Culminatin of Law Quarterly
13nd Year, No.2, Summer 2022
http://dx.doi.org/10.22034/thdad.2021.535936.1904

The principle of legality On Seizing the Computer Data and System in the criminal process; Effects and Guarantees

Sadegh Tabrizi[1], Mohammadreza Elahimanesh[*2], Hassan Alipour[3], Javad Tahmasebi[4], Mahdi Fazli[5]

1. PhD student in criminal law and criminology, Faculty of Law and Humanities, North Tehran Branch, Islamic Azad University, Tehran, Iran.

2. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Human Sciences, North Tehran Branch, Islamic Azad University, Tehran, Iran.

3. Assistant Professor, Department of Criminal Law and Criminology, University of Tehran (Farabi Campus), Qom, Iran

4. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Human Sciences, North Tehran Branch, Islamic Azad University, Tehran, Iran.

5. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law and Human Sciences, North Tehran Branch, Islamic Azad University, Tehran, Iran.

Article Type:
Original Research

Pages: 109-140

Received: 2021 August 13

Revised: 2021 August 22

Accepted: 2021 November 22

Abstract

The principle of legality On Seizing the Computer Data and System means to comply with legal rquirements since the issuance of the judicial order to stop the seizure. the effects of the principle of legality On Seizing the Computer Data and System are that: justice-oriented, according to which the Seizing the Computer Data can lead to the discovery of a crime or identification of the accused or evidence of a crime, judgment- oriented, based on which just seizure is based on a judicial authorization, and officers, even in obvious crimes, do not have the authority to do so. Consent oriented that the occupier has given permission the Computer Data and System to seize the Data and System and her presence at the time of seizure is a condition.The present article uses the method of description and analysis to explain the principle of legality On Seizing the Computer Data and System and by examining the challenges of this principle, especially from the relevance of 671 to 682 to each other and from the point of view of the condition of individual or sharing Seizing On the System. It has been concluded that the principle of legality On Seizing the Computer Data and System, although in the Code of Criminal Procedure, this is a step forward,but the judicial procedure is generally measured in terms ofconfiscation of property and objects, while the foundation of theelectronic environment and cyber space is based on data confidentiality and privacy.The purpose of this paper isto emphasize the difference between thedata and thesystem with theseizure ofphysical property in order to balance the balance between justice and the confidentiality of the data and the system.

Keywords: Principle of legality, seizure the Computer Data and System, legal effects of seizure, legal seizure guarantees.

* Corresponding Author: M.elahimanesh92@yahoo.com

فصلنامه تعالی حقوق
سال سیزدهم، شماره ۲، تابستان ۱۴۰۱
http://dx.doi.org/10.22034/thdad.2021.535936.1904

اصل قانون‌مندی توقیف داده و سامانه در فرآیند کیفری؛ جلوه‌ها و تضمین‌ها

صادق تبریزی[۱]، محمدرضا الهی‌منش[۲*]، حسن عالی‌پور[۳]، جواد طهماسبی[۴]، مهدی فضلی[۵]

۱. دانشجوی دکتری حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی، تهران شمال؛ ایران.

۲. استادیار گروه حقوق جزا و جرم شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

۳. استادیار گروه حقوق جزا و جرم شناسی، دانشگاه تهران (پردیس فارابی)، قم، ایران

۴. استادیار گروه حقوق جزا و جرم شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

۵. استادیار گروه حقوق جزا و جرم شناسی، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران

نوع مقاله: علمی پژوهشی

صفحات: ۱۰۹-۱۴۰

تاریخ دریافت: ۱۴۰۰/۰۵/۲۲

تاریخ بازنگری: ۱۴۰۰/۰۵/۳۱

تاریخ پذیرش: ۱۴۰۰/۰۹/۰۱

چکیده

اصل قانونمندی توقیف داده و سامانه به معنای رعایت الزامات قانونی از زمان صدور دستور قضایی مبنی بر توقیف تا زمان رفع توقیف از آنها است. جلوه های اصل قانونمندی توقیف داده‌ها و سامانه عبارتند از؛ عدالت‌محوری که بر اساس آن توقیف داده بتواند به ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم منتهی شود، قضاوت محوری که بر پایه آن، توقیف صرفاً مبتنی بر مجوز قضایی است و ضابطان به جز در جرایم مشهود، اختیار چنین اقدامی را ندارند، رضایت محوری که اذن متصرف داده یا سامانه در توقیف داده و سامانه و نیز حضور وی در زمان توقیف شرط است و پیامد محوری که توقیف داده باید با لحاظ پیامدهای الکترونیکی یا فیزیکی سنجیده و اعمال شود. نوشتار حاضر با روش توصیف و تحلیل به تبیین اصل قانونمندی توقیف داده و سامانه پرداخته است و با بررسی چالش های این اصل به ویژه از جهت ارتباط مواد ۶۷۱ تا ۶۸۲ قانون آیین دادرسی کیفری ۱۳۹۲با همدیگر و نیز از منظر شرط انفراد یا اشتراک شرایط توقیف سامانه در ماده ۶۷۶ قانون اخیر به این نتیجه رسیده است که اصل قانونمندی توقیف داده و سامانه گرچه در قانون آیین دادرسی کیفری، گامی رو به جلو است ولی از جهت رویه قضایی عموماً با شرایط توقیف اموال و اشیا سنجیده می شود در حالی که چون اساس محیط الکترونیکی و فضای سایبر بر محرمانگی داده و سامانه است، راهکار این نوشتار تاکید بر تفاوت گذاری میان توقیف داده و سامانه با توقیف اموال فیزیکی در راستای ایجاد توازن میان عدالت قضایی و محرمانگی داده و سامانه است.

واژگان کلیدی: اصل قانونمندی، توقیف داده و سامانه، جلوه های قانونی توقیف، تضمینات توقیف قانونی

* نویسنده مسئول: M.elahimanesh92@yahoo.com

درآمد

یکـــی از مهمترین پیوندهای منفی که برای داده و ســـامانه می‌توان ذکر کرد، اســـتفاده مجرمانه از آنها است. داده و ســـامانه می‌توانند هم به عنوان موضوع جرم در جرایمی همچون ســـرقت، کلاهبرداری، جعل و ... بکار گرفته شـــوند و هم می‌توانند به عنوان وســـیله ارتکاب واقع شـــوند. در مورد موضوع جرم باید بیان داشت که هر جرمی الزامـــا باید دارای موضوع باشـــد و جرم بدون موضوع نمی‌تواند وجود خارجی داشـــته باشد. مثلاً در قتل خود انســـان موضوع جرم قرار می‌گیرد و در توهین و افترا، حیثیت و آبـــروی وی موضوع جرم قرار می‌گیرد. در جرم ســـرقت و کلاهبرداری، اموال موضوع جرم می‌باشـــند. در برخی از جرایم رایانه‌ای نیز موضوع جرم خود داده‌ها و ســـامانه‌ها هستند مثلا در سرقت داده یا سامانه، ابزارهای اخیر موضوع جرم هستند در جعل داده و ســـامانه و بسیاری از جرایم دیگر نیز وضعیت به همین صورت می‌باشد یعنی جرم بر روی داده و ســـامانه اتفاق می‌افتد. زمانی که داده و سامانه موضوع جرم قرار می‌گیرد، وضعیت تحصیل، کشف، حفظ صحنه جرم، توقیف، نگهداری و استنادپذیری متفاوت از حالت‌های سنتی است که موضوع جرم مثلاً انسان یا اموال هستند. در مواردی که داده و ســـامانه به عنوان وســـیله ارتکاب جرایم رایانه‌ای نیز قرار می گیرد وضعیت به همین منوال است و با سایر وسیله و عناصر ارتکاب جرایم سنتی تمایز زیادی دارد.

از جمله تفاوت‌های بین این دو می‌توان به فرایند توقیف داده و شـــرایط و اصول حاکم بر آنها به عنوان ادله اثبات جرم اشاره کرد. برخلاف ادله سنتی که توقیف و مداخله در آنها دارای تعریف شده بوده و در قوانین کشورها، مقررات مشخصی برای آنها پیش‌بینی شـــده برای توقیف داده و سامانه، ابهامات و مشـــکلات تقنینی، قضایی و اجرایی متعددی وجود دارد. با توجه به همین مشکلات موجود بر سر راه توقیف ادله الکترونیکی که بیشتر کشـــورهای دنیا از جمله فرانسه و بلژیک در قوانین مربوط به خود با نقصان در این رابطه مواجه می‌باشـــند، توصیه‌نامه شـــورای اروپا در خصوص مشـــکلات آیین دادرسی مصوب ســـپتامبر[1] ۱۹۹۵ به عنوان نقشه راه ، تا حدودی توانست در رفع مشکلات یاد شده موثر باشد. از جمله مهمترین مواردی که به عنوان راهنما در این توصیه نامه آمده‌اند عبارتند از:

1. Council of Europe Recommendation on the Rules of Procedure, adopted in September 1995

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

۲. قوانین آیین 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 محدوده آن حوزه که بوسیله یک شبکه به هم متصل نشده‌اند، تعمیم دهند و داده‌های موجود در آنها را توقیف کنند.

۴. در صورتی که داده‌ها به طور خودکار پردازش شود و از لحاظ عملکرد با یک سند سنتی برابر باشد، مقررات موجود در آیین دادرسی کیفری مربوط به تفتیش و توقیف اسناد باید بطور یکسان برای آنها اجرا شود» (دزیانی، ۱۳۸۴: ۳۰).

در نظام حقوقی ایران نیز؛ با تصویب قانون مجازات جرایم رایانه‌ای و الحاق آن به تعزیرات و مجازات‌های بازدارنده مصوب ۱۳۷۵ و همچنین تصویب قانون آیین دادرسی جرایم نیروهای مسلح ، دادرسی الکترونیکی و آیین دادرسی جرایم رایانه ای و الحاق آن به قانون آیین دادرسی کیفری مصوب ۱۳۹۲؛ ساز و کارهای تقنینی برای کشف، جمع آوری و استناد به ادله الکترونیکی و توقیف داده و سامانه پیش بینی شده است. منظور از فرایند توقیف داده و سامانه، فرایندهای تعریف شده در مقررات شکلی هستند که تا قبل از تصویب قانون آیین دادرسی کیفری مصوب ۱۳۹۲ تنها در بخش دوم قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ذکر شده بودند که به همین دلیل مقنن در همین بخش و در راستای پر کردن خلأ های 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 قضایی، تحقیقات مقدماتی و رسیدگی به آنها می‌طلبید، ارجاع قانونگذار به مواد قانون آیین دادرسی کیفری در راستای پر کردن خلأ ناشی از مواد شکلی قانون جرایم رایانه‌ای نیز به تنهایی نمی‌توانست راهگشای تمامی مسایل مربوط به فرایندهای دادرسی در جرایم رایانه‌ای باشد. بعد از تصویب قانون آیین دادرسی کیفری مصوب ۱۳۹۲ فرایند دادرسی جرایم

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

مساله اصلی نوشتار حاضر، ابعاد و جلوه‌های اصل قانونمندی توقیف داده و سامانه است. از یک سو، توقیف داده و سامانه از جهت ویژگی‌های داده و سامانه که امروز در همه شؤون جامعه و در اختیار عموم افراد قرار دارند، مرز آشکاری با توقیف اموال فیزیکی و دارایی‌های سنتی دارند و از همین منظر، اصل قانونمندی توقیف داده و سامانه به اصل قضایی بودن آن تقلیل می یابد. به عبارت دیگر، این مقام قضایی است که در نهایت تشخیص می‌دهد چه داده و سامانه‌ای در راستای کشف جرم یا ادله وقوع بزه توقیف شود. دلیل این امر، تمرکز قانون بر صلاحدید قضایی هم از جهت تشخیص ارتباط توقیف داده و سامانه با ظن وقوع جرم و هم از جهت اختیار در صدور مجوز قضایی است. این میزان از اختیارات قضایی می تواند اصل قانونمندی را تحت الشعاع قرار دهد. ولی از سوی دیگر، اصل قانونمندی توقیف داده و سامانه به واقع فراتر از تشخیص قضایی و اعمال صلاحدید قاضی در توقیف است و عرصه‌ای برای توازن میان اختیار قضایی، رضایت متصرف داده و سامانه و نیز اقتضای ماهیت داده و سامانه است که همه اینها باید در کنار هم در نظر گرفته شوند تا توقیف داده و سامانه چهره قانونی به خود بگیرد. در این رویکرد، اختیار قضایی باید با دیگر جلوه های مقرر در قانون هماهنگ باشد. در این نوشتار البته بر رویکرد دومی تاکید می شود ولی در راستای انتخاب رویکرد دوم باید ابتدا مفهوم اصل قانونمندی و سپس جلوه های آن بررسی شود و در نهایت از تضمین های این اصل نیز سخن شود:

۱. مفهوم اصل قانونمندی توقیف داده و سامانه

اصل قانون‌مندی توقیف داده و سامانه از اصل قانونی بودن در حقوق کیفری الهام گرفته است. بدلیل اهمیت این اصل در حقوق کیفری، در قانون اساسی نیز به این اصل و لزوم رعایت آن تأکید شده است. اصل یکصد و شصت و ششم اشعار می‌دارد: «احکام دادگاه‌ها باید مستدل و مستند به مواد قانون و اصولی باشد که براساس آن حکم صادر شده است». برخی از اصول این قانون، ارتباط نزدیکی با قانون‌مند بودن شناسایی و تحصیل دلایل دارد؛ به عنوان نمونه در قانون اساسی برای اجرای عدالت در زمینه تحصیل دلیل بر استقلال قضات تأکید کرده است تا در هنگام جمع‌آوری دلایل هیچ مقامی نتواند بر او نفوذ نماید. همچنین در اصل سی و هشتم قانون اساسی آمده است: «هرگونه شکنجه برای گرفتن اقرار و یا کسب اطلاع ممنوع است». در قوانین جزایی ایران نیز به اصل قانونی بودن تاکید شده است. در قانون مجازات اسلامی مصوب ۱۳۹۲ فصل مستقلی به اصل قانونی بودن جرایم و مجازات‌ها اختصاص یافته است. ماده ۱۳ این قانون مقرر می‌دارد: «حکم به مجازات یا اقدام تامینی و تربیتی و اجرای آنها حسب مورد نباید از میزان و کیفیتی که در قانون یا در حکم دادگاه مشخص شده است، تجاوز کند و هرگونه صدمه و خسارتی که از این جهت حاصل شود، در صورتی که از روی عمد یا تقصیر باشد، حسب مورد موجب مسئولیت کیفری و مدنی است و در غیر این صورت، خسارت بیت‌المال جبران می‌شود». این اصل، همچنین در ماده ۲ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ به این صورت پیش‌بینی شده است: «آیین دادرسی کیفری باید مستند به قانون باشد. حقوق طرفین دعوا را تضمین کند و قواعد آن نسبت به اشخاصی که در شرایط مساوی به سبب ارتکاب جرم تحت تعقیب قرار می‌گیرند، به طور یکسانی اعمال شود».

در مورد اصل قانون‌مندی در توقیف داده و سامانه نیز می‌توان گفت ایده حاکمیت قانون رکن رکین حقوق جزای ماهوی در پهنه تمامی قوانین و مقررات است. همچنین این اصل در حقوق جزای شکلی نیز از مهم ترین اصول حاکم بر دادرسی‌های عادلانه بشمار می‌آید که بر اساس آن دادرسی و ترتیبات آن از جمله تحصیل و توقیف ادله باید مبنای قانونی داشته باشد. بنابراین؛ این ایده افزون بر قوانین ماهوی در قوانین شکلی نیز به عنوان اصل اولیه محسوب شده و به معنای قانونی بودن تمامی تصمیمات

و اختیارات مقامات قضایی و ضابطین دادگستری در فرایند دادرسی از جمله در توقیف داده و سامانه است. «اولین و مهمترین کارکرد اصول‌گرایی کیفری، قاعده‌مند ساختن حقوق کیفری به‌طورکلی و آیین دادرسی به‌طور خاص است؛ قاعده‌مندسازی خصیصه ذاتی اصول‌گرایی کیفری محسوب می‌شود» (پاک‌نیت، ۱۳۹۶: ۴۲). از این‌رو است که قانون‌مداری را یکی از منزلت‌های ثابت حقوقی دانسته‌اند که بر پهنه رشته‌های مختلف حقوق سایه افکنده است. اصولا حقوق کیفری بدون پشتوانه و رعایت این اصل بی‌وجه است. به دیگر سخن تجلی‌گاه دامنه حقوق جنایی، اصل مترقی قانونمندی است؛ از دیگر سو، استواری و بنیان حقوق بشر وامدار اصل حکومت قانون بوده و عدم رعایت جایگاه بنیادین قانونمداری در دامنه حقوق کیفری به‌منزله نقض حقوق بشر است. این اصل یک اصل تاریخی و عقلی است تا آنجا که می‌توان ادعا کرد از مستقلات عقلیه محسوب می‌شود و حتی با وجود دلیل نقلی همواره در طول تاریخ خِرَدِ بشری به آن اذعان داشته است و سستی در رعایت آن آفتی است که نظام حقوقی و سیاسی را دچار تهدید می‌کند. منبع و ملاک اصلی قانون‌مداری، اصولی عقلانی و اصل لزوم رعایت عدالت است (حبیب زاده و توحیدی فرد، ۱۳۸۸: ۱۰). «اصل قانونی بودن را می‌توان اصلی قاعده‌ساز خارج از فرایند دادرسی دانست که قلمرو خود را به فرایند دادرسی گسترش داده است. در یک دولت قانون‌مدار، همه‌چیز تابع اصول حقوقی و قانونی است و به‌طورکلی می‌توان از حاکمیت قانون سخن به میان آورد. تأکید دادرسی قانونی در امور کیفری به این خاطر است که قضات، اختیار تام در چگونگی محاکمه نداشته باشند، چراکه در این صورت به‌طرف یکی از اصحاب دعوی سوق داده می‌شوند» (میلانی، ۱۳۸۶: ۱۲۶). بر همین اساس در توقیف داده و سامانه نیز به عنوان جزئی از فرایند دادرسی، اشخاصی که به عنوان مجریان قانون یا ضابطین دادگستری اقدام به توقیف داده یا سامانه می‌کنند باید به اصل قانون‌مندی توجه داشته باشند و بدانند که آنان مجری قانون هستند و نه واضع آن. اصل قانونی بودن، علاوه بر اینکه جزء اصول مسلم در توقیف انواع مختلف ادله از جمله ادله الکترونیکی است، یکی از مهم‌ترین اصول در قوانین کشورهاست و در قوانین جزایی ماهوی و شکلی کشورها بر آن تأکید شده است.

در ارتباط با قانون‌مندی در کسب ادله از جمله شناسایی، توقیف و ضبط آن

می‌تـــوان گفت که؛ «در نظام حقوقی ایران، هر چند در دعاوی کیفری بر خلاف دعاوی حقوقی، ادله اثبات دعوا از سوی قانونگذار احصاء نشده و اصل بر تحصیل آزادانه دلایل اســـت، اما این‌گونه نیســـت که هر دلیلی قابل ارائه در محاکم و قابل اســـتناد در اتخاذ تصمیمات قضائی باشد، بلکه محدودیت‌هایی نیز متوجه مقامات قضایی و ضابطین است که یکی از مهم‌ترین آنها این است که تنها دلیل قانونی که از راه‌های قانونی و با رعایت مقررات واجب‌الرعایه تحصیل شده، قابل ارائه به دادگاه است» (حبیب‌زاده، ۱۳۹۲: ۴۷). با این اوصاف باید توقیف داده و سامانه و به طور کلی هر ادله دیگری را که با تمسک به اقدامات و رفتارهای مخالف با اوامر و نواهی قانونی تحصیل شده است از لحاظ حقوقی، غیر قابل قبول و استناد در محاکم و دادسراها دانست. بنابراین هر چند دلیل در حقوق کیفری آزاد است ولی پذیرش چنین ادعایی به صورت مطلق، صحیح نیست. همه چیز باید در پرتو حکومت قانون تعریف شـــود و دلیل نیز باید توســـط قانون تعیین و حدود اعتبار آن معلوم گردد. بنابراین، اصل آزادی دلیل باید با اصل اساسی دیگری یعنی اصل قانونی بودن، هماهنگ باشـــد. «وضعیت ادله رایانه‌ای در هر کشور به اصول اساسی ادله در آن کشـــور بستگی دارد. در کشـــورهای دارای حقوق رومی و ژرمنی اصل بر آزادی تحصیل و ارزیابی ادله اســـت. از این‌رو پذیرش سوابق رایانه‌ای در این کشورها به‌آسانی صورت می‌گیرد؛ اما در نظام کامن‌لا رســـیدگی‌ها شفاهی و تدافعی است و علم حاصل از منابع فرعی از قبیل اشـــخاص دیگر، کتاب‌ها یا سوابق پذیرفته نیست» (زیبر ۱۳۸۳: ۴۷). «این کشـــورها در پذیرش ســـوابق رایانه‌ای به عنوان دلیل تردید دارند یا آن را با شرایط سخت مورد پذیرش قرار می‌دهند» (نوری ۱۳۸۳: ۱۹۲).

مقنن ایران در تدویـــن قوانین از جمله در قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و همچنیـــن در قانون آیین دادرســـی کیفری مصوب ۱۳۹۲ بـــه صراحت به این اصل نپرداخته اســـت، اما در موادی از قوانین مذکـــور می‌توان به‌طور ضمنی قانون‌مند بودن فرایند توقیف داده و ســـامانه را اســـتنباط کرد. ماده ۶۷۱ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ در این خصوص مقرر می‌دارد : «تفتیش و توقیف داده‌ها یا ســـامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضایی و در مواردی به عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد». مواد ۶۷۲ و ۶۷۳ نیز می‌توانند به عنوان جلوه‌هایی از اصل قانون‌مندی از جمله در توقیف داده و سامانه بعنوان

ادلـــه الکترونیکی محســـوب گردند. در این خصوص باید گفت کـــه چون اصولاً توقیف داده‌ها و اطلاعات کامپیوتر به همراه قطعات و ســـخت‌افزارهای مربوط به آن‌هاســـت، بنابراین، نباید لزوم قانون‌مندی توقیف ادله الکترونیکی مورد تردید واقع شـــود. از این زاویه اختیار برای توقیف و ضبط قطعات سخت‌افزاری کامپیوتر به داده‌ها و ادلّه غیرقابل لمـــس همراه آن تســـرّی می‌یابد؛ امـــا در مجموع، باتوجه به فقـــدان یک رویه قضایی اطمینان بخش در این عرصه، به نظر می‌رســـد تصریـــح به اصل قانون‌مندی در توقیف داده‌ها و سامانه‌ها می‌تواند از تفسیرهای مختلف احتمالی جلوگیری نموده و توقیف ادله را قانع‌کننده و اطمینان‌بخش‌تر نماید.

لزوم قانون‌مندی توقیف ادله الکترونیکی در اســـناد بین‌المللی و منطقه‌ای نیز مورد تاکید قرار گرفته اســـت. ماده (۱۹) کنوانسیون جرایم سایبر (۲۰۰۱ - بوداپست)[1] در خصوص قانون‌مندی توقیف مقرر داشته است که؛

«۱- هر یک از اعضا باید به گونه‌ای به وضع قوانین و دیگر تدابیر اقدام کنند که بـــه مقامات ذی‌صلاح این اختیار را دهند که در صورت لزوم و در موارد ذیل به تفتیش یا دسترسی مشابه اقدام کنند:

الف) از تمام یا بخشی از یک سیستم رایانه‌ای و داده‌های رایانه‌ای ذخیره شده در آن،

ب) از رسانه ذخیره‌ساز داده‌های رایانه‌ای که ممکن است آن داده‌ها بر روی آن رسانه در قلمرو عضو مدنظر ذخیره شده باشد.

۲. هـــر یک از اعضا باید به گونه‌ای به وضع قوانین و دیگر تدابیر اقدام کنند که در صـــورت لزوم اطمینان دهند در جایی که مقامات ذیصلاح آنها سیســـتم رایانه‌ای یا بخشـــی از آن را مطابق بند «۱» (الف) مورد تفتیش یا دسترسی مشابه قرار می‌دهند و زمینه‌های موجد این اعتقاد در اختیار دارند که داده مورد نظر آنها در سیستم رایانه‌ای دیگر یا بخشـــی از آن در منطقه تحت قلمروشـــان قرار دارد و داده‌های مذکور به طور قانونی از سیســـتم اولیه قابل دسترسی اســـت و بتوانند هرچه سریعتر دامنه تفتیش یا دسترسی مشابه را نسبت به سیستم ثانویه گسترش دهند.

۳. هر یک از اعضا باید به گونه‌ای به وضع قوانین و دیگر تدابیر اقدام کنند که به مقامات ذیصلاح خود این اختیار را دهند که در صورت لزوم به توقیف یا تأمین مشـــابه نسبت به داده‌های رایانه‌ای دسترسی یافته مطابق بندهای «۱» یا «۲» اقدام کنند. این

1. Cyber Crime Convention 2001 Budapest

تدابیر شامل اعمال اختیارات ذیل خواهد بود:

الف) توقیف یا تأمین مشابه سیستم رایانه‌ای یا قسمتی از آن یا رسانه ذخیره‌ساز داده‌های رایانه‌ای،

ب) کپی‌برداری از داده‌های رایانه‌ای مدنظر و نگهداری از آنها،

ج) حفظ تمامیت داده‌های رایانه‌ای ذخیره شده مربوط،

د) غیرقابل دسترس بودن یا حذف داده‌های رایانه‌ای از روی سیستم رایانه‌ای که در دسترس قرار گرفته است.

۴. هر یک از اعضا باید به گونه‌ای به وضع قوانین و دیگر تدابیر اقدام کنند که به مقامات ذی‌صلاح خود این اختیار را دهند که در صورت لزوم به شخصی که اطلاعاتی درباره عملکرد سیستم رایانه‌ای یا تدابیر امنیتی داده‌های رایانه‌ای دارد، چنانچه متعارف باشد، دستور دهند اطلاعات ضروری را ارائه دهد تا بتوانند تدابیر مندرج در بندهای «۱» و «۲» را اجرا کنند».

در دستورالعمل اتحادیه اروپا درباره حمایت از داده (۲۴ اکتبر ۱۹۹۵) که مهمترین سند حقوقی در زمینه حمایت از داده‌های شخصی، دستورالعمل EC/46/95 پارلمان اروپا مصوب ۲۴ اکتبر ۱۹۹۵ تحت عنوان "دستورالعمل حمایت از افراد در زمینه پردازش خودکار داده‌های شخصی و جریان آزاد این داده‌ها" است نیز به قانون‌مندی توقیف و نگهداری داده‌ها پرداخته شده است. در فصل دوم این دستورالعمل از مواد ۵ الی ۲۱ قواعد کلی راجع به قانونمندی پردازش داده را بیان شده است. در این فصل اصل قانون‌مندی مربوط به کیفیت داده، معیارهایی برای قانونی کردن پردازش داده، انواع و طبقات خاصی از پردازش داده، قانون‌مندی در اطلاعاتی که بایستی به موضوع داده ها ارائه شود، قانون‌مندی در دستیابی و توقیف داده، استثنائات و محدودیت‌ها، حق موضوع داده‌ها بر اعتراض، محرمانگی و امنیت پردازش و اطلاع به مقام ناظر مورد توجه و تاکید قرار گرفته است.

این دستورالعمل در حال حاضر با قانون «مقررات عمومی حفاظت از داده اتحادیه اروپا»[1] جایگزین شده است. مقررات عمومی حفاظت از داده اتحادیه اروپا؛ مقرراتی است که در مورد حفاظت از داده و محرمانگی همه اشخاص و خروج داده

1. The General Data Protection Regulation (GDPR) (EU) 2016/679

در اتحادیه اروپا و منطقه اقتصادی اروپا وضع شـــده است. هدف این مقررات اساساً قانون‌مندی اعطای کنترل داده‌ها به شهروندان و ساکنان این منطقه و ساده‌سازی محیط مقررات‌گذاری برای کســـب و کارهای بین‌المللی از طریق یکسان‌ســـازی مقررات اســـت.[۱] مطابق مقررات این قانون، قانون‌مندی بایـــد به عنوان اصل اولیه مورد توجه قرار بگیرد و تنها به دلایل مشـــخص شـــده در ذیل امکان پردازش و توقیف داده امکان‌پذیر است:

۱. «برای منافع مشـــروع کنترل‌کننده داده یا یک شخص ثالث، مگر اینکه این منافع با منشور حقوق بنیادی اتحادیه اروپا در تعارض باشد (به ویژه در مورد کودکان)،

۲. برای اجرای وظیفه‌ای در خدمت عموم یا یک مرجع رسمی،

۳. برای رعایت تکالیف قانونی کنترل‌کننده داده،

۴. برای تحقق الزامات قراردادی با شخص موضوع داده،

۵. برای ایفای تعهداتی که به واســـطه درخواست شـــخص موضوع داده که در فرایند عقد قرارداد یا کنترل‌کننده داده قراردارد،

۶.برای حفاظت از منافع حیاتی شخص موضوع داده یا یک شخص دیگر».

شـــورای اروپا با بررسی اســـناد بین‌المللی و منطقه‌ای پیرامون اصول حاکم بر جرم‌انگاری، تحقیقات مقدماتی و دادرســـی جرایم سایبری؛ طی گزارشی نتایج توجه به اصل قانون‌مندی در تحقیقات مقدماتی جرایم سایبری از جمله در توقیف داده و سامانه بدین شرح بیان شده است:

۱. داده‌های شـــخصی بایـــد از طریق منصفانه و قانونی جمع‌آوری شـــود (اصل جمع‌آوری قانونی)

۲. میزان داده‌های شخصی جمع‌آوری شده باید به آنچه لازم است محدود شود (اصل حداقلی)

۳. داده‌های شـــخصی باید برای اهداف مشخص و قانونی جمع آوری شوند و به روش‌هایی که با آن اهداف ناسازگار است پردازش نشوند (اصل هدفمندی)

---

۱. لازم به ذکر اســـت که قانون «مقررات عمومی حفاظت از داده اتحادیه اروپا» در ۱۴ آوریل ۲۰۱۶ وضع شـــد و بعد از ســـپری شدن دو ســـال به عنوان دوره گذار، از ۲۵ مه ۲۰۱۸ به اجرا درآمد. اعمال این قانون نیازمند تصویب قانون جداگانه در کشورهای عضو اتحادیه نمی‌باشد و به‌طور خودکار در همه آن‌ها لازم‌الاجراست.

۴. اســـتفاده از داده‌های شخصی برای مقاصدی غیر از موارد مشخص شده فقط باید با رضایت شخص داده یا با مجوز قانونی انجام پذیرد (اصل عدم تخطی)

۵. اطلاعات شخصی باید دقیق، کامل و مرتبط با اهداف مورد نظر باشد که آنها پردازش می‌شوند (اصل کیفیت داده)

۶.اقدامات امنیتی باید برای حفاظت از اطلاعات شـــخصی بکار گرفته شـــود به طوری که از افشای غیرمجاز، تخریب یا اصلاح آنها جلوگیری نماید (اصل امنیت داده).

۷. اشخاص مسئول پردازش داده‌ها باید در مورد رعیات اصول یاد شده پاسخگو باشند (اصل پاسخگویی) (توصیه‌نامه شورای اروپا، ۲۰۱۸: ۱۶-۱۴)

با عنایت به موارد یاد شده می‌توان گفت که اصل قانون‌مندی توقیف داده و سامانه به صورت ضمنی در قانون آیین دادرســـی کیفری ۱۳۹۲ مورد پذیرش قرار داده است. در اسناد، توصیه‌نامه‌ها و دستورالعمل‌های اتحادیه اروپا نیز پیرامون این اصل، کشورهای عضو به لزوم توجه و تصریح به در قوانین خود به اصل قانون‌مندی راهنمایی شده‌اند.

۲. جلوه‌های قانونی توقیف داده و سامانه

بـــا توجه بـــه اینکه توقیف داده‌های ذخیره شـــده در ســـامانه‌ها و توقیف خود ســـامانه‌ها مستلزم برخی از اقدامات نظیر ورود و بازرسی محل نصب کامپیوتر و توقیف داده‌ها و سامانه‌هاســـت، در کمیسیون جرایم ســـایبری، توصیه‌نامه و دستورالعمل‌های کمیته شورای اروپا و همچنین در قوانین ایران و کشورهای اروپایی از جمله انگلیس و فرانسه شرایطی برای توقیف داده‌ها و سامانه‌ها در نظر گرفته شده است که از مهمترین آنها می‌توان به موارد ذیل اشاره کرد:

الف: لزوم مجوز قضایی برای توقیف داده و سامانه

اولین شرط برای توقیف داده و ســـامانه، لزوم مجوز قضایی یا همان مستند به دســـتور مقام قضایی بودن توقیف است. به مانند محیط فیزیکی که هر گونه تفتیش و توقیف به جز در جرایم مشهود، منوط به دستور مقام قضایی می‌باشد، در محیط سایبر نیز، به جز در جرایم مشهود که نیازمند اقدام فوری ضابطین بوده و مقنن اختیاراتی را برای توقیف بدون دســـتور قضایی پیش‌بینی نموده است، توقیف در جرایم غیرمشهود اعم از توقیف داده یا توقیف سامانه نیازمند دستور قضایی می‌باشد.

دستور توقیف در فضای اینترنتی یک مکانیسم تسریعی است که از ارائه‌دهندگان سرویس می‌خواهد تا داده‌های موجود که مختص معامله یا مشتری هستند را ذخیره کند. چنین مکانیسم رویه‌ای در چارچوب شواهد الکترونیک حائز اهمیت است؛ چراکه چنین شواهدی را می‌شود در مقایسه با اسناد فیزیکی به سهولت پاک یا مخدوش کرد. اساساً دستور حفظ (نگهداری)، یک دستور «پاک نکن» است. دستور حفظ، ماهیتی موقتی داشته و با تأمل و شور و همکاری نهادهای اجرای قانون صورت می‌گیرد که جهت کسب داده‌ها، اختیار قانونی لازم را به دست می‌آورند (همچون حکم جهت ضبط داده‌ها یا دستور تولید جهت انتشار داده‌ها) (روبینز، ۲۰۱۹: ۱۴۰).

دستور توقیف، از متولیان و سرپرست اسناد می‌خواهد تا اسناد را به عوامل اجرای قانون در ضمن یک دوره مشخص زمانی تحویل داده و در اختیار بگذارند. دستورهای توقیف مشابه احکام تفتیش هستند، اگرچه در یک دستور توقیف، سرپرست اسناد به‌جای پلیس، عمل جستجو و تفتیش را انجام می‌دهد. این نوع دستور کم‌تر مختل‌کننده بوده؛ چراکه متولی اغلب در موضع بهتری جهت شناخت مکان دقیق اسناد مدنظر قرار دارد. در محیط اقتصادی کنونی امری عادی است که شرکت‌ها داده‌ها را بیرون از حوزه قضایی که در آن مشغول به کارند ذخیره می‌کنند تا اغلب از هزینه‌های ذخیره‌سازی ارزان‌تر داده سود ببرند. احتمال دارد یک حکم سنتی جست‌وجو و تفتیش در چنین اوضاع و احوالی نامتناسب باشد؛ درحالی‌که دستورهای مبنی بر توقیف داده، مالک داده یا سرپرست و متولی آن را قادر می‌کند تا اسناد و بایگانی‌ها را بازیابی کند (روبینز، ۲۰۱۹: ۱۴۲-۱۴۱).

به طور کلی برای قانونی قلمداد شدن توقیف داده‌ها یا سامانه‌ها سه حالت متصور است:

۱. خود شخص رضایت کتبی برای توقیف بدهد؛

۲. جرم مشهود بوده و بنابر وجود دلایل و فوریت امر، ضابطین بدون دستور قضایی اقدام به توقیف داده‌ها و سامانه‌ها نماید؛

۳. توقیف داده و سامانه با دستور قضایی همراه باشد.

در مورد رضایت شخص باید بیان داشت که در حقیقت، یکی از مواردی که ممکن است تفتیش و توقیف یک مکان و یا دسترسی به ادله، بدون صدور قرار قضایی مجاز شمرده شود، موقعیت‌هایی است که ذیل دکترین «شخص ثالث» مطرح می‌گردد.

«هر یک از افراد جامعه (امروزه) خواسته یا ناخواسته، داده‌های زیادی را در اختیار دولت و برخی از مؤسسات بخش خصوصیِ قرار می‌دهند.» (انصاری، ۱۳۸۷: ۲۰۲) و عمده‌ی این خدمات، امروزه به کمک فن‌آوری‌های نوین سایبری در حال ارائه هستند و فن‌آوری‌های اطلاعاتی و ارتباطی تبدیل به ابزاری شده‌اند که کنار گذاشتن آن غیرممکن است (یزدان‌پور ، ۱۳۸۴: ۲۳). ویژگی‌ای که دکترین شخص ثالث دارد این است که هم ساده است و هم به نحو جامعی قابلیت اعمال دارد. این ویژگی‌ها، موجب شده است که در دهه‌های گذشته، تئوری مذکور به‌شدت مورد استقبال سیستم پلیسی، قضایی و به‌ویژه نهادهای امنیتی در کشورهای مختلف قرار گیرد و دولت‌ها در گسترش کاربرد این دکترین زیاده‌روی نمایند. در مقابل، در نظر برخی قضات و حقوقدانان، این مفهوم همواره درگیر و در ارتباط با مفاهیم حریم خصوصی و انتظار برای رعایت حق حفظ محرمانگی و رازداری در زندگی اجتماعی هر شهروند بوده و لذا چنین تأکیداتی در رویه‌ی قضایی نیز راه یافته است (براتاین، ۲۰۱۶: ۱۹۷).

در مورد حالت دوم، یعنی در جرایم مشهود نیز تفسیر موسع از مشهود بودن در فضای سایبر مورد توجه و پذیرش قرار گرفته است و بندهای ماده ۴۵ ق.آ.د.ک ۱۳۹۲ نمی‌توانند در این فضا نیز مبین مشهود بودن جرایم باشند به عنوان نمونه بر خلاف جرایم سنتی که در مرئی و منظر بودن فیزیکی به عنوان یکی از مصادیق مشهود بودن جرم تلقی می‌شود، در جرایم رایانه‌ای نیازی به فیزیکی بودن رویت نیست و صرف گشت در فضای مجازی و رویت ارتکاب جرم مشهود توسط ضابطین می‌تواند مشهود قلمداد شده و با اختیارات قانونی که مقنن در چنین مواردی به ضابطین اعطا نموده اقدام نمایند مثلا محل را مورد تفتیش قرار داده یا داده‌ها و حتی سامانه‌ها را توقیف نمایند. بنابراین در مورد تعریف و قلمروی جرم مشهود در فضای مجازی خلاء وجود دارد و نیاز است مقنن نسبت به رفع این خلاء به صورت خاص یا با اضافه نمودن تبصره‌ای به ماده ۴۵ یاد شده این خلاء را رفع نماید.

در مورد حالت سوم، یعنی لزوم اخذ دستور قضایی؛ بند دو توصیه‌نامه شورای اروپا مقرر می‌دارد: «قوانین آیین دادرسی کیفری باید به مقامات تحقیق اجازه دهند که تحت شرایط مشابه مانند آنچه که طبق اختیارات سنتی تفتیش و توقیف مطرح شده است، سیستم های کامپیوتری را تفتیش و داده‌ها را توقیف کنند».

در ایران نیز در قوانین و مقررات مختلف همانند ماده ۶۷۱ قانون آیین دادرسی کیفری ۱۳۹۲ به لزوم اخذ دستور قضایی برای توقیف پرداخته شده است. مطابق ماده ۱۱ آیین‌نامه جمع‌آوری و استنادپذیری ادلّه الکترونیکی؛ «مقام قضایی در جریان تحقیق و فرایند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره‌شده را ازجمله داده‌های رمزنگاری‌شده، حذف، پنهان، فشرده یا پنهان نگاری شده و یا داده‌هایی که نوع و نام آن‌ها موقتاً تغییریافته و یا داده‌هایی که برای بررسی آن‌ها نیاز به سخت‌افزار مخصوصی می‌باشد، صادر نماید». در تبصره ۲ همین ماده آمده است: «قاضی مکلف است بلافاصله پس از اعلام ضابط قضایی نسبت به تأیید یا رد دستور حفاظت صادره توسط ضابط اظهارنظر نماید. مجری حفاظت تا تعیین تکلیف از ناحیه قاضی موظف به حفاظت از اطلاعات می‌باشد».

ب: تناسب دستورات قضایی توقیف داده و سامانه در رویه قضایی

یکی از مصادیق لزوم تناسب دستور 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 نمونه یک سامانه‌ای که موضوع جرم قرار گرفته یا جرم بر روی آن ارتکاب یافته، نمی‌توان سامانه یا داده‌ی دیگری که ارتباطی با موضوع جرم ندارد را توقیف کرد.

با بررسی دستورات صادره خطاب به ماموران و ضابطین به ویژه ماموران 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 شبکه های اجتماعی یا وب سایت ها 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 ماموران به داده و سامانه‌هایی که در مقام موضوع جرم قرار گرفته‌اند به ویژه در مورد محرمانگی داده و سامانه‌های مرتبط با امنیت ملی

۵. نحوه توقیف موضوع جرم؟
۶.نحوه نگهداری، کنترل و انتقال داده و سامانه‌های موضوع جرم.
۷. مدت زمان توقیف داده و سامانه‌های موضوع جرم.
۸. نحوه اقدام برای رفع توقیف؟

موارد یاد شـــده همه در ارتباط با تناســـب دستور توقیف داده و سامانه و مهلت زمان معقول هســـتند، که در دســـتورات قضایی خطاب به ماموران و ضابطین مشهود می‌باشند.[۱]

پ: لزوم رعایت حریم خصوصی و حفظ محرمانگی

از دیگر شرایط لازم برای توقیف داده و سامانه، لزوم توجه به حریم خصوصی و محرمانگی اطلاعات اکتسابی یا هر اطلاعات دیگر در مورد داده‌ها و سامانه‌ها و اشخاص مرتبط با آنهاست. با توجه به اینکه حریم خصوصی با محرمانگی تحقیقات مقدماتی به عنوان شـــرایط مشـــترک توقیف داده و سامانه ارتباط تنگاتنگی با هم دارد این دو را به عنوان یک شـــرط در کنار هم در نظر گرفته‌ایم. بر همین اساس؛ «در برخی حوزه‌های قضایی، جمـــع‌آوری داده‌ها به‌طـــور تنگاتنگی به‌موجب روال‌هـــای منصفانه اطلاعاتی محدود بوده و اغلب در قوانین مرتبط با صیانت از داده‌ها یا حریم خصوصی که متعاقب آن داده‌هـــا را تنها می‌توان برای اهدافی محدود جمع‌آوری کرده و تنها برای یک هدف تصریح‌شـــده همراه با رضایت آگاهانه و تابع دیگر تضمین‌ها جهت به‌کارگیری استفاده کرد (مثل کنترل‌هـــا در مورد تمامیت اطلاعات، برنامه‌ریزی شناخته‌شـــده تخریبی و دسترسی به سوژه) نهادینه‌شده‌اند» (بکن و تیکر، ۲۰۲۰: ۱۴).

تدابیر حفاظتی برای داده بایســـتی کافی و کارا بوده و جزء لاینفک محرمانگی ادله می باشد، در حفظ داده‌ها باید به مساله حفظ حریم خصوصی و محرمانگی داده‌ها توجه ویژه‌ای شـــود. حفاظت یک تدبیر نخستین اســـت که زمینه را برای سایر تدابیر قانونی به منظور دســـتیابی به داده ها یا افشـــای آنها فراهم می کند. لازمه محرمانگی این است که سایرین برای صدمه زدن یا پاک کردن داده‌ها نکوشند. از نظر شخصی که

۱. مستند موارد یاد شده از کتاب تشریح مواد قانون آیین دادرسی کیفری، معاونت آموزش و منابع انسانی دادگستری اســـتان تهران، چاپ اول، سال ۱۴۰۰ «دستورات صادره به پلیس فتا تهران بزرگ» از طرف مقامات قضایی- دادسرای ناحیه ۳۱ جرایم رایانه ای می باشد.

مخاطب دستور قرارگرفته، «سوژه داده‌ها»[1] یا اشخاص دیگری که ممکن است بوسیله 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 به موجب آن داده ها یاد آوری یا شناسایی شوند کمک می کند (جلالی‌فراهانی، ۱۳۹۷: ۶۷).

در مورد لزوم رعایت حریم خصوصی می‌توان گفت که؛ توقیف داده و سامانه، ارتباط نزدیکی با حریم خصوصی افراد دارد. حریم خصوصی را می‌توان یکی از بنیادی‌ترین و اساسی‌ترین حقوق بشری تلقی کرد که با شخصیت وی ارتباط مستقیم و تنگانگی دارد. حق انسان به تنها بودن و با خود بودن به وسیله دیگران مورد احترام قرار گرفتن و به دور از چشم و نگاه کنترل کننده دیگران و رها از تجسس و تفتیش دیگران؛ زیستن حقی است که لازمه یک شخصیت مستقل به شمار می‌آید. «با آزادی و استقلال انسان و حق تعیین سرنوشت برای خود نیز ارتباط ملازمی دارد» و اساساً شخصیت انسان در پرتو این مفاهیم معنی می‌یابد. نکته مهم در مورد حریم خصوصی آن است، که مفهوم و قلمرو این بعد از حق انسان نیز به دنبال تحولات و پیشرفت‌هایی که به مرور زمان در زمینه‌های علمی، اجتماعی و اقتصادی،... صورت گرفته است، تحت تأثیر قرار گرفته است. لذا، مفهوم و قلمرو حریم خصوصی در جامعه پیشرفته و متمدن امروزی با مفهوم و قلمرو آن در جامعه سنتی سابق متفاوت می‌باشد. کما اینکه مفهوم و قلمرو آن در دنیای کنونی در یک جامعه توسعه‌یافته، با یک جامعه عقب مانده یا در حال توسعه می‌تواند متفاوت باشد (رحمدل، ۱۳۸۴: ۱۲۰).

اهمیت صیانت از حریم خصوصی به حدی است که برخی با بررسی قوانین کشورهای فرانسه و بلژیک به این نتیجه رسیده‌اند که از شش اصل اساسی که به صورت عام در قوانین کشورهای مورد مطالعه مشهود بوده، صیانت از حریم خصوصی اصل عامی است که در تمامی این قوانین جزء اصول اساسی در تحقیقات مقدماتی جرایم سایبری وجود داشته است. این شش اصل عبارتند از: «(الف) صیانت از داده‌ها و صیانت از حریم خصوصی؛ (ب) ایجاد قوانین کیفری جهت پرداختن به جرم اقتصادی مرتبط با رایانه؛ (پ)

1. data subject

صیانـــت از مالکیت معنـــوی، (ت) صیانت در قبال محتـــوای زیان‌بار و غیرقانونـــی؛ (ث) لزوم پیش‌بینی صیانت در تدوین قوانین شـــکلی جزایی و (ج) لزوم وجود مقررات قانونی در خصوص تدابیر امنیتی همچون رمزنگاری و امضاهای دیجیتال» (یاسنسک و همکاران، ۲۰۱۹: ۲۱-۱۷).

رعایت حریم خصوصی، تنها به قوانین داخلی کشورها معطوف نبوده بلکه در در اســـناد بین‌المللی نیز همواره مورد تاکید قرار گرفته است. در این خصوص؛ کنوانسیون شورای اروپا مصوب ۱۹۸۱ به قواعد خاص راجع به نحوه بهره‌برداری از اطلاعات شخصی پرداخته است. آنچه در اصول این سند به رسمیت شناخته شده است، برخورداری همه جانبه اطلاعات شـــخصی در مقاطع جمع آوری و انتقال، ازحمایت و صراحت قانون می باشـــد. این کنوانسیون از آن رو دارای اهمیت اســـت که مقام تصویب کننده آن یعنی شـــورای اروپا، تنها مرجع فراملی است که می‌تواند در سطح منطقه‌ای قوانین و مقررات لازم‌الاجرا را وضع کند (حبیب‌زاده و توحیدفر، ۱۳۸۸: ۷۰). کنوانسیون اروپایی حقوق بشر نیز از طرح و حمایت موضوع حریم خصوصی چشم‌پوشی نکرده و در ماده ۸ آورده اســـت: «هر کس نســـبت به زندگی خصوصی، منزل و ارتباطات خود واجد حق است و مقامـــات دولتی حق هیـــچ گونه مداخله در اعمال حق مذکـــور را ندارند مگر مطابق با احکام و قوانین و در صورتی که مداخله آن‌ها در چهار چوب امنیت ملی، رفاه اقتصادی، حمایت از بهداشت یا بروای حمایت از حقوق دیگران ضروری باشد.»

همانطور که این ماده مشخص کرده، ورود به حریم خصوصی ممنوع است مگر در صورت وجود شـــرایط ۴ گانه فوق. البته همراه با یکی از ۴ شرط فوق باید مداخله مطابق قانون و مشروع باشد. دیوان اروپایی حقوق بشر نیز عبارت «مطابق قانون باشد» را در یکی از آراء خود تفســـیر کرده. بدین معنا که در حقوق ملی کشورها نه تنها باید قانونی در این باره وجود داشته باشد، بلکه کیفیت قانون نیز باید مطلوب باشد (انصاری، ۱۳۸۷: ۶۳).

همچنین مواد ۲ و ۳ کنوانســـیون جرایم ســـایبری معروف به «کنوانسیون جرایم سایبری بوداپست در راســـتای حمایت از حریم خصوصی هرگونه دسترسی عمدی و من غیرحق به سیســـتم رایانه‌ای، داده‌های رایانه‌ای و هرگونه شـــنود را جرم تلقی کرده و در ماده ۱۱ مقرر کرده که اعضا باید برای این افعال در حقوق داخلی خود جرم انگاری کنند. بنابراین حمایت از حریم خصوصی افراد در حوزه‌های مختلف از جمله در توقیف داده‌ها و سامانه‌های رایانه‌ای، مورد حمایت و تأکید این سند بین المللی قرار گرفته است.

در حقوق داخلی نیز در قوانین مختلف از جمله در قانون اساسی، قانون احترام به آزادی‌های مشروع و رعایت حقوق شهروندی، قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای و قانون آیین دادرسی کیفری، به لزوم رعایت حریم خصوصی در کلیه مراحل دادرسی از جمله توقیف اشاره شده است. به عنوان نمونه در قانون آیین دادرسی کیفری؛ حریم خصوصی اطلاعات که شامل مصونیت داده‌ها و حفظ اطلاعات اشخاص می‌باشد، به طور ضمنی در قانون آیین دادرسی کیفری مصوب ۱۳۹۲ مطرح شده است. به طوری که ماده ۱۴۷ این قانون، صرفاً اشیاء و اوراقی که مربوط به واقعه مجرمانه و کشف جرم باشد را قابل تحصیل دانسته است و خواستار رعایت احتیاط توسط قاضی نسبت به سایر اشیاء و اوراق می‌باشد. یا در مواد مختلفی از قانون آیین دادرسی کیفری مربوط به جرایم رایانه‌ای، حریم خصوصی مورد حمایت قرار گرفته که از جمله آنها می‌توان به تبصره ماده ۶۸۳ قانون مرقوم اشاره کرد. این تبصره اشعار می‌دارد: «دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک، در حکم شنود و مستلزم رعایت مقررات مربوط است.»

در حقوق کشورهای دیگر نیز همین وضعیت صادق است. به‌عنوان نمونه، در حقوق فرانسه براساس ماده 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 ضرورت های تحقیق این موضوع را منع نکنند، کپی یا تصویر اسناد یا داده‌های حاوی اطلاعات رایانه‌ای در اختیار دادگستری، می‌توانند در کوتاه‌ترین مدت، به هزینه اشخاص ذینفع که آن‌ها را درخواست کرده‌اند، به آنها داده می‌شود.

به عنوان نکته آخر لازم است به روش‌های نوینی که امروزه در جهت حفظ حریم داده‌های الکترونیکی بوجود آمده‌اند نیز پرداخته شود. دو شیوه رایج و جهانی که برای حفظ حریم داده‌ها مورد استفاده قرار می‌گیرند عبارتند از: ۱- رمزنگاری و استگانوگرافی و ۲- ناشناس کننده‌ها.

رمزنگاری و استگانوگرافی، هر دو برای مصون داشتن محرمانگی و تمامیت محتوای ارتباطات از تعرض‌های گوناگون به کار می‌رود. در رمزنگاری متن اصلی به

رمز نوشـــته تبدیل می‌شود و تا کلید رمزگشای آن فراهم نباشد، خواندنی نخواهد بود. ولی، اســـتگانوگرافی که شیوه نوینی است، به فرد امکان می‌دهد که محتوای پیام خود را در میان محتوای دیگری که ظن برانگیز نیســـت جای داده و بدین ترتیب، ذهن هر متعرضی را منحرف سازد. ناشـــناس‌کننده‌ها نیز ابزار بسیار کارآمد دیگری هستند که فضای سایبر در اختیار کاربرآن خود قرار داده تا از امور خصوصی خود حداکثر محافظت را به‌عمل آورند. این ابزار در واقع تکمیل کننده رمزنگارها و اســـتگانوگرافی است. زیرا مســـیر حرکت ارتباطات خصوصی را به گونه‌ای مخـــدوش می‌کند که ردیابی ان برای دیگران دشـــوار شـــود. این ابزارها همچنین می‌توانند در نگهداری و حفاظت از داده‌ها جهت حفظ محرمانگی آنها توسط پلیس یا مقامات قضایی نیز مورد استفاده قرار بگیرند تا از تعرض به حریم خصوصی و افشـــای اطلاعات داده‌های توقیف شده جلوگیری شود (جلالی‌فراهانی، ۱۳۹۷: ۸۷-۸۶).

در هر صـــورت با وجود تفاوت‌های بســـیار زیاد بین فضای فیزیکی و ســـنتی و پیچیدگی‌هـــای خاصی که در فضای ســـایبر وجود دارد، باز هم بایـــد اقدام‌های مجریان قانون ضابطه‌مند باشد تا از تعرض به حقوق مسلم کاربران به ویژه در حوزه حساس حریم داده‌های الکترونیکی‌شـــان جلوگیری شـــود یا پیامدهای آن به حداقل برســـد. به همین منظـــور همزمان با طرح بحث‌های مربوطه به توســـعه اختیارات مجریان قانون در فضای سایبر، مسائل مرتبط با عدم تعرض آنها به حریم ادله اشخاص نیز مطرح شده است.

ت: پاسداشت تمامیت و دسترس پذیری ادله توقیف شده

از جمله شرایطی که در توقیف ادله در محیط فیزیکی مورد توجه و تاکید مقنن قرار گرفته است، حفاظت از تمامیت و دسترس پذیری ادله است. در محیط مجازی نیز این اصل لازم‌الاجراست، لذا اقدامات قانونی که برای توقیف ادله در محیط فیزیکی لازم است برای توقیف داده و سامانه در محیط مجازی نیز باید بعمل آورد.

بنابراین؛ اگر شـــخص یا اشـــخاص خاصی باید به لحاظ وضعیت خاص خود به خارج از صحنه جرم که توقیف ادله و سامانه در آن مکان صورت می‌گیرد، منتقل شوند، باید مطمئن شد که پیش از ترک صحنه هیچ گونه ادله‌ای به همراه آنان نباشد. مطابق اصل حفاظت از داده و ســـامانه‌های توقیف شـــده، وضعیت ادله را نباید تغییر داد. اگر روشن هستند باید روشن باقی بمانند و اگر خاموش هستند، باید خاموش باقی بمانند.

کارشـــناس توقیف باید تمامـــی خطوط تلفنی که به دســـتگاه‌هایی نظیـــر مودم‌ها و نمایشگرهای شماره تلفن[1] متصل هستند باید شناسایی شوند. باید تمامی خطوط تلفن مستندســـازی شوند، قطع شـــوند، و تک تک برچسب زده شوند. همچنین ممکن است ارتباط دیگری نظیر خطوط شـــبکه در لحظه توقیف داده و سامانه وجود داشته باشند، در این حالت می‌بایست از کارشناسان خبره استفاده کرد (تراب‌زاده، ۱۳۸۸: ۹۴-۹۳).

تدابیر متنوعی برای حفاظت از داده‌ها و سامانه‌ها در برابر حملات وجود دارد و از جمله آنها، تدابیر نظارتی است که در فضای فیزیکی مشاهده می‌شوند که نمونه‌هایی از آن در قالب دوربین‌های مدار بسته جهت کنترل اماکن استفاده می‌شوند. اما آنچه در فضای ســـایبر به کار می‌رود، مجموعه‌ای از برنامه‌های رایانه ای است که بر حسب نوع برنامه ریزی که برایشـــان صورت گرفته، کلیـــه داده هایی را که با مبادلات الکترونیکی کاربران در مظان ارتکاب جرم، مرتبط هستند را جمع آوری می‌کند تا مسئولان ذیربط بـــه صورت زنده آن‌ها را بررســـی کنند. این اقدام تا حدی مـــورد توجه مجریان قانون کشورها قرار گرفته که برخی از آنها پلیس گشت سایبر نامیده شده اند، زیرا به گونه‌ای اوضاع ســـایبری را تحت کنترل دارند که هر گونه وقوع جرم یا دیگر ناهنجاری‌ها را به اطلاع مراجع ذیربط می‌رسانند.

به‌طور کلی روش‌های حفاظت از داده‌ها و ســـامانه‌های توقیف شده عبارتند از: حفاظت فیزیکـــی، حفاظت کارکنان، حفاظت ارتباطـــات و حفاظت عملیات که هدف همه آنها سخت تر ساختن دسترسی مجرمان به داده‌ها و سامانه‌های توقیف شده است (وروایی و میرزکی، ۱۳۹۰: ۷۰).

کارشناســـان بررســـی صحنه جرم ابتدا باید اقدامات لازم را جهت محافظت از افـــراد صحنه جرم بعمل آورند. پس باید به نحوی اقـــدام نمایند که تمامی ادله توقیف شده از هرگونه تغییری مصون بمانند تا اطمینان لازم از صحت تمامی ادله الکترونیکی بوجود بیاید (اشـــکرافت، ۲۰۰۱: ۲۱). بعد از محافظت از افراد و ادله موجود، کارشناس باید نســـبت به شناسایی ادله آشکار (معمولی و الکترونیکی) و همچنین ادله فرار اقدام کند. ســـپس کارشناس صحنه باید صحنه جرم را ارزیابی کرده و نحوه بررسی صحنه را طرح‌ریزی کند (تراب‌زاده، ۱۳۸۸: ۹۳).

---

1. Caller ID

به هیچ عنوان نبایدکاری کرد، که سبب اضافه شدن، تغییر داده‌ها و یا از بین رفتن داده‌های موجود در یک سامانه شود. رایانه ها تجهیزات الکترونیکی بسیار ظریفی هستند که نسبت به رطوبت، حرارت، الکتریسیته ساکن، ضربه یا تکان فیزیکی، منابع مغناطیسی و امواج الکترو مغناطیسی بسیار حساس هستند، بنابراین باید احتیاط خاص و ویژه‌ای را حین بسته‌بندی، حمل و نقل و نگهداری ادله الکترونیکی بعمل آورد. همچنین باید در تمامی مراحل توقیف و انتقال، مستندسازی صورت بگیرد (اشکرافت، ۲۰۰۱: ۲۱).

اگر مجریان قانون از دلایل گردآوری شده به نحوی حفاظت نکنند تا در دادگاه وضعیت اصلی‌شان را انعکاس دهند و همچنین مشخصات هر یک به انضمام مأمور(ان) دست‌اندرکار در فرم‌های مخصوص به طور کامل درج نشده باشد، استنادپذیری‌شان با تردید جدی مواجه خواهد شد. بند یک ماده ۱۶ کنوانسیون جرایم سایبر[1] در این رابطه بکارگیری هر گونه روش قانونی اعم از از استفاده از دستور قضایی یا دستورالعمل اداری و یا صدور دستور از جانب پلیس و سایر مقامات تعقیب را مجاز می داند (همان: ۶۴). ماده ۱۶ کنوانسیون یاد شده به موضوع حفظ فوری داده‌های رایانه‌ای ذخیره شده اختصاص یافته و در سه بند به شرح ذیل مصوب شده است:

۱. هر یک از اعضا باید به گونه‌ای به وضع قوانین و دیگر تدابیر اقدام کنند که در صورت لزوم برای حفظ فوری داده‌های رایانه‌ای خاص، نظیر داده ترافیک، که در یک سیستم رایانه‌ای ذخیره شده است، به ویژه در جایی که زمینه‌های موجد این اعتقاد وجود دارد که داده‌های رایانه‌ای در معرض صدمه یا تغییر قرار دارند، این اختیار را به مقامات ذی‌صلاح خود دهند که دستوراتی صادر کرده یا اقدامات مشابهی برای حفظ فوری این داده‌ها به عمل آورند؛

۲. چنانچه عضوی به مفاد بند «۱» ترتیب اثر می‌دهد و بدین منظور به شخص خاصی دستور می‌دهد داده‌های رایانه‌ای ذخیره شده خاصی را که در کنترل یا تصرف شخصی‌اش است حفاظت کند، این عضو موظف است در صورت لزوم، قوانین و تدابیر

---

۱. بموجب 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 داده های رایانه‌ای خاص ، نظیر داده ترافیک، که در یک سیستم رایانه‌ای خاص ذخیره شده است ، بویژه در جایی که زمینه‌های این باور وجود دارد که داده های رایانه‌ای 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».

دیگری را وضع کند که آن شـــخص را ملزم کند تا دوره زمانی مشـــخصی که ضروری است از داده‌های رایانه‌ای و تمامیت آنها حفاظت کند. این دوره حداکثر نود روز خواهد بود تا مقامات ذی‌صلاح بتوانند به کشـــف موضوعات خود نائل شوند. این عضو می‌تواند ترتیباتی اتخاذ کند که دوره مذکور با صدور دستور قضایی قابل تمدید باشد؛

۳- هـــر یک از اعضا باید به گونه‌ای به وضع قوانیـــن و دیگر تدابیر اقدام کنند که در صورت لزوم متصدی یا شـــخص که مسئولیت حفاظت از داده‌های رایانه‌ای را به عهده دارد ملزم شـــود اجرای چنین رویه‌هایی را تـــا دوره زمانی که قانون داخلی مقرر کرده محرمانه نگهدارد.

باید توجه داشـــت که مطابق آنچه کـــه در این ماده آمده؛ حفاظـــت از داده های رایانه‌ای مســـتلزم جلوگیری از هر گونه اصلاح، خدشـــه یا از بین رفتن داده های رایانه‌ای است که هم اکنون به صورت ذخیره وجود دارند. البته این مفهوم ضرورتاً به این معنا نیست که داده‌ها غیرقابل دســـترس 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 می کرده را تبیین نموده است. لذا این به عهده اعضاست که برای تأمین این هدف چه سازو کارهایی را در نظر بگیرند.

در همین راســـتا در رابطه با حفاظت از داده‌ها، بخشـــنامه شورا و پارلمان اروپا (بخشنامه اروپا EC/02/58) در خصوص پردازش داده‌های شخصی و حفاظت از حریم شـــخصی تدوین شده اســـت که هدف از تدوین آن به این صورت در مقدمه بیان شده اســـت: «تضمین یک ســـطح برابر برای حفاظت از حقوق و آزادی‌های اساسی، تضمین گردش آزاد چنین داده‌هایی، امکانات و خدمات مخابراتی در جامعه و کمک در حفاظت از منافع قانونی مشترکینی که اشخاص قانونی هستند». این بخشنامه شامل مفادی در رابطـــه با موضوعاتی مانند امنیت کلی، محرمانگی، اطلاعات اینترنتی، جابجایی و محل داده‌ها، آدرس‌ها، میل‌های ناخواســـته و حفظ داده‌هاســـت. این بخشنامه با چند اقدام خاص به موضوع محرمانگی ارتباطات و جابه‌جایی داده‌های مربوطه می‌پردازد؛ بنابراین، این بخشنامه شنود، ذخیره کردن یا هر نوع قطع یا نظارت را بدون رضایت قبلی کاربر ممنوع می‌کند و در آخر کشـــورهای عضو را نســـبت به قانون‌گذاری و تدوین مفاد این بخشنامه در قوانین خود دعوت می‌نماید (راسمل و والری، ۲۰۱۸: ۲۱۵-۱۹۴).

در راســـتای همین بخشـــنامه و همچنین مفاد کنوانسیون جرایم ســـایبری در قوانین کشورهای اروپایی مقرراتی پیش‌بینی شـــده است. به عنوان نمونه؛ براساس ماده ۱۰۷ قانون آیین دادرســـی کیفری فرانسه مقرر شده اســـت: «کلیه اشیاء، اسناد یا داده‌های حاوی اطلاعات تحت اختیار دادگســـتری، فورا فهرست‌برداری و مهر و موم می‌شود. اگر فهرســـت‌برداری آن‌ها در مکان با مشـــکل مواجه باشد، افسر پلیس قضایی بر طبق بند چهارم ماده ۵۶ اقـــدام می‌کند». همچنین ماده ۴-۱۰۰ همیـــن قانون اظهار می‌دارد: «بازپرس یا افســـر قضایی مامور از طرف وی، صورت جلسه هرکدام از اقدامات رهگیری و ضبط را تهیه می‌کند. در صورت جلســـه تاریخ و ســـاعتی که عملیات شروع و پایان پذیرفته اســـت، ذکر می‌شود. موارد ضبط شـــده مهرو موم می‌شود». ماده ۵-۱۰۰ نیز بیان می‌دارد که «بازپرس یا افسر پلیس قضایی مامور از طرف وی، ارتباطات مفید برای کشف حقیقت را ثبت و ضبط می‌کند. از این ثبت و ضبط، صورت جلسه تهیه می‌شود. رونوشتی از آن در پرونده نگهداری می‌شود» (تدین، ۱۳۹۱: ۱۱۳).

ث: قانون‌مندی اقدامات پلیسی

پلیس براساس قوانین کشور ایران، در تفتیش و توقیف داده‌ها نقش اساسی دارد و کلیهٔ مراحل توسط پلیس انجام می‌شود. پلیس سایبری با توجه به اینکه به تجهیزات فنی و افراد متخصص در حوزهٔ رایانه مجهز است، از داده‌ها حفاظت می‌کند تا در موارد دستور قضایی، بررسی شـــده و در صورت کشف جرم و درخواست ادله، مراتب به مقام قضایی ارائه شود. شنود داده‌ها به دلیل اینکه مستلزم داشتن تجهیزات فنی بوده، توسط پلیس انجام می‌شود. پلیس در نگهداری داده‌ها نقشی ندارد و نگهداری داده‌ها به عهدهٔ ارائه‌دهندگان خدمات دسترســـی و میزبانی بوده تا در مواقع نیاز و دســـتور ارائه داده‌ها توسط مقام قضایی، داده‌ها را تحویل گرفته و به بررسی آنها بپردازد.

بنابراین، براســـاس قوانین دو کشور و کنوانسیون، قسمت اعظم جمع‌آوری ادله توسط پلیس انجام می‌شود. در فرانسه، طبق حکم ۲۶ اکتبر ۲۰۰۷، شرکت‌های دولتی و خصوصی ملزم شـــده‌اند تا اطلاعات مشـــتریان خود را در دسترس پلیس قرار دهند (فرال شـــوول ، ۲۰۱۰: ۹۶). در قانون آیین دادرسی کیفری فرانسه در مرحلهٔ تحقیقات ابتدایی، افسران پلیس قضایی می‌توانند اقدام به توقیف اسناد، مدارک یا داده‌های رایانه کنند و افســـر پلیس قضایی فقط اشیاء اسناد، مدارک و اطلاعات رایانه‌ای که در کشف حقیقت مؤثر باشد را نگهداری می‌کند (کیسی، ۱۳۸۷: ۸۵).

کنوانسیون جرائم سایبری در بند ۱، ۲ و ۳ مادهٔ ۱۹، به تفتیش و توقیف داده‌های رایانه‌ای ذخیره‌شده اشاره و مقرراتی را پیشنهاد داده است. در خصوص شنود، قانونگذار فرانسه در سال ۱۹۹۱ در خصوص مسئله کنترل و شنود مکالماتی افراد، قوانین و شرایط ویژه‌ای وضع کرد (تدین، ۱۳۹۴: ۸۶). همچنین، کنوانسیون جرائم سایبری در مادهٔ ۲۱ شنود داده محتوا را در جهت جمع‌آوری ادله تجویز و به اعضاء اجازهٔ شنود و وضع قوانین در این خصوص داده است. ماهیت خاص دلایل الکترونیکی به گونه‌ای است که پذیرش آنها را در مراجع قضایی با چالش‌های جدی مواجه کرده است. در دلایل الکترونیک، کلیهٔ مراحل از لحظهٔ جمع‌آوری تا ارائه آن به مقام قضایی توسط پلیس سایبری تجزیه و تحلیل و ارزیابی می‌شود. با توجه به قوانین دو کشور و کنوانسیون، به‌طور کلی می‌توان گفت که در جرائم مشهود، پلیس بدواً می‌تواند به جمع‌آوری ادله و حتی توقیف آنها تا ۲۴ ساعت اقدام کند. بر اساس قوانین، جمع‌آوری دلایل الکترونیکی در جرائم غیرمشهود، مرکب از چهار مرحله است که عبارتند از: ۱- دستور قضایی، ۲- تحقیق و جمع‌آوری ادله، ۳- تجزیه و تحلیل، ۴- ارائه گزارش.

نتیجه اینکه؛ پلیس در جمع‌آوری ادله باید اصول و ضوابط فنی و حقوقی را رعایت کند، در صورت عدم رعایت این ضوابط و اصول نه تنها به دلیل سرعت بالای تغییر و تحریف داده‌ها، نمی‌توان ادله‌ای را جمع‌آوری کرد، بلکه ادلهٔ جمع‌آوری شده نیز در دادگاه رد می‌شود. جرائم سنتی به محیط فیزیکی و صحنهٔ جرم متمرکز بوده، ولی در جرائم رایانه‌ای، پراکندگی جغرافیایی صحنهٔ جرم وسیع بوده و حتی ممکن است صحنهٔ جرم و ادله در دورترین نقطهٔ کرهٔ زمین قرار گرفته باشد. ادلهٔ موجود در فضای مجازی با سرعت قابل ملاحظه‌ای تغییر و محو می‌شود. بنابراین، سرعت عمل و دقت در بررسی صحنهٔ جرم و جمع‌آوری ادله بسیار ضروری است و داشتن دانش بالای فنی و مهندسی موجب افزایش سرعت در رصد و پایش سایت‌های اینترنتی و شبکه‌های اجتماعی و سرعت تشخیص جرم و در نهایت افزایش دقت در جمع‌آوری ادله می‌شود. راهکارها و مقررات ارائه شده در قانون جرائم رایانه‌ای و آیین‌نامهٔ ایران، راهگشای مجریان بوده و جوابگوی نیازهای حقوقی و فنی حوزهٔ جمع‌آوری ادله است (دلخون و همکاران، ۱۳۹۸: ۱۴۶).

با عنایت به موارد یاد شده، در صورتی اقدامات پلیسی مطابق با اصل قانون‌مندی

خواهد بود که در جرایم مشـــهود و غیرمشـــهود، مطابق آنچه که گفته شد اقدام نماید. هر گونه اقدام خودسرانه، به ویژه در جرایم غیرمشهود، تعرض به اصل قانون‌مندی بوده که از یک ســـو ناقض حقوق شـــهروندان خواهد بود و از طرف دیگر موجبات مسئولیت انتظامی، حقوقی یا مسئولیت کیفری کارکنان پلیس را به دنبال خواهد داشت.

۳. تضمینات اصل قانون‌مندی در توقیف داده و سامانه

برای اینکه مقامات قضایی و ضابطان دادگســـتری، اصل حاکمیت قانون را مورد احترام قرار دهند لازم اســـت خود قانون‌گـــذار تضمینات لازم برای حمایت از این اصل را مورد تصریح قرار دهد. «بدیهی اســـت قانونگذار نمی‌تواند از نقض همه اصول و قواعد حقوقی پیشـــگیری نماید. ولی می‌تواند آثـــار آن را با اعلام بطلان و بی اعتباری ادله یا تحقیقات و یا منع دادرسان از پذیرش اعتبار و ارزش ادله تحصیلی از طریق غیرقانونی یا اقدامات نامشروع از بین ببرد. هرچند در مقررات کیفری ایران، چنین ضمانت اجرایی به طور صریح مورد توجه قانونگذار قرار نگرفته اســـت، اما نشانه‌هایی از پذیرش ضمنی آن در قوانین جاری از جمله قانون اساســـی و قانون آیین دادرسی کیفری ۱۳۹۲ دیده می‌شـــود. در این خصوص می‌توان به دو بطلان قانونی و قضایی اشـــاره نمود» (باقری نژاد، ۱۳۹۴: ۱۴۵-۱۴۴). منظور از بطلان قانونی بطلان‌هایی اســـت که قانونگذار موارد آنهـــا را در متون قانونی به صراحت پیش‌بینی می‌نمایـــد. در حقیقت، این نوع تضمین ضمانت اجرای نقض اصول قواعد و تشـــریفات اساسی دادرسی و منافع بنیادین اصحاب دعواست که مورد توجه قانونگذار قرار گرفته است. برای نمونه احترام به اصل مشروعیت تحصیل دلیل در اصل ۳۸ قانون اساســـی پذیرفته شـــده و به صراحت اجبار شخص به شـــهادت، اقرار یا سوگند ممنوع اعلام و چنین ادله‌ای فاقد اعتبار و ارزش دانسته شده اســـت. همچنین حق داشـــتن وکیل و تفهیم این موضوع به متهم به منظور احترام به حقـــوق دفاعی او، در ماده ۱۹۰ قانون آیین دادرســـی کیفری مصوب ۱۳۹۲ پیش‌بینی شده است. در راســـتای تضمین این حق، در تبصره این ماده تا قبل از اصلاحات مورخ ۱۳۹۴/۳/۲۴ آمده بود، ســـلب حق همراه داشتن وکیل یا عدم تفهیم این حق به متهم موجب بی اعتباری تحقیقات می‌شود (باقری نژاد، ۱۳۹۴: ۱۴۵). در کنار بطلان قانونی، از بطلان قضایی هم می‌توان سخن گفت. بطلان قضایی، توسط قانونگذار پیش‌بینی

نمی‌گردد و این رویه قضایی است که مصادیق آنها را تعیین می‌کند. در این دسته از ضمانت اجراهـــا، رویه قضایی با توجه به عدم رعایـــت اصول بنیادین و به ویژه نقض حقوق دفاعی متهم، فارغ از پیش‌بینـــی قانونگذار، ذاتاً تصمیمات و تدابیر قضایی صورت گرفته را باطل فرض می‌نماید (باقری نژاد، ۱۳۹۴: ۱۴۷). فقدان تاریخ یا امضای سند توسط بازپرس، عدم امضای دستور تعیین بازپرس، فقدان سوگند کارشناس، فقدان هر نوع بازپرسی از متهم در جریـــان تحقیقات و عدم اعلام تمدید مدت تحت نظر به عنوان مصادیقی از بطلان قضایی اقدامات و تدابیر دادرسی پذیرفته شده است (تدین،۱۳۸۷: ۸۶).

در کنـــار ضمانت‌اجرای بطلان عـــدم رعایت اصول حاکم بر دادرســـی از جمله اصل قانون‌مندی، ضمانت‌اجرای دیگری نیز برای ناقضین این اصول درنظر گرفته شـــده اســـت که به صورت مســـئولیت کیفری و مســـئولیت مدنی در قوانین تجلی یافته است. مسئولیت کیفری نقض قانون در ماده ۵۹۷ قانون مجازات اسلامی بخش تعزیرات مصوب ۱۳۷۵ بدین صورت مقرر شـــده اســـت: «هر یک از مقامات و مأمورین وابسته به نهادها و دستگاههای حکومتی‌که برخلاف قانون، آزادی شخصی افراد ملت را سلب کند یا آنان را از حقوق مقرر در قانون‌اساســـی جمهوری اسلامی ایران محروم نماید علاوه بر انفصال از خدمت و محرومیت یک تا پنج ســـال از مشـــاغل حکومتی به حبس از دو ماه تا سه سال محکوم خواهد شـــد». در مورد توقیف و بازداشت نیز ماده ۵۷۵ همین قانون مقرر داشته اســـت: «هرگاه مقامات قضائی یا دیگر مامورین ذیصلاح بر خلاف قانون توقیف یا دستور بازداشت یا تعقیب جزائی یا قرار مجرمیت کسی را صادر نمایند به انفصال دایم از سمت قضائی و محرومیت از مشاغل دولتی به مدت پنج سال محکوم خواهند شد». بدیهی است این مقررات قانونی هرچند از سلب آزادی اشخاص یا توقیف و بازداشت آنها سخن به میان آورده اســـت، در برگیرنده همه ترتیبات دادرسی از جمله توقیف داده و سامانه بر خلاف قانون را نیز در برمی‌گیرد. در مورد مســـئولیت مدنی نیز مطابق با مقررات مقرر در قانون مدنی و قانون مسئولیت مدنی واردکننده خسارات باید نسبت به جبران آن اقدام نماید.

در کنار این دو مســـئولیت، مقنن مســـئولیت انتظامی نیز برای اشخاصی که رابطه استخدامی دارند به مانند مقامات قضایی و ضابطان دادگستری که رابطه استخدامی با دولت و قوه قضاییه دارند، پیش‌بینی نموده است. بنابراین اگر اشخاص یاد شده بر خلاف ترتیبات قانونی اقدام به توقیف داده یا سامانه نمایند، مسئولیت انتظامی نیز بر متخلف بار خواهد شد.

برآمد

اصل قانون مندی توقیف داده و سامانه همانند اصل قانونمندی در حوزه های مختلف حقوق کیفری، بخشی جزیی از اصل قانونی بودن فرآیند رسیدگی است. گرچه وضوح این اصل به اندازه کافی قابل درک است ولی می تواند در همان حال اصلی شکننده باشد. اصل قانون مندی توقیف داده و سامانه به معنای ایجاد توازن میان صلاحدید قضایی، تشخیص قضایی، رضایت متصرف یا مالک داده و سامانه و توجه به ماهیت و کارکرد داده و سامانه در فرآیند توقیف است. همین توازن سبب می شود تا اصل قانون مندی توقیف داده و سامانه به یک اقدام قضایی تقلیل پیدا نکند.

از منظر منابع حقوقی، اصل قانون‌مندی توقیف داده و سامانه به عنوان یک اصل ضمنی مورد پذیرش قرار گرفته است یعنی، مقنن ایران در تدوین قوانین از جمله در قانون جرایم رایانه‌ای و همچنین در قانون آیین دادرسی الکترونیکی مصوب ۱۳۹۳ و قانون آیین دادرسی کیفری ۱۳۹۲ به صراحت به این اصل نپرداخته است، اما در موادی، از قوانین ذکر شده می‌توان به‌طور ضمنی قانون‌مند بودن فرایند توقیف داده و سامانه را استنباط کرد. لزوم قانون‌مندی توقیف ادله الکترونیکی در اسناد بین‌المللی و منطقه‌ای نیز مورد تاکید قرار گرفته است. ماده (۱۹) کنوانسیون جرایم سایبر (۲۰۰۱ - بوداپست) در خصوص قانون‌مندی توقیف داده و سامانه می‌باشد.

اولین و مهمترین جلوه اصل قانومندی توقیف داده و سامانه، لزوم مجوز قضایی یا همان مستند به دستور مقام قضایی بودن توقیف است که متناسب با نوع رفتار مجرمانه صادر می شود، مانند محیط فیزیکی که هر گونه تفتیش و توقیف به جز در جرایم مشهود، منوط به دستور مقام قضایی می‌باشد، در محیط سایبر نیز، به جز در جرایم مشهود که نیازمند اقدام فوری ضابطین بوده و مقنن اختیاراتی را برای توقیف بدون دستور قضایی پیش‌بینی نموده است، توقیف در جرایم غیرمشهود اعم از توقیف داده یا توقیف سامانه نیازمند دستور قضایی می‌باشد. در ایران، در قوانین و مقررات مختلف به لزوم اخذ دستور قضایی برای توقیف پرداخته شده است. ماده ۶۷۱ تا ۶۷۳ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ و ماده ۱۱ آیین‌نامه جمع‌آوری و استنادپذیری ادلّه الکترونیکی از جمله مهمترین مستندات پیرامون لزوم اخذ مجوز قضایی برای توقیف داده و سامانه هستند.

دومین جلوه اصل قانونمندی توقیف داده و سامانه، لزوم توجه به حریم خصوصی و

محرمانگی اطلاعات اکتسابی یا هر اطلاعات دیگر در مورد داده‌ها و سامانه‌ها و اشخاص مرتبط با آنهاست. در قوانین مختلف از جمله در قانون اساسی، قانون احترام به آزادی‌های مشروع و رعایت حقوق شهروندی، قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای و قانون آیین دادرسی کیفری، به لزوم رعایت حریم خصوصی در کلیه مراحل دادرسی از جمله توقیف اشاره شده است. رعایت حریم خصوصی در محیط سایبری از جمله در جمع‌آوری، توقیف و ... ادله الکترونیکی، در اسناد بین‌المللی نیز مورد تاکید قرار گرفته است. در این خصوص؛ کنوانسیون شورای اروپا مصوب ۱۹۸۱ به قواعد خاص راجع به نحوه بهره‌برداری از اطلاعات شخصی پرداخته است. آنچه در اصول این سند به رسمیت شناخته شده است، برخورداری همه جانبه اطلاعات شخصی در مقاطع جمع آوری و انتقال، ازحمایت و صراحت قانون می باشد.

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

نتیجتاً اصل قانونمندی توقیف داده و سامانه، مسیری را پیش روی قضات می نهد که در قبال داده و سامانه رویکردی متوازن داشته باشد. به همان اندازه که دلایل وقوع جرم یا بستر وقوع جرم در زمان حاضر با داده و سامانه پیوند خورده و بر همین اساس عموم داده ها و سامانه ها در مظان اتهام و در نتیجه مستحق توقیف اند، در همان حال نیز همه شهروندان و از جمله خود قضات به صورت فراگیر درگیر فعالیت های روزمره مرتبط با تبادل یا ذخیره داده یا عملکرد سامانه اند. بنابراین از این منظر، توقیف داده یا سامانه بسا که توقیف یک زندگی مجازی یا یک کسب و کار دیجیتالی باشد. به همین دلیل است که اصل قانونمندی، همچنان مقام قضایی را به سمتی فرا می خواند که صلاحدید و تشخیص قضایی را به عنوان یکی از جلوه های مهم اصل قانونمندی تلقی کند و نه به عنوان همه اصل قانومندی.

منابع

الف) فارسی

۱. قرآن کریم.
۲. انصاری، باقر، ***آزادی اطلاعات***، چاپ اول، تهران: دادگستر، ۱۳۸۷.
۳. باقری نژاد، زینب، ***اصول آیین دادرسی کیفری***؛ چاپ اول، تهران: خرسندی، ۱۳۹۴.
۴. پاک نیت، مصطفی، ***افتراقی شدن دادرسی کیفری***؛ چاپ اول، تهران: نشر میزان، ۱۳۹۶.
۵. تدین، عباس، ***آیین دادرسی کیفری فرانسه***. تهران: انتشارات خرسندی. چاپ اول، ۱۳۹۴.
۶. تدین، عباس، ***تحصیل دلیل در آیین دادرسی کیفری***، چاپ دوم، بنیاد حقوقی میزان، ۱۳۹۱.
۷. تدین، عباس، ***نظریه بطلان دلیل در فرایند دادرسی کیفری*** (با تاکید بر حقوق فرانسه)، مجله تحقیقات حقوقی، شماره ۱، ۱۳۸۷.
۸. تراب زاده، ***بررسی صحنه های جرم الکترونیکی***، کارآگاه، دوره دوم، سال دوم، شماره ۶، بهار ۱۳۸۸.
۹. جلالی فراهانی، امیر حسین، ***شنود ارتباطات الکترونیک در حقوق کیفری ایران***، مجلس و راهبرد، سال ۲۱، شماره ۷۸، ۱۳۹۷.
۱۰. جلالی فراهانی، امیر حسین، ***درآمدی بر آیین دادرسی کیفری جرائم سایبری***، انتشارات خرسندی، چاپ اول، ۱۳۸۹.
۱۱. حبیب زاده، جعفر و توحیدی فر، محمد، ***قانون مداری در قلمرو حقوق کیفری***؛ چاپ اول، تهران: دادگستر، ۱۳۸۸.
۱۲. دلخون اصل، رامین و ایرج گلدوزیان و کیومرث کلانتری، ***نقش پلیس در جمع‌آوری ادلهٔ الکترونیکی در فضای مجازی در نظام حقوقی ایران، فرانسه و کنوانسیون جرائم سایبری***، فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال چهاردهم جمعآوری ادلهٔ الکترونیکی شمارهٔ دوم، ۱۳۹۸.
۱۳. رحمدل، منصور، ***حق انسان بر حریم خصوصی***، مجله دانشکده حقوق و علوم سیاسی(دانشگاه تهران)، شماره ۷۰، زمستان ۱۳۸۴.

۱۵. فتحی، علی، ***ماهیت حقوقی امضای الکترونیک در اسناد تجاری***، مؤسسه مطالعات و پژوهشهای بازرگانی، تهران، ۱۳۹۱.
۱۶. کیسی، اوئن، ***دلایل دیجیتالی و جرم رایانه‌ای؛ علم قانونی، رایانه‌ها و اینترنت*** (امیرحسین جلالی فراهانی و علی شایان، مترجمان)، تهران: انتشارات سلسبیل. چاپ اول، ۱۳۹۸.
۱۷. محمودی‌جانکی، فیروز، ***نظام کیفردهی هدف‌ها و ضرورت‌ها***، تازه‌های علوم جنایی (مجموعه مقالات)، چاپ اول، تهران، انتشارات میزان، ۱۳۸۸
۱۸. میلانی، علیرضا، ***نگرشی بر اصل قانونی بودن جرایم و مجازات‌ها***، تهران: نشر میزان، ۱۳۸۶.
۱۹. نوری، محمد علی، ***حقوق تجارت الکترونیک***، چاپ اول، تهران، انتشارات گنج دانش، ۱۳۸۲.
۲۰. یزدان‌پور (مترجم)، اسماعیل، ***علم در جامعه اطلاعاتی***. تهران: کمیسیون ملی یونسکو در ایران، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۴.
۲۱. وروایی، اکبر، میرزکی، سیدشمس الدین، ***بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه ای پلیس آگاهی تهران سال ۱۳۸۶-۱۳۸۷***، کارآگاه، دوره دوم، سال چهارم، بهار ۱۳۹۰.

ب) انگلیسی

22. Anthony j. dreye ,***when postman beeps twice: the admissibility of electronic mail under the business records exception of the federal rules of evidence***, Fordham law review , 1996.
23. Ashcroft ,John, ***Electronic crime scene investigation for first responders***, 2001.
24. Brattain, B. (2016). "***The Electronic Communications Privacy Act: Does The Act Let The Goverment Snoop Through Your Emails And will It Continue?***" NCJL & Tech. On., 17.
25. Bacon, T. & Tikekar, R. (2019). ***Experiences with developing a computer security information assurance curriculum, Journal of Computing Sciences in Colleges***, 18(4), 254-267.

26. Council of Europe (2018)., ***Cybercrime investigation and the protection of personal data and privacy***, Economic Crime Division Directorate General of Human Rights and Legal Affairs Strasbourg, France Version 25 March 2018

27. Feral Schuhl, Christiane (2010). ***Cyberdroit Le droit à l'épreuve de l'Internet (Cyberright The right to the test of the Internet)***, Paris, Dalloz Publications, 6 edition

28. Robbins, J. (2020). ***An explanation of computer forensics***, 4th Edition, Incline Village, NV: National Forensics Center. SANS (System Administration, Networking and Security) Institute. www.sans.org

29. Rathmell, A., & Valeri, L. (2018). ***Handbook of legislative procedures of computer and network misuse in EU countries***, Study for the European Commission DirectorateGeneral Information Society. Cambridge: Rand Europe.

30. The General Data Protection Regulation (GDPR) (EU) 2016/679

31. Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., & Sommer, P. (2019). ***Computer forensics education***, Security & Privacy Magazine, IEEE, 1(4), 15-23.