی این است که مقامات تحقیق صلاحیت استفاده از ورودی‌های منتطقی را داشته باشند.

[25] . Gov Cert UK

در هر صورت اقدام پلیسی که باید توسط ضابطین در جهت توقیف ادله جرایم سایبری از جمله جرایم امنیتی انچام پذیرد، بدین ترتیب است که، بلافاصله پس از اطلاع از وقوع جـرم، باید اقداماتی را که برای حفظ آثار و دلایل جرم و جلوگیری از فرار یا اخـتفای مـتهم ضـروری است، انجام دهد و مراتب را به مقام قضایی اعلام کند. از آنجا که دلایل ارتکاب جرم در فضای مجازی، عمدتا ادلهء الکترونیک مـی‌باشند، پلیس بـه منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می‌شود که در سایر جرایم مـطرح نـیست. ادلهء دلایل الکـترونیک، ویژگی‌هایی دارند که آن‌ها را از دلایل سنتی متمایز می‌سازد. این گونه دلایل نسبت به اسناد و مدارک دیگر، آسیب‌پذیرتر هستند؛ زیرا بـه آسانی می‌توان آن‌ها را دستکاری یا جعل کرد و یا با استفاده از دانش فنی مناسب پنـهان کرد.

۳- اقدام قضایی

ماده ٦٧١ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ نیز مقرر داشته است: «تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد». مطابق ماده ۱۱ آیین‌نامه جمع‌آوری و استنادپذیری ادلّه الکترونیکی؛ «مقام قضایی در جریان تحقیق و فرایند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره‌شده را ازجمله داده‌های رمزنگاری‌شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده‌هایی که نوع و نام آن‌ها موقتاً تغییریافته و یا داده‌هایی که برای بررسی آن‌ها نیاز به سخت‌افزار مخصوصی می‌باشد، صادر نماید». در تبصره ۲ همین ماده آمده است: «قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می‌باشد».

در ایران؛ ماده ٦٧٥ آیین دادرسی کیفری ۱۳۹۲ بیان می‌دارد که توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذر واژه یا رمزنگاری و ضبط حامل های داده عمل می‌شود.

به تصریح ماده مذکور تـوقیف داده‌های رایانـه‌ای بـا رعـایت ضوابط مقرر از جـمله: تـناسب، نوع، اهمیت و نقش داده‌ها در ارتکاب جرم که تشخیص آن با مقام قضایی است امکان پذیر است. لازم به ذکر است، ماده ٦٧١ ق.آ.د.ک تفتیش و توقیف داده‌ها یا سامانه‌های رایانه ای و مخابراتی به موجب دستور قضایی و در مواردی به عمل می آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد. در مورد روش‌های توقیف نیز آنچه قابل توجه است این است که روش غیرقابل دسترس کردن داده‌ها از طریق تغییر گذر واژه یا رمزنگاری راه تاییدشده‌ای نیست و می‌بایست بـه عـنوان آخرین راهکار در جایی که اقدامات دیگر میسر نباشد به کارگرفته شود زیرا نرم‌افزارهایی ویژه وجود دارند که به راحتی هرگونه گذر واژه را خنثی می‌کنند (موذن‌زادگان و شایگان، ۱۳۸۸: ۹۳-۹۲).

در مورد توقیف سیستم‌های رایانـه‌ای قـانونگذار در ماده ٦٧٦ همین قانون مـوارد تـوقیف را به‌طور حصری معین کرده است. این موارد عبارتند از: الف) داده‌های ذخیره شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد؛ ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت‌افزاری امـکان‌پذیر نـباشد؛ ج) متصرف قانونی رضایت داده بـاشد؛ د) تـصویربرداری (کپی‌برداری) از داده‌ها به لحاظ فنی امکان پذیر نباشد؛ ه) تفتیش در محل باعث آسیب داده‌ها شود. شاید علت اینکه برخلاف توقیف داده‌های الکترونیکی، موارد توقیف سامانه‌های رایانه‌ای احصاء شده‌اند این باشد که گاه ممکن اسـت تـوقیف یک سیستم رایانه‌ای ضرورت پیدا کند که متصل به شبکه‌ای است که خدمات عمومی ارائه می‌کند که در اینجا بحث منافع عمومی نیز مطرح می‌شود. به همین خاطر قانونگذار در مورد توقیف سامانه‌های رایانه‌ای احتیاط بیشتری کرده است. ماده ٤٣ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی نیز در همین خصوص بیان می‌دارد که «ضابطان قضایی و سایر مأموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت وضعیت اولیه‌ای از سامانه رایانه‌ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت‌افزارها و حامل‌های داده متصل به آن که علامت گذاری و ثبت می‌شوند را تنظیم و به امضای تفتیش کننده یا توقیف کننده و متصرف قانونی که سامانه تحت کنترل اوست یا قائم مقام قانونی وی برسانند. برای ضبط دقیق مشخصات ابزار و اجزای آن تصویربرداری بلامانع است». نظیر همین اقدامات قضایی در کشورهایی که عضو اتحادیه اروپا بوده و به کنوانسیون‌های اروپایی ملحق شده‌اند نیز پیش‌بینی شده است. به‌عنوان نمونه؛ ماده ۹۷ قانون آیین دادرسی کیفری فرانسه بیان می‌کند که با موافقت بازپرس، افسر پلیس قضایی فقط اشیا، اسناد و داده‌های حاوی اطلاعات که برای کشف حقیقت مفید است را در توقیف نگه می‌دارد (تدین، ۱۳۹۱: ۱۰۹).

بند سوم: روش‌شناسی و مدل مفهومی تحقیق

تحقیق حاضر از نوع کیفی است، بدین معنی که روش‌ها و تکنیک‌های بکار رفته در جهت جمع‌آوری و تجزیه و تحلیل داده‌ها، ماهیتی کیفی و تفسیرگونه دارند. روش تحقیق کتابخانه‌ای–اسنادی بوده و ابزارگردآوری داده‌ها، فیش برداری می‌باشد.

مدل مفهومی پژوهش از نوع استدلال قیاسی است که با عنایت به ادبیات غنی با استفاده از روش تحقیق کتابخانه‌ای به مطالعه پیشینه و مبانی توقیف داده و سامانه‌های مرتبط با جرایم امنیتی سایبری پرداخته و چالش‌ها و معیارهای آن را مورد بررسی قرار می‌دهد.

بند چهارم: تجزیه و تحلیل

با تجزیه و تحلیل اقدامات پلیسی، اطلاعاتی و قضایی به شرحی که گذشت و مطالعه قوانین داخلی و اسناد بین‌المللی می‌توان به این نتیجه رسید که در جرایم امنیتی نیز مقامات قضایی، پلیسی و اطلاعاتی ملزم به رعایت یک‌سری شرایط برای توقیف داده و سامانه‌ها هستند؛ از مهمترین و اصلی‌ترین این شروط می‌توان به‌موارد ذیل اشاره کرد:

- اولین شرط برای توقیف داده و سامانه، لزوم مجوز قضایی یا همان مستند به دستور مقام قضایی بودن توقیف است. به مانند محیط فیزیکی که هر گونه تفتیش و توقیف به جز در جرایم مشهود، منوط به دستور مقام قضایی می‌باشد، در محیط سایبر نیز، به جز در جرایم مشهود که نیازمند اقدام فوری ضابطین بوده و مقنن اختیاراتی را برای توقیف بدون دستور قضایی پیش‌بینی نموده است، توقیف در جرایم غیرمشهود اعم از توقیف داده یا توقیف سامانه نیازمند دستور قضایی می‌باشد. در ایران، در قوانین و مقررات مختلف به لزوم اخذ دستور قضایی برای توقیف پرداخته شده است. ماده ٣٦ قانون جرایم رایانه‌ای، ماده ٦٧١ قانون آیین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی و ماده ١١ آیین‌نامه جمع‌آوری و استنادپذیری ادلّه الکترونیکی از جمله مهمترین مستندات پیرامون لزوم اخذ مجوز قضایی برای توقیف داده و سامانه هستند.

- از دیگر شرایط لازم برای توقیف داده و سامانه، لزوم توجه به حریم خصوصی و محرمانگی اطلاعات اکتسابی یا هر اطلاعات دیگر در مورد داده‌ها و سامانه‌ها و اشخاص مرتبط با آنهاست. در قوانین مختلف از جمله در قانون اساسی، قانون احترام به آزادی‌های مشروع و رعایت حقوق شهروندی، قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای و قانون آیین دادرسی کیفری، به لزوم رعایت حریم خصوصی در کلیه مراحل دادرسی از جمله توقیف اشاره شده است. رعایت حریم خصوصی در محیط سایبری از جمله در جمع‌آوری، توقیف و ... ادله الکترونیکی، در اسناد بین‌المللی مورد تاکید قرار گرفته است. در این خصوص؛ کنوانسیون شورای اروپا مصوب ١٩٨١ به قواعد خاص راجع به نحوه بهره‌برداری از اطلاعات شخصی پرداخته است. آنچه در اصول این سند به رسمیت شناخته شده است، برخورداری همه جانبه اطلاعات شخصی در مقاطع جمع آوری و انتقال، ازحمایت و صراحت قانون می باشد.

- شرط بعدی در فرایند توقیف داده و سامانه حفاظت از آنهاست. تدابیر متنوعی برای حفاظت از داده‌ها و سامانه‌ها در برابر حملات وجود دارد و از جمله آنها، تدابیر نظارتی است که در فضای فیزیکی مشاهده می‌شوند که نمونه‌هایی از آن در قالب دوربین‌های مدار بسته جهت کنترل اماکن استفاده می‌شوند. همانطور که بیان شد؛ روش‌های حفاظت از داده‌ها و سامانه‌های توقیف شده عبارتند از: حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت عملیات که هدف همه آنها سخت تر ساختن دسترسی مجرمان به داده‌ها و سامانه‌های توقیف شده است. در رابطه با حفاظت از داده‌ها، بخشنامه شورا و پارلمان اروپا (بخشنامه اروپا 02/58/EC) در خصوص پردازش داده‌های شخصی و حفاظت از حریم شخصی تدوین شده است.

بند پنجم: یافته‌های تحقیق (چالش‌ها و راهکارهای رفع آنها)

حقوق سنتی به دلیل گسترش فناوری‌های نوین با چالش‌های جدیدی روبرو شده است، به‌طوری که ادله غیر ملموس متعاقب فناوری‌های نوین جایگزین ادله ملموس در حقوق سنتی شده و مراجع اطلاعاتی، پلیسی و قضایی با مشکلات عدیده‌ای در زمینه تحقیق، تفتیش، توقیف و جمع آوری ادله مواجه شده‌اند. دلایل الکترونیکی انعکاس متفاوتی از سایر دلایل مطروحه در دنیای فیزیکی دارند و به علت دارا بودن ویژگی‌های منحصر به فرد خود مستلزم قواعد و تدابیر جدیدی می‌باشند. این چالش‌ها در توقیف داده و سامانه در جرایم امنیتی توسط هر یک از مراجع اطلاعاتی، پلیسی و قضایی قابل ذکر است. چالش مهم دیگری که در ارتباط با توقیف داده و سامانه در جرایم امنیتی وجود دارد، مربوطه به خود این فضای سایبر است. جرایمی که در این محیط ارتکاب می‌یابند از ویژگی‌های خاصی برخوردارند که این ویژگی‌ها موجب شده تا توقیف ادله در این فضا با رویکرد افتراقی همراه شده و از سیاست جنایی متفاوتی برخوردار گردد. بزه سایبری اساساً در فضایی فارغ از مرزهای متعارف بین‌المللی واقع می‌شود. بزهکار بدون نیاز به عبور از مرزهای مذکور می‌تواند در هر نقطه‌ای از کره خاکی مستقر باشد. در نتیجه‌ی چنین وضعیتی، اولاً: کشف جرم و شناسایی بزهکار با موانع عدیده‌ای روبرو است. ثانیاً: به دلیل گستره‌ی وسیع و پراکندگی حوزه ارتکاب جرم، در صورت کشف بزه و شناسایی بزهکار، پروسه‌ی جمع‌آوری مستندات قانونی، تعقیب و محاکمه بزهکار بسیار زمان برو پرهزینه خواهد بود. ثالثاً: در بسیاری موارد قانون حاکم و دادگاه صالح برای رسیدگی نظام عدالت کیفری را با چالش‌های جدی مواجه می‌سازد. رابعاً: فقدان قوانین لازم از یک سو و از سوی دیگر تعارض قوانین برخی از کشورها در کنار فقدان اسناد بین‌المللی لازم الاجرا و به ویژه با توجه به خصیصه فراملی بزه سایبری موانع جدی بر سر راه همکاری‌های قضایی و استرداد بزهکاران محسوب می‌شوند.

در جرایم سایبری هرروز به فراخور توسعه فناوری ابزارها شکل جدیدتری به خود می‌گیرند و در قالب برنامه‌های نرم افزاری و غیرقابل ملموس و محسوس هر روز جدیدتر می‌شود، همین موضوع موجب شده تا با تنوع ادله مواجه باشیم. اصل تنوع تنها خاص جرایم سایبری است و در واقع از اصول خاصی است که در جرم‌انگاری، کشف و مجازات مرتکبین جرایم سایبری باید مورد توجه قرار بگیرد. مجرمین حرفه‌ای با اتخاذ عملیات‌های فنی، تعداد بسیار زیادی داده پردازش شده در سیستم‌های داده‌پردازی به وجود آوردند که کنترل و محاسبه و حتی توقیف آنها به راحتی امکان‌پذیر نیست، مثلاً شخصی در یک فایل هزاران فولدر مشابه ساخته و مدارک و ادلّه جرم ارتکابی خود را در یکی از آن‌ها قرار دهد. این امر نیز می‌تواند مانعی در راه کشف و تعقیب جرایم محیط‌های دیجیتال، توقیف و در نتیجه استنادپذیری ادلّه ناشی از آن‌ها تلقی گردد. در جرایم سایبری؛ حجم اطلاعاتی که به شکل الکترونیکی ذخیره می‌شود، بسیار زیاد است که همین موضوع سبب می‌شود تا شناسایی، توقیف و کشف ادله استنادپذیر با مشکل همراه بوده و مجریان برای توقیف ادله الکترونیکی باید از میان حجم انبوهی از اطلاعات که احتمالاً برخی متناقض و لاینفک هستند اطلاعات مربوطه و موثری را پیدا کرده مورد استفاده قرار دهند. به همین دلیل گفته شده است که اصل تنوع؛ «سبب افزایش هزینه‌های کشف، طولانی شدن روند دادرسی و یا حتی نیافتن اطلاعات مربوطه می‌شود. برای رهایی از چنین مشکلی باید از راهکارها و برنامه‌های متناسب استفاده شود

(دیوید، ۲۰۰۹: ۲۲۶). لزوم توجه به اصل تنوع در اسناد بین‌المللی و در توصیه‌نامه‌ی شورای اروپا و همچنین در دستورالعمل‌های اتحادیه اروپا در زمینه‌ی آئین‌دادرسی جرائم فناوری اطلاعات از جمله تدابیری هستند که پیشنهاد شده کشورها در جرم‌انگاری، تحقیقات مقدماتی، کشف و توقیف ادله و مجازات مرتکبین مورد توجه قرار دهند. محیط سایبر، محیطی فیزیکی و ملموس نیست. این ویژگی فضای سایبر را خطرسازتر از محیط حقیقی می‌نمایاند. زیرا اولاً، عاملِ مراقب مثل پلیس، در این محیط وجود خارجی و ملموس ندارد تا جنبه بازدارندگی داشته باشد، به گونه ای که مرتکب خود را آزاد احساس کرده و ارتکاب جرم در ذهن او تسهیل می‌شود. البته پلیس سایبر با اسامی مختلفی چون پلیس شبکه، پلیس وب و غیره در که به صورت: آشورهای مختلف شکل گرفته است. نرم و اتفاقی در سایت ها گشت می زند و برای جلوگیری از تخریب، اقداماتی را بدون اینکه مرتکب او را ببیند، انجام می دهد. ثانیاً، بزهدیدگان جرایم سایبری، شامل هکینگ و کراکینگ با بزهکار مواجه نمی‌شوند و مجاورتی بین این دو وجود ندارد (نوریان، ۱۳۹۱: ۷).

بارزترین ویژگی فضای سایبر، دسترس‌پذیر ساختن سریع و با حداقل هزینهٔ کلیهٔ اطلاعات آنلاین است که بسیاری از نمونه‌های آن را در وب‌سایت های شبکهٔ جهانی اینترنت شاهد هستیم. این دسترس‌پذیری برای همگان فراهم آمده و هیچ‌گونه تبعیضی اعمال نشده است. جالت‌تر اینکه اگر صاحبان منابع اطلاعات، رأسا یا به واسطهٔ دیگران، به ویژه متصدیان شبکه‌های اطلاع‌رسانی رایانه‌ای، با اجرای تمهیدات گوناگون سخت‌افزاری و نرم‌افزاری، سعی در تحدید این میزان دسترس‌پذیری داشته باشند، توفیق چندانی نمی‌یابند. زیرا این فضا به همان راحتی انواع ابزارهای خنثی‌کننده را در اختیار همگان قرار داده است. به عبارت دیگر، تقریبا چیزی به نام تحدید دسترس به اطلاعات در فضای سایبر معنا ندارد (جلالی فراهانی، ۱۳۸۹: ۸۵). به گونه‌ای که افراد به راحتی با استفاده از رایانه‌ی شخصی یا حضور در کافی‌نت‌ها قادر خواهند بود از کلیه امکانات این فضا بدون محدودیت استفاده کنند. این ویژگی با توجه به محیط پرجاذبه و آسیب زای فضای مجازی ممکن است آثار نامطلوبی اعم ازشکل گیری جرایم یا انحرافات اخلاقی به ویژه در قشر کم سن و سال به بار آورد. برای مثال، می‌توان به قضیه شبکه‌های رایانه‌ای تله نت و دیتاپک اشاره کرد. استفاده کنندگان از این دو شبکه، ظرف مدت یک هفته شکایت هایی به مسئولان شبکه تسلیم کردند و معترض شدند که افرادی به صورت غیرمجاز به سیستم آنها دست یافته و مشکلاتی ایجاد کرده‌اند. چون سوءاستفاده الکترونیکی یاد شده وضع فراملی یافت، پلیس کانادا با همکاری پلیس آمریکا از طریق خطوط الکترونیکی شبکه ها، چهار نوجوان ۱۳ ساله مدرسه دالتون نیویورک را دستگیرکرد (پاکزاد، ۱۳۸۸: ۱۸).

از دیگر ویژگی‌های اساسی جرایم در فضای سایبری، سرعت ارتکاب آنها در کمترین زمان ممکن است. ارتکاب جرم در محیط سایبر کاری بسیار راحت است؛ هر کس با داشتن یک رایانه که امکان اتصال به اینترنت را دارد و اندک آشنایی به سواد رایانه‌ای می‌تواند مجرمی بالقوه خطرناک باشد؛ صد البته میزان آشنایی بیشتر به علوم رایانه‌ای مرتکب جرم را حرفه‌ای‌تر می‌نماید و بر درجات شدت ارتکاب جرم می‌افزاید. علاوه بر موارد بالا، محدودیت در ارتکاب جرایم در محیط واقعی به مراتب بیشتر از محدودیت در محیط سایبر است؛ برای مثال در ارتکاب سرقت از یک بانک، شاید مدت‌های زیادی برای برنامه‌ریزی و طراحی سرقت، از جمله آشنایی مقدماتی با محل، آشنایی و اطلاع کافی از وضعیت موجود بانک،

اطلاعات مالی، اطلاعات امنیتی و موشکافی در سایر جزئیات لازم باشد. از سوی دیگر محیط واقعی ایجاب می‌کند که برای شناسایی نشدن توسط نیروهای انتظامی و مردم تمام توان برای مخفی نگاه داشتن اقدامات و هویت مرتکبین صورت گیرد. لکن در جرایم محیط سایبر این محدودیت‌ها وجود ندارد؛ به راحتی می‌توان با نوشتن برنامه‌ای ساده به سیستم‌های محرمانه دولتی نفوذ کرد، بدون اینکه مرتکب کوچکترین واهمه شناسایی توسط دیگران را داشته باشد. جرایم رایانه‌ای غالباً بسیار سریع به وقوع می‌پیوندند و از شروع جرم تا اجرای آن فاصله‌ای وجود ندارد. گاهی فاصله تنها به اندازه فشردن یک کلید است.مرتکب می‌تواند، با استفاده از خصوصیات پیش گفته برای یک بار برنامه‌ای را روی رایانه هدف نصب نماید که مثلا به طور مکرر مبالغ ناچیزی از حساب یک فرد یا شرکت برای او واریز شود و این امر تا بی‌نهایت تکرار شود. این بدان علت است که عمل فیزیکی که مجرم انجام می‌دهد یک بار انجام می‌شود. اما رایانه به طور خودکار آن را تکرار می‌کند. مفهوم متعارف زمان و مکان در دنیای مجازی دچار تحول شده است. یکی از فاکتورهای کندی وقوع پدیده بزهکارانه در جهان واقعی بعد مکانی میان سه ضلع بزهکاری یعنی بزهکار، آماج بزه و مکان ارتکاب بزه است. ساختار فضای مجازی به گونه‌ای است که در آن قرابت مکان میان سه عنصر فوق ضرورتی ندارد. این وضعیت موجب صرفه جویی شگرفی از بعد زمان و هزینه برای بزهکاران گردیده و آنها را قادر ساخته است بدون وجود مانعی به نام مکان، جرایم متعددی را در سریع‌ترین زمان مرتکب شوند، هویتی را سرقت نمایند و یا پولی را از حسابی به حساب دیگرمنتقل نمایند.

پیچیدگی و تخصصی بودن یکی دیگر از ویژگی‌های فضای سایبر است. منظور از تخصصی بودن، وجود توانایی‌ای خاص در ورود به این فضا نیست. چرا که یک شخص عادی با استفاده از یک رایانه قادر به ورود به این فضا خواهد بود. لکن، پیچیدگی این فضا امری فراتر از صِرف ورود به این دنیاست. برنامه‌ریزی‌های رایانه‌ای تخصصی، تشخیص اقدامات آسیب زا در فضای سایبر، نحوه استفاده ایمن از این فضا، نحوه شناسایی و مقابله با منحرفین سایبری، تاثیر فضای سایبر بر فرهنگ و جامعه و بسیاری از امور اساسی و کلیدی که در این راستا باید بر آن اشراف داشت، نیازمندِ وجود تخصصی متناسب با پیچیدگی این فضاست.

با توجه به ویژگی‌های اختصاصی یاد شده، و اهمیت جرایم امنیتی در این فضا، راهبردهایی توسط مجامع بین‌المللی به تصویب رسیده است تا ضمن پیشگیری از ارتکاب جرایم امنیتی به ویژه از نوع تروریستی، زمینه‌های لازم برای کشف و مجازات مرتکبین این‌گونه از جرایم فراهم گردد. از جمله این اسناد می‌توان به قطعنامه‌های سازمان ملل متحد، شورای امنیت و شورای اقتصادی – اجتماعی اشاره کرد. این قطعنامه‌ها، بر دو موضوع مهم تاکید دارند: نخست اینکه لازم است تا زیرساخت‌های سایبری در هر کشور مطابق با استانداردهای بین‌المللی باشد تا امکان دفاع در برابر عملیات‌های تروریستی در فضای سایبری ممکن گردد و دیگر اینکه اجرای سیاست‌های مدنظر جز با همکاری بین‌المللی میسر نمی‌گردد. لذا، لازم است دولت‌ها در تدوین سیاست‌های خود در زمینه مقابله با جرایم امنیتی سایبری ضمن لحاظ نمودن استانداردهای بین‌المللی در این خصوص، زمینه‌های همکاری‌های منطقه‌ای و بین‌المللی را مهیا نمایند. لذا، در قوانین و سیاست‌های خود باید شرایط انجام چنین همکاری را فراهم نمایند. کنوانسیون جرایم سایبری افزایش اهمیت همکاری بین‌المللی را در مواد ۲۳ تا ۳۵ مورد بررسی قرارداده است. اعضای کنوانسیون باید از طریق اعمال ابزارهای بین‌المللی مربوط به همکاری

بین‌المللی در حوزه کیفری به منظور انجام تحقیقات یا دادرسی با یکدیگر همکاری نمایند (گرکی، ۱۳۸۹: ٤١٧-٤١٧). در این بستر، دفتر برنامه‌ریزی جرایم سایبری به عنوان نهادی موثر در زمینه همانندسازی قواعد جرم‌انگاری فضای سایبر قابل بحث و بررسی است. نهاد مذکور با کارکرد ظرفیت‌سازی خود، کار کمیته کنوانسیون سایبری جرم را تکمیل نموده و از طریق آن، دولت‌های عضو از اجرای کنوانسیون بوداپست پیروی می‌کنند. این دفتر وظیفه کمک به کشورهای سراسر جهان در راستای تقویت ظرفیت سیستم‌های حقوقی‌شان برای پاسخ‌گویی به چالش‌های ناشی از جرایم سایبری و ادله الکترونیکی بر اساس استانداردهای کنوانسیون بوداپست نسبت به جرایم سایبری را به همراه تقویت اثربخشی همکاری‌های بین‌المللی، ارتقا همکاری‌های عمومی/ خصوصی و ایجاد واحدهای تخصصی جرایم سایبری و پزشکی قانونی و بهبود همکاری‌های بین سازمانی بر عهده دارد. دفتر برنامه‌ریزی جرایم سایبری در بخارست به عنوان دیگر نهاد مبتنی بر معاهده دبیرخانه کمیته کنوانسیون جرایم سایبری دایر گردیده است. هدف این دفتر، اطمینان از اجرای پروژه‌های ظرفیت ساز در زمینه جرایم سایبری در کلیه مناطق جهان از طریق ظرفیت‌سازی در زمینه جرایم سایبری، مشاوره، پشتیبانی و هماهنگی در برنامه‌ریزی، مذاکره و اجرای به موقع فعالیت‌های هدفمند در زمینه جرایم سایبری، از جمله برنامه‌های مشترک با اتحادیه اروپا و سایر اهداکنندگان و ایجاد مشارکت در برابر جرایم سایبری با سازمان‌های بخش دولتی و خصوصی می‌باشد. این دفتر همچنین مسئول کمک به کشورهای جهان در تقو یت ظرفیت سیستم‌های حقوقی خود برا ی پاسخ‌گویی به چالش‌های ناشی از جرایم اینترنتی و شواهد الکترونیکی بر اساس استانداردهای بوداپست است (شورای اروپا، ۲۰۲۰). همچنین، «دستورالعمل در خصوص حملات علیه سیستم اطلاعاتی» مصوب ۲۰۱۳ با هدف مقابله با حملات سایبری در مقیاس بزرگ تدوین یافته است تا نیاز کشورهای عضو برای تقویت قوانین در حوزهٔ جرائم سایبری در سطح ملی و معرفی ضمانت اجراهای کیفری سخت‌تر را بیش از پیش مرتفع سازد. در سال ۲۰۱۷، کمیسیون گزارشی را منتشر کرده است که به موجب آن، ارزیابی می‌شود تا چه میزان کشورهای عضو اقدامات لازم را برای رعایت دستورالعمل انجام داده اند (مجله رسمی اتحادیه اروپا، ۲۰۱۳). لیکن، متأسفانه ایران تاکنون به هیچ یک از اسناد بین‌المللی مربوط به جرایم رایانه‌ای از جمله کنوانسیون بین‌المللی جرایم سایبری بوداپست ۲۰۰۱ ملحق نشده است. این امر یکی از چالش‌های اساسی نظام کیفری ایران در برخورد با جرائم ارتکابی در حوزه سایبر به شمار رفته و امکان نیل به یکسان‌سازی قواعد و اصول و همسان سازی تدابیر اجرایی را کمتر می‌نماید.

۱- چالش‌های پلیسی و اطلاعاتی و راهکارها رفع آنها

چالش‌های پلیسی‌گری در فضای سایبر که تعامل اجتماعی، محدودیت‌های فضای فیزیکی را ندارند، دو چندان شده است؛ مثل جرایم امنیتی که مجرمان و قربانیان ممکن است در کشورهای مختلف باشند. رویکردهای متعددی از جمله فعالیت عادی، مناطق جرم خیز، پلیسی‌گری جامعه محور و رویکردهای مشابه همگی قدرت خود را از ایجاد رابطه میان پلیسی‌گری و سرزمین می‌گیرند. این در حالی است که پلیسی‌گری فضای سایبر، حرکتی از پلیسی‌گری سرزمین به سوی پلیسی‌گری جمعیت‌های مظنون است و در عین حال حرکتی است از سوی نظارت به داده بینی. لذا، مقابله با جرایم سایبر، راهکارهای

بین‌المللی را می‌طلبد، زیرا که این مسئله اساساً جهانی است (رجبی، ۱٤۰۰، ٤). پلیس به منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می‌شود که در سایر جرایم مطرح نیست. ادله الکترونیکی، ویژگی‌هایی دارند که آن‌ها را از دلایل سنتی متمایز می‌سازد. این گونه دلایل نسبت به اسناد و مدارک دیگر، آسیب‌پذیرتر هستند؛ زیرا به آسانی می‌توان آن‌ها را دستکاری یا جعل کرد و یا با استفاده از دانش فنی مناسب پنهان کرد. همچنین مسایلی چون حریم محرمانگی، ارایه، استناد پذیری و ... نیز در این نوع ادله بسیار بحث برانگیز می باشد. البته، با وجود برخی اسناد بین‌المللی و اروپایی راهکارهایی در حال شکل گرفتن هستند. از جمله این اسناد، کنوانسیون جرایم سایبری است. هدف از این کنوانسیون آن است که دولت‌ها از طریق قوانین داخلی اشکال مختلفی از جرم سایبری جرم‌انگاری کنند و آئین‌های دادرسی ضروری برای بررسی چنین جرایمی را در چارچوب صلاحیت قوانین ملی خود بگنجانند. البته، پلیسی‌گری فضای سایبر که بالقوه غیرقابل کنترل است، علاوه بر دخالت دولت‌ها، نیازمند انتقال مسئولیت‌پذیری به کاربران و همکاری معماران سیستم است. مفهوم پلیسی‌گری چندگانه و تقسیم وظایف انتظامی یکی از علائم حاکمیت بر فضای سایبر است. لذا، مشکلات ناشی از ماهیت فراسرزمینی فضای سایبر جنبه‌های متعددی از معیارهای در حال تغییر زمامداری جزایی معاصر را نشان می‌دهد که در آن چندپارگی و فاصله به شدت افزایش می‌یابد. بر این اساس، جرایم سایبر به ویژه جرایم امنیتی نیازمند همکاری‌های بین‌المللی فراوان پلیس و حجم انبوهی از کار کارشناسی است و رویکرد مسئولیت‌پذیری و تعدد پلیسی‌گری از جنبه‌های حیاتی حاکمیت بر فضای سایبر تلقی می‌شود. به‌نظر می‌رسد در وضع کنونی، سیاست جنایی پلیس در ایران، کارایی مؤثر را برای پیشگیری از جرایم سایبری دارا نبوده و علیرغم افزایش جرایم سایبری، پلیس نتوانسته است به‌طور مؤثر به تهدیدات مطرح شده واکنش نشان دهد و این به دلیل آماده نبودن بستر و زمینه برای سیاست هماهنگ پلیس در بعد بین‌المللی می‌باشد. عدم هماهنگی در ابعاد بین‌المللی، هر چند در جرایم غیرامنیتی، قابل جبران بوده یا حداقل تاثیر موثری در امنیت کشور ندارد، اما، در جرایم امنیتی، تهدیدی برای امنیت ملی خواهد بود. بنابراین حل معضلات پلیسی و تغییر ماهیت اقدامات پلیسی از فضای سنتی به سایبری که نیازمند هماهنگی با اسناد بین‌المللی پیرامون اقدامات پلیسی می‌باشد، امری حیاتی و ضروری می‌باشد.

یکی دیگر از چالش‌های اساسی مأموران اجرای قانون، دشواری کشف جرایم سایبری است، که در همین ارتباط نیز هماهنگی بین‌المللی می‌تواند نقش موثری در رفع آن داشته باشد. جرایم سایبری در بستری رها و در پوششی ناشناخته و گمنامی نسبی بزهکاران انجام می‌شود و اثری ملموس و مادی از جرم و ردپای مجرم آن‌گونه که در جرایم سنتی برجای می‌ماند، مشاهده نمی‌شود و در بیشتر موارد همان اندک ادله الکترونیکی باقیمانده از جرم نیز به‌راحتی قابل پاک‌سازی است. آنچه بدیهی است نمی‌توان با برنامه‌ها و راهبردهایی که ناظر به جرایم سنتی است، نسبت به مبارزه با این جرایم اقدام نمود. افزون بر این، آن دسته از جرایم بر خلاف جرایم سنتی، از الگوهای فیزیکی و محدودیت‌های ناظر بر آن پیروی نمی‌کنند. در نتیجه، بزهکاران می‌توانند بدون تماس چهره به چهره و مجاورت با بزه‌دیده، مرتکب جرم شوند که این ویژگی ممتاز، ردیابی و شناسایی آنان را دشوار می‌سازد. از این‌رو تعقیب جرایم سایبری در اکثر موارد به دلیل اخفای این نوع جرایم با مانع مواجه است. برای نمونه جاسوسی رایانه‌ای از طریق نسخه‌پردازی از فایل‌های داده و سرقت مال معمولاً در شرکت‌های

بزه دیده به‌عنوان جرم نمایان نمی‌شود؛ زیرا این شرکت‌ها غالباً فرصت کشف و اثبات استفاده غیرمجاز از داده‌های خود در شرکت رقیب را که به خوبی از آن محافظت می‌شود، نمی‌یابند.

نداشتن تخصص کافی نهادهای اجرایی همگام با پیشرفت روزافزون فناوری‌ها در راستای توقیف ادله جرایم امنیتی سایبری نیز چالش دیگری محسوب می‌شود. تدابیر پیشگیرانه و مقابله‌ای در صورتی می‌توانند مؤثر واقع شوند که طرفین درگیر در قضیه قادر به پاسخگویی به درخواست‌های یکدیگر باشند و این امر در گام نخست، نیازمند روزآمد بودن سطح دانش هر یک از نیروهایی است که به نوعی در این فرآیند مشارکت دارند؛ چرا که صرف توان علمی بالای یکی از طرف‌های درگیری نمی‌تواند منجر به موفقیت پیشگیری از بزهکاری سایبری شود و اهمال و کاستی هر یک از طرفین می‌تواند همگان را با خسارات سهمگین سایبری مواجه کند. این شکاف، امروزه میان کشورهای توسعه‌یافته و کشورهای کمتر توسعه‌یافته یا توسعه‌نیافته به وضوح قابل مشاهده است. به همان میزانی که کشورهای اخیر با ضعف قوانین خود، پناهگاه‌هایی امن به شمار می‌آیند، عدم آگاهی نیروهای پلیس سایبری آنها نیز بزهکاران را در انتخاب این کشورها مصم می‌سازد (فرهادی آلاشتی و جوان جعفری بجنوردی، ۱۳۹۶: ۲۵). بدین ترتیب، به سبب عدم هماهنگی آموزش‌ها و مهارت‌های متخصصان با یکدیگر، هر یک از روش‌ها و شیوه‌های گوناگونی برای پاسخگویی به درخواست طرف یا طرف‌های مقابل استفاده می‌کنند و قادر به تعامل مناسب با یکدیگر نیستند و احتمال عدم موفقیت در تأمین خواسته‌های طرف مقابل وجود خواهد داشت. نتایج سوء ناشی از عدم هماهنگی سطح دانش نیروهای پلیس در سال‌های اخیر از نظر نهادهای بین‌المللی و منطقه‌ای مسئول مبارزه با جرایم سایبری پوشیده نمانده و آنان نیز به این اجماع دست یافته‌اند که هرگونه تلاش برای ایجاد فضای امن و پیشگیری مؤثر از جرایم سایبری در گام نخست نیازمند دانش تخصصی همگام با شیوه‌های نوین ارتکاب جرم می‌باشد. در حال حاضر، ایران جز صادرکنندگان تکنولوژی رایانه‌ای در دنیا نیست و به تبع، پلیس ایران نیز در زمینه شناسایی، کشف، جمع‌آوری ادله و پی‌جویی جرایم دارای ضعف‌هایی می باشد، به گونه ای که هر ساله شاهد ورود خسارت‌های هنگفت مالی و حیثیتی به اشخاص اعم از حقیقی و حقوقی هستیم. همچنین، میزان اعتبار ادله جمعآوری توسط ضابطان از دیگر چالش‌های بحث است. هرچند به نظر می‌رسد ادله الکترونیکی در چهارچوب نظرات کارشناس اعتبار می یابد، ولی نوع نگاه مراجع رسیدگی‌کننده به جرایم سایبری و میزان تخصص و آشنایی آن‌ها با ادله الکترونیکی نقشی تعیین‌کننده در سرنوشت تعقیب و اثبات این جرایم دارد. جهت تقویت در این حوزه باید به آخرین نوآوری‌ها دست یافته و از طریق همکاری با اینترپل و یوروپل از تجارب آنها بهره‌مند شد. همچنین، ضرورت ایجاد یک نهاد پلیسی بین‌المللی مرتبط با جرم سایبری مانند تشکیل پلیس جهانی اینترنتی می‌تواند نقش پررنگی در مقابله با این جرایم ایفا نماید (محسنی و صوفی زمرد، ۱۳۹۶: ۱۸۰-۱۷۹).

۲- چالش‌های قضایی و راهکارهای رفع آنها

در طول قرون متمادی، سیستم‌های قضایی بر موضوعات ملموس و عینی متمرکز شده‌اند و مقررات جزایی به حمایت از این دسته موضوعات پرداخته است. این در حالی است که امروزه اموال غیر مادی اهمیت بسیار یافته‌اند. داده‌ها و اطلاعات

تبدیل به نوعی دارایی شده‌اند که می‌توان موضوع ارتکاب جرم واقع شود و رژیم حقوقی مربوط به موضوعات این‌چنینی، تنها نمی‌توانند بر مبنای قیاس با قواعد موجود و مختص به موضوعات مادی بنا شود؛ زیرا نحوهٔ ارزیابی و حمایت داده‌ها و اطلاعات با آنچه در خصوص اشیای مادی مقرر است تفاوت قابل‌ملاحظه‌ای دارد ازهمین‌رو به تغییر در طرح و چهارچوب قضایی جاری نیازمندیم. به‌عنوان نمونه، ماهیت جرایم سایبری به این صورت است که چالش‌های عمیق موجود در نظام حقوق بین‌الملل همانند تعارض دادگاه‌ها و تعارض قوانین را شدت می‌دهد. زیرا، در جرایم سایبری محل وقوع جرم مشخص نیست تا دادگاه صالح به رسیدگی بر آن جرم را مشخص کند. از این‌رو، بسیاری از کشورها، مکان ارتکاب را بر مبنای دکترین (حضور درهر جا) تعیین می‌کنند. طبق این دکترین، جرم چنانچه، مقدار یا فقط بخشی از آن در یک مکان ارتکاب یافته باشد، تماماً ارتکاب یافته در آن محل فرض می‌شود، بدین ترتیب که طبیعی است که چند دولت خود را صالح به رسیدگی بدانند (شورای اروپایی جرایم سایبری، ۱۹۹۰: ۱۵۳). در مسائل بین‌المللی، اولین اثر جرایم امنیتی در محیط سایبری از منظر چالش‌های قضایی، بحث صلاحیت است. علی‌الخصوص در قواعد حاکم بر صلاحیت سرزمینی و مکان ارتکاب، مقام صالح دچار مشکل می‌شود. زیرا جرایم رایانه‌ای، فراملی بوده که موجب تعدد محل ارتکاب و تعدد صلاحیت‌ها می‌شوند، از همین‌رو باید با نگرش به پیش‌بینی‌های صورت گرفته در اسناد بین‌المللی و منطقه‌ای و به ویژه مقررات پیش‌بینی شده در شورای اروپا پیرامون محیط سایبر، نسبت به اصلاح قوانین و هماهنگی برای همکاری‌های قضایی در سطح بین‌المللی اقدام گردد.

جرایم رایانه‌ای، مبتنی بر فناوری اطلاعات است و در جهان شبکه‌ای امروز، دیگر هیچ جزیره‌ای منزوی محسوب نمی‌شود. از این رو، جرایم رایانه‌ای طبع جهانی دارد و مقابله با آنها اقدامات یکسان بین‌المللی را می‌طلبد و چنانچه این جرایم در سیستم‌های قضایی کشورهای مختلف به صو رت یکسان تعریف نشوند، تلاش‌های ضابطان اجرایی برای برخورد هماهنگ با این جرایم، غامض و پیچیده خواهد شد. پلیس بین‌الملل، کنوانسیون اروپایی جرایم مجازی همگی در این زمینه به دنبال ادبیات واحدی هستند. به نظر می‌رسد که قواعدی نیز باید وضع گردد تا مسئولیت رسیدگی به جرایم در سطح بین‌المللی را مشخص نماید (حیدری، شهبازی و شیبانی، ۱۳۹۷: ٤٨). با توجه به جنبه فراملی بودن جرایم رایانه‌ای در حوزه پیشگیری از جرم و آئین دادرسی، کشف جرایم سایبری، تعقیب متهمان، دستگیری، انتقال محکومان، نیابت قضایی و بازجویی رویه یکسانی در کشورها به خصوص ایران در بعد بین‌المللی به چشم نمی‌خورد. در واقع، کشورها ناگزیر هستند در راستای گسترش همکاری‌های بین‌المللی، چهارچوب‌های حقوقی و رویه‌های اجرایی جدیدی تعریف نمایند تا سیاست اجرایی بتواند نقش مؤثری ایفا نماید (اشرر، ۲۰۱۲: ۱۳٤). با توجه به ویژگی فرامرزی بودن برخی جرایم رایانه‌ای، قانون ایران و کنوانسیون جرایم سایبری راهکاری در خصوص جمع‌آوری موجود در خارج از مرزهای کشور ارائه نکرده‌اند و این امر به عنوان مهمترین چالش در پلیس سایبری کشورها مطرح شده و راهکاری در این خصوص ارائه نشده است (جلالی فراهانی، ۱۳۹٤: ٤٧). در حالی که، اگر مجرمان و اهداف در کشورهای مختلفی قرار داشته باشند، پیگرد جرم سایبری نیاز به همکاری پلیس در همه کشورهای تحت تأثیر دارد؛ مجرمان نیاز به‌حضور در همان مکانی که هدف قرار گرفته، ندارند. مکان امن در

کشورهایی با قانونگذاری ضعیف می‌تواند از محدودیت‌های نهادهای اجرایی بین‌المللی باشد (گرکی، ۱۳۸۹: ۱۳۵۳). این عوامل تهدیدکننده، افزایش پویایی دستگاه های اجرایی را ضروری می‌سازد.

نتیجه‌گیری

با عنایت به بررسی‌های صورت گرفته نتایج ذیل حاصل شد:

۱- یکی از مهمترین پیوندهای منفی که برای داده و سامانه می‌توان ذکر کرد، استفاده مجرمانه از آن است. زمانی که از داده و سامانه به عنوان وسیله ارتکاب جرم یا به عنوان موضوع جرم استفاده می‌شود، یکی از اقدامات پلیسی و قضایی، توقیف داده و سامانه می‌باشد. با توجه به تبیین اقدامات پلیسی، امنیتی و قضایی پیرامون توقیف داده و سامانه و همچنین بررسی شرایط توقیف آنها در جرایم امنیتی سایبری ذکر شد می‌توان به این نتیجه رسید که در توقیف جرایم امنیتی سایبری نیز به مانند سایر جرایم سایبری باید اصولی همچون اصل قانون‌مندی، اصل تناسب و تنوع مورد رعایت قرار گرفته و شرایط قانونی پیش‌بینی شده برای توقیف داده‌های و سامانه‌های مرتبط با جرایم سایبری رعایت شود.

۲- توقیف داده و سامانه و بطور کلی توقیف ادله در جرایم سایبری دارای جهات اشتراک و افتراق متعددی در مقایسه با توقیف ادله در جرایم امنیتی سایبری هستند. در مورد جهات اشتراکی می‌توان به این جمع‌بندی رسید که هم در جرایم سایبری و هم در جرایم امنیتی سایبری وظیفه توقیف، بر عهده ضابطین دادگستری است. شیوه اقدام آنها نیز در جرایم مشهود و غیرمشهود معمولاً مشابه هم می‌باشد، اصل قانون‌مندی توقیف، لزوم دستور قضایی برای توقیف نیز از دیگر جهات اشتراکی آنها می‌باشند. در مورد جهات افتراق توقیف ادله در جرایم سایبری در مقایسه با جرایم امنیتی سایبری نیز، نتایج نشان می‌دهد که با توجه به اهمیت جرایم امنیتی سایبری و شیوه‌های متعددی که توسط مجرمین در راستای ارتکاب جرایم امنیتی در این فضا انجام می‌دهند، شیوه توقیف، نحوه نگهداری، قابلیت استنادپذیری و آثاری که توقیف ادله در جرایم امنیتی سایبری دارد متفاوت از جرایم سایبری خواهد بود.

۳- بدلیل تفاوت‌هایی که بین جرایم امنیتی سایبری و جرایم سایبری وجود دارد، مقامات قضایی، انتظامی و اطلاعاتی، برای توقیف داده و سامانه‌های الکترونیکی با چاش‌هایی مواجه می‌باشند که در یک نقسیم‌بندی کلی می‌توان آنها را به چالش‌های قضایی و چالش‌های انتظامی –اطلاعاتی تقسیم‌بندی کرد. برای فائق آمدن بر این چالش‌ها، فراهم نمودن زیرساخت‌های لازم و ایمنی بخشی داده‌ها و سامانه‌ها و همکاری‌های بین‌المللی می‌توانند راهکارهای کاربردی باشند.

٤- ماهیت جرایم امنیتی سایبری متفاوت از سایر جرایم در این فضا بوده و با ابزارهای مختلف ممکن است حاکمیت کشورها توسط بزهکارن جرایم امنیتی مورد مخاطره قرار بگیرد. برای مقابله با این جرایم و در راستای کشف و توقیف ادله الکترونیکی مرتبط با جرایم امنیتی اقداماتی برای مراجع قانونی پیش‌بینی شده است. مراجع قانونی

که وظایفی در ارتباط با توقیف ادله الکترونیکی جرایم امنیتی سایبری بر عهده دارند؛ عبارتند از: مراجع اطلاعاتی، مراجع پلیسی و مراجع قضایی. این مراجع اقدامات اطلاعاتی، پلیسی و قضایی را برای پیش‌بینی، پیشگیری، پی‌جویی، کشف، تحقیقات مقدماتی و رسیدگی به جرایم امنیتی سایبری انجام می‌دهند. با وجود اینکه راهبردهای متعددی توسط اسناد بین‌المللی و اروپایی در ارتباط با نحوه اقدام توسط مراجع یاد شده پیش‌بینی شده، همچنان، این مراجع جهت انجام وظایف خود، با چالش‌هایی همراه می‌باشند. مراجع یاد شده در ایران، بدلیل عدم الحاق به کنوانسیون جرایم سایبری و عدم همکاری لازم با مراجع بین‌المللی و پلیسی سایر کشورها وضعیت مطلوبی ندارد.

پیشنهادها

با عنایت به نتایج بدست آمده، پیشنهادهای ذیل کاربردی به‌نظر می‌رسد:

۱. لزوم پویایی و تکامل‌پذیری مقرره‌های توقیف داده و سامانه در نظام حقوقی ایران با الگوپذیری و در همگرایی با اسناد اروپایی جهت ایجاد وحدت رویه در توقیف داده‌ها و سامانه‌های مرتبط با جرایم امنیتی سایبری؛
۲. لزوم بسترسازی برای همکاری‌های منطقه‌ای و جهانی در راستای توسل به رویه‌های واحد در توقیف داده و سامانه جرایم امنیتی سایبری در سطح ملی و بین المللی؛
۳. لزوم هماهنگی با مقررات بین‌المللی به ویژه اسناد اروپایی که دارای نظام قاعده‌مندی در خصوص جرم-انگاری جرایم امنیتی سایبری، کشف، تفتیش و توقیف داده و سامانه، تحقیقات مقدماتی، ادله اثبات، استنادپذیری و ... می‌باشند.
٤. لزوم ارائه آموزش‌های فراگیر و متناسب به مقامات قضایی و ضابطان دادگستری با تاکید بر تمایزات توقیف داده‌ها و سامانه‌های مرتبط با جرایم امنیتی سایبری در مقایسه با سایر جرایم سایبری.

فهرست منابع و مآخذ

۱- بهره‌مند، حمید؛ داودی، ذوالفقار (۱۳۹۷). پیشگیری اجتماعی از جرایم امنیتی ــ سایبری، فصلنامه مطالعات حقوق کیفری و جرم‌شناسی دانشگاه تهران، شماره ۱، ۱-۲.
۲- پاکزاد، بتول (۱۳۸۸)، تروریسم سایبری، رساله دکتری حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی،
۳- تدین، عباس (۱۳۹۱)، قانون آیین دادرسی کیفری فرانسه، چاپ اول، معاونت حقوقی قوه قضاییه، انتشارات خرسندی، تهران،
٤- جلالی فراهانی، امیر حسین (۱۳۸۹)، تروریسم سایبری، مجله فقه و حقوق، شماره ۱۰، ۸۵.

۵- جلالی فراهانی، امیرحسین (۱۳۹٤)، درآمدی بر آیین‌دادرسی کیفری جرائم سایبری، چاپ اول، انتشارات خرسندی،
٦- حسینی، پرویز؛ ظریف‌منش، حسین (۱۳۹۲)، مطالعه تطبیقی ساختار دفاع سایبری کشورها، فصلنامه پژوهش های حفاظتی امنیتی دانشگاه جامع امام حسین(علیه السلام)، سال دوم، شماره ی ۵، ۵۷.
۷- حیدری، مسعود؛ شهبازی، امید؛ شیرانی، پویا (۱۳۹۷)، چالش‌ها و فرصت‌های پیش روی پلیس در برخورد با جرایم سایبری. فصلنامه کارآگاه، شماره ۱۲، ٤۸.
۸- زندی، محمدرضا (۱۳۸۹)، تحقیقات مقدماتی در جرایم سایبری، چاپ اول از ویرایش جدید، انتشارات جنگل، تهران.
۹- عالی‌پور، حسن؛ تبریزی، صادق، الهی‌منش، محمدرضا (۱٤۰۱)، اصل تناسب در توقیف داده و سامانه در فرایند کیفری، مجله حقوقی دادگستری، شماره ۱۱۷، ٤۰،
۱۰- عاملی، سعید رضا (۱۳۸۲)، دو جهانی شدن و آینده جهان، کتاب ماه علوم اجتماعی،
۱۱- غلامی، حسین (۱۳۹۱)، اصل حداقلی حقوق جزا». فصلنامه‌ی حقوق کیفری، سال اول، ش ۲، ٤۵.
۱۲- گرکی، مارکو (۱۳۸۹)، جرایم سایبری؛ راهنمایی برای کشورهای در حال توسعه، ترجمه: مرتضی اکبری، چاپ اول، انتشارات پلیس فضای تولید و تبادل اطلاعات ناجا،
۱۳- مرادی، صادق؛ شکرچی‌زاده، محسن؛ نقش، امیررضا؛ مسعود، غلامحسین (۱٤۰۱)، تهدیدات و جرایم سایبری علیه امنیت و چالش های پیش رو، فصلنامه فقه جزایی تطبیقی، شماره ۱، ۱-۲.
۱٤- میرمحمدصادقی، حسین (۱۳۹٦)، حقوق کیفری اختصاصی ۳، تهران، انتشارات میزان،
۱۵- مؤذن زادگان، حسن علی؛ شایگان، محمد رسول (۱۳۸۸)، استناد پذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران، مجله دیدگاه های حقوق قضایی، شماره ٤۸، ۹۳.
۱٦- نجفی‌ابرندآبادی، علی حسین (۱۳۹۵)، جرم‌شناسی در آغاز هزاره سوم، درآمد در: دانشنامه جرم‌شناسی، چاپ چهارم، انتشارات گنج دانش،
۱۷- یزدیان جعفری، جعفر (۱۳۹۵)، تقابل امنیت فردی و ملی در جرایم علیه امنیت، پژوهش حقوق کیفری، سال چهارم، شماره چهاردهم، ٦۰.
۱۹. Cyber Security Strategy of the United Kingdom safety (2010), security and resilience in cyber space published by TSO.
۲۰. Council of Europe – cybercrime (1990), Recommendation No. 89, Strasbourg, the translation of the High Council of Informatics, Management and Planning Organization of Iran, 1376.

٢١. European court of Auditors. (2019), Challenges to effective EU cybersecurity policy. Briefing Paper. 1-74.
٢٢. European Cybercrime Centre. (2020), Combating crime in a digital age. Europol, 2014. https://www.europol.europa.eu/ec3 (last visited on 6/5/2020).
٢٣. Europol (2020), About Europol. https://www.europol.europa.eu/about-europol (last visited on 7/5/2020).
٢٤. Europol (2020), EC3 Programme Board. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-programme-board (last visited on 6/6/2020).
٢٥. Europol. (2020), Operations. https://www.europol.europa.eu/activities-services/europol-in-action/operations (last visited on 6/6/2020).
٢٦. Scherrer, Joseph H., Grund, William, C. (2012), A Cyberspace Command and Control Model. Maxwell Paper No. 47, Air War, College.

Seizing of data and system in security crimes; Challenges and criteria

Abstract

Security crimes have a mixed nature from the point of view of the time of crime behavior.The three-stage process of intelligence action, police action and judicial action alternately includes criminal behaviors on the verge of occurrence, during occurrence and after occurrence.With the computerization of crimes against national security, whether the computer is the subject of a crime or a platform for the realization of traditional security crimes, the importance of data and system seizure for three measures of intelligence, police and justice is obvious; However, there are three major challenges facing data and system seizure; First, to what extent can data seizure and the system for information action be used for police and judicial actions. Second, to what extent the data seizure and the system follow the principles stipulated in the Criminal Procedure Law. Thirdly, to what extent is the seizure of the data and the system at the stage when the crime has not yet occurred or is about to occur or is occurring, to what extent is it compatible with the principles of criminal law and respecting the rights of citizens. The present article tries to explain the challenges of data and system seizure in security crimes by descriptive and analytical methods and to present the correct criteria for seizure. The findings of this research show that the challenge of data and system seizure is a function of the characteristics of the cyberspace, security attitudes towards the cyberspace, the nature of cybercrimes and the role of judicial officers in the direction of judicial authorities in prosecuting security crimes. In addition, the written solution is in line with compliance as much as possible with the principles and criteria of data seizure on legality, proportionality and documentation.

Abstract: security crimes, cyber space, data and system seizure, Informational and judicial action