Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/mtlj.2023.390545.1188

Research requirements of Communication and information data privacy in cyberspace

Vahid Nekoonam

Assistant Prof., Faculty of Humanities, Hazrat Masoumeh University, Qom, Iran.

Article Info

Original Article

Received:
20-03-2023
Accepted:
24-09-2023

Keywords:
Privacy
Communication Data
Preliminary
Investigation
Fair Trial

Abstract

Today, the Internet is considered the best tool for speed and price. These advantages have caused a significant part of communication and information to be stored and transmitted in this space. However, the open nature of the network has paved the way for various people to enter so that they can quickly check data and control people without a warrant from a judicial authority. These concerns at the world level have caused increasing measures to be established in the laws of countries and international documents to prevent this and protect people's privacy. Law enforcement, network service providers or other people can violate this privacy. During the proceedings, judicial authorities and bailiffs may attempt to violate this privacy under the pretext of discovering a crime and finding a reason, so it is necessary to anticipate the mechanisms required in this field. With these explanations, the main question of this research is to what extent will the general rules of criminal procedure regarding protecting the privacy of information and communications in cyberspace be responsive to how the prosecution authorities deal with the investigation? This research investigates the current situation and expresses the gaps using library sources and looking at international laws and documents. According to the findings of the study, there is a high possibility of information and communication privacy violations by the investigating authorities in the judicial process, and despite the provision of defensible measures in the computer crimes law and the electronic commerce law, there are still deficiencies in some areas; Therefore, it is suggested to adopt measures such as using artificial intelligence and biometrics in this regard.

***Corresponding author**
e-mail: Vahid.nekoonam@gmail.com

How to Cite:
Nekoonam, V. (2024). Research requirements of communication and information data privacy in cyberspace. *Modern Technologies Law*, *5*(9), 27-40.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

حقوق فناوری های نوین

http://doi.org/10.22133/mtlj.2023.390545.1188

بایسته‌های تحقیق از حریم خصوصی داده‌های ارتباطاتی و اطلاعاتی در فضای سایبر

وحید نکونام

استادیار دانشکدهٔ علوم انسانی، دانشگاه حضرت معصومه، قم، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۱۲/۲۹

تاریخ پذیرش:
۱۴۰۲/۰۷/۰۲

واژگان کلیدی:
حریم خصوصی
داده‌های ارتباطی
تحقیقات مقدماتی
دادرسی عادلانه

چکیده

امروزه اینترنت یکی از ابزارهای ارتباطاتی است که به‌منزلهٔ ابزار پرسرعت با مناسب‌ترین قیمت تلقی می‌شود. این مزایا سبب شده است بخش درخور توجهی از ارتباطات و اطلاعات در این فضا ذخیره شود و انتقال یابد. با وجود این، طبیعت باز شبکه راه را برای ورود افراد مختلف هموار ساخته است؛ به‌نحوی که به‌راحتی و بدون داشتن حکمی از مقام قضایی اقدام به بررسی داده‌ها و کنترل افراد می‌کنند. این نگرانی‌ها در سطح جهان سبب شده تدابیر فزاینده‌ای در قوانین کشورها و اسناد بین‌المللی برای پیشگیری از این امر و حفظ حریم خصوصی افراد وضع شود. این حریم را ممکن است مجریان قانون، ارائه‌کنندگان خدمات شبکه‌ای یا سایر افراد نقض کنند. در جریان دادرسی، مقامات قضایی و ضابطان به بهانهٔ کشف جرم و تحصیل دلیل چه‌بسا اقدام به نقض این حریم کنند؛ بنابراین پیش‌بینی سازوکارهای لازم در این عرصه امری بایسته است. با این توضیحات، سؤال اصلی این پژوهش آن است که قواعد عمومی آیین دادرسی کیفری درخصوص حفظ حریم خصوصی تا چه حد پاسخ‌گوی چگونگی برخورد مقامات تعقیب در تحقیق از حریم خصوصی اطلاعاتی و ارتباطاتی در فضای سایبر خواهد بود؟ این پژوهش به روش توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای و نگاهی به قوانین و اسناد بین‌الملل به بررسی وضع موجود و بیان خلأها می‌پردازد. براساس یافته‌های پژوهش، این امکان که مقامات تحقیق در فرایند دادرسی، حریم خصوصی اطلاعاتی و ارتباطاتی را نقض کنند به‌شدت وجود دارد و به‌رغم پیش‌بینی تدابیر قابل دفاع در قانون جرایم رایانه‌ای و قانون تجارت الکترونیکی اما همچنان در برخی حوزه‌ها نقایصی دیده می‌شود؛ ازاین‌رو اتخاذ تدابیری مانند بهره‌گیری از هوش مصنوعی و بیومتریک در این راستا پیشنهاد می‌شود.

***نویسندهٔ مسئول**

رایانامه: Vahid.nekoonam@gmail.com

نحوهٔ استناددهی:

نکونام، وحید (۱۴۰۳). بایسته‌های تحقیق از حریم خصوصی داده‌های ارتباطاتی و اطلاعاتی در فضای سایبر. حقوق فناوری‌های نوین، ۵(۹)، ۲۷-۴۰.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

در فرایند دادرسی کیفری، تحقیقات بی‌گمان مهم‌ترین مرحله است؛ زیرا زیربنای اقدامات مقام قضایی و دادرسان مبتنی‌بر همین تحقیقات است. حقوق کیفری در تعامل و تعارض دو اصل تأمین نظم عمومی و حقوق و آزادی‌های فردی است و این امر نوعی جدال میان امنیت‌گرایی و دادرسی منصفانه ایجاد کرده است. برخی نویسندگان غربی دو مدل کنترل جرم[1] و دادرسی عادلانه و منصفانه را برای این تضاد پیشنهاد کرده‌اند (packer, 2013). یکی از جلوه‌های دادرسی عادلانه[2]، حق بر رعایت حریم خصوصی[3] و ممنوعیت کنکاش در اموری است که ارتباطی با جرم ارتکابی ندارند. گفتمان عدالت آیینی[4] یا رویه‌ای بر رسیدگی منصفانه در فرایند دادرسی تأکید دارد. حق بر حریم خصوصی حدود یک‌دهه است که بیش از گذشته در ادبیات حقوقی ایران مطرح شده و به تبع آن، قانون‌گذار نیز برخی مواد قانونی را در راستای حمایت از این حق به تصویب رسانیده است. مبنای داشتن چنین حقی، اصل آزادی به‌منزلهٔ بن‌مایهٔ گوهر انسانی است. قانون اساسی جمهوری اسلامی ایران در اصول ۲۲ و ۲۵، به جلوه‌هایی از این حق اشاره کرده است. دلیل این امر آن است که جامعهٔ انسانی توقع دارد محدوده‌ای از زندگی شخصی افراد بدون دخالت و حضور دیگران حفظ شود. این حریم دربردارندهٔ حریم خصوصی جسمانی، مکانی، اطلاعات و ارتباطات است و طبعاً کنترل و ورود به این حوزه که شامل ورود غیرمجاز به اماکن خصوصی، استراق سمع و بصر، دسترسی به اطلاعات خصوصی و تصاویر اشخاص و مکالمات آنان، از منظر عموم مردم قبیح بوده با واکنش همراه است. با گسترش ابزارهای الکترونیکی، نقض حریم خصوصی بیش از پیش تسهیل شده است و حتی مأمورین کشف جرم می‌توانند با برنامه‌هایی که بر روی سیستم‌های الکترونیکی نصب می‌شود تمامی فعالیت‌های شبکه‌ای کاربران و حتی نقاطی که ازطریق موس کلیک کرده‌اند یا ضربات بر روی صفحه کلید را رصد کنند.

فراگیری استفاده از سیستم‌های الکترونیکی حوزهٔ حریم خصوصی را گسترش داده و اهمیت آن را دوچندان ساخته است؛ چراکه بیشتر افراد تجربه و توانایی لازم را در حفاظت از این حریم ندارند و همچنین دسترسی به اطلاعات از راه دور زمینهٔ ورود ناروا به این حوزه را بیشتر کرده است.

اهمیت پرداختن به موضوع در این است که به‌رغم تصویب قوانین قابل دفاع در حوزهٔ حقوق دفاعی متهم، در بحث استفاده از محدودیت‌های ورود به حوزهٔ خصوصی ارتباطاتی و اطلاعاتی افراد در فضای اینترنت تدابیر چندانی پیش‌بینی نشده و در عرصهٔ آثار پژوهشی نیز تاحدی در این خصوص خلأ وجود دارد؛ بنابراین واگرایی این اثر نسبت به موارد مشابه تمرکز بر حقوق شکلی است و درخصوص حقوق ماهوی و ضمانت اجراهای کیفری بحثی به میان نمی‌آورد؛ چنان‌که در حوزهٔ حقوق کیفری نیز آثار متعددی به رشتهٔ تحریر درآمده است.

۱. مفهوم حریم خصوصی و گسترهٔ آن

حق بر حریم خصوصی معادل انگلیسی right of privacy و در زبان عربی حق الخلوه (بعلبکی، ۱۹۹۵، ص ۴۹۹) است. فرهنگ حقوقی بلک در تعریف حریم خصوصی بیان داشته است: وضعیت یا حالت رهابودن از توجه عمومی به‌منظور مزاحمت یا مداخله نسبت به اعمال یا تصمیمات فرد (Garner, 2004, p. 1255). حقوق‌دان دیگری حریم خصوصی را حقی برای افراد دانسته که آنان را در برابر مداخله بدون اذن سایرین در زندگی شخصی‌شان حمایت می‌کند (Landwehr-Heitmeyer, 2011, p. 43).

سند کنفرانس حقوق‌دانان دربارهٔ حریم خصوصی در نروژ در سال ۱۹۷۶[5] در بند ۲، حق حریم خصوصی را حق نسبت به تنهاماندن، زندگی‌کردن با سلیقهٔ خود و با حداقل مداخلهٔ دیگران دانسته است. همچنین براساس سند این کنفرانس، این حق مدنی شامل حمایت از فرد در برابر ورود و مداخلات دیگران، صدابرداری و تصویربرداری پنهانی از وی یا استراق سمع ارتباطات وی می‌شود.

1. crime control model
2. fair trial
3. the right of privacy
4. procedure justice
5. Nordic conference of jurists on the right to respect for privacy-1976

مادهٔ ۲ لایحهٔ حریم خصوصی در تعریف این حریم آورده است: قلمرویی از زندگی هر شخص است که آن شخص یا با اعلان قبلی در چارچوب قانون، انتظار دارد دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم، البسه و اشیای همراه افراد، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شوند.

در فلسفهٔ غرب، نگاه رویکرد تقلیل‌گرایی[1] و ذات‌گرایی[2] به این مقوله متفاوت است. تقلیل‌گراها وجود مستقل حریم خصوصی را منکرند، اما دستهٔ دوم قائل به اساسی‌بودن و پیوستگی منافع حریم خصوصی هستند (Staples, 2007, p. 406)؛ حتی با پذیرش نگاه دوم با دو مبنای متفاوت در موضوع مواجه‌ایم. عده‌ای حریم خصوصی را حقی ذاتاً مطلق می‌دانند که رعایت آن وابسته به امر دیگری نیست؛ درحالی‌که مطابق رویکرد دوم حریم خصوصی حقی ذاتاً مقید است؛ بنابراین رعایت آن منوط به چارچوبی است که ارتباطی با غیر نداشته باشد (سروش، ۱۳۹۳، ص ۱۸۵)

هریک از این دو رویکرد نتایجی را در پی دارد. در رویکرد اول، تحدید حریم خصوصی نیازمند ادلهٔ متقن و احراز اهم‌بودن موضوع در مقام تزاحم است؛ درحالی‌که در نگاه دوم هرگاه این حریم به غیر ارتباط یابد، اساساً حریم خصوصی محسوب نمی‌شود تا مصداقی از نقض این حریم تلقی شود.

اثر دوم آن‌که با پذیرش نظریهٔ اطلاق حق حریم خصوصی و عدم تقیید رعایت آن دانسته می‌شود که نسبت به فرد «اصل واجب مفروض» به امری دیگر، این حکم مشکوک، اصاله الاطلاق را جاری و حکم اولیه یعنی حرمت تعدی به حریم خصوصی در فرد مشکوک عنوان، جاری می‌شود. اما مبتنی‌بر مبنای دوم در موارد مشکوک، یعنی جایی که نمی دانیم نقض شئون حریم خصوصی لازم و ضروری است یا غیرضروری یا به‌عبارت‌دیگر، موضوع متعلَق حکم حریم خصوصی است یا متعلَق حکم مصلحت عمومی، براساس اصل اباحه، اصل اولیه بر حرمت نبوده، و می‌توان شئون حریم خصوصی را نقض کرد (میرزازاده و همکاران، ۱۴۰۰، ص ۲۱۲).

گفتمان در ساحت حریم خصوصی از چند منظر مدنظر قرار می‌گیرد: اولاً از منظر یک حق منفی که به معنای حریمی است که از حوزهٔ مداخلهٔ دولت دور است؛ ثانیاً به‌منزلهٔ یک حق مثبت که در آن ابزارهای سیاست جنایی در حمایت از این حق بررسی می‌شود؛ ثالثاً از منظر سازوکارهای قانونی که ازطریق آن می‌توان این حریم را نقض کرد.

در قانون اساسی جمهوری اسلامی، صراحتاً به حریم خصوصی اشاره نشده، اما در برخی اصول آن موضوع رعایت مصادیقی از حریم خصوصی مورد توجه بوده است؛ برای مثال اصل ۲۵ قانون اساسی مقرر می‌دارد: بازرسی و نرساندن نامه‌ها، ضبط و فاش‌کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون.

از منظر تطبیقی نیز دادگاه اروپایی حقوق بشر[3] در آرای خود برای حریم خصوصی حوزهٔ گسترده‌ای را قائل است که شامل حریم جسمانی و روانی اشخاص می‌شود (رحیم خویی، ۱۳۹۶، ص ۲۷۲)

سازمان ملل متحد نیز در سال ۲۰۱۳ با اجماع موضوع حفظ حریم خصوصی اطلاعاتی افراد را به‌منزلهٔ یکی از جلوه‌های حقوق بشر قلمداد کرد و در این راستا، کشورهای گوناگون قوانینی را تحت عنوان حمایت از داده[4] یا صیانت از حریم خصوصی اطلاعاتی[5] به تصویب رساندند.

با توسعهٔ روزافزون علم گستره این حریم نیز تحول یافته است. یکی از ابعاد موضوع حق اشخاص در امنیت و محرمانه باقب ماندن محتوای کلیهٔ اشکال و صور مراسلات و مخابرات متعلق به ایشان است. این شق از حریم خصوصی به‌لحاظ قدمت و سابقهٔ نسبی پست و

1. Reductionism
2. Coherentism
3. European Court of Human Rights
4. Data Protection Act
5. Information Privacy Act

مخابرات، پذیرش و تداول بیشتری نسبت به مبحث مربوط به حریم خصوصی اطلاعات دارد؛ البته امروزه این حق با ظهور اشکال جدید مراسلات همچون پست الکترونیکی، ارتباطات ماهواره‌ای تلفن های بی‌سیم و امثال آن با مسائل جدیدتری روبه‌رو شده و توسعهٔ مضاعف یافته است. ازجمله مباحث قابل طرح ذیل این عنوان علاوه‌بر مصون‌بودن نامه‌ها و بسته‌های پستی از تفتیش و بازرسی، امنیت و مصونیت مکالمات تلفنی از شنود، محرمانه‌بودن قبوض و صورت‌حساب تلفن اشخاص که نشان‌دهندهٔ فهرست تماس‌های آن‌هاست، امنیت مراسلات داخل شبکهٔ دیجیتالی ازجمله اینترنت و شبکه‌های اینترنتی، همچنین درج یا عدم درج نام شخص و شماره تلفن متعلق به او در دفترچه‌های راهنمای تلفن هستند (محمد حسینی، ۱۳۹۸، ص ۲۸۱).

این نوع حریم خصوصی به ابعادی از محرمانگی و شخصی بودن ارتباطات افراد در جامعه اطلاق می‌شود. براساس قواعد حاکم بر این نوع حریم، هر شخصی در برخی از انواع ارتباطات فردی و اجتماعی خویش می‌تواند جنبه‌هایی از سرّی‌بودن روابط و ارتباطات را از جامعه انتظار داشته باشد؛ به‌نحوی که از دید عموم محفوظ مانده و افراد غیرمجاز حق تجسس و پایش و رهگیری آن‌ها را نداشته باشند. این نوع حریم شامل کلیهٔ انواع ارتباطات انسانی از قبیل پست عادی و پست الکترونیکی و مکالمات تلفنی، تلگراف و غیره می‌شود و یکی از نهادهای حقوقی سنتی است که از دیرباز به آن توجه می‌شده است. در این نوع حریم، قواعدی حاکم است که چگونگی ارتباطات متقابل اشخاص از طرق فیزیکی و الکترونیکی را تنظیم و تحت قاعده درمی‌آورد (اصلانی، ۱۳۸٤، ص ۲۸۷).

در سیستم‌های الکترونیکی و شبکه‌های اجتماعی نیز اطلاعات و ارتباطات فرد در حوزهٔ حریم خصوصی قرار می‌گیرد. این موارد شامل هویت کاربر، عکس‌ها و فیلم‌های ذخیره‌شده، ارتباطات با سایر اشخاص به هر شکل ازجمله پیام یا تماس می‌شود. بنابراین، حریم خصوصی در شبکه‌های اجتماعی عبارت است از حفظ اطلاعات و ارتباطات شخصی از دید عموم و سوءاستفاده‌نکردن از این اطلاعات و ارتباطات برعلیه کاربر؛ به این معنا که هر کاربر در شبکه‌های اجتماعی دارای اطلاعات و ارتباطات شخصی است که نباید برای همگان مشخص شود یا از آن سوءاستفاده کنند (خانمحمدی و همکاران ، ۱۳۹۵، ص ۸۵). با این اوصاف، ورای نگاه فلسفی به اصل حریم خصوصی، چگونگی مواجههٔ بازیگران عدالت کیفری با این حریم و حیطهٔ ورود به این حریم حتی در حالت تحقیقات مقدماتی حول رفتار مجرمانه اهمیت بسزایی دارد.

۲. حفاظت از حریم خصوصی ارتباطاتی و اطلاعاتی در اسناد بین‌المللی

اسناد بین‌المللی را در موضوع بحث می‌توان به دو دسته تقسیم کرد: دستهٔ اول اسنادی که عمدتاً قدیمی بوده و به‌طور کلی به رعایت حریم خصوصی اشاره کرده است. بند ۱۲ اعلامیهٔ جهانی حقوق بشر مصوب ۱۹۴۸[1]، مادهٔ ۵ پیمان‌نامهٔ بین‌المللی رفع هرگونه تبعیض نژادی مصوب ۱۹۶۵[2]، مادهٔ ۱۷ عهدنامهٔ بین‌المللی حقوق مدنی و سیاسی مصوب ۱۹۶۶[3]، بند ۱۸ کنوانسیون بین‌المللی حقوق بشر یا اعلامیهٔ تهران مصوب ۱۹۶۸[4]، مادهٔ ۱۱ کنوانسیون امریکایی حقوق بشر مصوب ۱۹۶۹[5]، مادهٔ ۹ معاهدهٔ شورای اروپا برای حفاظت از افراد در برابر پردازش خودکار داده‌های شخصی مصوب ۱۹۸۱[6]، مادهٔ ۱۸ اعلامیهٔ حقوق بشر اسلامی مصوب ۱۹۹۰[7] به رعایت حریم زندگی خصوصی، خانوادگی، منزل یا مکاتبات افراد اشاره کرده و دولت‌ها را از دخالت خودسرانه و غیرقانونی بر حذر داشته است.

علاوه‌بر موارد مذکور، برخی اسناد بین‌المللی به‌طور خاص به موضوع حریم خصوصی ارتباطاتی و داده‌های الکترونیکی اشاره دارد. برخی از این اسناد شامل مصادیق زیر است:

1. Universal Declaration of Human Rights
2. International Convention on the Elimination of All Forms of Racial Discrimination
3. Convention for the Protection of Human Rights and Fundamental Freedoms
4. International Conference on Human Rights or Tehran Declaration
5. American Convention on Human Rights
6. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
7. Cairo Declaration on Human Rights in Islam

۱) راهنمای حفاظت از دادهٔ اتحادیهٔ اروپا مصوب ۱۹۹۵[1] که نحوهٔ تدوین قوانین در حوزهٔ پردازش داده‌های شخصی شهروندان را در کشورهای عضو اتحادیهء اروپا مشخص می‌کند.

۲) دستورالعمل اتحادیهٔ اروپا در حمایت از اشخاص حقیقی در مقابل پردازش داده‌های شخصی و گردش آزاد داده مصوب ۱۹۹۵[2]. این دستورالعمل کشورهای عضو را موظف به حفظ حریم خصوصی پردازش داده‌های شخصی افراد دانسته است.

۳) دستورالعمل حریم خصوصی الکترونیکی مصوب ۲۰۰۲ که با هدف فراهم‌کردن امنیت فراهم‌کنندگان خدمات ارتباطی الکترونیکی همچون آی اس پی‌ها و نیز پیشگیری از پایش اطلاعات خصوصی افراد به‌دست اعضا ازطریق شنود مکالمات، نظارت فرانگاره‌ها و سایر اشکال جاسوسی ایجاد شده است. مطابق مادهٔ ٦ این دستورالعمل، فراهم‌کنندگان خدمات اینترنتی ملزم به پاک‌کردن داده‌های مربوط به ترافیک اینترنتی کاربران یا دست‌کم ذخیرهٔ گمنام آن هستند.

۴) دستورالعمل نگه‌داری داده‌های شخصی تولید و پردازش‌شده در چارچوب تأمین خدمات ارتباطی الکترونیکی مصوب ۲۰۰٦[3]. این دستورالعمل، که مشتمل بر ۱۷ ماده است، اصلاحاتی را در دستورالعمل سابق ملحوظ داشته است؛ ازجمله مشخص‌کردن داده‌هایی که قابلیت نگه‌داری دارند، دورهٔ نگه‌داری و وظایف نهادهای حاکمیتی بر نحوهٔ نگه‌داری این داده‌ها، جرایم ناقض حریم خصوصی در ارتباط با نگه‌داری داده‌های شخصی.

۵) اعلامیهٔ حقوق بشر سازمان ملل (بازبینی در سال ۲۰۱۳)[4]. در این سال، سازمان ملل به اتفاق آرا حق حفظ حریم خصوصی اطلاعاتی افراد را به‌منزلهٔ یکی از حقوق اساسی بشر پذیرفت. براین‌اساس، هرگونه ارتباطات برخط افراد مورد احترام بوده و حفظ می‌شود، قوانین ملی باید ضمن جلوگیری از تجاوز به حریم خصوصی انسان‌ها، با حق حفظ این حریم سازگاری داشته باشند و سازوکارهایی برای شفافیت عملکرد دولت‌ها در نظارت بر انتقال داده‌ها تعریف شود (sharwood, 2013).

۶) پارلمان و شورای اروپا در ۲۷ آوریل ۲۰۱٦ مقررات حمایت از داده‌های اشخاص را به تصویب رساندند.[5] مطابق مادهٔ ۱ و ۲ این مقرره، حمایت از اشخاص حقیقی در رابطه با پردازش داده‌های شخصی حقی اساسی است و صرف‌نظر از ملیت و محل سکونت آنان باید به‌رسمیت شمرده شود.

۷) مقررات پردازش داده‌های شخصی توسط نهادها و مؤسسات، مصوب اکتبر ۲۰۱۸ که در آن قواعد حفاظت از داده‌ها توسط مؤسسات اتحادیهٔ اروپا و نیز وظایف سرپرست حفاظت از داده‌های اتحادیهٔ اروپا را تعیین کرده است؛ همچنین در حوزهٔ انتظامی و قضایی نیز در می ۲۰۱۸ دستورالعمل حفاظت از اشخاص نسبت به پردازش داده‌های شخصی در مسائل جنایی تصویب شد.

البته باید اذعان کرد که مصوبهٔ ۲۰۱٦ اتحادیهٔ اروپا (GDPR) در مقایسه با سایر اسناد مشابه اتحادیهٔ اروپا و نیز سایر اسناد بین‌المللی از جنبهٔ ایجاد وحدت رویهٔ قانونی، پیش‌بینی ابزارهای نوآورانه در راستای حفاظت حداکثری از داده‌های شخصی، حمایت‌های فرامرزی، موضوع داده‌های شخصی حساس و... پیشرفت شایان توجهی داشته است.

نتیجهٔ آن که در دو دههٔ اخیر، اسناد بین‌المللی در راستای گسترش مفهوم حریم خصوصی گام نهاد البته رویکرد امنیت محوری در حقوق کیفری و نگرانی‌ها به‌منظور اقدامات تروریستی تا حد زیادی میان آرمان‌گرایی‌های این اسناد و عمل‌گرایی دولت‌ها فاصله انداخته است و با وجود

1. EU Data Protection Directiv
2. EU Directive on the protection of natural persons against processing Personal data and free circulation of data
3. DIRECTIVE 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks
4. United Nations Declaration of Human Rights (revision in 2013)
5. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

تأکید این اسناد و استفاده از فنّاوری‌هایی مثل رمزنگاری، افزایش‌دهنده‌های حریم خصوصی[1] و ناشناس‌کننده[2] اما نمی‌توان ادعا کرد که این حریم نقض نمی‌شود؛ چنان‌که مدیر پیشین بخش اطلاعاتی یونسکو نکات تکان‌دهنده‌ای را درخصوص دخالت کشورهای غربی در نقض حریم خصوصی افراد مطرح کرده است. به اذعان ایشان امریکا با همکاری انگلیس، کانادا، استرالیا و نیوزلند از شبکه‌های اطلاعاتی در اختیارشان برای شنود، کنترل و پردازش اطلاعات روزانه بیش از سه‌میلیارد پیام تلفنی، دورنگار و پست الکترونیکی در سراسر دنیا استفاده می‌کند (معتمدنژاد ،۱۳۸٤، ص ۳۳۳).

۳. اصول حاکم بر تحقیقات از حریم خصوصی اطلاعات و ارتباطات

فرایند بررسی ادلهٔ الکترونیکی به‌طور کلی شامل چهار مرحله است:

۱) کشف و جمع‌آوری اطلاعات[3]؛ ۲) نگه‌داری[4] از داده‌ها؛ ۳) پالایش[5] اطلاعات و درنهایت ارائهٔ داده‌ها به مرجع قضایی[6] دقت در این مراحل، این معنا را متبادر به ذهن می‌سازد که پیش‌بینی‌نکردن سازوکارهای دقیق زمینه نقض این حریم خصوصی را حتی بسیار بیش از سایر مصادیق فراهم می‌سازد.

مادهٔ ۱۲ قانون تجارت الکترونیکی مقرر می‌دارد: اسناد و ادلهٔ اثبات دعوی ممکن است به‌صورت داده پیام بوده و در هیچ محکمه یا ادارهٔ دولتی نمی‌توان براساس قواعد ادلهٔ موجود، ارزش اثباتی «داده پیام» را صرفاً به‌دلیل شکل و قالب آن رد کرد. این ماده به‌نوعی از مادهٔ ۱۹ قانون نمونهٔ آنسیترال درخصوص تجارت الکترونیکی[7] اقتباس شده است. زمانی که قانون‌گذار چنین ادله‌ای را به‌رسمیت می‌شناسد، طبعاً باید اصول اساسی رعایت حقوق متهم و حریم خصوصی وی در این حوزه مورد توجه قرار گیرد. در ذیل به بررسی این اصول می‌پردازیم.

۱) اصل قانونی‌بودن تحقیقات از داده‌های اطلاعاتی ـ ارتباطاتی:

اصل اولیه در تحقیقات، ممنوعیت تجسس و تفتیش به‌منظور اثبات جرم یا عدم تحقق جرم است و مادامی که ادلهٔ کافی بر اثبات تبهکاری نیست انکار پذیرفته می‌شود. بااین‌حال در حق‌الناس و به‌منظور عدم تضییع حقوق مردم و درصورت وجود ادلهٔ کافی مبنی‌بر احتمال تحقق جرم، امکان انجام تحقیق میسور است، اما درهرحال حیطهٔ عملکرد مقامات تحقیق باید منطبق بر قانون باشد. از همین روی، اصل ۵۲ قانون اساسی بیان داشته است: بازرسی و نرساندن نامه‌ها، ضبط و فاش‌کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هرگونه تجسس ممنوع است؛ مگر به حکم قانون. مصادیق مذکور در این اصل اصولاً به حریم خصوصی ارتباطاتی مربوط است.

در نظام‌های حقوقی گوناگون نقض این حریم خصوصی با دو شیوه پاسخ داده می‌شود:

اول: مطابق مقرره‌های سنتی که به‌طور کلی حریم خصوصی افراد را حمایت کرده است مثل منع افشای اسرار یا شنود غیرقانونی.

دوم: مقرره‌هایی که به‌طور خاص ناظر به فنّاوری اطلاعات و فضای مجازی است. در حقوق ایران، هر دو رویکرد ملاحظه می‌شود.

قانون مجازات اسلامی در مادهٔ ۵۸۲ بخش تعزیرات ضمانت اجرای کیفری موضوع را بیان داشته است. این مواد به‌منظور عدم شمول به‌تمامی مصادیق حریم خصوصی نقص دارد؛ از همین روی ماده ۳۷ منشور حقوق شهروندی برای تعمیم موضوع به تمامی مصادیق تفتیش، گردآوری، پردازش، به‌کارگیری و افشای نامه‌ها اعم از الکترونیکی و غیر الکترونیکی، اطلاعات وداده‌های شخصی و نیز سایر مراسلات پستی و ارتباطات از راه دور نظیر ارتباطات تلفنی، نمابر، بی‌سیم و ارتباطات اینترنتی خصوصی و مانند این‌ها را ممنوع اعلام کرد؛ مگر به موجب قانون.

1. privacy-enhancing technologies (PET)
2. Anonymizing
3. Discovery and collection
4. Preservation
5. Filtering
6. Providing information to the court
7. UNCITRAL Model Law on Electronic Commerce with Guide Enactment 1996

مادهٔ ۳۶ این منشور نیز تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی را به موجب قانون و با فرض ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم پذیرفت.

این منشور از این منظر که قوهٔ مجریه تنظیم کرده جنبهٔ الزام‌آور نداشته و فاقد ضمانت اجراست. بااین‌حال، مادهٔ ۴۸ قانون جرایم رایانه‌ای برای رفع این نقیصهٔ شنود، محتوای درحال انتقال ارتباطات غیرعمومی را در سامانه‌های رایانه‌ای می‌پذیرد و رعایت مقررات شنود مکالمات تلفنی را بر آن ضروری می‌داند. تبصرهٔ این ماده حتی دسترسی به اطلاعات غیرعمومی نظیر پست الکترونیکی و پیامک را در حکم شنود دانسته است. اهمیت توجه خاص به رعایت اصل قانونی‌بودن حریم خصوصی در این حوزه به ماهیت آن باز می‌شود؛ چراکه به‌منظور طبیعت باز شبکهٔ راه برای نیروهای پلیس آنچنان هموار است که بدون داشتن حکم بازرسی می‌توانند افراد را تحت کنترل درآورند (احمدی، ۱۳۸۷، ص ۱۰۱) و این امر تجاوز به حریم خصوصی اطلاعاتی و ارتباطاتی را تسهیل می‌کند و رکن محرمانگی[1] داده‌ها نقض می‌شود.

با توجه به مواد قانونی مطروحه، داده‌های شخصی منحصراً باید ازطریق ابزارهای قانونی و منصفانه و با اطلاع و رضایت افراد به‌دست آیند و محدودیت‌هایی در جمع‌آوری این داده‌ها لحاظ شود. در موضوع داده‌های ارتباطاتی به‌دلیل تنوع و پراکندگی اطلاعات مسئلهٔ چگونگی کشف و جمع‌آوری این ادله در مقایسه با ادلهٔ سنتی متفاوت است و قانون‌گذار تا حد زیادی به افتراقی‌سازی در این مقوله توجه کرده است.

۲) اصل سرعت در تحقیقات

متهم در مواجهه با اتهام انتسابی به‌نوعی دچار تحیر و سرگردانی و نگرانی از آینده است؛ بنابراین سرعت در انجام تحقیقات و تعیین تکلیف وی یکی از اصول دادرسی منصفانه است. اصل ۳۲ قانون اساسی به این حق اشاره کرده است و مواد ۳، ۳۴، ۳۵ و ۱۸۹ قانون آیین دادرسی کیفری بر این امر تأکید مؤکد دارد.

اصل سرعت در تمامی جریان دادرسی اعمال می‌شود؛ هرچند تحقیقات مقدماتی بیشترین تأثیر را در تحقق این اصل دارد. معنای این اصل آن است که دادرسی گام سریعی را بردارد، بدون این‌که به حقوق اساسی افراد و نظم عمومی و قضایی لطمه بزند (خزایی، ۱۳۷۷، ص ۱۴۳).

توجه به این اصل در حوزهٔ تحقیق از داده‌های ارتباطاتی و اطلاعاتی علاوه‌بر نکات مذکور، از این منظر اهمیت دارد که در بررسی داده‌های ارتباطاتی زمان حائز اهمیت است؛ چرا که داده‌ها در کمترین زمان پس از تحقق جرم، قابل حذف، جابه‌جایی و تغییر ماهیت هستند و مجرم با اقداماتی می‌تواند کشف جرم را با مشکل مواجه سازد. در این موارد یکی از راهکارها آن است که همان‌گونه که به ضابطان در حوزهٔ جرائم مشهود اختیارات وسیعی داده شده است به آن‌ها اختیارات وسیع‌تری داده شود و حق مداخلهٔ فوری را داشته باشند. این موضوع هرچند به جلوگیری از تلف یا تغییر داده‌ها کمک می‌کند، اما به‌شدت حریم خصوصی افراد را به خطر می‌اندازد و خوف آن می‌رود که مقامات تحقیق به بهانهٔ این امر بدون ضابطه، تمامی داده‌های ارتباطاتی و اطلاعاتی متهم را بررسی کنند. راهکار در این عرصه حفظ داده‌ها بدون بررسی آن‌ها تا زمان مداخلهٔ مقام قضایی است.

۳. اصل استنادپذیری داده‌ها به متهم

قابلیت استنادپذیری داده‌ها دشوار است؛ چراکه انتساب این داده‌ها به فرد مظنون یا متهم نیاز به دقت نظرهای تخصصی دارد. دلیل این امر ها نیازمند نیروی ماهر و ابزارهای پیشرفته است. این موضوع در داده‌های الکترونیکی آن است که هرگونه تغییر در داده‌ها آسان است و شناسایی آن تر خواهد بود. بنابراین، شناخت هویت پدیدآورنده امری اساسی برخط، که امکان دسترسی و مداخلهٔ افراد زیادی در آن‌ها متصور است، جدی است؛ زیرا یکی از ویژگی‌های این ادله ناشناختگی[2] است. در فضای الکترونیکی، فعالیت‌های متعددی انجام می‌پذیرد که امکان انتساب دلیل به پدیدآورنده را مشکل می‌سازد؛ برای مثال صرف ارسال متن یا صوت در چنین فضایی، دلیل بر انتساب آن به فرد خاصی نیست؛ البته اصل بخش نیست. از همین روی، در کنندهٔ محتوا یا داده است و این قرینهٔ خوبی است؛ اما اطمینان‌اولیه آن است که صاحب محیط یا صفحه ایجاد

1. Confidentiality
2. Anonymity

برخی موارد مقامات پلیس برای شناسایی هویت صاحب داده در فضای مجازی، بدون اذن مقام قضایی ورود غیرمجاز انجام می‌دهند و حتی در برخی صور پیام‌های اخطار به صفحات خصوصی افراد صورت می‌گیرد که این امر با قواعد دادرسی کیفری مغایر است.

٤. اصل محدودیت جمع‌آوری[1]:

در سیستم‌های ارتباطاتی، میلیون‌ها اطلاعات مرتبط و غیرمرتبط وجود دارد؛ حتی امروزه جمع‌آوری اطلاعات به صنعتی کوچک مبدل شده است (Brown, 2006, p. 12) و مؤسساتی در این عرصه فعالیت می‌کنند. این موضوع هرچند بررسی و کشف جرایم را با هزینهٔ کمتر میسور می‌سازد (Taipale, 2003)، اما به‌شدت تسهیلگر دخالت در حوزهٔ خصوصی افراد خواهد بود. همچنین ورود ارائه‌دهندگان خدمات اینترنتی به این حوزه و تلقی آنان در مقام نمایندهٔ حکومت[2] در بحث جمع‌آوری اطلاعات نیز همین اثر را در پی خواهد داشت. مطابق بند ۱ و ۲ کنوانسیون اروپایی حقوق بشر، صرف ذخیره‌سازی اطلاعات مربوط به حریم خصوصی افراد ناقض اصل حق احترام به زندگی اشخاص است؛ لذا در برخی پرونده‌ها مانند شکایت آمان بر علیه دولت سوییس ذخیره‌سازی اطلاعات تماس شاکی با سفارت روسیه ازطریق سرویس اطلاعاتی سوییس ناقض مواد ۱ و ۲ کنوانسیون قلمداد شد و دادگاه اروپایی حقوق بشر این کشور را محکوم کرد[3].

مادهٔ ۳۲ قانون جرایم رایانه‌ای به وظیفهٔ ارائه‌دهندگان خدمات اینترنتی در این حوزه اشاره کرده است و مادهٔ ۳۵ نیز امکان در اختیار قرار دادن این اطلاعات به مقام قضایی و نه ضابطان را مورد توجه قرار داده است؛ بااین‌حال اجازهٔ دسترسی و تحقیق از این اطلاعات بدون تعیین چارچوب و مصادیق آن ناقض حق بر حریم خصوصی است؛ بنابراین تأکید مضاعف بر اصل محرمانگی اطلاعات و دخالت‌نکردن در حوزه‌های غیرمرتبط موضوعی انکارناپذیر است.

در مواردی که به‌طور کلی امکان تحقیق و بازرسی از متهمان وجود دارد رعایت اصل گردآوری قانونی و منصفانهٔ داده‌ها امری ضروری است. در این راستا، استفاده از داده‌کاوی[4] با فنّاوری هوش مصنوعی[5] (taniar, 2008, p. 119)، که بدون دخالت انسان موضوعات مرتبط با جرم احصا و از دخالت در داده‌های بی‌ارتباط اجتناب می‌شود، شیوهٔ معقولی است.

٥. اصل محدودیت بهره‌برداری[6]:

براین‌اساس، داده‌های شخصی فقط به‌منظور اهداف مشخص‌شده در دسترس خواهند بود. در غیر این موارد، رضایت مالک داده یا نهادهای قانونی اخذ می‌شود. در این راستا، مادهٔ ٥٦ آیین دادرسی کیفری مقرر داشته است: ضابطین دادگستری مکلف‌اند طبق مجوز صادره عمل نمایند و از بازرسی اشخاص اشیا و مکان‌های غیرمرتبط با موضوع خودداری کنند. همچنین مطابق مادهٔ ۵۷ این قانون، چنانچه ضابطان دادگستری در هنگام بازرسی از محل، ادله، اسباب و آثار جرم دیگری را که تهدیدکنندهٔ امنیت و آسایش عمومی جامعه است مشاهده کنند، ضمن حفظ ادله و تنظیم صورت‌مجلس، بلافاصله مراتب را به مرجع قضایی صالح گزارش و وفق دستور وی عمل می‌کنند.

درخصوص اسناد و اشیایی که ماهیت مجرمانه ندارند، دو ماده صراحتاً نظر بر عدم مداخله دارد، اما در مواردی که این مصادیق ماهیت مجرمانه دارند اما به جرم فعلی ارتباطی ندارند چگونه باید برخورد کرد و آیا ضابطان باید آن را صورت‌جلسه کنند و طبق نظر مقام قضایی عمل کنند یا اساساً حق مداخله در این مصادیق را ندارند. به‌نظر می‌رسد جز در مواردی که موضوع به امنیت و آسایش عمومی مربوط است، در سایر موارد نه‌فقط وظیفه‌ای در مداخله ندارند، بلکه اساساً چنین حقی نیز برای آنان متصور نیست.

بند ۸ ماده واحدهٔ قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی بیان داشته است: بازرسی‌ها و معاینات محلی برای دستگیری متهمان فراری یا کشف آلات و ادوات جرم براساس مقررات قانونی و بدون مزاحمت و در کمال احتیاط انجام شود و از تعرض به اسناد و مدارک

1 . Collection Limitation Principle
2. Agency of state
3. Amann V. Switzerland, 2000
4. Data mining
5. Artificial intelligence
6. Use limitation Principle

و اشیایی که ارتباطی به جرم نداشته یا به متهم تعلق ندارند و افشای مضمون نامه‌ها و نوشته‌ها و عکس‌های فامیلی و فیلم‌های خانوادگی و ضبط بی‌مورد آن‌ها خودداری شود.

فرمان هشت‌ماده‌ای امام خمینی، که در ۲۴ آذر ۱۳۶۱ صادر شد، با صراحت بیشتری بر این امر تأکید کرد که هیچ‌کس حق ندارد به خانه یا مغازه و یا محل کار کسی، بدون اذن صاحبشان وارد شود یا کسی را جلب کند، یا به نام کشف جرم یا ارتکاب گناه تعقیب و مراقبت کند و یا به فردی اهانت کند و اعمال غیرانسانی اسلامی مرتکب شود، یا به تلفن یا نوار ضبط صوت دیگری به نام کشف جرم یا کشف مرکز گناه گوش کند و یا برای کشف گناه و جرم، هرچند گناه بزرگ باشد، شنود بگذارند و یا دنبال اسرار مردم باشند و تجسس از گناهان غیر کند یا اسراری که از غیر به او رسیده ولو برای یک نفر فاش کند (امام خمینی، ۱۴۰۳ق، ص ۱۳۹).

درخصوص موضوع چند نکته حائز اهمیت است: اولاً مشروط‌ساختن موضوع مادهٔ ۵۷ به عبارات مبهمی مانند مصلحت عمومی و امنیت بدون تعیین مصادیق در عمل معیار شخصی مقام تحقیق و تعقیب را جایگزین معیار نوعی می‌کند و باب نقض حریم خصوصی را باز می‌کند. ثانیاً در بحث حریم خصوصی داده های ارتباطی به دلیل آشکار نبودن محتوای داده تا زمانی که نقض حریم خصوصی صورت نگیرد تشخیص موارد خلاف امنیت و مصلحت عمومی میسور نیست؛ برای مثال مقام قضایی یا ضابطان تا محتویات داده‌ها را بررسی نکنند نمی‌توانند تحقق شرط مدنظر را تشخیص دهند؛ بنابراین نقض حریم خصوصی در این موارد حتمی است.

مادهٔ ۱۴۶ قانون آیین دادرسی کیفری نیز مقرر می‌دارد: از اوراق، نوشته‌ها و سایر اشیای متعلق به متهم فقط آنچه درباره‌ی جرم است تحصیل و درصورت لزوم، به شهود تحقیق ارائه می‌شود. بازپرس مکلف است درمورد سایر نوشته‌ها و اشیای متعلق به متهم با احتیاط رفتار کند موجب افشای مضمون و محتوای غیرمرتبط آن‌ها با جرم نشود؛ در غیر این صورت وی به جرم افشای اسرار محکوم می‌شود. با وجود صراحت این ماده و لزوم اتخاذ تدابیر مقتضی برای حفظ حریم داده‌های بی‌ارتباط با جرم اما مادهٔ ۴۳ قانون جرایم رایانه‌ای امکان گسترش دامنهٔ تفتیش و توقیف را به سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارد پذیرفته است. این امر هرچند با دستور قضایی صورت می‌گیرد، اما به‌دلیل گسترهٔ ورود به سایر داده‌ها و عدم اطلاع مقام قضایی از حجم و ماهیت این موارد ضروری است این مقام دلایل صدور دستور تفحص از سایر داده‌ها و نیز گسترهٔ آن را دقیقاً مشخص کند.

۶. اصل تدابیر حفاظتی امنیتی[1]:

در برابر خطراتی مانند دسترسی غیرمجاز، تخریب یا افشای غیرقانونی داده‌ها باید تدابیر امنیتی معقولی اتخاذ شوند. مادهٔ ۳۴ قانون جرایم رایانه‌ای مقرر داشته است: هرگاه حفظ داده‌های رایانه‌ای ذخیره‌شده برای تحقیق یا دادرسی لازم باشد، مقام قضایی می‌تواند دستور حفاظت از آن‌ها را برای اشخاصی که به‌نحوی تحت تصرف یا کنترل قرار دارند صادر کند. در شرایط فوری، نظیر خطر آسیب‌دیدن یا تغییر یا ازبین‌رفتن داده‌ها، ضابطان قضایی می‌توانند رأساً دستور حفاظت را صادر کنند و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضایی برسانند. این تدبیر از این روی حائز اهمیت است که مادهٔ ۱۴ قانون تجارت الکترونیکی به شرطی برای اطلاعات ارتباطاتی اعتبار اسناد معتبر و قابل استناد در مراجع قضایی قائل است که کلیهٔ داده پیام‌ها به طریقی مطمئن ایجاد و نگه‌داری شده باشند. بند ۲ این قانون نیز سیستم مطمئن را برمی‌شمرد. فارغ از سازوکارهایی که به یک داده پیام جنبهٔ اطمینان‌بخش می‌دهد رویکرد قانون‌گذار در سپردن اختیار حفاظت از داده‌ها، حتی بدون اذن مقام قضایی، زمینهٔ ورود به حریم خصوصی افراد را فراهم می‌سازد؛ چراکه ضابطان قضایی و مقام تحقیق برای آن‌که ادلهٔ تحصیل‌شده قابلیت استناد را داشته باشند به تمامی ابزارهای لازم برای حفظ این ادله تمسک می‌جویند. برای پیشگیری از این آسیب، می‌توان از ایمن‌سازی اطلاعات با استفاده از بیومتریک بهره جست. این شیوه یکی از تدابیری است که تاحد زیادی ضمن حفظ حریم خصوصی افراد، امنیت اطلاعات ارتباطاتی را تضمین می‌کند و دسترسی افراد غیرمجاز را به اطلاعات اشخاص محدود می‌سازد. این روش داده‌هایی از اشخاص را به‌طور خودکار و با توجه به الگوی عمومی دریافت و درصورت نیاز آن را پردازش و تحلیل می‌کند تا بتواند در جامعهٔ آماری بزرگ‌تر، افراد را از یکدیگر متمایز سازد و مانع

1. Security Safeguards Principle

از سرقت اطلاعات یا جعل آن یا دسترسی غیرمجاز به داده‌ها و اطلاعات اشخاص شود و ازاین‌رو، از امنیت افراد حمایت کند (موذن‌زادگان و همکاران، ۱۳۹٤، ص۸۱). نکتهٔ دیگر درخصوص موضوع، انتقال فرامرزی داده‌ها میان کشورهای مختلف و چالش‌های آن است. این امر تا این حد جدی بوده است که دیوان دادگستری بین‌المللی توافقنامهٔ بندگاه امن میان اتحادیهٔ اروپا و امریکا را نامعتبر دانست؛ بنابراین در سال ۲۰۱٦، اتحادیهٔ اروپا توافقنامهٔ حامی حریم خصوصی را به تصویب رسانید. براساس آن، سازمان‌ها و شرکت‌هایی که قصد پردازش و ذخیره‌سازی داده‌های افراد شاغل در اتحادیهٔ اروپا را دارند باید مقررات عمومی حمایت از دادهٔ اتحادیه اروپا را رعایت کنند (Calder, 2016). این مقرره هرچند تدابیر حفاظتی داده‌ها و قابلیت استناد آن‌ها را در اتحادیهٔ اروپا تاحد زیادی حل می‌کند، اما همچنان در عرصهٔ بین‌المللی خلأ وجود سندی جامع درخصوص انتقال، اصول حفاظتی و قابلیت استناد داده‌های فرامرزی احساس می‌شود.

۷. اصل شفافیت[1] و مشارکت فردی[2]:

اصل شفافیت به معنای توضیح‌پذیری، بازبودن و قابلیت دسترسی و مشاهدهٔ روندها و داده‌هاست (Felzmann, 2020). مطابق اصل مشارکت فردی نیز هر فرد باید این حق را داشته باشد که تصدیقی از کنترل‌کننده‌ها به‌دست آورد که این کنترل‌کننده داده‌های وی را در اختیار دارد یا خیر. ازجمله موضوعاتی که سازمان همکاری و توسعهٔ اقتصادی[3] (OCDE)[4] پیشنهاد کرده دو اصل ذکرشده است. براساس این اصول، باید مشخص شود که چه نهادی و با چه هدفی داده‌های شخصی را در اختیار دارد و چگونه از آن استفاده می‌کند و این اطلاعات به چه میزان نگه‌داری می‌شوند. در این راستا، مادهٔ ۳۷ قانون جرایم رایانه‌ای مقرر می‌دارد: تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به‌نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه‌ها، انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

این ماده نمی‌تواند به طور کامل دو اصل شفافیت و مشارکت فردی را محقق سازد؛ چراکه اولاً صرف حضور متصرف، مقامات تحقیق را ملزم نمی‌سازد که حیطهٔ تفتیش را برای وی مشخص سازند؛ ثانیاً قانون‌گذار امکان تفتیش بدون حضور متصرف را با دستور مقام قضایی پذیرفته است؛ بدون آن‌که چارچوب موضوع و مصادیق روشن شود؛ ثالثاً امکان اعتراض به این تصمیم قاضی پیش‌بینی نشده است. به همین منظور، استفاده از هوش مصنوعی به‌مثابهٔ ابزار تحقیقات (مصطفوی اردبیلی و همکاران، ۱٤۰۱، ص ٥٦) می‌تواند کمک شایانی در موضوع شفافیت تحقیقات کند؛ چراکه از اقدامات خودسرانهٔ ماموران تحقیق پیشگیری به عمل می‌آورد و حوزه‌های دخالت سامانه در داده پیام‌های افراد کاملاً مشخص می‌شود.

۸. منع دام‌گستری در اخذ داده‌ها

یکی از شیوه‌هایی که به این منظور برای کشف جرم استفاده می‌شود دام‌گستری است. از منظر فقهی، با توجه به اصل صیانت از کرامت انسانی و حقوق متهم، رعایت حریم خصوصی افراد و نیز شأن سیستم قضایی در به‌کارگیری ابزارهای مشروع در تحصیل دلیل اصل اولیهٔ منع استفاده از چنین ابزارهایی است؛ خاصه آن‌که در سیاست جنایی اسلام در حقوق الناس رویکرد ترویج گذشت و در حقوق الله بحث خطاپوشی و تشویق به توبه و ستر گناه چنین اقتضایی دارد.

از منظر قضای اسلامی، در کتب فقهای متقدم، در نفی یا تأیید چنین شیوه‌هایی بیانی ملاحظه نمی‌شود. بااین‌حال، روایتی از امام سجاد (ع) نقل شده است که حضرت پس از آن‌که شنیدند همسرشان به امیرالمومنین(ع) ناسزا می‌گوید برای اطمینان در خانه مخفی شدند و پس از احراز صحت این امر وی را طلاق دادند (کلینی، ۱٤۰۷ق، ص ۳٥۱؛ حرعاملی، ۱٤۰۹، ص ٥٥۱). این روایت در بسیاری از کتب روایی

1. Openness Principle
2. Individual Participation Principle
۳. این سازمان را کشورهای غربی در سال ۱۹٦۰ تاسیس کردند و بعدها با پیوستن کشورهایی مانند ژاپن، کرهٔ جنوبی، مکزیک و فنلاند به سی کشور افزایش یافت. مأموریت‌های این سازمان ترویج سیاست‌هایی است که رفاه اقتصادی و اجتماعی را در سراسر جهان بهبود بخشد. این نهاد هرچند بر مسائل اقتصادی متمرکز است، اما در حوزه‌های اجتماعی و محیط زیست نیز وارد شده است. سازمان در موضوع حفاظت از حریم خصوصی شهروندان در فضای مجازی اصولی را پیشنهاد کرده است.
4. Organization for Economic Cooperation and Development

نقل شده است و از نظر سندی نیز بر آن خدشه‌ای وارد نیست، اما از آن نمی‌توان جواز دام‌گستری را استنباط کرد؛ زیرا امام (ع) اقدامی برای تحریک مرتکب انجام ندادند، بلکه تنها نظاره‌گر موضوع به‌نحو پنهانی بودند. علاوه‌براین، در مشی ائمه اطهار مواردی از نظارت به‌نحو مخفیانه نسبت به عملکرد کارگزاران حکومتی (حمدبن‌حسین شریف‌الرضی، حکمت ۳۳) یا استفاده از جاسوس در جنگ‌ها دیده می‌شود (طبسی، ۱۳۹۳، ص ۹۳)، اما از این مصادیق نیز نمی‌توان جواز دام‌گستری در تحصیل دلیل را استنباط کرد؛ زیرا به‌دلیل قاعدهٔ مصلحت و دفع افسد به فاسد چنین مواردی ب نحو محدود پذیرفته شده است.

قوانین ایران نیز در این خصوص ساکت است و همین امر به نوعی سبب تشتت رویه در موضوع شده است.

درخصوص موضوع حریم خصوصی اطلاعاتی و ارتباطاتی ضابطان در راستای کاهش فعالیت مجرمانه در شبکه‌های گپ هم‌زمان، اغلب تلاش می‌کنند تا با جازدن خود به‌منزلهٔ کودک یا شریک مجرم، اعتماد آن‌ها را جلب کنند. این رهیافت هرچند اصولاً به دستگیری مرتکبان می‌انجامد، اما از این روی مورد انتقاد قرا می‌گیرید که مأموران افراد روی شبکه‌های آی آر اس را فریب داده‌اند و چه‌بسا اساساً قصد ارتکاب جرم را نداشته‌اند، اما این فریب منتهی به دستگیری آنان شد. در برخی مواقع، حقوقدان‌ان شبهه در وجود عنصر معنوی در مجرم را مطرح کرده‌اند (Casey, 2011, p. 160).

نکته‌ای که به‌نوعی با حریم خصوصی مرتبط می‌شود آن است که جست‌وجو در این عرصه، معمولاً با هزاران منبع و داده که بسیاری از آن‌ها ارتباط مستقیمی با بزهکار ندارند انجام می‌شود و مأموران لامحاله مجبور خواهند بود با استفاده از زبان پایگاه داده‌ای یا موتورهای جست‌وجو به پالایش بپردازند و همین امر ضابطان را به ورطه‌هایی سوق می‌دهد که برای جازدن خود در مقام فرد دارای ویژگی‌های مدنظر بزهکار باید حریم خصوصی برخی از افراد را نقض کنند؛ مانند استفاده از پست الکترونیکی شخص ثالث.

نتیجه‌گیری

اصل اولیهٔ منع تعرض به حریم خصوصی داده‌های ارتباطاتی و اطلاعاتی افراد است و این مهم مورد تأکید مبانی فقهی و اسناد بین‌المللی است. بااین‌حال دولت‌ها در دوگانهٔ امنیت و حریم خصوصی، برتری را به امنیت داده و درصددند به طرق مختلف این حریم را به بهانهٔ نظم عمومی نقض کنند. این رویکرد در بحث تحقیقات مقدماتی بیش از پیش امکان تحقق دارد و البته پیشرفت‌های بشری و استفاده از فضای مجازی و اینترنت این موضوع را تسهیل می‌کند. در حقوق ایران، به‌رغم تصویب قوانینی مانند مجازات جرایم رایانه‌ای و تجارت الکترونیکی، فقدان قانون اختصاصی مرتبط با حریم خصوصی با توجه به پیشرفت‌های حوزهٔ سایبر و فضای مجازی ملموس است.

در این پژوهش، اصول حاکم بر تحقیقات از حریم خصوصی اطلاعات و ارتباطات بیان شد؛ برخی از اصول مورد تأکید مثل اصل قانونی‌بودن، اصل تسریع در فرایند تحقیق، اصول کلی در تحقیقات مقدماتی هستند؛ بااین‌حال تأکید مجدد ازاین‌روی است که در این موارد نیز به‌دلیل وضعیت خاص داده‌های ارتباطاتی و اطلاعاتی افتراقی‌سازی دادرسی و تأکید مؤکد امری بایسته است.

با توجه به موضوع‌های مطروحه پیشنهاد می‌شود:

۱) تدوین قانون مستقل و جامع درخصوص حریم خصوصی و عدم واگذاری احصا موارد خاص نقض حریم خصوصی داده‌های ارتباطاتی به مقام قضایی؛

۲) ارائهٔ تعریفی جامع و مانع از حریم خصوصی و تحدید مواردی که امکان تحقیق و تفتیش ضابطان از این حریم وجود دارد؛

۳) با وجود پیش‌بینی ضمانت اجرای کلی برای نقض حریم خصوصی، مادامی که وضعیت ادله‌ای که با تجسس غیرقانونی از حریم خصوصی ارتباطاتی و اطلاعاتی افراد به‌دست می‌آید مشخص نشود امکان نقض آن کماکان متصور است؛

۴) در تحقیق از داده‌های ارتباطاتی و اطلاعاتی اتخاذ تدابیری چون بهره‌گیری از هوش مصنوعی و بیومتریک، که دخالت انسان را به حداقل رسانیده و مصادیق غیرمرتبط حذف می‌شود، امری ضروری است.

منابع

احمدی، احمد (۱۳۸۷). نقض حریم خصوصی، چالشی فراروی پیشگیری وضعی از جرم. فصل‌نامهٔ مطالعات پیشگیری از جرم، ۳(۶)، ۷۷-۱۰۸.

اصلانی، حمیدرضا (۱۳۸۴). حقوق فناوری اطلاعات. تهران: نشر میزان.

امام خمینی، روح الله (۱۴۰۳ق). صحیفهٔ نور. تهران: مؤسسهٔ تنظیم و نشر آثار امام خمینی.

بعلبکی، روحی (۱۹۹۵). المورد. بیروت: دارالعلم للملایین.

حرعاملی، محمد (۱۴۰۹ق). وسایل‌الشیعه. قم: مؤسسهٔ آل‌البیت.

خانمحمدی، کریم و شاملی، علی‌اکبر (۱۳۹۵). اخلاق اسلامیِ حریم خصوصی در شبکه‌های اجتماعی سایبر. نشریهٔ اسلام و مطالعات اجتماعی، ۴(۱۴)، ۸۰-۱۰۳. https://doi.org/10.22081/jiss.2016.22417

خزایی، منوچهر (۱۳۷۷). بررسی نظری و عملی ضرورت تسریع در آیین دادرسی کیفری، فرآیند کیفری (مجموعه مقالات). تهران: انتشارات گنج دانش.

رحیم خویی، الناز و رستم‌زاده، حسین (۱۳۹۶). تحلیل و نقد عملکرد دیوان اروپایی حقوق بشر در برخورد با ادعاهای نقض مادهٔ۸ کنوانسیون اروپایی حقوق بشر، مجلهٔ حقوقی بین‌المللی، ۳۴(۵۶)، ۲۶۳-۲۸۹. https://doi.org/10.22066/cilamag.2017.25173

سروش، محمد (۱۳۹۳). مبانی حریم خصوصی. تهران: انتشارات سمت.

طبسی، نجم‌الدین (۱۳۹۳). مبانی فقهی جاسوسی و ضدجاسوسی. قم: انتشارات مرکز تخصصی ائمه اطهار علیه السلام.

کلینی، محمد (۱۴۰۷ ق). الکافی. تهران: دارالکتب الاسلامیه.

محمدبن‌حسین شریف‌الرضی (۱۳۹۷). نهج البلاغه: سخنان، نامه‌ها و حکمت‌های امیرالمومنین امام علی‌بن ابی‌طالب (ع). ترجمهٔ سیدمحمدمهدی جعفری. تهران: انتشارات ذکر.

محمدحسینی، عباس (۱۳۹۸). اهمیت تفتیش و بازرسی در دادرسی‌های کیفری با تأکید بر احترام به حریم خصوصی اشخاص در اسناد بین‌المللی و حقوق داخلی ایران. نشریهٔ مطالعات حقوق شهروندی، ۵(۱۰)، ۲۵۲-۲۸۹.

مصطفوی اردبیلی، سید محمدمهدی، تقی‌زاده انصاری، مصطفی و رحمتی‌فر، سمانه (۱۴۰۱). کارکردها و بایسته‌های هوش مصنوعی از منظر دادرسی منصفانه. مجلهٔ حقوق فناوری‌های نوین، ۳(۶)، ۴۷-۶۰.

معتمدنژاد، کاظم (۱۳۸۴). جامعهٔ اطلاعاتی: اندیشه‌های بنیادی، دیدگاه‌های انتقادی و چشم‌اندازهای جهانی. تهران: انتشارات مرکز پژوهش‌های ارتباطات.

موذن‌زادگان، حسنعلی، سلیمانی دهکردی، الهام و یوشی، مهشید (۱۳۹۴). حفظ صحت و استنادپذیری ادلهٔ الکترونیک با استفاده از بیومتریک و رمزنگاری. پژوهش حقوق کیفری، ۴(۱۲)، ۶۹-۹۷.

میرزازاده، زهرا و موسوی، سید محمدصادق (۱۴۰۰). حمایت از حریم خصوصی در کشف جرائم مشهود. مجلهٔ فقه و مبانی حقوق اسلامی، ۵۴(۱)، ۲۰۵-۲۲۰.

Brown, C. L. (2009). *Computer evidence: Collection and preservation*. Charles River Media, Inc.

Calder, A. (2016). *EU GDPR & EU-US Privacy Shield: A Pocket Guide*. IT Governance Publishing.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Del Carmen, R.V. (2009). *Criminal Procedure: Law and Practice.* United States.Wadsworth Publishing.

European Commission (2016). Guide to the EU-U.S. Privacy Shield, Directorate-General for Justice and Consumers. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_2461

Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. *Science and Engineering Ethics*, *26*(6), 3333-3361..

Garner, B. A. (2004). *Blackss LwwDictiorrr y.* Thomson West, 8th ed, USA.

Landwehr, C. E., Heitmeyer, C. L., & McLean, J. (2011). *A security model for military message systems: Retrospective*. Naval Research Laboratory Washington DC.

Packer, H. L. (1964). Two models of the criminal process. *University of Pennsylvania law review*, *113*(1), 1-68.

Sherwood, S. (2013). United Nations Signs Off on 'right to Privacy in the Digital age", *The Register*. Available at: www.theregister.co.uk/2013/12/19/ ,united_nations_signs_off_on_right_to_privacy.

Staples, W. G. (2007). *Encyclopedia of Privacy*, Vol1&2.

Taipale, K. A. (2003). Internet and Computer Crime: System Architecture as Crime Control. *Center for Advanced Studies Working Paper* (03-2003).

Taniar, D. (Ed.). (2008). *Data mining and knowledge discovery technologies*. IGI Global. https://www.igi-global.com/book/data-mining-knowledge-discovery-technologies/230