فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره سوم | پاییز ۱۴۰۲ | شماره پیاپی ۱۱
ویگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN: 2821-126X

The Ratio of Seizure of Data Related to Crime and Criminal Jurisdiction in the Process of Handling Cybercrimes

Akbar Alizadeh
Department of Law - Amin University of Law and Security Sciences
Tahmineh Adalatjo
Law. Faculty of Humanities. Islamic Azad University, West Tehran Branch.
Hassan Alipour
Assistant Professor, Department of Criminal Law and Criminology, Farabi Campus, University of Tehran, Qom.
Sadegh Tabrizi
Tehran - Tehran Public and Revolutionary Prosecutor's Office. (Corresponding author).
Email: tabrizi.sadegh1400@gmail.com

Keywords:
Cyber Crimes, Criminal Jurisdiction, Data Seizure, Place of Crime, Place of Crime Discovery

Abstract

Data or system seizure (as a means of crime or related to a crime or its subject) is the process of taking possession of information and computer tools by a competent authority. Given the numerous challenges in determining the competent authority for conducting preliminary investigations and handling cybercrimes, data seizure can play a role as a factor in determining jurisdiction. This article is a descriptive-analytical type that was written using a documentary-library method, and researchers have tried to assess the feasibility of the relationship between data seizure and criminal jurisdiction. The research findings show that data seizure can be related to criminal jurisdiction in three ways and help in its determination: one is for detecting a crime where the place of occurrence of the crime is not definitely known. The place of data and system seizure is a clear clue for the detection of the crime. The second is for the purpose of criminal behavior. The place of data or system seizure can indicate the permanent or temporary place of jurisdiction (judicial representation or referral) for handling the crime. Third, in terms of the status of the data or system in relation to criminal behavior, if the data or system was used as a means of committing a crime, was the subject of a crime, or obtained from a crime, it can play an effective role in determining jurisdiction, depending on the case. Considering the three situations mentioned; although there is no direct relationship between data seizure and criminal jurisdiction, due to the numerous jurisdictional challenges related to crimes committed in cyberspace, data seizure could be used as a criterion or indicator to establish criminal jurisdiction.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره سوم | پاییز ۱۴۰۳ | شماره پیاپی ۱۱

صفحات مقاله ۸۱ الی ۹۴

نسبت توقیف داده‌های مرتبط با جرم و صلاحیت کیفری در فرآیند رسیدگی جرایم سایبری

اکبر علیزاده

گروه حقوق- دانشگاه علوم انتظامی امین

تهمینه عدالت‌جو

گروه حقوق، دانشکده علوم انسانی. دانشگاه آزاد اسلامی واحد تهران غرب

حسن عالی‌پور

استادیار گروه حقوق کیفری و جرم شناسی، پردیس فارابی دانشگاه تهران، قم

صادق تبریزی

گروه حقوق دانشگاه آزاد اسلامی واحد تهران غرب

(نویسنده مسئول) پست الکترونیک: tabrizi.sadegh1400@gmail.com

تاریخ دریافت: ۱۴ بهمن ماه ۱۴۰۲ تاریخ پذیرش: ۱۶ شهریور ماه ۱۴۰۳

چکیده

توقیف داده یا سامانه (به‌عنوان وسیله جرم یا مرتبط با جرم یا موضوع آن)، فرآیند در اختیار گرفتن اطلاعات و ابزارهای رایانه‌ای توسط مقام صالح است. با توجه به چالش‌های عدیده‌ای که در تعیین مرجع صالح برای انجام تحقیقات مقدماتی و رسیدگی به جرایم سایبری وجود دارد، توقیف داده می‌تواند به‌عنوان یک عامل در تعیین صلاحیت نقش داشته باشد. مقاله حاضر از نوع توصیفی - تحلیلی است که به روش اسنادی – کتابخانه‌ای به‌نگارش در آمده و محققین کوشیده‌اند تا رابطه میان توقیف داده را با صلاحیت کیفری امکان سنجی کند. یافته‌های تحقیق نشان می‌دهد که توقیف داده به سه صورت می‌تواند با صلاحیت کیفری مرتبط و در تشخیص آن کمک‌کننده باشد: یکی از جهت کشف جرم در جایی که به طور قطعی محل وقوع جرم مشخص نباشد. مکان توقیف داده و سامانه قرینه آشکاری برای کشف جرم است. دوم از جهت وقوع رفتار مجرمانه. محل توقیف داده یا سامانه می‌تواند گویای محل صلاحیت‌دار دائمی یا موقتی (نیابت قضایی یا احاله) برای رسیدگی به جرم باشد. سوم از جهت وضعیت داده یا سامانه نسبت به رفتار مجرمانه که اگر داده یا سامانه به عنوان وسیله ارتکاب جرم بوده یا اینکه موضوع جرم یا تحصیل‌یافته از جرم باشد، حسب مورد می‌تواند نقش موثری در تشخیص صلاحیت ایفا نماید. با توجه به وضعیت‌های سه‌گانه‌ی یاد شده؛ هر چند بین توقیف داده و صلاحیت کیفری رابطه مستقیم وجود ندارد ولی به جهت چالش‌های عدیده صلاحیت در ارتباط با جرایم ارتکابی در فضای سایبر، توقیف داده می‌تواند به‌عنوان یک قرینه یا شاخص برای تثبیت صلاحیت کیفری به کار آید.

واژگان کلیدی: جرایم سایبری، صلاحیت کیفری، توقیف داده، محل وقوع جرم، محل کشف جرم

دانشگاه آزاد اسلامی واحد مرند

مقدمه

بحث صلاحیت سایبری برای اقداماتی نظیر توقیف، تفتیش و ... از جمله مهمترین چالش‌هایی است که بدلیل تفاوت‌های متعدد بین فضای سنتی و سایبری و در واقع ماهیت متفاوت‌شان وجود دارد. بدین‌ترتیب، ماهیت جرم سایبری، چالش قانونی بزرگی بر سر راه نظام‌های ملی عدالت کیفری و صلاحیت‌های قضایی‌شان به وجود آورده که به لحاظ سنتی مبتنی بر اصل سرزمینی بوده و تنها از خلال دیگر اصول همچون شخصی فعال (به عبارتی صلاحیت قضایی نسبت به جرایم ارتکاب‌یافته از سوی شبکه‌هایی که در خارج هستند)، شخصی منفعل (به‌عبارتی صلاحیت قضایی نسبت به‌جرایمی علیه تبعه‌های خودی) کامل شده است اما چنین رویه‌ای در جرایم سایبری با توجه قلمرو جغرافیایی گسترده و فراملی بودن این جرایم نمی‌تواند پاسخگوی صلاحیت رسیدگی برای جرایم سایبری باشد. در حقوق کیفری محل وقوع جرم معیار اصلی و اولی برای تعیین صلاحیت محلی است و در صورتی که محل وقوع جرم مشخص نباشد نوبت به رسیدگی به محل کشف جرم، محل دستگیری متهم یا محل اقامت او می‌رسد. در موارد یاد شده تفاوتی بین جرایم سنتی و سایبری وجود ندارد؛ اما بحثی که وجود دارد و منجر به تفاوت در حوزه صلاحیت محاکم کیفری در رسیدگی به جرایم سنتی و سایبری گردیده این است که فضای الکترونیکی و اینترنت با فضای جغرافیایی مورد نظر در حقوق سنتی متفاوت است، به‌طوری‌که این فضا کاملاً غیرملموس و مجازی است و مرز جغرافیایی نمی‌شناسد. این تفاوت منجر به ابهام در تعیین صلاحیت برای اقدامات قضایی و انتظامی به‌منظور شناسایی، توقیف، تحصیل و نگهداری داده‌ها گردیده است. نتیجه اینکه، بحث صلاحیت در فضای سایبر با چالش‌هایی از قبیل نامعین بودن حیطه‌های جغرافیایی و به‌تبع آن مشکل تعیین محل ارتکاب جرم، مشکل تعیین تابعیت مرتکب و ... مواجه است. در این مقاله، هدف تبیین «نسبت توقیف داده‌های مرتبط با جرم و صلاحیت کیفری در فرآیند رسیدگی جرایم سایبری» است. همان‌گونه که بیان شد؛ صلاحیت سایبری بر همه اقدامات انتظامی و قضایی اثرگذار بوده و توقیف داده‌ها در صورتی امکان‌پذیر است که صلاحیت چنین اقدامی پیش‌بینی شده باشد. حتی در جرایم مشهود نیز که تحت شرایطی امکان توقیف داده برای ضابطان پیش‌بینی شده، با مشخص شدن عدم صلاحیت، بلافاصله باید داده‌های توقیف شده به‌مرجع صلاحیت‌دار ارسال گردد. از این‌رو؛ بین توقیف داده و صلاحیت کیفری رابطه یا نسبت وجود دارد. اما بسته به اینکه، داده چه نقشی در وقوع جرم دارد وضعیت‌های متعددی قابل تصور است. در جرائم سایبری، در برخی از موارد، داده به‌عنوان وسیله ارتکاب جرم و در مواردی به‌عنوان موضوع جرم سایبری و در نهایت در مواردی تحصیل یافته از جرم سایبری محسوب می‌شود. بنابراین، یک داده ممکن است در جرایم سایبری در سه وضعیت متفاوت نقش داشته باشد. مسئلهٔ اصلی که در این مقاله بدنبال پاسخ به آن هستیم، نسبت‌سنجی بین توقیف داده در هر یک از وضعیت‌های سه‌گانه یاد شده با صلاحیت سایبری است. در پاسخ به این مسئله، ابتدا به تبیین چیستی توقیف داده و صلاحیت سایبری و سپس ضمن تحلیل وضعیت صلاحیت کیفری در جرایم سایبری، به نسبت‌سنجی توقیف داده و صلاحیت برای توقیف داده در هر یک از وضعیت‌های سه‌گانه می‌پردازیم.

۱- چیستی توقیف داده

برای پی بردن به چیستی اصطلاح توقیف داده و سامانه، لازم است ابتدا به تفکیک و اختصار تعریفی از هر یک ارائه گردد.

توقیف به معنای ضبط کردن، بازداشت نمودن، قبضه کردن و واقف گردانیدن آمده است (عمید، ۱۳۷۵: ۱۳۵۳) و در عالم حقوق به معنای تصرف قانونی و تحت حفظ قرار دادن هر شی که بتواند به عنوان دلیل مورد استفاده مقامات قضایی و مراجع قانونی قرار بگیرد، به کار می‌رود. در فرهنگ دهخدا بیش از همه بر وصف «ایستانیدن» در توصیف توقیف تکیه شده و توقیف کردن به معنای ضبط کردن، بازداشت کردن و واقف گردانیدن آمده است (دهخدا، ۱۳۷۷: ۷۳۷).

«داده» به صورت خاص در نظام حقوقی ایران تعریف نشده است ولی به‌صورت «داده پیام» و «داده ترافیک» از آن تعریف به عمل آمده است. به موجب بند (الف) ماده یک قانون تجارت الکترونیک: «داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود. داده ترافیک نیز در

تبصره یک ماده ۳۲ قانون جرایم رایانه‌ای (تبصره ۱ ماده ۶۶۷ ق.آ.د.ک ۱۳۹۲) 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. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود».

سامانه معادل فارسی واژه «سیستم[1]»، است. سیستم، واژه‌ای است انگلیسی که در عربی به‌عنوان نظام شناخته می‌شود و سامانه به عنوان معادل فارسی برای آن پیشنهاد شده است. سامانه از نظر لغوی به معنای «مجموعه‌ای متشکل از عناصر مرتبط با یکدیگر که مسئول انجام کار خاصی هستند» (عمید، ۱۳۷۵: ۲۶۴) تعریف شده است. در ادبیات فارسی؛ از واژگان «جهاز»، «دستگاه»، «سیستم»، «نظام» و «الگو» به عنوان مترادف‌های واژه سامانه یاد شده است. در بین این مترادف‌ها، واژه «سیستم[2]»، بیشترین کاربرد را داشته و همان‌طور که بیان شد، معادل انگلیسی واژه سامانه می‌باشد. با توجه به تعاریفی که از سیستم، نظام و سامانه به عمل آمده می‌توان به این جمع‌بندی از منظر لغوی رسید که «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». اصطلاح «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 یا سامانه توقیف شده دخل و تصرفی نماید (تبریزی و همکاران ، ۱۴۰۰: ۱۳۴). روش‌هایی که مقنن برای توقیف داده و سامانه ذکر کرده حصری نیستند، اما روش‌های توقیف داده با روش‌های توقیف سامانه متفاوتند. به موجب بند الف ماده ۳۸ آئین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی و قسمت اخیر ماده ۶۷۵ قانون دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۳؛ شیوه‌ها یا روش‌های خاص توقیف داده به صورت تمثیلی و به شرح ذیل بیان شده است:

چاپ داده‌ها

تصویربرداری از تمام یا بخشی از داده‌ها

غیر قابل دسترس کردن داده‌ها

در مورد شیوه‌های توقیف سامانه نیز مقنن در ماده ۶۷۶ قانون دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی موارد توقیف را به‌طور حصری معین کرده است. مطابق این ماده روش‌ها یا شیوه‌های توقیف سامانه عبارت‌اند از: الف) داده‌های ذخیره‌شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد؛ ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت‌افزاری امکان‌پذیر نباشد؛ ج) متصرف قانونی رضایت داده باشد؛ د) تصویربرداری (کپی‌برداری) از داده‌ها به لحاظ فنی امکان‌پذیر نباشد؛ ه) تفتیش در محل باعث آسیب داده‌ها شود.

۲- چیستی صلاحیت سایبری

قبل از تبیین چیستی صلاحیت سایبری؛ مفهوم شناسی صلاحیت و انواع آن در دادرسی‌های کیفری به‌عنوان یک مقدمه در اینجا ضروری است. در مفهوم‌شناسی صلاحیت باید بیان داشت که مقنن تعریفی از صلاحیت ارائه نداده است. با این وجود می‌توان با استنباط از مقررات پیرامون صلاحیت در قوانین و مقررات جاری و عقیده صاحب‌نظران، صلاحیت را به‌معنای شایستگی و توانایی مرجع قضایی تعریف نمود که به‌موجب قانون جهت رسیدگی به دعاوی پیش‌بینی شده است. صلاحیت در هر دو نوع دعاوی حقوقی و کیفری از جمله مباحث بسیار مهم می‌باشد (علیزاده و همکاران، ۱۴۰۱: ۵۰۵). «صلاحیت در اصطلاح حقوقی، توانایی و الزامی است که مراجع قضایی در رسیدگی به دعاوی به‌موجب قانون دارند» (گلدوست جویباری، ۱۳۹۳: ۲۷۳) و در تعریف دیگر صلاحیت کیفری «عبارت از شایستگی و اختیاری می‌باشد که به موجب قانون برای مرجع رسیدگی به امور کیفری واگذار شده است» (خالقی، ۱۳۹۴: ۱۵۸). در امور کیفری، صلاحیت بر مبنای نوع و عنوان رفتار مجرمانه، اهمّیت بزه ارتکابی و میزان مجازات جرم ارتکابی و شخص مرتکب جرم تعیین می‌شود و به سه قسم ذاتی، محلی و شخصی تقسیم می‌شود. صلاحیت

[1] system
[2] system

ذاتی به معنای تفکیک و تقسیم دعاوی میان دادگاه‌ها به‌موجب قوانین است. در امور کیفری، صلاحیت ذاتی محاکم کیفری بر مبنای عنوان رفتار مجرمانه، مجازات جرم تعیین می شود. صلاحیت ذاتی از نظر صنف، نوع و درجه دارای انواع متعددی ا ست. منظور از صنف؛ تشخیص اداری یا قضایی بودن محاکم است. منظور از نوع، تشخیص عمومی یا اختصاصی بودن محاکم است و منظور از درجه، تشخیص بدوی (تالی) یا عالی بودن محاکم می‌باشد. به‌عنوان نمونه دادگاه کیفری دو از نظر صنف، نوع و درجه به ترتیب؛ قضایی، عمومی کیفری و بدوی ا ست (علیزاده و همکاران، ۱۴۰۱: ۵۰۷). صلاحیت محلی‌که برخی آن را « صلاحیت جغرافیایی» خوانده‌اند، ناظر به صلاحیت دادگاه در حوزه قضایی و محدوده جغرافیایی معین است. در امور کیفری صلاحیت محلی به این معنی ا ست که حدود جغرافیایی انجام وظیفه دادگاه یا هر مرجع قضایی دیگر مبتنی بر عنصر مکان تعیین می شود، این مکان ممکن ا ست علاوه بر محل وقوع جرم به‌عنوان مبنای ا صلی، محل‌های دیگری مثل محل کشف جرم، د ستگیری متهم، ذخیره ادله، استقرار سامانه‌های رایانه‌ای یا محل فرود هواپیما باشد. بر این اساس گفته می‌شود در امور کیفری صلاحیت محلی را می‌توان بر حسب ضوابط مختلف از قبیل محل وقوع جرم، کشف جرم، محل دستگیری متهم، محل بازداشت یا اقامتگاه او م شخص کرد (آ شوری، ۱۳۹۸: ۱۰۳). بالاخره صلاحیت شخصی به‌عنوان سومین م صداق از انواع صلاحیت، به معنای تعیین صلاحیت بر مبنای شخصیت مرتکب‌جرم ا ست. به‌عبارت‌دیگر، گاهی به‌جای مو ضوع اتهام، شخصیت مرتکب، ضابطه تعیین صلاحیت دادگاه قرار می‌گیرد و قانون رسیدگی به اتهامات افرادی معین را در صلاحیت مرجعی خاص قرار می‌دهد. به‌عنوان نمونه، در صورتی‌که یک قا ضی مرتکب جرم سایبری گردد، بر مبنای شخصیت وی، دادگاه صالح به ر سیدگی (به‌موجب ماده ۳۰۷ ق.آ.د.ک ۱۳۹۲)، دادگاه‌های کیفری مرکز (تهران) است.

با این مختصر در ارتباط با تعریف صلاحیت و انواع آن؛ در خصوص صلاحیت در جرایم سایبری می‌توان گفت که در این‌گونه جرایم به‌دلیل م شخصه‌ی بارز آنها یعنی «بزهکاری بدون مرز»، صلاحیت چند بعدی ا ست. به بیان دیگر، با توجه به عدم تعیین مکانی جرم سایبری، برای تعیین معیار صلاحیت این نوع از جرایم می‌توان جنبه‌های مختلفی را لحاظ نمود. با مداقه در عناصر جرم سایبری نظیر بستر ارتکاب جرم و چگونگی انجام آن، کاربر یا مرتکب و نیز بزه‌دیدهٔ جرم سایبری و ... می‌توان فروض مختلفی را برای اعمال صلاحیت در نظر گرفت. محلی‌که وسیله ارتکاب، نظیر کامپیوتر در آن مستقر است؛ محلی که سرویس‌دهنده خدمات اینترنتی در آن مستقر است؛ محلی‌که کاربر در آن اقامت است؛ محلی‌که بزه‌دیده در آن اقامت دارد؛ محلی‌که بارگذاری و پیاده‌سازی داده‌ها در آن انجام می‌گیرد؛ محلی که جرم در آن محقق می‌شود و ... از جمله فروضی هستند که در بحث صلاحیت سایبری مطرح می‌شوند. موارد یاد شده را می‌توان در قالب دو دسته از معیارهای تعیین صلاحیت دسته‌بندی کرد: نخست؛ تعیین صلاحیت کیفری به اعتبار قواعد معمول صلاحیت و دوم، تعیین صلاحیت کیفری به اعتبار ویژگی‌های جرم سایبری (طهماسبی و شاهمرادی، ۱۳۹۷: ۱۴۵).

در تعیین صلاحیت به اعتبار قواعد معمول صلاحیت؛ معیارهای سنتی تعیین صلاحیت یعنی صلاحیت سرزمینی، صلاحیت مبتنی بر تابعیت متهم، صلاحیت مبتنی بر تابعیت بزه‌دیده، صلاحیت حمایتی و صلاحیت جهانی مورد توجه قرار گرفته و بر مبنای آنها مرجع صالح تعیین می‌گردد. در تعیین صلاحیت به اعتبار ویژگی‌های جرم سایبری نیز، نظریه محل ا ستقرار سیستم رایانه‌ای یا سرور، نظریه محل بارگذاری و نظریه محل پیاده‌سازی؛ از جمله مهمترین نظریاتی هستند که برای تعیین مرجع صلاحیت‌دار بیان گردیده‌اند.

۳- امکان سنجی ارتباط توقیف داده و مرجع صالح

با عنایت به آنچه که پیرامون معیارهای صلاحیت بیان گردید، برای تعیین صلاحیت، باید مسائل متعددی مورد توجه قرار بگیرد. نوع اقدام مجرمانه، محل وقوع جرم، اقدامات ضابطان و مقامات قضایی از جمله در تفتیش، توقیف و نگهداری داده‌ها و نظایر اینها مواردی هستند که در تعیین صلاحیت محاکم قضایی در مراحل مختلف دادرسی نقش دارند. بدین‌ترتیب؛ توقیف داده و فرایندهای مرتبط با آن از جمله اقداماتی هستند که با صلاحیت محاکم در ارتباط می‌با شند. فرایند توقیف داده یک اقدام انتظامی

بوده که در عمل راساً (در جرایم مشهود) یا به‌دستور مقام قضایی (در جرایم غیرمشهود) توسط ضابطان دادگستری انجام می‌شود. بدین‌ترتیب؛ توقیف داده، فرایندهای تعریف شده در مقررات شکلی هستند که تا قبل از تصویب قانون آئین دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی مصوب ۱۳۹۲ تنها در بخش دوم قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ذکر شده بودند که به‌همین دلیل قانون‌گذار در همین بخش و در راستای پرکردن خلاهای دادرسی در این جرایم، به قانون آئین دادرسی کیفری ارجاع داده بود. ولی با توجه به‌ماهیت 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 ناشی‌از مواد شکلی قانون جرایم رایانه‌ای نیز به‌تنهایی نمی‌توانست راهگشای تمامی مسایل مربوط به فرایندهای دادرسی در جرایم رایانه‌ای باشد. بعد از تصویب قانون آئین دادرسی کیفری مصوب ۱۳۹۲ فرایند دادرسی جرایم رایانه‌ای و به تبع آن فرایندهای پیرامون توقیف داده به صورت خاص پیش‌بینی شد. این فرایند (که مشتمل بر ضوابط و اصول حاکم بر دادرسی‌های کیفری در جرایم سایبری بخصوص در مرحله تحقیقات مقدماتی است)، ضمن اینکه از ضوابط عمومی حاکم بر فضای سنتی پیروی می‌کند، دارای قواعد خاصی است که در تحقیقات مقدماتی و رسیدگی به‌جرایم سایبری باید رعایت شود. برای مشخص شدن این ضوابط، پلیس یا مقام قضایی، باید ابتدائاً وضعیت پنج عامل درگیر در هر وقوع این دسته از جرایم را مشخص نماید. این پنج عامل عبارتند از:

مالک وب سایت: که می‌تواند خصوصی باشد مانند وبسایت یک شرکت، یا دولتی باشد مانند سایت ریاست جمهوری، قوه قضائیه، یا تلفیقی باشد، مانند سایت یک نهاد خصولتی.

محتوی وب سایت: می‌تواند آموزشی، فرهنگی، سیاسی، خبری یا هر محتوی دیگری باشد.

میزبان وب سایت و دارنده (مالک) آن: میزبان می‌تواند در داخل کشور یا خارج کشور باشد.

دامنه وب سایت: می‌تواند در یکی از دامنه‌های عمومی ثبت شده باشد مانند com؛ یا دامنه‌های مرتبه کد بالای کشوری مانند ir .

کاربر وب سایت: کاربر می‌تواند تبعه ایران یا خارجی باشد که در داخل یا خارج کشور مستقر است.

در کنار وب سایت‌های اینترنتی، شبکه‌های پیام رسان مانند telegram و سیستم‌های ارتباطاتی مانند بستر پست الکترونیکی Yahoo و Google می‌توانند در گستره جرایم اینترنتی دخیل باشند (پارک، ۲۰۱۶: ۲۱). بدین‌ترتیب؛ در نسبت‌سنجی بین توقیف داده و صلاحیت برای توقیف داده، باید مشخص شود که داده چه نقشی را در ایجاد یا تحقق جرم داشته است. در کل یک داده می‌تواند به‌عنوان وسیله ارتکاب جرم بکار رود یا موضوع جرم سایبری باشد. علاوه‌بر این، داده ممکن است اثر یا نتیجه ارتکاب جرم سایبری و در واقع تحصیل‌یافته از جرم باشد. بدین‌ترتیب، داده در جرایم سایبری یکی‌از سه نقش، وسیله ارتکاب جرم، موضوع جرم یا تحصیل‌یافته از جرم را خواهد داشت. بسته به اینکه داده در کدام یک‌از این سه نقش در ارتکاب جرم دخیل باشد، موضوع مهمی است که در تمامی اقدامات مرتبط با تحقیقات مقدماتی و رسیدگی‌های قضایی از جمله در تعیین صلاحیت باید مورد توجه قرار گیرد. در ادامه در راستای نسبت‌سنجی بین توقیف داده و صلاحیت کیفری، به تفکیک نقش داده در هر یک‌از سه موقعیت ذکر شده مورد بررسی قرار گرفته و تاثیر آن بر صلاحیت محاکم قضایی در رسیگی به جرایم سایبری مطالعه می‌شود.

۵- جلوه‌های ارتباط توقیف داده و صلاحیت کیفری

با عنایت به موارد یاد شده تبیین ارتباط بین توقیف داده و صلاحیت محاکم قضایی بستگی مستقیم به نقشی دارد که داده در جرم سایبری ایفا می‌نماید. همان‌گونه‌که بیان شد؛ این نقش‌ها بسته به اینکه داده به‌عنوان وسیله ارتکاب جرم بوده یا موضوع جرم یا تحصیل یافته از جرم بوده باشد، تاثیر متفاوتی بر صلاحیت محاکم دارد. در بحث صلاحیت محاکم؛ هر چند با بکارگیری قواعد و

ضوابط قانونی پیش‌بینی شده در رعایت ترتیبات (ابتدا محل وقوع جرم، سپس محل کشف و ..) تعیین مرجع قضایی، آسان به‌نظر برسد؛ با این‌حال ممکن است داده‌های مرتبط با جرم یا ناشی‌از جرم یا وسیله جرم در فضای سایبر، در یک مکان مشخص، مستقر نباشند و همین امر چالشی برای صلاحیت کیفری سایبری خواهد بود. در اینجا؛ چالش اصلی این است که توقیف داده‌های مرتبط با جرم در موقعیت‌های مختلف چه تاثیری بر صلاحیت کیفری می‌تواند داشته باشد؟ در ادامه در راستای پاسخ به این سوال، جلوه‌های ارتباطی بین داده و صلاحیت کیفری مطالعه و صلاحیت کیفری در هر یک از جلوه‌های سه‌گانه (یعنی؛ ۱- صلاحیت در مورد داده‌هایی که خود مرتبط یا موضوع جرم سایبری بوده‌اند، ۲- صلاحیت در مورد داده‌هایی که وسیله ارتکاب جرم سایبری بوده‌اند و ۳- صلاحیت در مورد داده‌هایی که تحصیل یافته از جرم سایبری بوده‌اند) مورد بررسی قرار می‌گیرد.

۱-۵- صلاحیت کیفری در توقیف داده‌های موضوع جرم سایبری

یکی‌از اصلی‌ترین جلوه‌های ارتباطی بین توقیف داده و صلاحیت کیفری، مربوط به‌جایی است که در آنها ادله الکترونیکی خود موضوع جرم بوده است. در این موارد، جرم‌انگاری به این دلیل است که خود داده یا سامانه دستکاری یا مورد سوءاستفاده قرار می‌گیرد. برخی در تعریف جرایمی که داده و سامانه‌های الکترونیکی به‌عنوان موضوع جرم هستند، گفته‌اند: «سوءاستفاده از کامپیوتر یعنی هر واقعه‌ای که توأم با تکنولوژی کامپیوتر شود و به واسطه آن بزه‌دیده متحمل خسارتی شود و مرتکب به عمد مالی یا منفعتی کسب کند یا بتواند کسب کند» (محمدی فردوئی، ۱۳۹۷: ۴۶۲). کمیته متخصصان شورای اروپا اعلام کرده‌اند: «جرایمی که داده و سامانه‌های الکترونیکی به‌عنوان موضوع جرم هستند، بر تیپ‌های مختلف جرائمی گفته می‌شود که اغلب بوسیله برخی [دولت‌های] عضو، جرم شناخته شده‌اند و برخی از [دولت‌های] عضو هنوز بحث قانع کننده‌ای درباره آن ارائه نکرده‌اند. به دلیل طراحی رهنمودهایی برای جرم کامپیوتری ضرورت ارائه یا گزینش تعریفی رسمی از جرم کامپیوتری بیشتر رخ می‌نماید. این امر به‌قانونگذاران ملی واگذار شد تا با توجه به سنن تاریخی سیستم قضایی خود، در کنار رهنمودهای کمیته تعریفی ارائه کنند که دو لیست حداقل و اختیاری را در برداشته باشد» (محمدی فردوئی، ۱۳۹۷: ۴۶۳-۴۶۲). سازمان ملل متحد در شماره ۴۴ نشریه بین‌المللی سیاست جنایی با اذعان به اینکه در زمینه جرایم کامپیوتری تعریف مورد توافقی وجود ندارد، جرایم کامپیوتری را از یک سو شامل فعالیت‌های مجرمانه با ماهیت سنتی مثل سرقت و جعل دانسته که همگی معمولاً در همه جا مشمول ضمانت اجراهای کیفری می‌شوند و از سوی دیگر شامل فعالیت‌های مجرمانه نوینی که در آنها کامپیوتر امکان این‌گونه سوء استفاده‌ها را مهیا ساخته که پیش از این امکان‌پذیر نبوده است. اعمال صلاحیت بر مبنای موضوع جرم بودن ادله الکترونیکی در برخی از جرایم راهکار موثرتری بوده و با قواعد صلاحیت سنخیت بیشتری دارد. جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی نظیر دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی نظیر سرقت و کلاهبرداری رایانه‌ای، تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی، جرائم علیه عفت و اخلاق عمومی و جرایم علیه هتک حیثیت و نشر اکاذیب از جمله این جرایمی هستند که مقنن، داده و سامانه را به عنوان موضوع جرم آنها در نظر گرفته و محل وقوع جرم را اصلی‌ترین معیار برای اعمال صلاحیت در نظر گرفته است (ر.ک: مواد ۶۶۴ و ۶۶۵ ق.آ.د.ک).

در جایی‌که داده به‌عنوان موضوع جرم بوده، نظریه غالب برای اعمال صلاحیت، محل وقوع جرم است. در واقع برای توقیف داده، مرجعی صالح است که محل وقوع جرم در حوزه آن قرار دارد. تقریبا تمامی اسناد بین‌المللی و منطقه‌ایی مربوط به جرم سایبر که مقررات خاصی را به بحث صلاحیت اختصاص داده‌اند، اصل صلاحیت سرزمینی را مورد شناسایی قرار داده و دول عضو را مجاز می‌دانند تا نسبت به جرایمی که طبق سند جرم تلقی شده و در داخل مرزهای جغرافیای سرزمینی آنها ارتکاب می‌یابند اعمال صلاحیت کنند. پیش‌بینی اصل صلاحیت سرزمینی عینی در برخی از اسناد به وضوح حاکی از آن است که از نظر تدوین کنندگان این اسناد لازم نیست تمامی ارکان یک جرم در داخل قلمرو یک کشور به منظور شمول صلاحیت آن دولت ارتکاب یابند؛ گزارش تفصیلی کنوانسیون اروپایی جرم سایبر، به‌عنوان مثال، مشخص می‌دارد که تحت اصل صلاحیت سرزمینی، دولت

عضو می‌تواند ادعای دارا بودن صلاحیت کند زمانی‌که: ۱- شخص حمله‌کننده به یک سیستم رایانه‌ایی و سیستمی که مورد حمله قرار گرفته است در داخل مرزهای آن کشور قرار گرفته باشد و ۲- جایی که سیستم کامپیوتری مورد حمله قرار گرفته در داخل مرزهای آن دولت قرار دارد؛ حتی اگر شخص حمله‌کننده در داخل مرزهای آن کشور حضور نداشته است (روزگار، ۱۳۹۶: ۲۱۸-۲۱۷).

پیش‌نویس قانون نمونه کمسا در ماده‌ی (f) ۴۰ صلاحیت را بر مبنای معیار محل ارتکاب جرم مشخص می‌کند و دستورالعمل اتحادیه‌ی اروپا در خصوص استثمار جنسی کودک نیز صلاحیت را بر اساس محل ارتکاب تمام یا بخشی از جرم در قلمرو سرزمینی یک دولت تصریح دارد. ارتکاب جرم به وسیله‌ی تکنولوژی اطلاعات و ارتباطات نیز که از درون یک سرزمین مورد دسترسی قرار گرفته است طبق این سند به منزله‌ی ارتکاب بخشی از جرم از و در درون آن سرزمین است حتی اگر تکنولوژی مورد استفاده قرار گرفته در درون آن سرزمین مستقر نبوده باشد. تصمیم اتحادیه‌ی اروپایی در خصوص حملات علیه سیستم‌های اطلاعاتی در دو حالت جرم را ارتکاب یافته در درون سرزمین تلقی کرده است: ۱- حملات توسط مرتکبی که به صورت فیزیکی در داخل سرزمین حاضر می‌باشد علیه سیستم‌های اطلاعاتی راه اندازی شده باشد (صرف‌نظر از اینکه این سیستم‌ها در درون سرزمین محل حضور مرتکب قرار گرفته باشند یا خیر)، ۲- حملات علیه سیستم‌های اطلاعاتی در درون سرزمین راه‌اندازی شده باشند (خواه مرتکب حمله به صورت فیزیکی در درون سرزمین حاضر باشد یا خیر) (ماده ۱۰).[1]

در رویه قضایی نیز موضوع جرم در تعیین صلاحیت مورد توجه قرار گرفته است و با صدور رای وحدت رویه شماره ۷۲۹ توسط هیأت عمومی دیوان عالی کشور در تاریخ ۱۳۹۱/۱۲/۱ شکل عام و در حکم قانون نیز به خود گرفت. به‌موجب رأی وحدت رویه شماره ۷۲۹ هیات عمومی دیوان‌عالی کشور: «نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز مستفاده از ماده ۲۹ مورد تأیید قانون گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه، هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضایی مختلف صورت گرفته باشد، دادگاهی که بانک افتتاح کننده حساب زیان دیده از بزه که پول به طور متقلبانه از آن برداشته شده در حوزه آن قرار دارد، صالح به رسیدگی است». با عنایت به رای ذکر شده، دادگاه صالح دادگاهی است که محل وقوع نتیجه یا موضوع جرم در آنجا بوده است. در توجیه اعطای صلاحیت محلی جهت توقیف داده به مراجعی که موضوع جرم در آن واقع است، می‌توان گفت که برخی از جرایم ارتکابی در فضای سایبر چنان اثر زیان‌باری در این فضا و عالم خارج از خود بر جای می‌گذارند که محل تحقق اثر، خود می‌تواند نقش مهمی در فرآیند دادرسی این جرم داشته باشد. پذیرفتن نظریه محل وقوع گاهی اوقات ممکن است منطبق با سایر نظریاتی که در این خصوص مطرح شده است باشد. نظریه مزبور در واقع از اصلی تحت عنوان «اصل صلاحیت سرزمینی عینی» گرفته شده که ناظر به صلاحیت رسیدگی به جرایم از جنبه فرامرزی و بین‌المللی بودن آن است.

۲-۵- صلاحیت کیفری در توقیف داده‌های وسیله ارتکاب جرم سایبری

یکی دیگر از جلوه‌های ارتباطی توقیف داده و صلاحیت کیفری، مربوط به جایی است که داده به‌عنوان وسیله ارتکاب جرم مورد استفاده است. به طور کلی هر داده و سامانه‌ای یا وسایل مرتبط با آنها می‌تواند به‌عنوان وسیله ارتکاب جرم باشد. بنابراین سامانه‌های رایانه‌ای اعم‌از رایانه‌های شخصی یا رایانه‌های ارائه‌کننده خدمات، انواع حافظه‌های جانبی و داده‌های درون سامانه‌های الکترونیکی به عنوان وسایل ارتکاب جرم بکار گرفته می‌شوند (حسینی و ظریف‌منش، ۱۳۶۲: ۲۴). نظریات متعددی پیرامون صلاحیت کیفری برای توقیف ادله الکترونیکی که به‌عنوان وسیله ارتکاب جرم بوده‌اند، بیان شده است. یکی از مهمترین نظریات پیرامون صلاحیت سایبری؛ نظریه محل قرارگیری وسیله‌ی مؤثر در ارتکاب جرم است.[2] این وسیله سیستم رایانه‌ای نام دارد؛ منظور از رایانه یا سیستم رایانه‌ای موضوع بحث برابر تعریف ماده ۱ کنوانسیون جرائم سایبری عبارت است از: «هر دستگاه یا

1 European Union Council Framework Decision on attacks against information systems (EU Decision on Attacks against Information Systems), 2005/222/JHA, 24 February 2005, Article 10

2 Location of Computer

مجموعه‌ای از دستگاه‌های مرتبط یا متصل به یکدیگر است که یک یا چند تای آنها مطابق یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد». با توجه به تعریف فوق اولاً؛ کامپیوترهای شخصی و غیر متصل که نقشی در فضای سایبر ندارند از موضوع بحث خارج می‌باشند. در فضای سایبر تنها کامپیوترهایی مدنظرند که در شبکه، مرتبط «متصل» به یکدیگر می‌باشند. ثانیاً؛ فضای سایبر اختصـــاص به اینترنت ندارد و موارد دیگری نظیر ماهواره‌ها و ... را نیز در بر می‌گیرد، لیکن به جهت اینکه اینترنت واجد تمام ویژگی‌های خاص فضای سایبر است بیشتر به آن پرداخته می شود. بر اساس قوانین برخی از کشورها، ملاک در تعیین و اعمال صلاحیت محاکم برای تحقیقات مقدماتی و رسیدگی محل قرار گرفتن رایانه یا وسیله ارتکاب جرم سایبری است لذا چنانچه عمل مجرمانه‌ای نظیر انتشـــار یک ویروس یا اعمال متقلبانه نظیر کلاهبرداری و جعل از طریق کامپیوتری که در یک محل قرار گرفته صورت گیرد دادگاه آن محل صالح به رسیدگی می‌باشد. خواه مرتکب در کشور یا محل قرار گرفتن کامپیوتر ساکن باشد یا نباشد وخواه تبعه آن کشور باشد یا نباشد و خواه اینکه عمل در داخل کشور یا خارج از آن کشور صورت گرفته باشد. (مایر، ۲۰۱۰: ۱۷۵-۱۴۲).

«در این نظریه جایی که کامپیوتر تأثیرگذار در وقوع جرائم سایبری قرار دارد، محل ارتکاب محسوب شده و نظام قضایی همان محل جهت تعقیب جرم ارتکابی صالح خواهد بود. برای مثال، یکی از رایج‌ترین اقداماتی که هکرها انجام می‌دهند این است که برای ارتکاب انواع جرائم سایبری نظیر پخش انواع ویروس، نشر هرزه‌نگاری یا حتی تعقیب ایذایی، یک رایانه بی‌گناه را حتی در یک کشور دیگر به‌عنوان پایگاه خود قرار می‌دهند و از طریق آن مرتکب جرائم سایبری می‌شوند (روشن‌فر، ۱۳۹۲: ۱۱۳).

قانون آئین دادرسی کیفری در بخش آئین دادرسی جرائم رایانه‌ای و در ماده ۶۶۴، این نظریه را نسبت به سیستم‌های واقع در قلمرو حاکمیت کشور ایران پذیرفته است. ماده‌ی مذکور مقرر می‌دارد: «علاوه بر موارد پیش‌بینی شده در دیگر قوانین، دادگاه‌های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود: الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به‌کار رفته‌اند به هر نحو در ســیســتم‌های رایانه‌ای و مخابراتی یا حامل‌های داده‌ی موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد. ب) جرم از طریق تارنماهای دارای دامنه بالای کد کشوری ایران (ir) ارتکاب یافته باشد.

برخی این نظریه را به‌گونه‌ای دیگر و تحت عنوان نظریه «صـلاحیت بر اسـاس محل اسـتقرار سـرور»[1] مطرح کرده‌اند و محل مذکور را همیشـــه عامل مؤثر تلقی کرده و آن را محل ارتکاب جرم قلمداد کرده‌اند. منظور این اســت که از آنجا که هر داده و اطلاعاتی که به‌عنوان وسیله جهت ارتکاب جرم مورد استفاده قرار می‌گیرد حتماً در بستر فضای سایبر تأثیر خود را می‌گذارد و فضای سایبر بستری جز سرورهای محدود و معدود ندارد. «در واقع فضای سایبر همین بستر است که در آن داده های الکترونیکی ذخیره و پردازش و می‌شوند. بنابراین در هر کشور که مراکز تولید کننده بسترهای الکترونیکی، که به آنها مراکز داده اینترنتی گفته می‌شـود، وجود داشـته و از لحاظ فنی به ارائه خدمات میزبانی و ملزومات تبعی آن می‌پردازند، آن محل جزو قلمرو حاکمیتی آن کشـور قرار دارد (حیدری و میلانی، ۱۴۰۱: ۵-۴). بنابراین، باید دید که جرم از فضـای کدام سـرور عبور کرده اسـت، که در این صورت محل استقرار همان سرور صالح به رسیدگی خواهد بود.

این نظریه علیرغم انطباق بیشتر با واقعیت قابلیت اجرایی آن بسیار ضعیف است. این نظریه از آن جهت با واقعیت منطبق است که بر روی خاک واقعی فضای سایبر دست گذاشته و از آنجا که این سرورها در روی یک قلمرو زمینی معین قرار دارند در واقع قاعده‌ی صلاحیت سرزمینی سنتی را، که مادر قواعد صلاحیتی محسوب می‌شود، اجرا کرده است. چون در واقع جرائم سایبری در جزئی از خاک همان محل ارتکاب یافته است. در خصوص قابلیت اجرایی چنین نظریه باید گفت که جهت اجرای این نظریه باید کلیه‌ی بزه‌دیدگان جرائم سایبری از سراسر جهان مجبور شوند به سه یا چهار کشور دارنده‌ی سرور جهت شکایت مراجعه کنند و نزد محاکم آنها اقامه دعوا کنند و آن مراجع مجبور شوند به صدها هزار پرونده سایبری رسیدگی کنند. درحالی‌که چنین عملی نه‌تنها مشکل بلکه غیرممکن می‌نماید و شاید به همین دلیل بوده است که تاکنون کشورهای صاحب این سرورها حتی به

1 The Theory of The Server

فکر اجرایی کردن این نظریه نیفتاده‌اند. چرا که در حال حاضر بیش از ۸۰ ٪ مراکز اینترنتی دنیا در آمریکای شمالی و شمال اروپا واقع هستند و بعید است آنها به اعمال چنین صلاحیتی برای رسیدگی به طیف بسیار متنوع و عظیم جرائم ارتکابی در فضای سایبر از سراسر جهان (که به مجرمانه بودن برخی از آنها نیز اعتقاد ندارند) تن در دهند (فروغی و البوعلی، ۱۳۹۱: ۲۱۱).

نظریه دیگری که در خصوص تعیین صلاحیت برای توقیف داده‌هایی که به‌عنوان وسیله ارتکاب جرایم سایبری بوده‌اند، می‌توان نام برد؛ نظریه صلاحیت بر اساس محل حضور بارگذاران و پیاده سازان محتوای شبکه‌ای است. با این توضیح که بطور کلی در فضای سایبر دو گروه عمده ایفای نقش می‌کنند. اشخاصی که داده‌ها را از طریق کامپیوتر در این فضا قرار می‌دهند که به آنها بارگذار یا (Up loader) گفته می‌شود یا اشخاصی که داده‌ها را از این فضا و از طریق کامپیوتر دریافت می‌کنند که به آنها پیاده‌ساز (Down loader) گفته می شود. در اینجا نیازی نیست که هویت همگی این افراد مشخص بوده و یا از یکدیگر مطلع باشند لذا نباید آنها را با فرستنده۱ و گیرنده۲ که معمولاً هویتشان در ارتباطات الکترونیکی معلوم است اشتباه گرفت همچنین معیار بارگذاری و پیاده‌سازی را نباید و نمی‌توان بر عناوین «بزهکار و بزه‌دیده» حمل کرد چه آنکه همان قدر که ممکن است بارگذار مرتکب جرم باشد، احتمال دارد بزه‌دیده جرم تلقی شود. مثلاً در جایی که بارگذار محتوی مجرمانه‌ای را نظیر تصاویر مستهجن یا هتک حرمت و یا ویروس یا توهینی را بر روی شبکه قرار می‌دهد مرتکب جرم است اما هنگامی که داده‌های مشروعی را بارگذاری کرده ولی این داده‌ها بطور غیرمجاز توسط یک پیاده ساز مورد سوء استفاده قرار می‌گیرد، بزه‌دیده است. لذا در این‌گونه موارد ملاک تعیین صلاحیت حسب مورد محل شخص بارگذار یا پیاده‌ساز است، از همین روست که در قوانینی ایالات آرکانزاس و کارولینای شمالی آمده که ارتباطات رایانه‌ای چه از این ایالت نشأت گرفته یا به آن ختم شود (یعنی خواه بارگذاری و خواه پیاده‌سازی شده باشد) مراجع قضایی این ایالت صالح به رسیدگی خواهند بود. لذا می‌توان گفت که اعطاء صلاحیت به دادگاه‌ها می‌تواند تحت تأثیر و محل استقرار کامپیوترهایی باشد که مورد استفاده بارگذار یا پیاده ساز باشد همچنان که در برخی از ایالات آمریکا اینگونه عمل می‌شود (ویدیاساگر، ۲۰۱۰: ۲۹-۲۴).

قائلین به این نظریه معتقدند فعالیت در فضای سایبر از دو حالت خارج نیست یا باید اطلاعات را در آن قرار داد که به این کار بارگذاری می‌گویند یا اینکه اطلاعات را از فضای سایبر پیاده کرد که به آن پیاده سازی می‌گویند. بنابراین، برای تمام اطلاعات و محتویات فضای سایبر می‌توان یک مبدأ و یک مقصد مشخص کرد که در آن مبدأ یعنی بارگذار محتوای موردنظر خود را در یکی‌از اجزای بستر فضای سایبر قرار می‌دهد تا پیاده‌ساز که مقصد آن محتویات بوده است به آنها دسترسی پیدا کند. در خصوص بارگذاری گفته می‌شود که چنانچه بارگذاری متضمن محتویات یا اعمال غیرقانونی و نامشروع باشد چنین بارگذاری غیرقانونی و مجرمانه است و بدیهی است که محل آن، محل ارتکاب جرم است. پیاده‌سازی هم به این صورت آن‌را محل ارتکاب دانسته‌اند که افراد تا اطلاعات غیرقانونی را پیاده نکنند عملاً جرمی اتفاق نیفتاده است. اگرچه فعل اصلی از سوی مرتکب جرم اولیه (بارگذار) بوده است ولی تا زمانی که کاربران اینترنتی آن‌را پیاده نکنند، کامل و در واقع محقق نشده است.

۳-۵- صلاحیت کیفری در توقیف داده‌های تحصیل یافته از جرم سایبری

نظریه محل تحقق اثر یا نتیجه جرم مرتبط‌ترین نظریه جهت توقیف داده‌های تحصیل یافته از جرم است. در این تئوری نتیجه عبارت است از آثار زیانبار و مضر جرم که به دیگران می‌رسد اعم از اینکه ناشی از یک جرم مقید یا مطلق باشد. چرا که برخی جرائم مطلق در فضای سایبر اتفاق می‌افتند ولی چنان اثر خسارت‌باری در محیط سایبر و عالم خارج بر جای می‌گذارد که محل تحقق اثر خود می‌تواند نقش مهمی در فرایند دادرسی آن جرم داشته باشد، اگرچه آن اثر به‌عنوان نتیجه یک جرم مقید تلقی نمی‌گردد (صالحی و حسینی، ۱۳۹۵: ۱۹۱). با این توضیح که استناد به محل تحصیل ادله برای صلاحیت توقیف داده و سایر اقدامات قضایی، مطلق نبوده و دستگاه عدالت کیفری که به دنبال تحقق عدالت و دادرسی منصفانه است، نمی‌تواند فقط به

1 Sender
2 Receiver

محصول کسب دلیل توجه نموده و از شیوه‌های تحصیل آن غافل گردد. بنابراین نقطه آغاز تضمین دادرسی منصفانه، رعایت اصول و قواعد حاکم بر ادله کیفری به ویژه در مقام تحصیل و به کارگیری آنها در فرآیند رسیدگی‌های کیفری است» (تدین و باقری‌نژاد، ۱۳۹۰: ۲۱۵). بر همین اساس، اصل مشروعیت تحصیل دلیل در قوانین مختلف مورد تأیید قرار گرفته است، به طوری که می‌توان آن را مقید و مخصص اصل تحصیل آزادانه دلیل که در قانون مجازات اسلامی ۱۳۹۲ همچون اصل ارزیابی آزادانه دلیل در تمامی جرایم مورد پذیرش قرار گرفته، دانست. در مصادیق متعدد جرایمی که تحصیل‌یافته از جرایم سایبری هستند؛ همیشه نمی‌توان با توسل به یک قاعده نسبت بین توقیف داده و سامانه با مرجع صالح به رسیدگی را مشخص نمود بلکه بسته به محل وقوع جرم سایبر، محل کشف جرم سایبر و همچنین محل توقیف داده باید قائل به تفکیک شده و مطابق با اصول و ضوابط پیش‌بینی شده در قانون و آرای وحدت رویه نسبت بین توقیف داده و مرجع صالح را مشخص نمود.

در نظام دادرسی کیفری ایران؛ ماده ۶۶۵ ق.آ.د.ک ۱۳۹۲ محل کشف و یا گزارش را مرجع صالح برای صلاحیت معرفی کرده است. محل کشف و گزارش در جرایم سایبری همان محلی است که ادله تحصیل یافته از جرم سایبری در آن قرار گرفته است. مطابق ماده ۶۶۵: «چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد». بدین‌ترتیب؛ قانونگذار ایران با عنایت به ویژگی خاص جرائم سایبری، یعنی فرامکانی بودن، بدون اهمیت گذاشتن به مکان وقوع جرم به‌عنوان ضابطه‌ی تعیین مرجع صالح توجه خود را به محل کشف یا گزارش آن معطوف کرده است و دادگاه محلی که داده‌ها تحصیل یافته یا آثار استفاده از داده‌ها کشف یا گزارش شده را صالح جهت رسیدگی و از جمله تفتیش، توقیف و جمع‌آوری این داده‌ها معرفی کرده است. دیوان عالی کشور نیز در رأی وحدت رویه شماره (۷۲۱)[1] دادگاه صالح را دادگاه محل استقرار و حضور مخاطب تماس تلفنی (به تعبیر دیوان عالی کشور «محل حدوث نتیجه») اعلام نموده است.

۶. راهبردهای نوین و تطبیقی در زمینه کارآمدی

به دلیل واقع شدن جرم سایبری در فضای مجازی و غیرواقعی، اثری ملموس و مادی و یا رد پایی از مرتکبین آن، آن‌گونه که در جرایم سنتی متداول است به جای نمی‌ماند و آثار به‌جای مانده به راحتی قابلیت امحاء و پاک سازی را دارند. از این‌رو رقم سیاه بزهکاری در جرایم سایبری بسیار زیادتر از جرایم فیزیکی و سنتی است. همچنین تحصیل و کشف ادله و به دنبال آن قابلیت استنادی ادله بدست‌آمده با توجه به احتمال نقض حریم خصوصی و ... بسیار پائین است و همواره با اشکالاتی همچون تحصیل غیرقانونی مواجه هستند. بنابراین بحث توقیف و صلاحیت از جمله مسائل بسیار مهمی هستند که ضرورت دارد راهبردهای نوینی در ارتباط با آنها اتخاذ گردد چرا که قواعد سنتی جهت توقیف داده و احراز صلاحیت نمی‌تواند کاربردی باشد.

بررسی وضعیت تقنینی در خصوص تعیین مرجع صالح برای توقیف داده مشخص می‌نماید که نظام صلاحیتی تعریف شده برای تعیین مرجع صالح برای رسیدگی و تحقیقات مقدماتی با توجه به ایراداتی که دارد، کارآمدی لازم برای تعیین مرجع صالح را ندارد. مبتنی بودن قواعد تعیین صلاحیت بر عامل فیزیکی بدون توجه به ماهیت دیجیتالی فضای مجای، تاکید بر معیارهای سنتی در تعیین محل وقوع جرم، عدم توجه به بزه‌دیده در اعلام محل نتیجه به‌عنوان مرجع صالح از جمله مهمترین ایراداتی هستند که نظام قانون‌گذاری ایران با آنها مواجه است. به این موارد باید کثرت پرونده‌ها که نظام قضایی ایران با آن مواجه می‌باشد را نیز

---

۱ رای وحدت رویه شماره ۷۲۱ مورخ ۱۳۹۰/۴/۲۱: «وقوع بزه مزاحمت برای اشخاص به وسیله تلفن یا دستگاه‌های مخابراتی دیگر ـ موضوع ماده ۶۴۱ قانون مجازات اسلامی ـ منوط به آن است که نتیجه آن که مقصود مرتکب است محقق گردد، بنابراین در مواردی که اجرای مزاحمت از یک حوزه قضایی شروع و نتیجه آن در حوزه قضایی دیگر حاصل شود، محل حدوث نتیجه مزبور، محل وقوع جرم محسوب و مناط صلاحیت دادگاه رسیدگی‌کننده نیز همین امر خواهد بود. بر این اساس رأی شماره ۱۰۴۵ـ۱۳۸۵/۷/۲۰ شعبه بیست و هفتم دیوان عالی کشور که با این نظر مطابقت دارد به اکثریت آراء صحیح و منطبق با موازین قانون تشخیص می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی کشور و دادگاه‌های سراسر کشور لازم‌الاتباع است».

اضافه نمود. با این توضیح که، در مواردی به دلایل یاد شده ممکن است مقامات پلیسی و قضایی رغبتی برای تشکیل پرونده و رسیدگی نداشته و دنبال توجیهی برای عدم تشکیل پرونده باشند. همانگونه که بیان شد، این توجیه در جرایم سایبری با توجه به ابهام در تعیین صلاحیت فراهم هست. به این موارد باید مشکلات پیرامون کثرت داده‌ها، نحوه شناسایی و ابهام در نحوه توقیف و نگهداری آنها را نیز افزود. با این توضیح که در توقیف داده‌ها ممکن است مکان تحت تفتیش و توقیف دارای سیستم رایانه‌ای باشد که از آن فقط جهت تامین دسترسی به داده‌های ذخیره شده در یک سیستم متفاوت مستقر در مکانی دور دست استفاده شود. در چنین شرایطی لازم است ماموران تفتیش حکم تفتیشی در اختیار داشته باشند که به حد کافی موسع باشد و سیستم رایانه‌ای دور دست را نیز در برگیرد. در این مورد قانون جرایم رایانه‌ای در ماده ۴۳ قانون جرایم رایانه‌ای (ماده ۶۷۸ ق.آ.د.ک ۱۳۹۲)[1] به ضابطان این اجازه را داده است که در صورت ضرورت در برخورد با سیستم‌های رایانه‌ای که در قرار تفتیش و بازرسی ذکر نشده است حیطه تحقیق خود را گسترش دهند مشروط بر اینکه به دستور مقام قضایی باشد (موذن‌زادگان و شایگان، ۱۳۸۸: ۹۳). البته مشکلات سر راه توقیف داده‌ها و ابهام در صلاحیت برای توقیف، خاص کشور ما نبوده و بیشتر سیستم‌های حقوقی کشورهای دنیا در قوانین مربوط به خود با نقصان در این رابطه مواجه می‌باشند. از همین‌رو راهبردهای بین‌المللی در این خصوص اتخاذ گردیده است. از جمله این راهبردها؛ توصیه‌نامه شورای اروپا در خصوص مشکلات آئین دادرسی مصوب سپتامبر ۱۹۹۵ در خصوص تفتیش و توقیف، است که می‌تواند راهنما و تا حدودی رافع برخی از مشکلات در توقیف داده‌ها باشد.[2]

در ابعاد بین‌المللی نیز راهبردهای متعددی جهت حل تعارضات پیرامون صلاحیت بیان شده است که از مهمترین آنها ایجاد دادگاه بین‌المللی سایبری است. گفته شده که بر مبنای نظریه دادگاه سایبری؛ بدلیل اینکه مرجع صالح به تمامی جرایم ارتکابی در فضای یاد شده رسیدگی می‌نماید و نظام واحد قضایی حکفرماست لذا تعارض صلاحیت منتفی است و این به معنی عدم امکان ایجاد تعارض صلاحیتی در چنین دادگاهی می‌باشد همچنین ایجاد یک دادگاه دیجیتالی با سازکارهای متفاوت از دیگر پیشنهادهایی است که در این حوزه مطرح گردیده است. اینها دادگاه دیجیتالی را به این‌گونه تعریف کرده‌اند: «دادگاه دیجیتالی که ویژه‌ی جرائم دیجیتالی می‌باشد بر اساس اختصاص محاکم به‌صورت ویژه از قبیل خانواده، جنایات و امور حقوقی، به امور جرائم دیجیتالی می‌پردازد که این دادگاه مستلزم امکانات بشری و جغرافیایی می‌باشد» (رضوان، ۲۰۰۶: ۱۳). این دادگاه به جرائم رایانه‌ای خواه جرم به‌وسیله رایانه، خواه علیه آن ارتکاب شود، همچنین به جرائم شبکه‌ای و اینترنتی ازجمله شبکه‌ی جهانی اینترنت و جرائم تلفن‌های سیار یا موبایل رسیدگی می‌کند.

نتیجه‌گیری

نتایج بدست آمده نشان می‌دهد که با وجود مزایای بی‌شماری‌که فناوری‌های نوین اطلاعاتی و ارتباطی دارد؛ بکارگیری داده و سامانه نه‌تنها راه‌های نوینی برای ارتکاب جرم و سوءاستفاده از فضای سایبر به روی مجرمین گشوده بلکه مشکلات جدی‌ای را

---

[1] ماده ۶۷۸: چنانچه در حین اجرای دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارند ضروری باشد، ضابطان با دستور مقام قضایی دامنه تفتیش و توقیف را به‌سامانه‌های دیگر گسترش می‌دهند و داده‌های مورد نظر را تفتیش یا توقیف می‌کنند.

[2] از جمله این راهبردهای می‌توان به موارد ذیل اشاره کرد:

۱. تمایز حقوقی بین تفتیش سیستم‌های رایانه‌ای و توقیف داده‌های ذخیره شده در آنها و شنود الکترونیکی داده در جریان انتقال، باید به‌روشنی مطرح و عمل شود.

۲. قوانین آئین دادرسی کیفری باید به مقامات تحقیق اجازه دهند که تحت شرایط مشابه مانند آنچه که طبق اختیارات سنتی تفتیش و توقیف مطرح شده است، سیستم‌های رایانه‌ای را تفتیش و داده‌ها را توقیف کنند.

۳. در طی اجرای یک تفتیش، مقامات تحقیق باید اختیار داشته باشند پیرو تضمین‌های مقتضی، تفتیش را به سایر سیستم‌های رایانه‌ای موجود در محدوده‌ی صلاحیت قضایی‌شان که به‌وسیله‌ی یک شبکه بهم متصل نشده‌اند، تعمیم دهند و داده‌های موجود در آنها را توقیف کنند..

۴. در صورتی‌که داده‌ها به‌طور خودکار پردازش شود و از لحاظ عملکرد با یک سند سنتی برابر باشد، مقررات موجود در آئین دادرسی کیفری مربوط به تفتیش و توقیف اسناد باید به‌طور یکسان برای آنها اجرا بشود.

نیز در زمینه آئین ر سیدگی کیفری و بکارگیری از مدارک و دلایل الکترونیکی نا شی آنها در فرایند کیفری بوجود آورده ا ست که توقیف داده از جمله مهمترین این زمینه‌هاست. در خصوص دادگاه صالح برای توقیف داده؛ نظریات متعددی با توجه به رویه‌های بین‌المللی، قوانین سایر کشورها و قوانین و رویه داخلی ارائه شده است که در کل مشتمل بر سه دسته از نظریات هستند که با استناد به هر یک، مرجع قضایی صالح برای توقیف مشخص می شود. با وجود ابهام یاد شده؛ می‌توان نتیجه گرفت که بسته به جرم ارتکابی و نقش داده در آن، بین توقیف داده و صلاحیت سایبری تنا سب برقرار ا ست که بسته به هر یک از و ضعیت‌های توصیف شده و نقش داده در آن؛ صلاحیت مرجع قضایی برای توقیف داده متفاوتی خواهد بود. بنابراین برای نسبت‌سنجی بین توقیف داده و صلاحیت برای توقیف داده، باید مشخص گردد که داده به‌عنوان و سیله ارتکاب جرم یا مو ضوع جرم یا تحصیل یافته از جرم می‌با شد. نتیجه اینکه؛ برای نسبت سنجی بین توقیف داده و صلاحیت کیفری باید نقش و موقعیت داده در ارتکاب جرم مشخص شده به صورت خاص و به تفکیک توقیف داده با صلاحیت در هر یک از موقعیت‌های سه‌گانه یاد شده ارتباط‌سنجی گردد. یکی از چالش‌های پیرامون صلاحیت محاکم در توقیف داده‌ها، مربوط به مواردی است که داده به‌عنوان وسیله ارتکاب جرم مورد استفاده قرار گرفته است. در نظام حقوقی ایران، صلاحیت در مواردی که داده به‌عنوان وسیله ارتکاب جرم بوده مشخص نگردیده ا ست، اما در این خصوص رای وحدت رویه شماره ۷۲۹ می‌توان راه‌گشا بوده و در تبیین نسبت توقیف داده با صلاحیت کیفری موثر واقع شود. با توجه به رای وحدت رویه، در تعیین صلاحیت محلی، در مواردی که داده به‌عنوان وسیله ارتکاب جرم می‌باشد، اصل بر صلاحیت محل وقوع جرم است. که با توجه به رای یاد شده، محل وقوع جرم، محلی است که نتیجه ارتکاب جرم حا صل شده ا ست. زمانی که داده مو ضوع جرم قرار می‌گیرد، و ضعیت توقیف داده متفاوت از حالت‌های سنتی ا ست که مو ضوع جرم مثلاً ا نسان یا اموال ه ستند. مثلاً صحنه جرم در جرایم الکترونیکی با جرایم دنیای واقعی متفاوت است. با عنایت به بررسی‌های انجام یافته می‌توان نتیجه گرفت که در تعیین صلاحیت در توقیف داده‌هایی که در آنها داده موضوع جرم بوده، بحث صحنه جرم و پهنه آن ملاک می‌باشد. در مورد وضعیت داده در حالتی که تحصیل‌یافته از جرایم سایبری می‌باشد نیز، ابهام در صلاحیت از جمله برای توقیف داده‌ها وجود دارد. ویژگی‌های ادله نا شی از فن‌آوری اطلاعات و مشکلات نا شی از آن سبب شده است که داده و سامانه تحصیل یافته از جرم موانعی برابر استنادپذیری ادله الکترونیک بوجود آید. از همین‌روست که گفته می‌شود باید تمام ادله دیجیتالی جمع‌آوری شده به درستی مستند، برچسب، علامت گذاری و عکس برداری شده باشند، همچنین برای تسهیل مونتاژ مجدد سیستم در آینده، اتصالات و دستگاه‌های متصل را به درستی برچسب گذاری شوند. داده و سامانه تحصیل یافته از جرم دارای مصادیق مختلفی می‌باشند و برای استنادپذیری هر یک باید تحصیل آنها با مشروعیت همراه باشد. در این خصوص همانگونه که بیان شد؛ نمی‌توان با توسل به یک قاعده نسبت بین توقیف داده و سامانه با مرجع صالح به رسیدگی را مشخص نمود بلکه بسته به محل وقوع جرم سایبر، محل کشف جرم سایبر و همچنین محل توقیف داده باید قائل به تفکیک شده و مطابق با اصول و ضوابط پیش‌بینی شده نسبت بین توقیف داده و مرجع صالح را مشخص نمود. بررسی وضعیت تقنینی در خصوص تعیین مرجع صالح برای توقیف داده مشخص می‌نماید که نظام صلاحیتی تعریف شده برای تعیین مرجع صالح برای رسیدگی و تحقیقات مقدماتی با توجه به ایراداتی که دارد، کارآمدی لازم برای تعیین مرجع صالح را ندارد. در کل می‌توان؛ مبتنی بودن قواعد تعیین صلاحیت محاکم در رسیدگی به جرایم سایبری بر عامل فیزیکی بدون توجه به ماهیت دیجیتالی فضای مجازی، تاکید بر معیارهای سنتی در تعیین محل وقوع جرم، محل کشف و محل نتیجه، عدم توجه به بزه‌دیده در اعلام محل نتیجه به‌عنوان مرجع صالح از جمله مهمترین ایرادات نظام قانون‌گذاری ایران در بحث صلاحیت محاکم بیان کرد. نظام قضایی نیز در این خصوص با توجه به برداشت‌های متفاوت و کثرت پرونده‌ها با تشتت روبرو است که نشئت گرفته از وضعیت مبهمی است که نظام قانون‌گذاری در تعیین مرجع صالح برای انجام تحقیقات مقدماتی و رسیدگی به جرایم سایبری بوجود آورده است. با عنایت به موارد یاد شده، پیشنهاد مشخص تحقیق این است که با در نظر گرفتن ماهیت دیجیتالی و متفاوت جرایم سایبری، قانون‌گذار باید از قواعد سنتی و فیزیکی کنونی حاکم بر تعیین صلاحیت فاصله گرفته و برای تعیین مرجع صالح، قواعد نوین و سازگار با ماهیت این دسته از جرایم را ملاک قرار دهد.

منابع

آشوری، محمد (۱۳۹۸). آئین دادرسی کیفری. جلد ۲. چاپ بیستم. تهران: انتشارات سمت.

تدین، عباس و باقری‌نژاد، زینب (۱۳۹۰). تضمین دادرسی منصفانه در پرتو اصل مشروعیت تحصیل ادله کیفری. مجله تحقیقات حقوقی، ۲ (۵۳)، ۲۱۵.

حسینی، پرویز و ظریف‌منش، حسین (۱۳۹۲). مطالعه تطبیقی ساختار دفاع سایبری کشورها. فصلنامه پژوهش‌های حفاظتی امنیتی دانشگاه جامع امام حسین (علیه السلام). ۲ (۵)، ۲۴.

حیدری، حسن و میلانی، علیرضا (۱۴۰۱). بررسی تطبیقی جایگاه صلاحیت سرزمینی در رسیدگی به جرایم سایبری با تکیه بر نظام کیفری ایران، فصلنامه علمی حقوق و مطالعات نوین، ۳ (۴)(۹)، ۵ -۴.

زندی، محمدرضا (۱۳۹۳). تحقیقات مقدماتی در جرایم سایبری. چاپ اول از ویرایش جدید. تهران: انتشارات جنگل.

روشن‌فر، عزیز (۱۳۹۲). موانع و مقتضیات تعیین قلمرو مکانی قوانین کیفری در حوزه جرایم سایبری. رساله دکتری حقوق جزا و جرم‌شناسی، دانشکده حقوق پردیس فارابی دانشگاه تهران.

روزگار، حسین (۱۳۹۶). اجرای عدالت کیفری در جرایم سایبری؛ چالش‌ها و راهکارها. رساله دکتری دانشگاه شهید بهشتی.

رضوان، محمد (۲۰۰۶). هلال، المحکمه الرقمیه – مفهوم‌ها و مقومات‌ها. الطبعه الاولی. القاهره. دار العلم للنشر و التوزیع.

صالحی، کفایت و حسینی، سید کرامت (۱۳۹۵). بررسی صلاحیت کیفری در فضای سایبر در چهارچوب مبانی حقوق کیفری. علوم انسانی اسلامی، ۲ (۱۱)، ۱۱۹.

طهماسبی، جواد و شاهمرادی، خیراله (۱۳۹۷). چالش‌ها و خلأهای موجود در فرایند رسیدگی به‌جرایم سایبری. مجله حقوقی دادگستری، ۸۲ (۱۱۴)، ۱۴۵.

علیزاده، اکبر، نظری، سمیه و طالبی، علی‌مراد (۱۴۰۱). محشای آئین دادرسی کیفری با اخرین اصلاحات و الحاقات. تهران: انتشارات فرقلم.

عمید، حسن (۱۳۷۵). فرهنگ عمید. جلد دوم. تهران: موسسه انتشارات امیرکبیر.

فروغی، فضل‌الله و البوعلی، امیر (۱۳۹۱). صلاحیت کیفری مراجع قضایی در فضای سایبر. مجله تحقیقات حقوقی دانشگاه شهید بهشتی، ۱۲ (۴)، ۲۱۱.

1. Ashcroft, John. (2010). Electronic crime scene investigation for first responders,
2. European Union Council Framework Decision on attacks against information systems (EU Decision on Attacks against Information Systems), 2005/222/JHA, 24 February 2005.
3. Brenner, Susan. (2010). Criminal Threats from Cyber Space, Green Wood Publishing Group,
4. Maier, Bernhard. "How Has the Law Attempted to Tackle the Borderless Nature of the Internet," International Journal of Law and Information Technology 18.
5. Park, J, and Noe, S. (2016). Control of International Cyber Crime, Journal of the Korea Society of Computer and Information, Vol. 21.
6. Vidyasagar, Adithya S V. (2010). Jurisdictional Issues in Cyber Space. Acta Iuridica Olomucensis 5.
7. Wang, Faye Fangfe. (2010). Internet Jurisdiction and Choice of Law: Legal Practices in EU, US and China. New York: Cambridge University Press.