شناسهٔ دیجیتال (DOI): 10.22106/JLJ.2021.531735.4218

مجله حقوقی دادگستری

مقالهٔ پژوهشی، دورهٔ ۸۶، شمارهٔ ۱۱۷، بهار ۱۴۰۱، صفحات ۱۳۱ تا ۱۵۲
تاریخ دریافت: ۱۴۰۰/۰۳/۲۳ - تاریخ پذیرش: ۱۴۰۰/۰۵/۱۴

اصل تناسب در توقیف داده و سامانه در فرایند کیفری[1]

صادق تبریزی*، حسن عالی‌پور**، محمدرضا الهی‌منش***

چکیده

درک اصل تناسب در توقیف داده و سامانه در گرو فهم درست ماهیت داده و سامانه است. داده به‌عنوان اطلاعات یا هر نماد قابل‌ذخیره، انتقال و پردازش از طریق سامانه‌های رایانه‌ای و سامانه، بستری برای کنش‌ها و قابلیت‌های مرتبط با داده است. پیوستگی این دو به هم، بستر رایانه‌ای و سپهر فناوری اطلاعات و ارتباطات را شکل می‌دهد که اصل تناسب باید با توجه به همین ویژگی معنا شود. اصل تناسب در توقیف داده، به معنای برقراری توازن میان چهار عنصر ضرورت توقیف، اهمیت داده و سامانه، ارتباط داده یا سامانه با جرم و ارتباط داده یا سامانه با داده‌ها و سامانه‌های دیگر است. نوشتار حاضر با بهره‌گیری از منابع کتابخانه‌ای و تصمیمات قضایی، به روش توصیف و تحلیل کوشیده تا نشان دهد، تناسب در توقیف داده و سامانه، با توقیف بستر فعالیت قابل‌مقایسه است و نه توقیف مال یا سند و به این نتیجه رسیده است که 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.

واژگان کلیدی: داده، سامانه، تحقیقات مقدماتی، توقیف داده یا سامانه، اصل تناسب

۱. این مقاله برگرفته از رسالهٔ دکتری تخصصی آقای صادق تبریزی تحت عنوان «بررسی تطبیقی توقیف داده و سامانه در مرحلهٔ تحقیقات مقدماتی در نظام کیفری ایران و نظام حقوقی اتحادیه اروپا» با راهنمایی آقایان دکتر حسن عالی‌پور و محمدرضا الهی‌منش و مشاورهٔ آقایان دکتر جواد طهماسبی و دکتر مهدی فضلی در دانشگاه آزاد اسلامی است.

* قاضی دادگستری، دانشجوی دکتری حقوق جزا و جرم شناسی، دانشکدهٔ حقوق و علوم انسانی، دانشگاه آزاد اسلامی (واحد تهران شمال)، تهران ، ایران tabrizi.sadegh1400@gmail.com

** استادیار گروه حقوق جزا و جرم‌شناسی، دانشگاه تهران (پردیس فارابی)، قم، ایران (نویسندهٔ مسئول)
hassan.alipour@gmail.com

*** استادیار حقوق جزا و جرم شناسی، دانشکدهٔ حقوق و علوم انسانی، دانشگاه آزاد اسلامی (واحد تهران شمال)، تهران ، ایران m.elahimanesh92@yahoo.com

مقدمه

در نظام کیفری ایران، یکی از مهم‌ترین اصول، اصل تناسب است که در بسیاری از مباحث حقوق جزای ماهوی و شکلی مورد توجه قرار گرفته است. در مباحث حقوق ماهوی جزایی می‌توان مهم‌ترین جلوهٔ اصل تناسب را بین جرم و مجازات توصیف کرد که بر این اساس باید بین جرم ارتکابی و مجازاتی که مقنن برای آن در نظر گرفته، تناسب برقرار باشد. بر همین اساس، تناسب، هماهنگی و هم‌سویی میان مجازات و جرم از لوازم یک نظام کیفری متعادل است. در حقوق جزای شکلی نیز در مواد مختلفی از قانون آیین دادرسی کیفری و در مراحل مختلف دادرسی به لزوم توجه به این اصل تصریح شده است. مهم‌ترین جلوه اصل تناسب در آیین دادرسی کیفری مربوط به تحصیل دلیل و صدور قرار تأمین کیفری می‌باشد. در این راستا فقط باید دلایلی را که برای اثبات جرایم مؤثر و مرتبط هستند را تحصیل و در جهت اثبات جرایم مورد استفاده قرار داد.

تناسب بر وزن تفاعل (مصدر)، ثلاثی مزید از ریشه «نَسَب و نسبتَه» دارای مفهوم فعلی طرفینی است. در لغت به معنای به «همدیگر پیوند شدن، با هم مناسبت داشتن، وجود داشتن و نسبت و رابطه میان دو کس یا دو چیز و برابری دو نسبت است» (عمید، ۱۳۷۵: ۱۹۰۲). در متون اسلامی، بعضی از فقها ریشهٔ تناسب را عدل و عدالت دانسته و در اصطلاح قرآنی عدل به معانی متعدد تعبیر گردیده است که یکی از آن‌ها اعطای حق به ذی‌حق است (حجرات: ۱۳، الرحمن: ۷ تا ۸، شوری: ۴۰، یونس: ۲۷، غافر: ۴۰، بقره: ۱۹۴ و نساء: ۲۳). بنابراین در بحث تناسب داده و سامانه، می‌توان گفت که تناسب به معنای هماهنگی‌ای است که باید بین جرم ارتکابی و داده و سامانه توقیف شده برقرار باشد. در علم حقوق نیز در گرایش‌های مختلف آن، بسته به نوع موضوع حقوقی، اصل تناسب مورد استفاده قرار گرفته است. از همین‌رو گفته می‌شود؛ تناسب یک اصل حقوقی است که در تمام مواردی که برخوردی میان یک قدرت ورای ارادهٔ فرد با حقوق و آزادی‌های مشروع فرد مطرح می‌شود، مورد توجه قرار می‌گیرد و به‌تبع آن حوزه، رنگ خاص آن را به خود می‌گیرد. با این حال، خاستگاه نظری اصل تناسب را باید در توصیف منشأ و مشروعیت قدرت سیاسی دید. در واقع، «مبنای نظری اصل تناسب بیش از آنکه در نظریهٔ کیفری و حتی نظریهٔ حقوقی استوار گردد، ریشه در نظریهٔ سیاسی دارد» (فلچر، ۲۰۰۶: ۳۸-۱۸). به‌تبع آن، جایگاه اصل تناسب را باید در بخشی از حقوق جست که عهده‌دار تنظیم روابط نابرابر و اقتداری است یعنی، حقوق عمومی. در عین حال، اصل تناسب مستقل از مبنای سیاسی مورد نظر به‌مثابهٔ یک نتیجهٔ منطقی عقلی قابل‌استنتاج به نظر می‌رسد. در واقع، هرچند از حیث مبانی نظریات سیاسی مختلف، حدود اعمال اقتدار و مداخلهٔ حاکمیتی دولت می‌تواند بسیار متغیر و متفاوت باشد، با این همه در یک نکته مشترک‌اند و یا دست‌کم نمی‌توانند از

آن عدول کنند که مداخلهٔ دولت، هدفی را دنبال می‌کند و به هر روی، این مداخله باید با برآوردن این هدف «متناسب» باشد. در واقع، مسئلهٔ تناسب منطقی نتیجهٔ اصل ضرورت است، چراکه مدلول اصل ضرورت در حوزهٔ حقوق عمومی این است که اعمال قدرت عمومی، امری استثنایی و خلاف اصل است که مجاز نیست مگر در مورد ضرورت. یعنی جواز امر استثنایی تا جایی است که ضرورت موجب جواز آن استثنا، اجازه می‌دهد و این بیان، چیزی جز همان تناسب نیست.

همچنین، اصل تناسب در پیوند با سایر اصول حاکم بر توقیف داده و سامانه، به‌ویژه اصل ضرورت معنا می‌یابد. قاعدهٔ آزادی در تحصیل دلیل، با توجه به ضرورت تحصیل دلیل و به‌تبع آن ضرورت توقیف آن به طریق قانونی و مشروع محدود می‌گردد. همان گونه که اصل در اعمال انسانی، اباحه و آزادی است و نمی‌توان محدودیتی برای این اصل پیش‌بینی کرد مگر اینکه ضرورت‌هایی همچون نظم عمومی یا حقوق شهروندان ایجاب نماید. در توقیف ادله نیز تنها باید ادله‌ای که برای کشف جرایم ضرورت داشته باشد توقیف شود. بنابراین ضرورت با چرایی توقیف در ارتباط است و در واقع باید در توقیف هر گونه ادله‌ای چرایی آن پاسخ داده شود اگر پاسخ به چرایی مرتبط با جرم ارتکابی و یا بدون توقیف آن، ادلهٔ مرتبط با جرم نیز غیرقابل‌توقیف باشد، ضرورت برای توقیف داده و سامانه فراهم شده است اما در صورتی که پاسخی برای چرایی وجود نداشته باشد و ادله‌ای توقیف شده با جرم ارتکابی متناسب نباشد و توقیف آن بی‌تأثیر در کشف باشد، ضرورت فراهم نبوده باید از توقیف آن اجتناب شود.

منظور از فرایند توقیف داده و سامانه، فرایندهای تعریف شده در مقررات شکلی هستند که تا قبل از تصویب قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ تنها در بخش دوم قانون جرایم رایانه‌ای[1] مصوب ۱۳۸۸ ذکر شده بودند که به همین دلیل مقنن در همین بخش و در راستای پر کردن خلأهای 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 مسائل مربوط به فرایندهای دادرسی در جرایم رایانه‌ای باشد. بعد از تصویب قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی فرایند دادرسی جرایم رایانه‌ای و به‌تبع آن فرایندهای پیرامون توقیف داده و سامانه در این قانون به‌صورت خاص مورد پیش‌بینی قرار گرفتند. این فرایندها که مشتمل بر ضوابط و اصول قانونی حاکم بر آیین دادرسی کیفری جرایم سایبر (به‌خصوص

۱. این قانون به صراحت به موجب مادهٔ ۶۹۸ قانون آیین دادرسی کیفری نسخ شده است.

در مرحلهٔ تحقیقات مقدماتی) ضمن اینکه از ضوابط عمومی حاکم بر فضای سنتی پیروی می‌کند، دارای قواعد خاصی است که در فرایند 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 شود.

مسئلهٔ اصلی نوشتار حول محور معیار تناسب است. از یک‌سو تناسب مبتنی بر رویکرد اقدام‌محور است که بر اساس آن باید میان اقدام مقام قضایی در توقیف داده و سامانه با موضوع توقیف، نسبت توازن برقرار باشد یعنی کیفیت و شیوهٔ توقیف با لحاظ ویژگی‌های موضوع توقیف محقق شود. از سوی دیگر، تناسب رویکردی نتیجه‌محور دارد و این اصل می‌کوشد تا مقام قضایی را به‌تبعات توقیف گوشزد کند. توقیف داده و سامانه در فضای رایانه‌ای شدهٔ امروز با لحاظ ابعاد کلان فعالیت‌های سایبری و با لحاظ مؤلفه‌های زمانی و مکانی، سبب می‌شود تا ملاک پیامدمحوری در تناسب از اقدام محوری برجسته‌تر شود. همین چالش در تناسب در توقیف اموال ملموس و یا اسناد نیز مدنظر است ولی چالش اصلی این نوشتار در همین سنجش است که آیا اولاً می‌توان نسبتی میان توقیف داده و سامانه با توقیف اموال ملموس برقرار کرد و ثانیاً ملاک تناسب در توقیف در هر دو حوزه تا چه اندازه با هم هم‌پوشانی دارند؟ همچنین، موضع قانون‌گذار ایران در مقایسه با اسناد بین‌المللی به‌ویژه اسناد اروپایی چگونه می‌باشد؟ برای پاسخ به این پرسش‌ها؛ در ادامه ابتدا مفهوم‌شناسی داده، سامانه، توقیف و تناسب مطالعه و سپس ابعاد مختلف اصل تناسب در توقیف داده و سامانه در حقوق ایران و اسناد اروپایی بررسی خواهد شد.

۱. مفهوم توقیف داده و سامانه

به‌منظور آشنایی با تعاریفی که از واژگان کلیدی در این پژوهش مدنظر قرار گرفته، در ادامه ابتدا تعاریف واژگان کلیدی بررسی و سپس به بازشناسی توقیف داده و سامانه از اصطلاحات مشابه دیگر ازجمله پالایش داده و سامانه پرداخته می‌شود.

۱-۱. تعریف داده و سامانه

واژهٔ داده در فرهنگ کامپیوتر مایکروسافت به معنای «فقره یا فقراتی از اطلاعات» (هیأت مولفان و ویراستاران انتشارات مایکروسافت، ۱۳۸۱: ۷۵) تعریف شده است. «کنوانسیون راجع به جرایم رایانه‌ای (نیز) داده را عبارت از هر نوع اطلاعات یا مفاهیم قابل‌پردازش در سیستم رایانه‌ای دانسته است» (نوری و نخجوانی، ۱۳۸۳: ۵۹). واژهٔ «داده» به‌صورت خاص در نظام حقوقی ایران تعریف نشده است ولی به‌صورت «داده پیام» و «داده ترافیک» از آن تعریف به عمل آمده است. داده ترافیک نیز در تبصره ۱ مادهٔ ۶۶۷ قانون آیین دادرسی کیفری تعریف شده است: «داده ترافیک، هرگونه داده‌ای

است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می‌کنند تا امکان ردیابی آن‌ها از مبدأ تا مقصد وجود داشته باشد.»

در علم حقوق، این داده مورد مفهوم‌شناسی قرار نگرفته و در قوانین جاری تعریفی از سامانه یا سیستم ذکر نشده است. اما در بین مقررات، برای اولین بار در آیین‌نامهٔ نحوهٔ استفاده از سامانه‌های رایانه‌ای یا مخابراتی مصوب ۱۳۹۵ که در اجرای مواد (۱۷۵)[۱] و (۱۷۶)[۲] قانون آیین دادرسی کیفری تنظیم شده بود این واژه به‌صورت ترکیبی با رایانه و مخابرات مورد مفهوم‌شناسی قرار گرفته است. بند «ب» مادهٔ ۱ آیین‌نامهٔ اخیر؛ سامانهٔ رایانه‌ای را به این صورت تعریف کرده است: «مجموعه‌ای از نرم‌افزارها و سخت افزارهای مرتبط که از طریق یک شبکه رایانه‌ای جهت اجرای فرایندهای کار مشخصی، به یکدیگر متصل‌اند». بند «پ» مادهٔ ۱ آیین‌نامه نیز سامانه مخابراتی را به این صورت تعریف می‌کند: «هر نوع دستگاه یا مجموعه‌ای از دستگاه‌ها برای انتقال الکترونیکی اطلاعات میان یک منبع (فرستنده، منبع نوری) و یک گیرنده یا آشکارساز نوری از طریق یک یا چند مسیر ارتباطی به وسیله قراردادهایی که برای گیرنده قابل‌فهم و تفسیر باشد».

۲-۱. تعریف توقیف داده و سامانه

با نگاهی به لغت‌نامه‌های فارسی همچون لغت‌نامه دهخدا و معین مشخص می‌شود که توقیف در لغت به معنای حبس، ضبط، جلب، و زندانی و... کردن است. پس 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. روش‌هایی که مقنن برای توقیف داده و سامانه ذکر کرده حصری نیستند، اما روش‌های توقیف داده با روش‌های توقیف سامانه متفاوت از همدیگر است. مطابق بند الف مادهٔ ۳۸ آیین‌نامهٔ جمع‌آوری و

۱. مادهٔ ۱۷۵ قانون آیین دادرسی کیفری مقرر می‌دارد: «استفاده از سامانه‌های (سیستم‌های) رایانه‌ای و مخابراتی، از قبیل پیام‌نگار (ایمیل)، ارتباط تصویری از راه دور، نمابر و تلفن، برای طرح شکایت یا دعوی، ارجاع پرونده، احضار متهم، ابلاغ اوراق قضایی و همچنین نیابت قضایی با رعایت مقررات راجع به دادرسی الکترونیکی بلامانع است». تبصره- «شرایط و چگونگی استفاده از سامانه‌های رایانه‌ای و مخابراتی موضوع این ماده بر اساس آیین‌نامه‌ای است که ظرف شش‌ماه از تاریخ لازم‌الاجراء شدن این قانون توسط وزیر دادگستری تهیه می‌شود و به تصویب رییس قوه قضاییه می‌رسد».

۲. مادهٔ ۱۷۶ قانون آیین دادرسی کیفری مقرر می‌دارد: «قوه قضاییه می‌تواند ابلاغ اوراق قضایی را به بخش خصوصی واگذار کند. چگونگی اجرای این ماده به موجب آیین‌نامه‌ای است که ظرف شش‌ماه از تاریخ لازم‌الاجراء شدن این قانون توسط وزرای دادگستری و ارتباطات و فناوری اطلاعات تهیه می‌شود و به تصویب رییس قوه‌قضاییه می‌رسد».

استنادپذیری ادله الکترونیکی «... الف: در توقیف داده‌ها از طریق چاپ داده‌ها، غیرقابل‌دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده». همین مقررات در بند قسمت اخیر مادهٔ ۶۷۵ قانون دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی تکرار شده است. در قسمت اخیر این ماده آمده است: «در توقیف داده‌ها... به روش‌هایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل‌دسترس کردن داده‌ها با روش‌هایی از قبیل تغییرگذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود».

۲. شناخت اصل تناسب در حقوق

یکی از مهم‌ترین مباحث پیرامون تناسب توقیف داده و سامانه، بررسی معیارهایی هستند که باید برای توقیف داده و سامانه در نظر گرفته شوند. بدیهی است که این معیارهای توقیف باید به اعتبار نقشی که داده و سامانه دارد، متفاوت و متناسب با آن باشد. به‌طور کلی و با عنایت به مقررات جاری معیارهایی که برای تناسب توقیف داده و سامانه باید مورد توجه قرار بگیرند به سه دستهٔ تناسب به اعتبار اهمیت موضوع توقیف، تناسب به اعتبار روش توقیف، و بالأخره تناسب به اعتبار نقشی که در ارتکاب جرم دارند تقسیم‌بندی می‌شوند که در ادامه این معیارها مورد بررسی قرار می‌گیرد.

۲-۱. تناسب به اعتبار اهمیت موضوع توقیف

موضوع توقیف ممکن است صرفاً یک موضوع شخصی و در تقابل‌حقوق دو شخص انجام بگیرد. در چنین مواردی موضوع توقیف از اهمیت بالایی برخوردار نیست اما در برخی از موارد نظیر جرایم امنیتی، جرایم عمومی و... موضوع توقیف از اهمیت بسیار بالا و حساسی برخوردار می‌شود که لازم است توقیف متناسب با آن انجام یا اینکه در برخی از موارد موضوع توقیف داده یا سامانه یک درگاه عمومی یا داده‌هایی باشند که با آن‌ها خدمات عمومی ارائه می‌شود و لذا برای توقیف آن باید شرایط پیش‌بینی شده فراهم باشد یا در برخی از موارد موضوع توقیف، داده و سامانه‌ای است که از نظر قانون‌گذار به جز در موارد استثنایی غیرقابل‌توقیف می‌باشد. از همین‌رو تنها در موارد استثنایی پیش‌بینی شده توقیف آن‌ها امکان‌پذیر است. در مادهٔ ۶۷۹ قانون دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی آمده است: «توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی‌شود، ممنوع است مگر اینکه توقیف برای اجرای موضوع اهم نظیر حفظ امنیت کشور ضرورت داشته باشد». همچنین، مقنن در مادهٔ ۲۹ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی[1] مقرر می‌دارد: «چنانچه پس

۱. با وجود نسخ صریح مواد (۷۵۶) الی (۷۷۹) الحاقی مورخ ۵ /۳ /۱۳۸۸ به قانون مجازات اسلامی (تعزیرات و ←

از اجرای دستور توقیف و یا در زمان اجرای دستور توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی بیم لطمه جانی یا خسارت مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی برود مراتب از مرجع قضایی صادرکننده دستور توقیف کسب تکلیف شده و در صورت تشخیص قاضی حسب مفاد ماده ۴۴ قانون عمل می‌گردد. در موارد یاد شده امکان توقیف وجود ندارد مگر اینکه اجرای موضوع اهم نظیر حفظ امنیت کشور ضرورت داشته باشد که در این‌صورت حتی با وجود تهدیدات جانی و مالی و اخلال در ارائه خدمات عمومی به‌دلیل قانون اهم امکان توقیف فراهم شده است.»

با عنایت به موارد یاد شده می‌توان به این نتیجه رسید که بسته به اهمیتی که موضوع داده و سامانه دارد باید توقیف متناسب با آن و به اعتبار آن انجام بگیرد.

۲-۲. تناسب به اعتبار روش توقیف

دومین حالت تناسب به اعتبار روش توقیف است. همان طور که بیان شد، داده‌ها و سامانه‌ها ممکن است به روش‌های متعددی توقیف شوند لذا باید بین روش توقیف داده و سامانه با نوع داده و سامانه تناسب برقرار باشد و هر داده و سامانه‌ای را نمی‌توان بدون توجه به روشی که برای توقیف آن متناسب می‌باشد توقیف کرد.

در مورد روش‌های توقیف داده در قوانین و مقررات داخلی تصریح شده است. مطابق بند الف مادهٔ ۳۸ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی «... الف: در توقیف داده‌ها از طریق چاپ داده‌ها، غیرقابل‌دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده». همین مقررات در بند قسمت اخیر مادهٔ ۶۷۵ قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی تکرار شده است در قسمت اخیر این ماده آمده است: «در توقیف داده‌ها ... به روش‌هایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل‌دسترس

مجازات‌های بازدارنده) به موجب ماده ۶۹۸ قانون آیین دادرسی کیفری ۱۳۹۲ که در واقع همان مواد قانون جرایم رایانه‌ای مصوب ۱۳۸۸ بودند که به قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) الحاق شده بودند، به نظر می‌رسد که آیین‌نامه جمع‌آوری و استناد پذیری ادله الکترونیکی که در اجرای ماده ۷۸۲ ق.م.ا ۱۳۷۵ (ماده ۸۴ قانون جرایم رایانه‌ای) به تصویب رئیس قوه قضاییه رسیده به قوت خود باقی باشد چرا که این آیین‌نامه در ۱۳۹۳/۵/۱۲ به تصویب رسیده و اگر نظر مقنن بر نسخ آن بود به مانند قانون جرایم رایانه‌ای به صراحت نسخ آن را نیز در ماده ۶۹۸ ق.آ.د.ک تصریح می‌کرد. علاوه بر این قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳/۷/۸ بوده که به موجب ماده ۶۹۹ به ق.آ.د.ک ۱۳۹۲ الحاق گردیده، لذا این قانون نیز که با توجه به تاریخ تصویب (۱۳۹۳/۷/۸) بعد از تصویب آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی (مصوب ۱۳۹۳/۵/۱۲) به تصویب مقنن رسیده، ذکری از نسخ آیین‌نامه یاد شده در این قانون نیامده است.

کردن داده‌ها با روش‌هایی از قبیل تغییرگذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود». مطابق مستندات یادشده شیوه‌های خاص توقیف داده به‌صورت تمثیلی بیان شده و مشتمل بر موارد ذیل خواهند بود:

۱. چاپ داده‌ها، ۲. تصویربرداری از تمام یا بخشی از داده‌ها،۳. غیرقابل‌دسترس کردن داده‌ها.

مادهٔ ۳۹ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی نیز در ادامه شیوه‌های توقیف اشعار داشته است که «دستور توقیف سامانه شامل سایر سخت‌افزارها یا حامل‌های داده متصل به آن نمی‌شود، مگر آنکه در دستور قضایی تصریح گردد. در صورت نیاز به حفظ فوری سخت‌افزارها یا حامل‌های داده، ضابطان یا سایر مأموران در حدود وظایف قانونی می‌توانند نسبت به حفظ فوری آن مطابق ماده ۳۴ قانون و رعایت مقررات این آیین‌نامه اقدام نمایند». مادهٔ ۲۵ همین آیین‌نامه بیان می‌دارد که «در دستور تفتیش یا توقیف داده یا سامانه باید محل تفتیش یا توقیف تعیین و حتی‌الامکان در محل استقرار سامانه انجام پذیرد». در برخی کشورها سعی شده با اعمال اصلاحات قانونی، موارد ابهام و راه‌های گریز موجود در حوزهٔ بازرسی و ضبط داده‌ها یا اطلاعات برطرف شود. در انگلستان، اختیارات کلی ضبط بر اساس مادهٔ ۱۹ از قانون «ادلهٔ اثبات کیفری و پلیس» مصوب سال ۱۹۸۴ به هر چه که در محل موردنظر باشد دلالت دارد و در شرایط خاص نیز این اختیار را فراهم می‌آورد که هرگونه اطلاعات مستقر در رایانه که مورد نیاز باشد، به دست آید (چپتر، ۱۹۸۴: ۲۲). قانون آیین دادرسی کیفری فرانسه در مرحلهٔ تحقیقات ابتدایی، افسران پلیس قضایی می‌توانند اقدام به توقیف اسناد، مدارک یا داده‌های رایانه‌ای نمایند. ضبط و توقیف اطلاعات و داده‌های رایانه‌ای ضروری برای کشف حقیقت و قرار دادن آن در اختیار دادگستری، از طریق ضبط سخت‌افزار این اطلاعات و داده‌ها یا کپی آنها، در حضور اشخاصی که به جرم بازرسی کمک کرده‌اند، صورت می‌گیرد. در صورت تهیه کپی از داده‌های رایانه‌ای، بر اساس تعلیمات و دستورات دادستان شهرستان، اطلاعات موجود بر روی سخت‌افزارهایی که در اختیار دادگستری نیست و نگهداری یا استفاده از آن‌ها مضر به امنیت اشخاص یا اموال باشد، به‌صورت قطعی پاک می‌شود. با موافقت دادستان شهرستان، افسر پلیس قضایی فقط اشیاء اسناد مدارک و اطلاعات رایانه‌ای که در کشف حقیقت مؤثر باشد را نگهداری می‌کند (کیسی ۱۳۸۶: ۸۵). کنوانسیون جرایم سایبری در بند ۱ تا ۳ مادهٔ ۱۹، به برخی شیوه‌های توقیف داده‌های رایانه‌ای ذخیره‌شده اشاره و مقرراتی را پیشنهاد داده است.

در مورد توقیف سیستم‌های رایانه‌ای مقنن در مادهٔ ۶۷۶ قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی موارد توقیف را به‌طور حصری معین کرده است. این موارد عبارت‌اند از: الف) داده‌های ذخیره‌شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد؛ ب) تفتیش و

تجزیه‌وتحلیل داده‌ها بدون سامانه سخت‌افزاری امکان‌پذیر نباشد؛ ج) متصرف قانونی رضایت داده باشد؛ د) تصویربرداری (کپی‌برداری) از داده‌ها به‌لحاظ فنی امکان‌پذیر نباشد؛ ه) تفتیش در محل باعث آسیب داده‌ها شود. شاید علت اینکه برخلاف توقیف داده‌های الکترونیکی، موارد توقیف سامانه‌های رایانه‌ای احصا شده‌اند این باشد که گاه ممکن است توقیف 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. مادهٔ ۴۳ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی بیان می‌دارد که «ضابطان قضایی و سایر مأموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت‌وضعیت اولیه‌ای از سامانه رایانه‌ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت‌افزارها و حامل‌های داده متصل به آنکه علامت‌گذاری و ثبت می‌شوند را تنظیم و به امضای تفتیش کننده یا توقیف‌کننده 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». چنین مقرره‌ای در نظام حقوقی فرانسه نیز مورد توجه قرار گرفته است. مادهٔ 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).

با عنایت به آنچه در مورد شیوه و روش‌های توقیف داده و سامانه بیان شد، می‌توان به این نتیجه رسید که بسته به نوع داده و سامانه ممکن است روش خاصی با نظر مقام قضایی و ضابطان برای توقیف آن‌ها به‌کارگرفته شود که الزاماً باید روش توقیف متناسب با نوع داده و سامانه در راستای قانون باشد که در موضوع مربوط به رویه قضایی حاکم به قسمتی از آن اشاره خواهیم کرد.

۳-۲. تناسب به اعتبار نقش در ارتکاب جرم

داده‌ها و سامانه‌ها بسته به نقشی که در ارتکاب جرم دارند و متناسب با آن باید مورد توقیف قرار بگیرند. با این توضیح که ممکن است داده و سامانه پیوند مثبتی با ارتکاب جرم داشته و در جهت کشف جرم مورد توقیف قرار بگیرد یا مقابل‌ممکن است به‌دلیل استفاده از آن به‌عنوان وسیلهٔ ارتکاب جرم پیوند منفی با ارتکاب جرم داشته باشد بدیهی است که در هر یک از این دو حالت روش توقیف باید متناسب با نقشی باشد که در ارتکاب جرم دارد. در این خصوص ذکر این نکته ضروری است که هرچند توقیف داده و سامانه در اغلب موارد در مواردی مطرح می‌شود که داده و سامانه نقش منفی در ارتکاب جرم داشته باشند یعنی به‌عنوان وسیله یا موضوع جرم مورد استفاده قرار بگیرند. اما این به معنای عدم امکان توقیف داده و سامانه در موردی که نقش مثبت دارند نیست. در چنین مواردی نیز

در صورتی که برای کشف حقیقت نیاز باشد با دستور مقامات صلاحیت‌دار توقیف داده و سامانه‌های مرتبط در موارد پیش‌بینی شده در قوانین و مقررات امکان‌پذیر است. به‌عنوان نمونه مقنن در مادهٔ ۳۱ آیین‌نامه مقرر داشته است: «اشخاصی که داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی را تحت کنترل و یا تصرف دارند، موظف به همکاری در اجرای دستور تفتیش و توقیف می‌باشند. در صورتی که به واسطه عدم همکاری یا عدم دسترسی به این اشخاص، تفتیش یا توقیف امکان پذیر نباشد، نحوه دسترسی به داده‌ها یا سامانه‌ها از قبیل ورود به محل، رفع موانع استفاده از سخت افزار و نرم افزار، رمزگشایی و امثال آن با دستور مقام قضایی تعیین خواهد شد».

از پیوندهای مثبت بین داده و سامانه با فرایند دادرسی، استفاده از این ابزارهای فناورانه برای کنترل متهمین و مجرمین است. این کارکرد، امروزه، به‌عنوان یک رویکرد نوین مدیریتی در مقابل‌مجرمان در سیاست جنایی برخی از کشورها، در حال شکل‌گیری است که به دنبال سیاست‌های پیشگیرانه به‌خصوص از نوع وضعی مورد توجه سیاست‌گذاران کیفری قرار گرفته است. در این رویکرد، با هدف کنترل بزهکاری و کاهش آن به سطح قابل‌تحمل و برای دفاع و حفاظت از جامعه، همچنین در جهت کشف جرایم، متهمین و مجرمان (حرفه‌ای و خطرناک) باید مشمول تدابیر نظارتی و ناتوان‌ساز کیفری و سایر مجرمان، مشمول تدابیر ناتوان‌ساز غیرکیفری و تدابیر پیشگیرانهٔ وضعی قرار گیرند، لذا توقیف داده و سامانه با اهداف یاد شده باید متناسب باشد.

در مورد پیوندهای منفی نیز باید بین توقیف با نوع نقش منفی که داده و سامانه در ارتکاب جرم داشته تناسب برقرار گردد. ممکن است داده و سامانه به‌عنوان وسیلهٔ ارتکاب جرم باشند و یا اینکه داده و سامانه به‌عنوان صحنهٔ جرم محسوب گردد؛ در هر یک از حالات یاد شده یا دیگر حالاتی که داده و سامانه پیوند منفی با ارتکاب جرم داشته، روش متناسب با آن جهت توقیف استفاده شود. به‌عنوان نمونه یکی از مهم‌ترین پیوندهای منفی که برای داده و سامانه می‌توان ذکر کرد، استفاده از آن‌ها به‌عنوان موضوع جرم است. در برخی از جرایم رایانه‌ای موضوع جرم خود داده‌ها و سامانه‌ها هستند مثلاً در سرقت داده یا سامانه، ابزارهای اخیر موضوع جرم هستند در جعل داده و سامانه و بسیاری از جرایم دیگر نیز وضعیت به همین صورت می‌باشد یعنی جرم بر روی داده و سامانه اتفاق می‌افتد، در هر یک از موارد یاد شده توقیف باید به اعتبار نقشی که در ارتکاب جرم داشته متناسب باشد. با توجه به آنچه در این بحث بیان شد، این نتیجه حاصل می‌شود که داده و سامانه ممکن است پیوند منفی یا مثبت با ارتکاب جرم برقرار نماید، لذا در توقیف آن‌ها باید به منفی یا مثبت بودن نقش داده و سامانه در ارتکاب جرم توجه شود و توقیف متناسب با نقشی باشد که داده و سامانه در ارتکاب جرم داشته اشت.

۳. اصل تناسب در فرایند توقیف داده و سامانه در ایران

اصل تناسب به‌صراحت در قانون تجارت الکترونیک، قانون آیین دادرسی کیفری و در قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ پیش‌بینی شده است. با توجه به اینکه بسیاری از این مقررت در آخرین ارادهٔ مقنن در قانون اخیرالذکر تکرار شده، لذا فقط به بررسی مستندات ذکرشده در این قانون پیرامون اصل تناسب در فرایند توقیف داده و سامانه در نظام حقوقی ایران پرداخته می‌شود. مادهٔ ۶۷۵ قانون آیین دادرسی کیفری درخصوص اصل تناسب در توقیف داده و سامانه مقرر داشته است: «در 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 گذر واژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود.» به تصریح این ماده توقیف داده‌های رایانه‌ای با رعایت ضوابط مقرر از جمله تناسب داده‌ها در ارتکاب جرم امکان‌پذیر است. در مورد شیوه‌های توقیف سامانه‌های رایانه‌ای نیز مادهٔ ۶۷۷ قانون مذکور؛ رعایت 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.

علاوه بر این، مقنن در آیین‌نامهٔ استنادپذیری ادلهٔ الکترونیکی، نیز به‌صراحت به لزوم رعایت اصل تناسب در توقیف داده و سامانه تصریح کرده است. مطابق مادهٔ ۳۸ آیین‌نامهٔ استنادپذیری ادلهٔ الکترونیک مصوب ۱۳۹۳ «توقیف با رعایت تناسب نوع اهمیت و نقش داده یا سامانه‌های رایانه‌ای یا مخابراتی به روش‌های زیر انجام می‌شود: الف - توقیف داده‌ها از طریق چاپ داده ها، غیرقابل‌دسترس کردن داده‌ها به روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده؛ ب- توقیف سامانه‌های رایانه‌ای یا مخابراتی از طریق تغییر گذرواژه، پلمپ سامانه در محل استقرار یا ضبط سامانه». در واقع در این ماده مقنن؛ اولاً به لزوم رعایت اصل تناسب در توقیف داده و سامانه تصریح نموده و ثانیاً به لزوم تناسب روش‌های توقیف آن‌ها با نوع داده و سامانه تصریح کرده است. به این صورت که بسته به اینکه داده و سامانه از چه نوعی هستند و همچنین بسته به رایانه‌ای یا مخابراتی بودن آن‌ها، باید روش متناسبی برای توقیف اتخاذ گردد و نمی‌توان داده و سامانهٔ رایانه‌ای را به همان روشی که برای توقیف داده و سامانه رایانه‌ای امکان‌پذیر است توقیف نمود و در مورد توقیف داده و سامانهٔ رایانه‌ای و مخابراتی نیز بسته به اینکه از چه نوعی هستند باید با روش متناسب و مختص آن توقیف شوند.

در مورد جرایم فراملی و تروریسم نیز دادگاه حقوق بشر اروپا در رسیدگی‌های خود از اصل

تناسب غافل نشده و در کنار ضرورت دسترسی و توقیف داده‌ها و سامانه‌های مرتبط با این جرایم، به لزوم احترام به اصل تناسب در دسترسی به داده‌ها و سامانه‌ها تأکید کرده است. بنابراین دادگاه حقوق بشر اروپا از یک طرف به‌دلیل روش‌های پیچیده فرار از داده توسط شبکه‌های جنایی، دسترسی و انتقال داده‌های مرتبط با این جرایم را ضروری می‌داند، از طرف دیگر، کمیسیون حقوق بشر حدود و تناسب نظارت الکترونیکی را تعریف می‌کند. در واقع با توجه به دشواری دولت‌ها در مبارزه با این اشکال جرم، دادگاه منافع مشروع کشورهای عضو را برای موضع‌گیری قاطع می‌پذیرد، اما همچنین تأکید می‌کند که هم دسترسی به داده‌ها و هم انتقال آن‌ها باید به اصل تناسب احترام بگذارند.

در توصیه‌نامهٔ شورای اروپا که در زمینهٔ آیین‌دادرسی جرایم فناوری اطلاعات در سال ۱۹۹۵ تحت عنوان توصیه‌نامهٔ ۱۳ (۹۵) R توسط این شورا تصویب شده؛ ازجمله پیشنهادها برای قانون‌گذاری در قوانین کشورهای عضو، لزوم توجه به تناسب در ادلهٔ توقیفی و احتراز از سایر اطلاعات اشخاص است. در دستورالعمل اتحادیهٔ اروپا دربارهٔ حمایت از داده نیز به لزوم متناسب بودن نگهداری داده‌های توقیف شده و ایمنی آن‌ها تأکید شده است.

کنوانسیون جرایم سایبر با ارج نهادن بر اصل تناسب، پیش از ورود به ضوابط مربوط به آیین دادرسی کیفری، در بند ۱ مادهٔ ۱۵، به‌طور واضح ضمن تأکید بر حقوق و آزادی‌های بشری، لزوم توجه به اصل تناسب را در پیش‌شرط‌ها و تضمین‌های این حقوق و آزادی‌ها اعلام داشته و مقرر می‌دارد: «۱- اعضا باید اطمینان دهند که تصویب، اجرا و اعمال اختیارات و رویه‌های پیش‌بینی شده در این بخش، در شرایط و تضمین‌های حقوق داخلی‌شان گنجانیده‌اند و در راستای حمایت شایسته از حقوق و آزادی‌های بشری است که از جملهٔ آنها، حقوق برخاسته از تعهداتی است که آن‌ها در کنوانسیون شورای اروپا راجع به حمایت از حقوق و آزادی‌های اساسی بشر (۱۹۵۰) و میثاق حقوق مدنی و سیاسی سازمان ملل متحد (۱۹۶۶) و دیگر اسناد بین‌المللی لازم‌الاجرای حقوق بشر پذیرفته‌اند. این شرایط و تضمین‌ها باید به دنبال برقراری اصل تناسب باشند. ۲- این شرایط و تضمین‌ها همان گونه که برای اختیارات یا رویه‌های مربوط متناسبند، باید شامل سایر نظارت‌های مستقل یا قضایی، زمینه‌های اجرایی موجه و محدودیت حوزه و دوره زمانی اعمال چنین اختیارات یا رویه‌هایی نیز باشند».

با عنایت به موارد یاد شده؛ قبول شدن مدارک الکترونیک باید بر اساس مقررات هماهنگ که در بخشنامه‌ها و اسناد اروپایی آمده متناسب با ویژگی‌های داده‌ها و سامانه‌هایی باشند که دستور توقیف در آن خصوص صادر شده است. قانون معیارهایی برای قبول مدارک الکترونیک تعیین کرده که اصل تناسب می‌تواند جایگاه مدارک دیجیتال را که در یک صحنهٔ جرم جمع‌آوری شده تقویت کند. نتیجه

اینکه مقبولیت مدارک الکترونیکی نیز تا حد زیادی بستگی به تناسب توقیف با ویژگی‌های داده‌ها و سامانه‌ها دارد. کنوانسیون اروپایی جرایم سایبر نیز اصل تناسب را در ارتباط با حقوق کاربران ازجمله حریم خصوصی آن‌ها برگزیده و بر اساس اصل تناسب اگرچه حساسیت‌های ناشی از مصون ماندن حریم داده‌های الکترونیکی افراد در قبال تعرض از سوی مجریان قانون را پذیرفته، در عین حال قبول دارد که اگر مجریان قانون از اختیار عمل جهت انجام وظایف مقرره برخوردار نباشند، مجرمین بدون واهمه از تعقیب و دستگیری، بیشتر به ارتکاب اعمال مجرمانه سوق می‌یابند» (جلالی‌فراهانی، ۱۳۸۶: ۲۳). با عنایت به اسناد یاد شده، می‌توان نتیجه گرفت که اصل تناسب جزء اصول مورد احترام در اسناد اروپایی بوده و لزوم توجه و رعایت آن در مورد داده و سامانه نیز به‌صراحت در اسناد ذکر شده ازجمله در کنوانسیون اروپایی جرایم سایبری و توصیه‌نامه‌های شورای اروپا که درخصوص تحقیقات مقدماتی ازجمله توقیف داده و سامانه به کشورهای عضو صادر شده، مورد تأکید قرار گرفته است.

۴. تناسب توقیف داده و سامانه در رویهٔ قضایی ایران

در نظام حقوقی ایران، هرچند قانون به‌عنوان منبع اصلی احکام قضایی می‌باشد اما رویهٔ قضایی نیز به‌عنوان منبع ارشادی و در برخی از موارد منبع اصلی (آرای وحدت‌رویه) مورد توجه قرار گرفته و در تفسیر قضایی نقش بسیار مهمی دارد. در مورد توقیف نیز باید بیان داشت که توقیف دارای انواع مختلف بوده و ممکن است مخاطب دستور مقام قضایی؛ اشیاء، اموال، اسناد و حتی اشخاص قرار بگیرند. در مورد توقیف داده و سامانه نیز رویهٔ قضایی می‌تواند در روند اجرایی شدن قوانین و چگونگی عملیاتی شدن دستورات مبتنی بر توقیف کمک نماید. به‌عنوان نمونه در دستورات صادره، حدود و اختیارات مأموران صلاحیت‌دار باید مشخص شود و همچنین مفاد دستورات باید مرتبط و متناسب با داده و سامانه‌ای باشد که به نوعی پیوند مثبت یا منفی در جرم ارتکابی داشته باشد. همچنین با عنایت به عدم پیش‌بینی ضابطهٔ مشخص در مورت مدت زمان توقیف، با بررسی دستورات قضایی مهلت متناسب و متعارف از منظر مقامات قضایی مشخص می‌شود.

به‌طور کلی می‌توان گفت که برای برقراری تناسب توقیف داده و سامانه، باید مقامات قضایی بررسی نمایند که توقیف داده و سامانه به چه منظوری انجام می‌پذیرد. با این توضیح که داده و سامانه ممکن است در مقام موضوع جرم یا وسیلهٔ ارتکاب جرم مورد توقیف قرار بگیرد که در هر مورد باید متناسب با آن دستور صادر گردد. بنابراین ازجمله موضوعات مهم در رویهٔ قضایی به‌منظور صدور دستور توقیف داده و سامانه؛ بررسی نقشی است که داده و سامانه در ارتکاب جرم داشته است و همان طور که بیان شد ممکن است داده و سامانه در مقام موضوع جرم، وسیله ارتکاب جرم مورد توجه مقام قضایی قرار بگیرد. با توجه به تفاوتی که این موارد با همدیگر دارند در ادامه هر یک از

موارد یاد شده با مطالعه موردی دستورات صادره در رویه قضایی مورد بررسی قرار می‌گیرند.

۱-۴. تناسب توقیف داده و سامانه در مقام موضوع جرم در رویهٔ قضایی

یکی از مصادیق لزوم تناسب توقیف داده و سامانه، توقیف داده و سامانه‌هایی هستند که در مقام موضوع جرم می‌باشند. در چنین مواردی دستورات صادره باید با موضوع جرم مرتبط باشند یعنی اگر به فرض نمونهٔ یک سامانه‌ای که موضوع جرم قرار گرفته یا جرم بر روی آن ارتکاب یافته، نمی‌توان سامانه یا دادهٔ دیگری که ارتباطی با موضوع جرم ندارد را توقیف کرد. همان طور که بیان شد؛ یکی از مهم‌ترین پیوندهای منفی که برای داده و سامانه می‌توان ذکر کرد، استفاده از آن‌ها به‌عنوان موضوع جرم است. در مورد موضوع جرم بدواً باید بیان داشت که هر جرمی الزاماً باید دارای موضوع باشد و جرم بدون موضوع نمی‌تواند وجود خارجی داشته باشد. مثلاً در قتل خود انسان موضوع جرم قرار می‌گیرد و در توهین و افترا، حیثیت و آبروی وی موضوع جرم قرار می‌گیرد. در جرم سرقت و کلاهبرداری اموال اعم از مادی و معنوی موضوع جرم می‌باشند. در برخی از جرایم رایانه‌ای نیز موضوع جرم خود داده‌ها و سامانه‌ها هستند، مثلاً در سرقت داده یا سامانه، ابزارهای اخیر موضوع جرم هستند در جعل داده و سامانه و بسیاری از جرایم دیگر نیز وضعیت به همین صورت می‌باشد یعنی جرم بر ماهیت داده و سامانه اتفاق می‌افتد. زمانی که داده و سامانه موضوع جرم قرار می‌گیرد، وضعیت تحصیل، کشف، حفظ صحنهٔ جرم، توقیف، نگهداری و استنادپذیری متفاوت از حالت‌های سنتی است که به‌عنوان نمونه انسان یا اموال موضوع جرم هستند. مثلاً صحنهٔ جرم در جرایم الکترونیکی با جرایم دنیای واقعی متفاوت است. زمانی که یک جرم الکترونیکی اتفاق می‌افتد، جمع‌آوری، نگهداری و تجزیه و تحلیل ادلهٔ الکترونیکی باید با دقت زیاد انجام پذیرد.

به‌طوری کلی گفته شده است: معمولاً چگونگی مواجهه با ادلهٔ الکترونیکی در صحنه‌های جرم شامل مراحل زیر می‌باشد: ۱. محافظت، تشخیص و شناسایی ادله الکترونیکی؛ ۲. مستندسازی صحنه جرم؛ ۳. جمع‌آوری ادلهٔ الکترونیکی؛ ۴. بسته‌بندی و حمل‌ونقل و نگهداری ادلهٔ الکترونیکی (اشکرافت، ۲۰۰۱: ۲۴).

نکتهٔ مهم دیگر درخصوص صحنهٔ جرم در مواردی که داده و سامانه به‌عنوان موضوع جرم هستند، شناخت پهنهٔ صحنهٔ جرایم ارتکابی سایبری بر روی این داده‌ها و سامانه‌هاست که اختلاف‌نظرهای عمده‌ای در این خصوص وجود دارد که موجب شده کشورها رویه‌های متفاوتی را در تشخیص پهنهٔ این‌گونه از جرایم اتخاذ نمایند. از همین‌رو، در این خصوص گفته می‌شود که هماهنگی با قوانین بین‌المللی به‌ویژه با توجه به استاندارد شدن نسبی فناوری‌های اطلاعات و شیوه‌های ارتکاب جرم در صحنهٔ جهانی، گستردگی جرایم و عدم توجه به مرزها به‌عنوان مانعی برای ارتکاب جرم، ضروری به

نظر می‌رسد چراکه فضای سایبر و اینترنت فارغ از مرزهای جغرافیایی عمل می‌کند؛ محدود به چهارچوب خطوطی که دولتمردان در طراحی نقشه‌های سیاسی رسم می‌کنند، نیست و از هیچ‌گونه محدودیت مکانی تبعیت نمی‌کند. سایبر یک گسترهٔ بدون مرز است که نمی‌توان در برابر آن خطوط مقسّم کشید یا با مرزهای طبیعی یا مصنوعی آن را تکه تکه و جدا ساخت (فضلی، ۱۳۸۹: ۶۶).

بنابر آنچه در این زمینه گفته شد، استفاده از تعاریف استاندارد جهانی، استفاده از تجربیات دیگر کشورها و وجود همکاری‌های دو یا چندجانبه در مواجهه با جرایم سایبری، از پیش‌شرط‌های موفقیت در این زمینه است.

فصل سوم کنوانسیون جرایم سایبری ۲۰۰۱ تحت عنوان همکاری بین‌المللی چند اصل کلی را در مادهٔ ۲۳ در این خصوص بر می‌شمارد که حدود و سمت و شیوهٔ همکاری‌های بین‌المللی را در مواردی که داده‌ها و سامانه‌ها موضوع جرم هستند معین می‌کند. این اصول عبارتند از:

همکاری بین‌المللی در میان اعضا باید در گسترده‌ترین وضعیت تأمین شود. همکاری باید تمامی جرایم مرتبط با داده‌ها و سیستم‌های رایانه‌ای و همچنین جمع‌آوری ادلهٔ الکترونیک را در بر بگیرد.

همکاری باید بر اساس توافق‌نامه‌های بین‌المللی در موضوعات کیفری و ترتیبات توافق شده بر اساس قانون‌گذاری متحدالشکل یا دوجانبه و قوانین داخلی به عمل آید.

در تعیین محل ارتکاب جرم اغلب به دکترین (حضور در هرجا)[1] استناد می‌شود. وقوع جرم در داخل حوزهٔ قضایی یک کشور در صورتی محرز می‌شود که یکی از عوامل تشکیل‌دهندهٔ جرم یا نتیجهٔ نهایی آن در داخل مرزهای آن کشور واقع شده باشد. در کشوری همانند انگلیس ضمن تأکید بر عمل فیزیکی از نظریهٔ آثار و نتایج نیز استفاده می‌شود. طبق این نظریه اگر جرمی در سرزمینی اتفاق افتد فرض می‌شود که آثار و نتایج جرم در آن سرزمین ظاهر شود و یا در واقع ظاهر شده است. بنابراین در مواردی که عوامل یا آثار مختلف یک جرم ممکن است در بیش از یک کشور واقع شود، ممکن است دو دکترین صلاحیت سرزمینی بر ادعاهای صلاحیتی شروع و متقارن منتهی شود (تعارضات مثبت). این تعارضات مثبت گر چه در ابتدا از لحاظ تعیین پاسخ عادلانهٔ مناسب چندان مسئله‌ساز به نظر نمی‌رسد اما خطرهای ذاتی به همراه دارد. عمده‌ترین مسئلهٔ آن به‌ویژه در سامانه‌های حقوق نوشته ازجمله فرانسه و ایران، خودداری از به کارگیری قاعدهٔ منع محاکمه دوباره است. بنابراین ممکن است به خاطر ارتکاب جرم واحد چندبار تعقیب شود (زندی، ۱۳۹۳: ۸۵). به طورکلی تعیین پهنای صحنهٔ جرم سایبری هم در تحصیل ادله و هم در تعیین صلاحیت می‌تواند مهم باشد.

1. Ubiquity

به‌عنوان نمونه در پروندهٔ کلاسهٔ ۹۹۰۹۹۸۲۱۲۶۵۰۰۱۴۸ شعبهٔ ۱۰۶۵ دادگاه کیفری دو مجتمع قضایی امور اقتصادی تهران که علیه متهم (م.ص) دائر بر معرفی و فعالیت غیرمجاز مشاورهٔ سرمایه‌گذاری بدون اخذ مجوز از سازمان بورس و اوراق بهادار (بزه موضوع بند ۱مادهٔ ۴۹ قانون بازار اوراق بهادار) و دستکاری بازار سرمایه از طریق اغوای اشخاص به انجام معاملات (بزه موضوع بند ۳ مادهٔ ۴۶ قانون بازار اوراق بهادار) صادر شده است در قسمت اخیر این رأی مقرر گردیده که «با توجه به تولید و انتشار محتوای مجرمانه در کانال تلگرامی و صفحه اینستاگرامی در اجرای مواد ۱۴۸ و ۶۷۱ از قانون آیین دادرسی کیفری محکوم‌علیها مکلف است در همان پیام‌رسان مراتب عدم فعالیت خود را به‌دلیل مغایرت آن با قانون بازار اوراق بهادار به مخاطبین کانال اعلام دارد و مراتب ممنوعیت فعالیت کانال و صفحه متعلق به او موسوم به ... برای اطلاع در سایت رسمی بورس «کدال» ثبت گردد».

همان طور که از این رأی بر می‌آید؛ اولاً باید مغایرت داده‌های مجرمانه در کانال تلگرامی و صفحهٔ اینستاگرامی انتشار یافته توسط محکوم‌علیه در همان پیام‌رسان‌ها (یعنی تلگرام و اینستاگرام) به اطلاع مخاطبین برسد و ثانیاً ممنوعیت متهم از فعالیت در سامانه‌های تلگرامی و اینستاگرامی که از آن‌ها به‌منظور تولید و انتشار محتوای مجرمانه استفاده می‌کرده نیز در سایت رسمی بورس ثبت گردد. نتیجه اینکه در این رأی، داده‌ها و سامانه‌هایی که به‌عنوان موضوع جرم مورد استفاده قرار گرفته‌اند، توقیف گردیده و نسبت به ادامهٔ فعالیت در آن‌ها تعیین تکلیف شده است.

با بررسی دستورات صادره خطاب به مأموران و ضابطین به‌ویژه مأموران پلیس فتا این نتیجه حاصل شد که در جهت لزوم تناسب توقیف داده و سامانه در مقام موضوع جرم، معمولاً موارد ذیل در دستورات قضایی قید می‌شوند:

۱. جرم در چه محیطی یا برروی چه دستگاهی واقع شده است؟ (اعم از شبکه‌های اجتماعی یا وب سایت‌ها و یا وبلاگ و...)؛ ۲. در صحنه جرم چه داده و سامانه‌ای باید توقیف، محافظت، کنترل، ذخیره و نگهداری شود؟؛ ۳. داده و سامانه در مقام موضوع جرم مربوط به خدمات عمومی است یا خصوصی؟؛ ۴. سطح دسترسی مأموران به داده و سامانه‌هایی که در مقام موضوع جرم قرار گرفته‌اند به‌ویژه در مورد محرمانگی داده و سامانه‌های مرتبط با امنیت ملی؛ ۵. نحوه توقیف موضوع جرم؛ ۶. نحوهٔ نگهداری، کنترل و انتقال داده و سامانه‌های موضوع جرم؛ ۷. مدت زمان توقیف داده و سامانه‌های موضوع جرم؛ ۸. نحوهٔ اقدام برای رفع توقیف.

موارد یاد شده همه در ارتباط با تناسب داده و سامانه و مهلت زمان معقول برای توقیف آن‌ها

هستند، که در دستورات قضایی خطاب به مأموران و ضابطین مشهود می‌باشند.[۱]

۲-۴. تناسب توقیف داده و سامانه در مقام وسیلهٔ جرم در رویهٔ قضایی

یکی دیگر از پیوندهای منفی که برای داده و سامانه می‌توان نام برد، استفاده به‌عنوان وسیلهٔ ارتکاب جرم است. به‌طور کلی هر داده و سامانه‌ای یا وسایل مرتبط با آن‌ها می‌تواند به‌عنوان وسیله ارتکاب جرم باشد. بنابراین سامانه‌های رایانه‌ای اعم از رایانه‌های شخصی یا رایانه‌های ارائه‌کنندهٔ خدمات، انواع حافظه‌های جانبی و داده‌های درون سامانه‌های الکترونیکی به‌عنوان وسایل ارتکاب جرم به‌کار گرفته می‌شوند.

امروزه با استفاده از پیشرفت‌هایی که در حوزهٔ فناوری ارتباطی و اطلاعاتی رخ داده، استفاده از اینترنت و سایر محیط‌های سایبری به‌عنوان یکی از حقوق انسان‌ها به رسمیت شناخته شده است. «شورای اروپا در مصوبات متعددی بر حق دسترسی به اینترنت تصریح کرده است. ازجمله در «اعلامیه اصول آزادی ارتباطات در اینترنت» (۲۰۰۳) می‌گوید: «دولت‌های عضو باید دسترسی همگان به تمام خدمات ارتباطی و اطلاعاتی اینترنتی را به‌گونه‌ای غیرتبعیض‌آمیز و با بهایی منطقی، فراهم کنند ...» در توصیه‌نامهٔ مورخ ۲۰۱۱ خود نیز بر فراهم کردن نهایت دسترسی به اینترنت برای قادر کردن افراد به اعمال حقوق و آزادی‌هایشان تصریح کرده است (انصاری، ۱۳۹۹: ۶۴). البته باید توجه داشت که تکنولوژی ارتباطی و فناوری اطلاعات، به‌سان تکنولوژی‌های دیگر که با انگیزهٔ خدمت و رفاه بشری پدید آمده است و گسترش می‌یابد، اثر دوگانه دارد: هم می‌تواند مطلوب جامعهٔ بشری واقع گردد و هم می‌تواند دارای جنبه‌های منفی و تهدیدکنندهٔ حقوق بشری باشد که حقوق افراد جامعه را تحت تأثیر قرار می‌دهد (رئیسی دزکی و قاسم‌زاده لیاسی، ۱۳۹۹: ۱۴۳). بنابراین؛ مانند تمامی محیط‌ها، سوءاستفاده از حق دسترسی به اینترنت و سایر حقوق مرتبط با آن ازجمله حق بی‌نامی، اصل بی‌طرفی شبکه‌ای و... منجر شده تا برای ارتکاب جرایم در محیط سایبری از وسایل متناسب با آن استفاده شود. با توجه به گسترش استفاده از فناوری اطلاعات و انجام بسیاری از امور سازمان‌ها و افراد در فضای مجازی و در واقع رواج استفاده از اینترنت، گرایش و تمایل به انجام جرم در این محیط نیز به دلایل مختلف افزایش می‌یابد. از طرف دیگر بسیاری از افرادی که در محیط‌های واقعی به دلایل متعدد ازجمله شرم و حیا، و ترس از برخورد پلیس و دلایل دیگر اقدام به انجام ارتکاب عمل مجرمانه نمی‌کنند، در این فضا به‌دلیل ویژگی‌های فضای مجازی تمایل به ارتکاب جرم پیدا می‌کنند. فضای مجازی با وجود مزایای فراوانش، به‌دلیل ویژگی‌هایی مانند امکان تحصیل هویت‌های گوناگون،

۱. مستند موارد یاد شده بررسی مجموع دستورات صادره به پلیس فتا تهران بزرگ از طرف مقامات قضایی می‌باشد.

گمنامی و سهولت انجام اعمال مختلف، موجب مهاجرت بسیاری از جرایم به آن شده است. امروزه بسیاری از امور فقط در این فضا امکان‌پذیر است و عملاً می‌توان گفت هر سند و مدرکی که راجع به آن‌ها لازم باشد، باید در این فضا و فقط به‌صورت الکترونیکی جست‌وجو کرد. نمونهٔ بارز این موضوع، طیف وسیعی از جرایم رایانه‌ای است که وقوع آن‌ها فقط در دنیای دیجیتال امکان‌پذیر است. امروزه اطلاعات مختلفی که در دعاوی حقوقی یا پیگردهای جزایی نقش مهمی ایفا می‌کنند، در یک سیستم رایانه‌ای، ذخیره و بایگانی می‌شوند، در پرونده‌های کاغذی، به همان نسبت که افراد و شرکت‌ها، اتکای خود را بر سیستم‌های رایانه‌ای افزایش داده‌اند، کارآگاهان و مقامات قضایی و وکلا نیز به ارزش ذخایر گران‌بهای الکترونیکی پی برده‌اند، ذخایری محفوظ در سیستم‌های رایانه‌ای که به‌طور گسترده‌ای استناد به آن‌ها برای کشف و به جریان انداختن انواع دعاوی آغاز شده است (گاتن، ۱۳۸۳: ۱). اما در عین حال، این‌گونه دلایل نسبت به اسناد و مدارک دیگر آسیب‌پذیرتر هستند؛ زیرا به آسانی می‌توان در آن‌ها دستکاری یا آن را جعل کرد و یا آن‌ها را با استفاده از دانش فنی مناسب پنهان کرد. نکتهٔ بسیار مهم درخصوص توقیف داده و سامانه به‌عنوان وسیلهٔ ارتکاب جرم، بحث نگهداری از این ادله است تا زمینه برای محافظت از آن‌ها در جهت استنادپذیری هموار شود.

در این راستا تدابیر متنوعی برای حفظ داده‌های و سامانه‌های تحصیل یافته از جرم وجود دارد که عبارتند از: حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت عملیات که هدف همهٔ آن‌ها سخت‌تر ساختن دسترسی مجرمان به سیستم‌های رایانه‌ای است (وروایی و میرزکی، ۱۳۹۰: ۷۰). به‌طور کلی مجموع اقدامات و تدابیری که بر روی داده و سامانه به‌عنوان وسیلهٔ ارتکاب جرم انجام می‌پذیرد شامل موارد ذیل هستند:

۱-۲-۴. حفظ فوری ادله

اگر مجریان قانون از دلایل گردآوری شده به‌نحوی حفاظت نکنند تا در دادگاه وضعیت اصلی‌شان را انعکاس دهند و همچنین مشخصات هر یک به انضمام مأموران دست‌اندرکار در فرم‌های مخصوص به‌طور کامل درج نشده باشد، استنادپذیری‌شان با تردید جدی مواجه خواهد شد. بند یک مادهٔ ۱۶ کنوانسیون جرایم سایبر[1] در این رابطه به‌کارگیری هر گونه روش قانونی اعم از استفاده

۱. به موجب این بند: «هر یک از اعضا باید به گونه ای اقدام به وضع قوانین و سایر تدابیر کنند که در صورت لزوم جهت حفظ فور داده‌های رایانه‌ای خاص، نظیر داده ترافیک، که در یک سیستم رایانه‌ای خاص ذخیره شده است، بویژه در جایی که زمینه‌های این باور وجود دارد که داده‌های رایانه ای در برابر از بین رفتن یا تغییر یافتن آسیب پذیرند، این اختیار را به مقامات ذیصلاح خود بدهند که دستوراتی صادر کرده یا اقدامات مشابهی به عمل آورند».

از دستور قضایی یا دستورالعمل اداری و یا صدور دستور از جانب پلیس و سایر مقامات تعقیب را مجاز می‌داند. حفاظت از داده‌ها و سامانه‌ها مستلزم جلوگیری از هر گونه اصلاح، خدشه یا از بین رفتن آن‌ها است که هم اکنون به‌صورت ذخیره وجود دارند. البته این مفهوم ضرورتاً به این معنا نیست که داده‌ها غیرقابل‌دسترس گردند، بلکه ممکن است مطابق شرایط و اوضاع و احوال این اختیار به کاربران داده شود که از کپی داده‌ها استفاده کنند. زیرا این ماده هیچ شیوه‌ای را برای حفاظت ذکر نکرده و تنها آن هدفی که دنبال می‌کرده را تبیین نموده است. لذا این به‌عهدهٔ اعضاست که برای تأمین این هدف چه سازوکارهایی را در نظر بگیرند (جلالی‌فراهانی، ۱۳۹۵: ۲۰). در حقوق فرانسه مادهٔ ۹۷ آیین دادرسی کیفری فرانسه بیان می‌کند که کلیهٔ اشیا، اسناد یا داده‌های حاوی اطلاعات فوراً فهرست‌برداری و مهروموم می‌شود. همچنین در ادامهٔ این ماده آمده است که به توقیف و ضبط داده‌های حاوی اطلاعات رایانه‌ای که برای کشف حقیقت ضروری است، با استقرار آن تحت اختیار دادگستری به‌صورت سخت‌افزار یا کپی گرفته شده از آن‌ها در حضور اشخاصی که در بازرسی حاضر هستند، اقدام می‌شود. اگر کپی در چهارچوب این دادرسی تهیه شود، بر اساس دستور بازپرس می‌توان به محو قطعی داده‌های اطلاعاتی از روی سخت‌افزاری که در اختیار دادگستری قرار نگرفته است و نگهداری یا استفاده از آن‌ها غیرقانونی یا برای امنیت اشخاص یا اموال خطرناک است، اقدام می‌شود (تدین، ۱۳۹۱: ۱۰۹).

در قوانین ایران نیز در مقام اجرا و به‌منظور توجه به این مهم در دستور مقام قضایی، مادهٔ ۱۵ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی مقرر داشته است: «دستور حفاظت باید فوری و باروش مطمئن به مجری حفاظت ابلاغ شود. این دستور همچنین به اشخاص ذی‌نفع نیز ابلاغ می‌شود؛ مگر آنکه ابلاغ به آن‌ها مخلّ رسیدگی باشد که در این صورت تشخیص زمان ابلاغ حسب مورد با مقام قضایی می‌باشد».

۲-۲-۴. حفاظت از ادله در برابر آسیب‌های محتوایی، محیطی و حفظ حریم خصوصی

تمامی اقدامات قانونی را برای حفظ صحنهٔ جرم باید به‌عمل آورد. اگر شخص یا اشخاص خاصی باید به‌لحاظ وضعیت خاص خود به خارج از صحنه منتقل شوند، باید مطمئن شد که پیش از ترک صحنه هیچ‌گونه ادله‌ای به همراه آنان نباشد. در این مرحله از پی‌جویی وضعیت ادله را نباید تغییر داد. اگر روشن هستند باید روشن باقی بمانند و اگر خاموش هستند، باید خاموش باقی بمانند و یا سایر دستگاه‌های مشابه یافت شوند. کارشناس صحنهٔ جرم باید توجه کند که هر که ممکن است حاوی ادلهٔ فرار باشند باید سریعاً محافظت شوند، مستندسازی شوند و از آن‌ها عکس تهیه شود. تمامی خطوط تلفنی که به دستگاه‌هایی نظیر مودم‌ها متصل هستند باید شناسایی شوند. باید تمامی خطوط تلفن

مستندسازی شوند، قطع شوند، و تک‌تک برچسب زده شوند. همچنین ممکن است ارتباط دیگری نظیر خطوط شبکه در صحنهٔ جرم وجود داشته باشند، در این حالت بهتر از مشاوره افراد یا شرکت‌های متخصص استفاده کرد (تراب‌زاده، ۱۳۸۸: ۹۴-۹۳). به هیچ عنوان نباید کاری کرد، که سبب اضافه شدن، تغییر داده‌ها و یا از بین رفتن داده‌های موجود در یک رایانه یا سایر رسانه‌ها شود. رایانه‌ها تجهیزات الکترونیکی بسیار ظریفی هستند که نسبت به رطوبت، حرارت، الکتریسیتهٔ ساکن، ضربه یا تکان فیزیکی، منابع مغناطیسی و امواج الکترو مغناطیسی بسیار حساس هستند، بنابراین باید احتیاط خاص و ویژه‌ای را حین بسته‌بندی، حمل‌ونقل و نگهداری ادلهٔ الکترونیکی داشته باشیم.

همچنین؛ در حفظ داده‌ها باید به مسئلهٔ حفظ حریم خصوصی و محرمانگی داده‌ها توجه ویژه‌ای شود. حفاظت یک تدبیر نخستین است که زمینه را برای سایر تدابیر قانونی به‌منظور دستیابی به داده‌ها یا افشای آن‌ها فراهم می‌کند. لازمهٔ محرمانگی این است که سایرین برای صدمه زدن یا پاک کردن داده‌ها نکوشند. از نظر شخصی که مخاطب دستور قرار گرفته، «سوژه داده‌ها»[1] یا اشخاص دیگری که ممکن است به‌وسیلهٔ داده‌ها یادآوری یا شناسایی شوند، محدودیت زمانی روشنی برای اقدام وجود دارد. الزام‌های دوگانه برای سالم و ایمن نگهداشتن داده‌ها و حفظ محرمانگی یک رویدادی که تدبیر حفاظت برای آن به اجرا در آمده است، به حفظ حریم خصوصی سوژه داده‌ها یا سایرینی که ممکن است به‌موجب آن داده‌ها یاد آوری یا شناسایی شوند کمک می‌کند (جلالی‌فراهانی، ۱۳۹۵: ۶۷). در آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی در مادهٔ ۱۶ مقرر داشته است که: «حفاظت از داده‌ها باید به‌نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود». در حقوق فرانسه بر اساس مادهٔ ۹۷ قانون آیین دادرسی کیفری هنگامی که مهر و موم‌های داده‌های رایانه‌ای بسته می‌شود، اسناد فقط با حضور اشخاص تحت بررسی، در معیت وکیل خود یا اشخاص مدعو، مفتوح و بررسی می‌شود. اشخاص ثالثی که در نزد آن‌ها توقیف و ضبط صورت گرفته است نیز برای حضور در این اقدامات دعوت می‌شوند. اگر ضرورت‌های تحقیق این موضوع را منع نکنند، کپی یا تصویر اسناد یا داده‌های حاوی اطلاعات رایانه‌ای در اختیار دادگستری، می‌توانند در کوتاه‌ترین مدت، به هزینهٔ اشخاص ذی‌نفع که آن‌ها را درخواست کرده‌اند، به آن‌ها داده می‌شود.

نتیجه

با عنایت به مطالعات صورت گرفته در این مقاله می‌توان به این نتیجه رسید که اصل تناسب توقیف با داده و سامانه در اثبات این‌گونه جرایم داری اهمیت بیشتری نسبت به سایر جرایم است

1. data subject

چون در این‌گونه جرایم؛ شکل ارتکاب، انگیزه و هدف مرتکبین، وسیله و ادلهٔ ارتکاب و... به‌گونه‌ای است که بدون در نظر گرفتن اصل تناسب و با یکسان‌انگاری این جرایم با جرایم سنتی هیچ‌کدام از جرایم اثبات نمی‌شود.

در جرایم سایبری ممکن است سامانه‌ای که برای ارتکاب جرم انتخاب شده، علاوه بر ادلهٔ جرم سایبری مشتمل بر سایر محتویات نیز باشد که با دسترسی به این سامانه در مواردی نظیر توقیف آن‌ها، محتویات یاد شده که ممکن است شخصی، محرمانه و خانوادگی باشد نیز در دسترس قرار می‌گیرد. در چنین مواردی باید به تفسیر مضیق از اصل تناسب پایبند بود و تنها اقداماتی را در جهت اثبات جرم لازم دانست که ارتباط مستقیمی با جرم ارتکابی داشته باشد و از محتویاتی که حتی ممکن است ارتباط غیرمستقیم به ارتکاب جرایم سایبری داشته باشند، خودداری کرد.

با عنایت به موارد یاد شده می‌توان گفت که علاوه بر قانونمند بودن توقیف داده و سامانه، تناسب ادلهٔ توقیف‌شده با نوع جرم ارتکابی به‌عنوان یکی دیگر از اصول حاکم بر توقیف ادلهٔ الکترونیکی می‌باشد. همان طور که بیان شد؛ رعایت اصل تناسب به‌صراحت در قوانین جاری در ایران از جمله در قانون آیین دادرسی کیفری ۱۳۹۲ و قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳ پیش‌بینی شده است.

در اسناد اروپایی نیز به اصل تناسب در توقیف ادلهٔ الکترونیکی توجه شده است. مطابق اسناد مرتبط با جرایم سایبری اصل تناسب جزء اصول مورد احترام بوده و توجه و لزوم رعایت آن در مورد داده و سامانه به‌صراحت در اسناد ذکر شده ازجمله در کنوانسیون اروپایی جرایم سایبری و توصیه‌نامه‌های شورای اروپا مورد تأکید قرار گرفته است. مسئلهٔ اصلی نوشتار حول محور معیار تناسب مورد تحلیل و ارزیابی قرار گرفت و همان طور که در مسئله‌شناسی فرض شده بود، تناسب؛ از یک‌سو مبتنی بر رویکرد اقدام‌محور است که با عنایت به رویهٔ قضایی بررسی شده این نتیجه حاصل شد که باید میان اقدام مقام قضایی در توقیف داده و سامانه با موضوع توقیف، نسبت توازن برقرار باشد یعنی کیفیت و شیوهٔ توقیف با لحاظ ویژگی‌های موضوع توقیف محقق شود. از سوی دیگر، با توجه به ضمانت‌اجراهای پیش‌بینی شده برای مقامات قضایی، در صورت عدم رعایت تناسب، مشخص می‌شود که تناسب رویکردی نتیجه‌محور دارد که می‌کوشد که بر اساس این رویکرد تبعات توقیف غیرمتناسب را به مقام قضایی گوشزد می‌کند.

منابع

فارسی

- انصاری، باقر (۱۳۹۹)، «حق دسترسی به اینترنت؛ مبانی و محتوا»، **مجله حقوقی دادگستری**، دورهٔ ۸۴، شمارهٔ ۱۱۲.
- تدین، عباس (۱۳۹۱)، **تحصیل دلیل در آیین دادرسی کیفری**، چاپ دوم، تهران: بنیاد حقوقی میزان.
- تراب زاده، حسین (۱۳۸۸)، «بررسی صحنه‌های جرم الکترونیکی»، **کارآگاه**، دوره دوم، سال دوم، شمارهٔ ۶.
- جلالی فراهانی، امیرحسین (۱۳۸۶)، «استنادپذیری ادله الکترونیکی در امور کیفری»، **فصلنامه حقوق اسلامی**، دورهٔ ۴، شمارهٔ ۱۵.
- جلالی فراهانی، امیرحسین (۱۳۹۵)، **درآمدی بر آیین دادرسی کیفری جرایم سایبری**، چاپ دوم، تهران: انتشارات خرسندی.
- رئیسی دزکی، لیلا و فلور قاسم‌زاده لیاسی (۱۳۹۹)، «چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر»، **مجله حقوقی دادگستری**، دورهٔ ۸۴، شمارهٔ ۱۱۰.
- زندی، محمدرضا (۱۳۹۳)، **تحقیقات مقدماتی در جرایم سایبری**، چاپ اول، تهران: انتشارات جنگل.
- فضلی، مهدی (۱۳۸۹)، **مسئولیت کیفری در فضای سایبر**، تهران: چاپ نخست، تهران: انتشارات خرسندی.
- گاتن، آلن (۱۳۸۳)، **ادله الکترونیکی**، ترجمه: مصیب رمضانی، شورای عالی توسعه قضایی، تهران: شورای عالی اطلاع‌رسانی.
- نوری، محمدعلی و رضا نخجوانی (۱۳۸۳)، **حقوق تجارت الکترونیکی**، تهران: کتابخانه گنج دانش.
- وروایی، اکبر و سیدشمس الدین میرزکی (۱۳۹۰)، «بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه‌ای پلیس آگاهی تهران سال ۱۳۸۶-۱۳۸۷»، **کارآگاه**، دورهٔ دوم، سال چهارم.

انگلیسی

- Fletcher, George, **Political Theory and Criminal Law**, Criminal Justice Ethics, Vol. 25, 2006.
- ICC, The Appeals Chamber, Judgment on the appeal of the Prosecutor against the "Decision on the Prosecution's Application for a warrant of arrest against Omar Hassan Ahmad Al Bashir", No.: ICC-02/05/01/09-73, 3 Feb 2010.
- ICC, Appeals Chamber, Judgment on the appeal of Mr. Thomas Lubanga Dyilo against the decision of Pre-Trial Chamber I entitled "Décision sur la demande de mise en liberté proviso ire de Thomas Lubanga Dyilo, 13 Feb 2007, No.: 01/04-01/06