Private Low
Vol. 19, No. 1, Spring & Summer 2022
Manuscript Type: Research

http://jolt.ut.ac.ir
Print ISSN: 2008-840X
Article Online ISSN: 2423-6209
DOI: 10.22059/jolt.2022.341558.1007090

The Condition of Considering the Data Personal in Cyberspace
Comparative Review of European General Data Protection Regulation and Iranian law

Mohammad Ali Sharifi Kia[1*], Farideh Shabani Jahromi[2]

1. M.Sc. in International Law, Faculty of law, College of Farabi, University of Tehran, Qom, Iran.
2. Assistant Professor, Faculty of law, College of Farabi, University of Tehran, Qom, Iran.

(Received: April 17, 2022 ; Accepted: June 29, 2022)

Abstract

Personal data is a piece of information about the privacy of individuals and is protected by lawmakers as a right to privacy. On the other hand, protecting users against the actions of data processing companies and the risks that may threaten the integrity and confidentiality of their personal data, requires familiarity with the characteristics of this particular type of data. The present study, using descriptive analytical method, tries to examine the text of the EU General Data Protection Regulation document as well as Iranian legal documents such as the Electronic Commerce Law of the Islamic Republic of Iran, Iranian electronic crime law and the draft bill on personal data protection, to explain the distinguishing features of personal data from other types of data in cyberspace. Finally, the findings of the present study indicate that personal data are necessarily related to the natural person and the common point which is observed in all types and instances of personal data, is the identifiability of data, thus if the identity of the data subject (and not other persons) can be accessed, either directly or indirectly, using conventional and logical data processing tools and devices, the data will be considered personal.

Keywords

Privacy, Cyberspace, Personal Data, General Data Protection Regulation (2016), Personal Data Protection, Data Subject Identification.

[*] **Corresponding Author, Email:** mo.ali.kia@gmail.com; ali.ghadamgahi@ut.ac.ir

حقوق خصوصی
دورهٔ ۱۹، شمارهٔ ۱، بهار و تابستان ۱۴۰۱
صفحات ۲۴۵ ـ ۲۲۱ (پژوهشی)

Print ISSN: 2008-840X
Online ISSN: 2423-6209
https://jolt.ut.ac.ir

شرط شخصی تلقی شدن داده‌ها در فضای سایبر
بررسی تطبیقی مقررات عمومی اروپایی حفاظت از داده و حقوق ایران*

محمدعلی شریفی‌کیا[۱]، فریده شعبانی جهرمی[۲]**

۱. دانش‌آموختهٔ کارشناسی‌ارشد رشتهٔ حقوق بین‌الملل، دانشکدهٔ حقوق، دانشکدگان فارابی، دانشگاه تهران، قم، ایران
۲. استادیار، دانشکدهٔ حقوق، دانشکدگان فارابی، دانشگاه تهران، قم، ایران

(تاریخ دریافت: ۱۴۰۱/۰۱/۲۸ ـ تاریخ پذیرش: ۱۴۰۱/۰۴/۰۸)

چکیده

داده‌های شخصی قسمی از اطلاعات مربوط به حریم خصوصی افراد است و توسط قانون‌گذاران تحت عنوان حق بر حریم خصوصی مورد حمایت قرار گرفته است. از طرفی حمایت از کاربران در مقابل اعمال شرکت‌های پردازندهٔ داده و خطراتی که ممکن است تمامیت و محرمانگی داده‌های شخصی ایشان را تهدید کند مستلزم آشنایی با ویژگی‌های این نوع خاص از داده‌هاست. در پژوهش حاضر با استفاده از روش تحلیلی- توصیفی تلاش شد با بررسی متن سند مقررات عمومی حفاظت از داده‌های شخصی اتحادیهٔ اروپا و همچنین اسناد حقوقی ایرانی- نظیر قانون تجارت الکترونیک، قانون جرایم رایانه‌ای، پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی- به تبیین ویژگی‌های متمایزکنندهٔ داده‌های شخصی از دیگر داده‌ها در فضای سایبر پرداخته شود. در نهایت یافته‌های پژوهش حاضر حاکی از آن بود که داده‌های شخصی لزوماً مرتبط با شخص حقیقی است و نقطهٔ اشتراکی که در همهٔ اقسام و مصادیق داده‌های شخصی مشاهده می‌شود قید شناسنده بودن آن داده‌هاست؛ بدین ترتیب که اگر بتوان با استفاده از ابزار و وسایل متعارف و منطقی پردازش داده، چه به صورت مستقیم چه به صورت غیرمستقیم، صرفاً و به‌تنهایی به هویت شخص موضوع داده (و نه اشخاص دیگر) دست پیدا کرد، داده‌ها شخصی تلقی خواهند شد.

کلیدواژگان

حریم خصوصی، حفاظت از دادهٔ شخصی، داده‌های شخصی، شناسایی موضوع داده، فضای سایبر، مقررات عمومی حفاظت از داده‌های شخصی اروپا.

---

* استخراج‌شده از پایان‌نامهٔ کارشناسی‌ارشد، در رشتهٔ حقوق بین‌الملل، دانشکدهٔ حقوق، دانشکدگان فارابی دانشگاه تهران، با موضوع «حق حفاظت از داده‌های شخصی در فضای سایبر، با تأکید بر دستورالعمل حفاظت از دادهٔ اتحادیهٔ اروپا (GDPR: 2018)»، تاریخ دفاع: ۱۴۰۰/۱۰/۳۰.

** **رایانامهٔ نویسندهٔ مسئول:** mo.ali.kia@gmail.com

مقدمه

حفاظت از داده‌های شخصی افراد در فضای سایبر همواره امری حائز اهمیت بین نهادهای قانون‌گذار در سرتاسر دنیا بوده است. بنابراین، مشاهده می‌شود که اتحادیهٔ اروپا نیز از طریق دو رکن اصلی خود، نظیر شورا و پارلمان اروپا، طی سال‌های ۱۹۹۵ تا ۲۰۱۶، مجموعه قواعدی در زمینه‌های مرتبط برای نظام‌مند ساختن پردازش و به‌کارگیری داده‌های شخصی کاربران در فضای سایبر، تحت عنوان «مقررات عمومی حفاظت از داده‌های شخصی اتحادیه اروپا»[1] به تصویب[2] و اجرا[3] درآورده است.

مقررات عمومی حفاظت از داده‌های شخصی اتحادیهٔ اروپا در سال ۲۰۱۶ و با هدف حفاظت از داده‌های شخصی کاربران در برابر شرکت‌های پردازشگر داده به تصویب پارلمان این سازمان بین‌المللی رسید و از سال ۲۰۱۸ در خصوص همهٔ کشورهای عضو اتحادیهٔ اروپا و همچنین سایر کشورهای غیرعضو و شرکت‌هایی که قصد تبادل اطلاعات با اتحادیه را دارند اجرا می‌شود.

این سند بین‌المللی قواعد جامعی را در خصوص حفاظت از اطلاعات شخصی افراد در فضای سایبر ارائه می‌کند. در شرح محتویات این سند نیز بیان شده است که حفظ اصول حقوق بشری به‌خصوص حمایت از اشخاص حقیقی در رابطه با پردازش داده‌های شخصی مرتبط با آنان یک حق اساسی است و همهٔ قواعد مرتبط با این مقوله، صرف‌نظر از ملیت یا محل سکونت افراد، باید به حقوق و آزادی‌های اساسی آن‌ها، به‌ویژه حق افراد برای حفاظت از داده‌های شخصی‌شان، احترام بگذارد؛ که این موضوع یکی از اهداف مهم آن در کنار سایر کاربردهای تجاری این سند است (GDPR, recitals: 1-2).

از طرف دیگر مقررات عمومی یادشده صرفاً در زمینهٔ داده‌های شخصی به تصویب رسیده و اعمال می‌شود و داده‌های غیرشخصی خارج از محدودهٔ عملکردی آن است. بنابراین تعریف این نوع داده‌ها و تشخیص وجوه تمایز بین داده‌های شخصی و غیرشخصی نیز اهمیت بالایی دارد. زیرا این وجوه تمایز تعیین می‌کنند که آیا یک موجودیت پردازش‌کنندهٔ داده مشمول تعهدات

1. general data protection regulation (GDPR: 2016).
2. April, 14, 2016.
3. May, 25, 2018.

مختلفی خواهد بود که این مقررات عمومی بر کنترل‌کننده‌ها و پردازشگران داده‌های شخصی تحمیل می‌کند یا خیر.

از این رو و به منظور تعیین دامنه و محدودهٔ استفاده از مقررات عمومی حفاظت از دادهٔ اروپا در مورد عملیات مختلف پردازشی که بر داده‌های کاربران صورت می‌گیرد، شناسایی و تشخیص اطلاعاتی که در طبقهٔ داده‌های شخصی قرار می‌گیرند، به طور فزاینده، مهم قلمداد می‌شود. زیرا مثلاً مسئولیت‌ها و جریمه‌های سنگینی که در اثر نشت اطلاعات شخصی کاربران متوجه شرکت‌های پردازندهٔ داده خواهد بود، در صورت اثبات شخصی نبودن داده‌ها، به‌سادگی قابل اجتناب است.

جمهوری اسلامی ایران نیز در دو دههٔ اخیر از طریق به تصویب رساندن قانون تجارت الکترونیکی ایران[۱]، قانون مبارزه با جرایم رایانه‌ای ایران[۲]، و همچنین آماده ساختن پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی[۳] گام‌های مؤثری جهت نظام‌مند ساختن تعاملات کاربران ایرانی در این خصوص برداشته است. از یک طرف، طبق توصیف ارائه‌شده در مادهٔ ۱ قانون تجارت الکترونیکی ایران، این قانون اساساً مجموعهٔ اصول و قواعدی است که برای مبادلهٔ آسان و ایمن اطلاعات در واسط‌های الکترونیکی و با استفاده از سیستم‌های ارتباطی جدید به کار می‌رود و از طرف دیگر هدف اصلی از ارائهٔ لایحهٔ صیانت و حفاظت از داده‌های شخصی صیانت از حیثیت و کرامت اشخاص موضوع داده[۴] اعلام شده است (مادهٔ ۱).

با توجه به اهمیت مطالبی که در خصوص حفاظت از داده‌های شخصی و همچنین لزوم شناسایی و طبقه‌بندی این نوع داده‌ها در فضای سایبر بیان شد، در پژوهش حاضر نگارنده ابتدا به علت وجود رابطهٔ تنگاتنگ و تشابه قابل ملاحظه بین مفاهیم حریم خصوصی و داده‌های شخصی اشاره‌ای به مفهوم حریم خصوصی می‌کند و پس از آن به بیان تعاریف ارائه‌شده برای مفهوم دادهٔ

---

۱. تاریخ تصویب: ۱۳۸۲/۱۰/۱۷.

۲. تاریخ تصویب: ۱۳۸۸/۰۵/۰۳.

۳. تاریخ رونمایی: ۱۳۹۷/۰۵/۰٦، تهران، نمایشگاه الکامپ ۲٤؛ با حضور وزیر ارتباطات و فناوری اطلاعات، رئیس مرکز پژوهش‌های مجلس و رئیس کمیتهٔ ارتباطات و فناوری اطلاعات مجلس.

4. data subject(s)

شخصی[1] در نظام اروپایی حفاظت از داده و همچنین نظام حقوقی ایران می‌پردازد و سپس با بررسی جنبه‌ها و جهت‌گیری‌های گوناگون در این زمینه و توسط سیستم‌های حقوقی و اسناد یادشده به این سؤال پاسخ خواهد داد که وجود چه خصیصه و چه ویژگی‌هایی داده‌های موجود در فضای سایبر را در دستهٔ داده‌ها یا اطلاعات شخصی قرار می‌دهد.

مفهوم حریم خصوصی در متون حقوقی اروپایی و ایرانی

تا کنون تعاریف مختلفی از حریم خصوصی توسط نظام‌های حقوقی مختلف و همچنین حقوقدانان گوناگون در سرتاسر جهان ارائه شده است. از طرفی می‌توان گفت با توجه به پیشینهٔ تاریخی و فرهنگی ملل مختلف هیچ‌گاه تعریف واحدی توسط همهٔ حقوقدانان برای آن مورد قبول واقع نشده است (قدمگاهی ۱۴۰۰: ۱۰). به عنوان اولین مثال برای تبیین مفهوم حریم خصوصی و حق بر آن، می‌توان به بند دوم اعلامیهٔ نهایی کنفرانس اروپایی حقوقدانان در نروژ با موضوع حق بر حریم خصوصی (Nordic Conference of Jurists on the Right to Respect for Privacy, 1976)[2] اشاره کرد که این اصطلاح را چنین تعریف می‌کند[3]: «حقی است که اشخاص برای حفظ زندگی خود نسبت به موارد زیر در برابر سایرین دارند: مداخلات دیگران در زندگی خصوصی، خانوادگی، و آزادی فکری آنان، تعرضات به آبرو و شهرت، استفاده از هویت، جاسوسی در مکاتبات و سوءاستفاده از ارتباطات خصوصی و افشای اطلاعات آنان.»

همچنین می‌توان به تعریف شورای اروپا در قطعنامهٔ ۱۹۷۰ اشاره کرد که این مقوله را چنین تعریف می‌کند: «حریم خصوصی عبارت است از امور مربوط به زندگی خصوصی، خانوادگی و مسکن، تمامیت جسمی و روحیه، آبرو، اعتبار و شهرت و حیثیت افراد، امتناع از اینکه چهره‌ای کاذب از شخص ساخته شود، عدم افشای وقایع و حقایق نامربوط و آزاردهنده، عدم افشای

---

1. personal data
2. https://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf.
۳. قطعنامهٔ کنفرانس استکهلم (۱۹۶۷) نیز به موارد مشابهی در توضیح (حق خلوت) اشاره می‌کند (برای مطالعهٔ بیشتر ← موسی‌زاده، ابراهیم؛ فهیم مصطفی‌زاده (۱۳۹۱). «نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی»، *بررسی‌های حقوق عمومی*، س ۱، ش ۲، زمستان، ص ۵۵ ـ ۵۶).

غیرمجاز تصاویر خصوصی، حمایت از عدم افشای اطلاعاتی که اشخاص بر اثر اعتماد به دست آورده با در اختیار آن‌ها قرار گرفته است.»[۱] (محسنی ۱۳۸۹: ۲۹). این قطعنامه حق بر حریم خصوصی را «حقی نسبت به تنها ماندن، زندگی کردن با سلیقه خود، و با حداقل مداخلهٔ دیگران» می‌داند (Council Of Europe, European Convention On Human Rights, 1976)[۲].

برخی حقوق‌دانان ایرانی نیز در تعریفی مشابه چنین می‌گویند که می‌توان حریم خصوصی را قلمرو اطلاعات کاملاً شخصی فرد که ارتباطی با جامعه، به طور عام، ندارد تعریف کرد (اسکندری ۱۳۸۹: ۱۵۵)[۳].

در نقاط گوناگون دنیا نظام‌های حقوقی مختلف با توجه به همین مفاهیم دست به فعالیت‌های تقنینی می‌زنند که در ادامه با بعضی از این موارد آشنا خواهیم شد؛ مثلاً برخی حریم خصوصی را قلمرویی از زندگی هر شخص می‌دانند که آن شخص به صورت عرفی یا با اطلاع قبلی به دیگران از آنان انتظار دارد تا بدون کسب رضایت از او به اطلاعات دربارهٔ آن محدوده و قلمرو دسترسی پیدا نکنند یا به آن ورود نکنند یا از نگاه کردن و نظارت بر آن به هر نوعی خودداری کنند و آن شخص را مورد تعرض قرار ندهند (انصاری ۱۳۸٦: ۳۸). حال آنکه برخی از پژوهشگران دیگر در همین نظام حقوقی به مفهوم فوق سه ایراد را وارد کرده‌اند: «اول اینکه انتظار تعبیری حقوقی نیست و برای دیگران الزام‌آور نمی‌باشد. دوم اینکه بر اساس این تعریف حریم خصوصی نسبی خواهد شد. و مورد آخر اینکه دو قید عرفاً یا با اعلان قبلی هیچ نقشی در توضیح معنای حریم خصوصی نداشته و زائد به نظر می‌رسند.» (اسکندری ۱۳۸۹: ۱٥٤).

اعلامیهٔ حقوق بشر اسلامی قاهره نیز در حمایت از حریم خصوصی چنین می‌گوید: «الف) هر انسانی حق دارد که نسبت به جان و دین و خانواده و ناموس و مال خویش در آسودگی زندگی کند. ب) هر انسانی حق دارد که در امور زندگی خصوصی خود (در مسکن و خانواده و مال و ارتباطات) استقلال داشته باشد و جاسوسی یا نظارت بر او و مخدوش کردن حیثیت او جایز

---

۱. همچنین: وثیقی، عبدالهادی (۱۳۹۵). حریم خصوصی در فقه مذاهب خمسهٔ اسلامی و قوانین کشور افغانستان، ۱۸.

۲. همچنین:

Freedman, W. (1982). The Right Of Privacy In The Age Of Computer Data And Processing, p. 1365.

۳. به نقل از: کدخدایی، عباس (۱۳۸۳). «شبکه‌های اطلاعاتی جهانی و نقض حقوق بشر با تأکید بر حریم خصوصی».

نیست و باید از او در مقابل هر گونه دخالت زورگویانه در این شئون حمایت شود. ج) مسکن در هر حالی حرمت دارد و نباید بدون اجازهٔ ساکنان آن یا به صورت غیرمشروع وارد آن شد و نباید آن را خراب یا مصادره کرد یا ساکنانش را آواره نمود.» (اعلامیهٔ حقوق بشر اسلامی قاهره ۱۹۹۰: مادهٔ ۱۸).

با این همه به نظر می‌رسد یکی از تعاریف مرتبط به بحث حاضر متعلق به آلن وستین[1] است که حریم خصوصی را چنین شرح می‌دهد: «قدرت تشخیص خودمان که چه زمانی، چگونه، و به چه میزان اطلاعات پیرامون ما به دیگران منتقل شود.» (حیدری ۱۳۹۶: ۳).»[2]

تعاریف این‌چنینی با مفهوم امروزی حریم خصوصی و اطلاعاتی که از آن ناشی می‌شود و در فضای سایبر قرار می‌گیرد (داده‌های شخصی) ارتباط بیشتری دارند. با توجه به تعاریف یادشده می‌توان دریافت که نقطهٔ اشتراک بین سیستم‌های اروپایی حقوق بشر و سیستم اسلامی آن در جامعهٔ امروز نه الفاظ موجود در تعاریف بیان‌شده بلکه بیشتر قلمرو و مصادیق حریم خصوصی اتس. مثلاً ارتباطات و حیثیت اشخاص حقیقی در همهٔ سیستم‌های حقوقی جزئی از حریم خصوصی افراد است و اشخاص حقیقی حق حمایت از آن‌ها را تحت عنوان حق بر حفاظت از حریم خصوصی خود دارند. موضوع حائز اهمیت دیگری که در تعریف قطعنامهٔ شورای اروپا به چشم می‌خورد حق بر زندگی کردن (به‌تنهایی، با سلیقهٔ خود، و با حداقل مداخلهٔ دیگران) است. اصل این تعریف از حق بر حریم خصوصی خود نقص دارد. زیرا امروزه ماهیت زندگی اجتماعی افراد و نحوهٔ گره خوردن زندگی فرد به جامعه به‌تنهایی ناقض قید «با سلیقهٔ خود» است.

از یک طرف طبیعتاً در جامعهٔ کنونی و با توجه به پیشرفت‌های فرهنگی حاصل‌شده در طول تاریخ تمدن بشر هر فردی می‌تواند با علایق و سلایق خویش زندگی کند، اما محدودهٔ این آزادی تا زمانی که با آزادی سایرین در همین زمینه‌ها برخورد و تلاقی نداشته باشد قابل گسترش است. از طرف دیگر در صورتی که هر فرد حقیقی با سلیقهٔ خود هر نوع اطلاعاتی از زندگی خصوصی خود را در فضای جامعه و به صورت داوطلبانه نشر دهد دیگر نهادهای حمایتی اجتماع عملاً

---

1. Alan Westin

۲. همچنین:

Westin, A. (1968). *Privacy and Freedom*, New York, Athenaeum, p. 7.

کاربردی در حفاظت از حریم خصوصی وی نخواهند داشت. به بیان دیگر نمی‌شود توقع داشت در همهٔ زمینه‌ها به سلیقهٔ شخصی عمل کرد و سپس انتظار حمایت از جامعه در زمینهٔ حریم خصوصی نیز داشت. به‌رغم وجود این خطا در تعریف یادشده، نقطهٔ قوت آن را نیز می‌توان عبارت «با حداقل مداخلهٔ دیگران» دانست. شاید معنی و مفهوم همین قید (حداقل مداخله دیگران) است، که مبدأ فعالیت‌های تقنینی کاربردی در زمینهٔ حفظ حریم خصوصی، در نظام های حقوقی گوناگون بوده است. با اندکی دقت در اکثر قواعد تنظیم‌شده در نظام‌های حقوقی مختلف حول محور حمایت از اشخاص حقیقی در فضای سایبر، به‌خصوص اتحادیهٔ اروپا، می‌توان دریافت که مثلاً در بحث گردآوری و پردازش داده‌های شخصی این اصل مهم به صورت حداقل‌سازی جمع‌آوری داده‌ها و پردازش‌های صورت‌گرفته روی آن‌ها در حال اجراست.

البته باید به این نکته نیز توجه داشت که حمایت از حریم خصوصی در برابر نقض آن قرار می‌گیرد و این نقض لزوماً مستلزم سرّی و محرمانه بودن اطلاعات نیست، بلکه هر گونه اطلاعات مربوط به اشخاص را شامل می‌شود و دول مختلف باید با اتخاذ تدابیر پیشگیرانه از هر گونه نفوذ و وارد شدن خدشه به تمامیت و محرمانگی اطلاعات، چه در فضای حقیقی چه در فضای مجازی، جلوگیری کنند (رئیسی و لیاسی ۱۳۹۹: ۱۲٦ ـ ۱۲۷).

مفهوم دادهٔ (اطلاعات) شخصی در نظام حقوقی ایران و مقررات عمومی حفاظت از دادهٔ اروپا

تا کنون تعاریف متنوعی در متون حقوقی و اسناد بین‌المللی برای ترکیب اطلاعات یا دادهٔ شخصی بیان شده است. از تعاریفی که برای این مفهوم در متون حقوقی ایرانی ارائه شده است می‌توان به این تعریف اشاره کرد: «داده‌ها یا اطلاعات زمانی با نام یا شخصی تلقی می‌شوند که به طور مستقیم شناسایی افراد حقیقی را ممکن سازد.» (زرکلام ۱۳۸٦: ۳).

بر مبنای این دیدگاه داده‌هایی که مستقیم شخصی تلقی می‌شوند عبارت‌اند از: «آدرس جغرافیایی یا پستی، شمارهٔ ملی، شمارهٔ گواهینامهٔ رانندگی، شماره حساب بانکی، شمارهٔ کارت بانکی، شمارهٔ اشتراک آب و برق و تلفن و گاز، همچنین عکس یا تصویری که شناسایی فرد را ممکن سازد.» (زرکلام ۱۳۸٦: ٤). همان‌گونه که از این تعریف و مصادیق بیان‌شده برمی‌آید می‌توان

گفت این دیدگاه هر داده‌ای را که بـه تشـخیص هویـت افـراد حقیقـی کمـک کنـد دادهٔ شخصـی می‌پندارد. از طرفی با دقت در مثال‌هایی که از این اطلاعات ارائه شده است چنین برداشت می‌شود که عملاً بخش قابل توجهی از اطلاعاتی که مرتبط با حریم خصوصی افراد اسـت، اگـر در فضـای سایبر قرار بگیرد، می‌توان از آن به عنوان داده‌های شخصی یاد کرد.

در توضیح این مدعا می‌توان این‌گونه ادامه داد که مثلاً شـمارهٔ کـارت بـانکی احـدی از افـراد حقیقی در مراودات روزانهٔ اشخاص با یک‌دیگر صرفاً مقصدی مجازی برای انتقال وجـوه مـالی در نظر گرفته می‌شود و قسمی از مصادیق حریم خصوصی آن شخص اسـت کـه مـی‌توانـد آن را در اختیار سایرین قرار دهد. اما هنگامی که همین شماره در فضای سایبر قرار گیرد و شخص ثالثی بـا اعمال غیرقانونی درصدد کشف هویت این فـرد برآیـد و فرضـاً بـا اسـتفاده از همـین شـماره بـه اطلاعات هویتی شخص یادشده در سرورهای بانک دسترسـی پیـدا کنـد مصـداقی از اطلاعـات و داده‌های شخصی خواهد بود و حمایت و حفاظت از آن نیز امری مهم و ضروری است. بـا توجـه به محوریت اتحادیهٔ اروپا و سند GDPR در بحث حاضر، با ارائهٔ تعریفـی کـه در فصـل اول ایـن مقررات عمومی برای مفهوم اطلاعات شخصی آورده شده است، بحث خود را ادامه می‌دهیم.

مطابق این تعریف، دادهٔ شخصی به هر گونه اطلاعاتی اطلاق می‌شـود کـه بـا شـخص حقیقـی شناسایی‌شده یا قابل شناسایی[1] مرتبط باشد (GDPR, Chapter 1: General provisions, Article: 4). از این تعریف چنین برمی‌آید که هر گونه داده‌ای که به طور مشخص و پس از عملیـات پردازشـی بتواند پل ارتباطی با احدی از اشخاص حقیقی برقرار کند، به گونه‌ای که هویت آن فرد از دیگـران متمایز شود، یا به هر نوع داده‌ای که پس از پردازش صـرفاً بـه یـک شـخص حقیقـی کـه از قبـل شناسایی شده است مرتبط شود دادهٔ شخصی گفته می‌شود یا به بیان ساده‌تر در صـورت شناسـایی شخص، به صورت مستقیم یا غیرمستقیم، با استفاده از پردازش و بـه‌کـارگیری اطلاعـات، داده یـا اطلاعات شخصی خواهد بود (Stala & Knight 2016: 299-300).

از طرفی با اندکی دقت در متن این ماده و ادامهٔ متن مقررات عمومی مـی‌تـوان دریافـت کـه نیازی به شناسایی کامل شخص حقیقی وجـود نـدارد، بلکـه صـرف امکـان[2] شناسـایی شـخص

1. identified or identifiable natural person
2. possibility

موضوع داده[1] داده‌ها را تحت عنوان شخصی قرار می‌دهد. همچنین در فصل دوم (اصول) تصریح می‌شود: «اطلاعات شخصی باید به گونه‌ای باشند که بتوانند شناسایی شخص موضوع داده را در مدت زمان معقول انجام دهند.» (GDPR, Chapter 2: Principles, Article: 5(2)).

از طرف دیگر این ماده با بیان اینکه برخی اطلاعات می‌توانند به صورت غیرمستقیم[2] (به احتمال زیاد به وسیلهٔ ترکیب شدن با اطلاعات دیگر) باعث شناسایی افراد حقیقی شوند و با توجه به این مطلب که متن مشخص نمی‌کند عملیات شناسایی باید توسط چه کسی صورت پذیرد بر این نکته تأکید دارد که لزوماً نباید در آن زمان به‌خصوص (زمان تحصیل اطلاعات) اطلاعات اضافی برای شناسایی فرد در اختیار پردازشگر[3] یا کنترل‌کننده[4] قرار داشته باشد تا بتوان داده‌های یادشده را در دستهٔ شخصی قرار داد؛ بلکه همین که بتوان با تجمیع این داده‌ها و سایر اطلاعاتی که در دسترس اشخاص حقیقی و حقوقی ثالث قرار دارد به هویت افراد پی برد داده‌های یادشده شخصی تلقی خواهند شد.

مثال در این زمینه تعریف مشابه از داده‌های شخصی است که در تیرماه ۱۳۹۷ از سوی وزارت ارتباطات و فناوری اطلاعات جمهوری اسلامی ایران و در پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی[5] ارائه شد. این پیش‌نویس، که داده‌های شخصی را به دو قسم عادی و حساس تقسیم می‌کند، در بخش دوم تعاریفی را برای مفاهیم یادشده بیان می‌دارد: «الف) دادهٔ شخصی عبارت است از داده‌ای که به‌تنهایی یا همراه داده‌های دیگر، مستقیم یا غیرمستقیم، شخص موضوع داده را از طریق ارجاع به یک شناسه می‌شناساند. ب) دادهٔ شخصی حساس عبارت است از دادهٔ شخصی که ریشهٔ قومی یا قبیله‌ای، نظرات سیاسی، مذهبی و فلسفی، مشخصات وراثتی یا اطلاعات سلامت شخص موضوع داده را آشکار می‌سازد.» (پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی، مادهٔ ۲).

1. data subject
2. indirect
3. processor
4. controller

۵. از این به بعد در این متن به‌اختصار «پیش‌نویس» درج می‌شود.

صرف‌نظر از این موضوع که با اندکی تأمل در مفاد این پیش‌نویس به وجود تشابه عمیق بین آن و GDPR پی می‌بریم، حتی در تعریف داده‌های شخصی نیز این تشابه کاملاً واضح است. تفاوتی که در این دو تعریف دیده می‌شود این است که پیش‌نویس به نوعی تفسیر تعریف مندرج در مقررات عمومی را نیز به عنوان بخشی از تعریف اصلی ارائه داده است. آنجا که شناساندن شخص موضوع داده به‌تنهایی یا به کمک داده‌های دیگر ویژگی منحصربه‌فرد این داده‌ها معرفی می‌شود نتیجه همان می‌شود که به بیان دیگر اطلاعات جزئی که دسترسی به نیمهٔ دیگر آن‌ها یا کامل کردن آن‌ها نیازمند تلاش و صرف هزینه و وقت بیش از حد نباشد نیز در دستهٔ داده‌های شخصی قرار می‌گیرند.

اما نکتهٔ قابل توجه بعدی قائل شدن قید حساسیت برای داده‌هایی با ماهیت قومی یا قبیله‌ای، سیاسی، مذهبی و فلسفی، مشخصات وراثتی، و اطلاعات مربوط به سلامت افراد است. در اصل این طبقه‌بندی نیز از متن اصلی GDPR مشتق شده است؛ درحالی‌که مقررات عمومی اتحادیه مانند پیش‌نویس این داده‌های شخصی را خاص[1] می‌داند، اما نه در حدی که آن‌ها را قسم جدید و مجزایی از داده‌ها در نظر بگیرد، بلکه صرفاً به اهمیت این داده‌ها اشاره می‌کند و پردازش آن‌ها را جز در برخی موارد که در متن به آن اشاره شده مجاز نمی‌داند (GDPR, Chapter 2: Principles, Article: 9(1)). به‌علاوه می‌توان این‌گونه گفت که به نظر نگارندگان پیش‌نویس در همهٔ بخش‌های خود (تعاریف، مفاهیم، مفاد) در اصل نسخهٔ بومی‌سازی‌شده و خلاصه‌شدهٔ GDPR است که با اندکی توجه و مقایسهٔ قواعد می‌توان این موضوع را دریافت. مثلاً همین تعریف داده‌های شخصی حساس در پیش‌نویس در حقیقت از مادهٔ ۹ فصل دوم GDPR استخراج شده است؛ درحالی‌که به علت متصور نبودن سایر گرایش‌های جنسی در دین مبین اسلام و مذهب تشیع، که مذهب رسمی و قانونی جمهوری اسلامی نیز هست، الفاظ «زندگی جنسی»[2] و «گرایش جنسی اشخاص»[3] از این تعریف حذف شده است، آنجا که بند اول این ماده می‌گوید: «پردازش داده‌های شخصی در ارتباط با افشاسازی مبدأ قومی و نژادی، اعتقادات فلسفی و مذهبی، اطلاعات ژنتیکی، اطلاعات بیومتریک

1. special categories of personal data
2. sex life
3. sexual orientation

با هدف شناسایی خاص افراد حقیقی، و همچنین اطلاعات مرتبط با سلامتی یا داده‌های مربوط به زندگی جنسی و گرایش‌های جنسی افراد حقیقی ممنوع است.» (GDPR, Chapter 2: Principles, Article: 9(1)). طبیعتاً مثال‌هایی از این قبیل درون متن پیش‌نویس به‌وفور مشاهده خواهد شد[1] که از حوصلهٔ این بحث و نوشتار خارج است و نگارنده به همین دو مثال بسنده می‌کند.

قانون جرایم رایانه‌ای ج.ا. ایران (مصوب ۱۳۸۸) نیز در مادهٔ ۱۷ خود می‌گوید: «هر کس به وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج‌میلیون ریال تا چهل‌میلیون ریال یا هر دو مجازات محکوم خواهد شد». این یکی دیگر از مواردی است که قوانین مربوط به حمایت از حریم خصوصی افراد و داده‌های شخصی ایشان با مبانی فکری و فرهنگی ایران هماهنگ شده است.

در نهایت با اندکی تدقیق در قواعد و مقررات حال حاضر ج.ا. ایران در زمینهٔ حفاظت از داده‌های شخصی، نظیر پیش‌نویس لایحهٔ حمایت از داده‌های شخصی (۱۳۹۷) و ق.ت.ا.ج.ا. ایران (۱۳۸۲) و قانون جرایم رایانه‌ای (۱۳۸۸)، و مقایسهٔ آن‌ها با سند مقررات عمومی حفاظت از داده‌های شخصی اروپا (۲۰۱۶) به این نتیجه می‌رسیم که نه‌تنها در زمینهٔ متون قانونی و تفاسیر حقوقی بومی در این زمینه با کمبود مواجهیم، بلکه لوایحی که بتوانند حامی حقوق کاربران ایرانی در این فضا باشند (نظیر پیش‌نویس لایحهٔ حمایت از داده‌های شخصی یا طرح صیانت از فضای مجازی) با مشکلات فراوان روبه‌رو هستند. مثلاً همان‌طور که اشاره شد از طرفی پیش‌نویس عملاً یک کپی‌برداری ناشیانه و بدون توجه به ساختارهای فرهنگی و مذهبی ایران و به‌شدت ناقص و سطحی است و از طرف دیگر طرح صیانت نیز هنوز قادر به کسب پایگاه اجتماعی درون تودهٔ

---

۱. در مثالی دیگر می‌توان به مقدمهٔ پیش‌نویس اشاره کرد که برخی از اهداف آن را اجرای اصول قانون اساسی جمهوری اسلامی ایران، اجرای سیاست‌های کلی نظام ابلاغی مقام معظم رهبری، اجرای برنامهٔ ششم توسعه یا اجرای پدافند غیرعامل، و به طور کلی مسائل بومی معرفی می‌کند؛ درحالی‌که مقدمهٔ GDPR به مباحثی از قبیل تجارت الکترونیک، دسترسی آزاد به اطلاعات، گردش آزاد اطلاعات، و برخی موارد اساسی دیگر می‌پردازد.

مردم ایران نشده است. جریمه‌های در نظر گرفته شده در قانون جرایم رایانه‌ای (۱۳۸۸) نیز ناچیز است و کاربرد چندانی ندارند. بنابراین، نیاز به تدوین و به‌روزرسانی و اصلاح قوانین ج.ا. ایران در این زمینه به‌شدت محسوس است.

مصادیق داده‌های شخصی از منظر سیستم حقوقی اتحادیهٔ اروپا و ایران

سیستم حقوقی اتحادیهٔ اروپا در خصوص مصادیقی که برای داده‌های شخصی برمی‌شمارد، برخلاف حریم خصوصی، از یکپارچگی بیشتری برخوردار است. به نظر می‌رسد علت آن را هم می‌توان در قیدی که GDPR در تعریف این داده‌ها گنجانده است یافت؛ آنجا که در تعریف داده‌های شخصی به این نکته اشاره می‌کند که ملاک برای شخصی بودن داده‌ها قابلیت آن‌ها در شناساندن افراد حقیقی است.

با توجه به همین تعریف در متن GDPR و هماهنگی‌های ایجادشده در نظام‌های حقوقی کشورهای عضو اتحادیه، پس از لازم‌الاجرا شدن آن[1]، اطلاعاتی از قبیل نام افراد، شناسه‌های ملی و کارگزینی، اطلاعات جغرافیایی و جی‌پی‌اس، معرف‌های برخط، عوامل مختص به هویت نظیر اطلاعات حرکتی و چهره‌شناسی، فیزیکی، ژنتیکی، اقتصادی، فرهنگی، روانی، اجتماعی، فیزیولوژیکی، بیومتریک[2]، و همچنین داده‌های مربوط به سلامت جسمی و پرونده‌های الکترونیک بهداشتی آنان، اطلاعات مربوط به رسیدگی‌های قضایی و محکومیت‌های حقوقی و کیفری، داده‌های مربوط به گرایش‌های دینی و مذهبی و قومیتی، و در نهایت داده‌های مرتبط با گرایش‌های جنسی افراد و دایرهٔ اشخاص مرتبط با آنان در دستهٔ اطلاعات شخصی قرار می‌گیرند (GDPR, Chapter 2).

در این زمینه می‌توان به مادهٔ ۲ قانون ت.ا.ج.ا.ا. (مصوب ۱۳۸۲) اشاره کرد که پس از اینکه «هر

---

۱. برای مطالعهٔ بیشتر در خصوص هماهنگی‌های ایجادشده توسط کشورهای عضو اتحادیهٔ اروپا و سایر دول جهان با قواعد GDPR می‌توان به آدرس https://www.dlapiperdataprotection.com مراجعه که به صورت خصوصی در حال رصد قوانین موضوعهٔ کشورها در این رابطه است و سیر تحولات قواعد مربوط به حمایت از اطلاعات شخصی افراد در کشورهای گوناگون جهان و آخرین قواعد به‌کارگیری‌شده توسط دولت‌های اتحادیه و سایر نظام‌های حقوقی دنیا را بررسی و تشریح کرده است.

۲. تشخیص هویت از طریق اطلاعات و مشخصات جسمی.

نمادی از واقعه، اطلاعات، یا مفهوم که با وسایل الکترونیکی، نوری، و با فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره، یا پردازش شود» را دادهٔ پیام[1] می‌خواند دادهٔ پیام‌های شخصی[2] را چنین تعریف می‌کند: «دادهٔ پیام‌های مربوط به یک شخص حقیقی (موضوع داده) مشخص و معین» (قانون تجارت الکترونیکی جمهوری اسلامی ایران ۱۳۸۲: ماده ۲). شاید همین تعاریف و اجرایی شدن مقررات عمومی GDPR موجب شده است که پیش‌نویس لایحهٔ حمایت از داده‌های شخصی جمهوری اسلامی ایران (۱۳۹۷) نیز داده‌های مرتبط با سلامت افراد، سرشماری‌های ملی، عقاید سیاسی، دینی یا مذهبی، قومیت، وضعیت جسمانی، حزبی، فلسفی، اتهامات و محکومیت‌های کیفری را شخصی قلمداد کند (پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی ج.ا. ایران: مواد ۱۵، ۱٦، ۱۸) و به حمایت از این داده‌ها بپردازد.

در مثالی دیگر می‌توان به مادهٔ ۳۲ قانون جرایم رایانه‌ای ج.ا. ایران (مصوب ۱۳۸۸) اشاره کرد که ارائه‌دهندگان خدمات دسترسی را موظف می‌کند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمهٔ اشتراک نگه دارند (قناد و عقیلی ۱۳۹۹: ۳۱۸). ایرادی که به این ماده وارد است استفاده از الفاظ عام «داده‌های ترافیک» و «اطلاعات کاربران» است که عملاً مشخص نیست این الفاظ به چه نوع اطلاعاتی اطلاق شده است و اگر شامل داده‌های شخصی کاربران ایرانی نیز می‌شود چه لزومی برای ذخیرهٔ این داده‌ها وجود دارد.

نکتهٔ حائز اهمیت در اینجا اختلاف بین معانی ارائه‌شده توسط GDPR و قوانین ایران، نظیر ق.ت.ا.ج.ا. (۱۳۸۲) و ق.ج.ر. (۱۳۸۸)، در توضیح و تعریف این نوع داده‌هاست. همان‌طور که بیان شد، مقررات عمومی اتحادیهٔ اروپا از لفظ «personal data»[3] برای این نوع اطلاعات استفاده کرده؛ درحالی‌که قانون تجارت الکترونیک ایران (۱۳۸۲) لفظ «private data»[4] و قانون جرایم رایانه‌ای (۱۳۸۸) لفظ «users data»[5] را در تعریف خود گنجانده است.

---

1. data massage

۲. در متن قانون یادشده به صورت «private data» آورده شده است.

۳. داده(های) شخصی، مربوط به هویت شخص.

٤. داده(های) خصوصی، مربوط به حریم خصوصی افراد.

۵. داده(های) کاربران.

این اختلاف در معانی خود می‌تواند سبب بروز مشکلات عدیده‌ای در تفسیر قوانین نشئت‌گرفته از آن شود. زیرا به نظر می‌رسد از لحاظ حقوقی انتخاب کلمات تعریف اتحادیهٔ اروپا دقیق‌تر و ظریف‌تر انجام شده و تقید بیشتری بین داده‌های مختلف ایجاد کرده است. اما از طرف دیگر الفاظ به‌کاررفته در تعریف قانون تجارت الکترونیک ایران (۱۳۸۲) دایرهٔ وسیع‌تری از داده‌ها را شامل می‌شود؛ هرچند که متن تعریف به دستهٔ خاصی از داده‌ها اشاره داشته باشد.

کاملاً واضح است که با توجه به تعاریف نسبتاً مشترک در این متون دادهٔ شخصی باید معرف شخص حقیقی باشد، حال آنکه لفظ «داده‌های خصوصی»، که قانون تجارت الکترونیک ایران (۱۳۸۲) از آن در متن خود استفاده کرده است، می‌تواند شامل هر نوع داده‌ای بشود که در نظر اشخاص مختلف در طبقه‌بندی خصوصی جای می‌گیرد، ولی قابلیت شناسایی آنان را به پردازندهٔ اطلاعات نمی‌دهد. مثلاً شاید اطلاعات و تصاویر خام مربوط به پروژه‌های تحصیلی یا کاری افراد را بتوان در دستهٔ خصوصی جای داد و مانع دسترسی دیگران به آن شد. ولی تا زمانی که با استفاده از سایر اطلاعات یا شناسه‌ها نتوانیم هویت شخص حقیقی را شناسایی کنیم (حداقل با توجه به تعاریف GDPR و پیش‌نویس لایحهٔ حمایت از داده‌های شخصی ایران) اطلاعات مورد بحث شخصی نخواهد بود.

بنابراین شاید بتوان گفت هر دادهٔ شخصی خصوصی نیز هست. اما عکس این مفهوم صادق نیست. بنابراین اهمیت دقت در انتخاب کلماتی که در تعریف مفاهیم مختلف حقوقی به کار می‌روند انکارناپذیر است. زیرا تعاریف گوناگون و استفاده از کلماتی که معانی موسع دارند می‌تواند به در بر گرفتن مصادیق بیشتر توسط تعریف یادشده و خارج شدن آن مصادیق از دایرهٔ منظور قانون‌گذار بینجامد. پس، می‌توان گفت بین داده‌های شخصی افراد و حریم خصوصی آنان رابطهٔ عموم و خصوص مطلق وجود دارد؛ به این نحو که همهٔ داده‌های شخصی مرتبط با شخص حقیقی زیرمجموعه‌ای از حریم خصوصی وی خواهد بود، لکن مثلاً اطلاعاتی که مربوط به زندگی شخصی فرد است و هنوز در فضای سایبر قرار نگرفته است دادهٔ شخصی به شمار نمی‌رود (قدمگاهی ۱٤۰۰: ۳۲ ـ ۳٤).

وجوه تمایز داده‌های (اطلاعات) شخصی با سایر داده‌ها

درک مفهوم داده‌های شخصی از آن جهت حائز اهمیت است که داده‌های حاصل از رفتار امروز کاربران ممکن است قادر به پیش‌بینی رفتار فردای آن‌ها یا دارای ارزش سیاسی و اقتصادی باشد (قناد و شریف ۱٤۰۰: ۳ ـ ٤). از آنجا که مسئولیت حقوقی پردازش‌های غیرقانونی بر دوش شرکت‌ها و خدمات‌دهندگان اینترنتی بار شده است، گاه نیاز است دادگاه‌های بین‌المللی، نظیر دیوان دادگستری اروپا[1] و محاکم ملی، برای احقاق حقوق اشخاص حقیقی در این زمینه ورود کنند.

با توجه به این نکته، به نظر می‌رسد در زمان حاضر یکی از جامع‌ترین تعاریف موجود برای اصطلاح داده‌های شخصی همان تعریف مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا (۲۰۱٦) است که گاه با اندکی تغییر یا عیناً در سایر متون حقوقی داخلی کشورهای عضو اتحادیه و همین‌طور کشورهای غیرعضو گنجانده شده است. مثلاً کشور فرانسه دقیقاً از همین تعریف استفاده می‌کند و تعریف ارائه‌شده در پیش‌نویس لایحهٔ حمایت از داده‌های شخصی ایران نیز شباهت زیادی با این تعریف دارد که در ادامه به آن اشاره خواهد شد.

همان‌گونه که بیان شد، تعریف GDPR از داده‌های شخصی از این قرار است: «هر گونه اطلاعات مربوط به شخص حقیقی شناسایی‌شده یا قابل شناسایی». این مقررات عمومی در توضیح شخص حقیقی قابل شناسایی[2] چنین ادامه می‌دهد که شخص حقیقی قابل شناسایی فردی است که مستقیم یا غیرمستقیم به سبب ارتباطی که با یک شناسنده[3]ـ نظیر شمارهٔ شناسایی، داده‌های مربوط به موقعیت مکانی، شناسایی‌کنندهٔ برخط، نام کامل، یا مجموعه‌ای از عوامل مختص به هویت روانی، ژنتیکی، فیزیولوژیکی، فیزیکی، اقتصادی، فرهنگی، و اجتماعی فرد یادشده‌ـ دارد سببی برای شناسایی و روشن شدن هویت آن شخص شود (GDPR, Chapter 1: General provisions, Article: 4). چند نکتهٔ حائز اهمیت برای درک بهتر مفهوم داده‌های شخصی در این تعریف وجود دارد که تحلیل و بررسی می‌شود.

---

۱. برای مطالعهٔ بیشتر در این خصوص می‌توان به پرونده‌های مرتبط با مقولهٔ داده‌های شخصی در دیوان دادگستری اروپا، نظیر پروندهٔ آقای گونزالز علیه شرکت گوگل اسپانیا یا پروندهٔ ناظر حفاظت از دادهٔ فرانسه علیه شرکت گوگل، مراجعه کرد.

2. identifiable natural person

3. identifier

اولاً، در زمینهٔ شناسایی فرد حقیقی برخی حقوقدانان قائل به وجود تمایز بین شخصی‌سازی[1] و شناسایی[2] هستند. زیرا اگر از تعریف مقررات عمومی صرفاً شناسایی برداشت شود، ممکن است اطلاعات کاملاً تصادفی با انجام دادن برخی پردازش‌ها و ادغام با برخی اطلاعات دیگر به افراد حقیقی گوناگون مرتبط شوند؛ حال آنکه به نظر می‌رسد هدف از شناسایی مشخص شدن هویت فرد به‌خصوصی از افراد باشد (skopek 2015: 691). به بیان ساده‌تر اگر یک سری از شناسه‌های گوناگون در فضای سایبر بتواند به افراد مختلف ارتباط پیدا کند دیگر از دایرهٔ تعریف خارج است؛ به این معنی که حتی اگر با استفاده از داده‌های در دسترس بتوان به هر فردی غیر از شخص مالک داده رسید یا داده‌ها به دو نفر یا بیشتر ارجاع بدهند، دیگر شخصی تلقی نمی‌شوند.

ثانیاً، از دیدگاه مقررات عمومی GDPR، که در زمینهٔ حفاظت از داده‌های شخصی نسبت به پردازش و انتقال آزاد داده‌ها برای همهٔ کشورهای عضو اتحادیهٔ اروپا لازم‌الاتباع است، کل این سند حول محور اطلاعات و داده‌های اشخاص حقیقی سازمان‌دهی شده است. این مقوله بدین معنی است که تدبیرهای حمایتی این سند صرفاً برای حمایت از داده‌های اشخاص حقیقی در فضای سایبر تدوین شده‌اند و داده‌های مرتبط با اشخاص حقوقی تحت حمایت خاص این سند نخواهند بود. حال آنکه با توجه به اختیار عمل نسبی که این سند به کشورهای عضو جهت اعمال برخی اصلاحات در متن قانون می‌دهد، بعضی از کشورهای عضو اتحادیه به‌رغم پذیرش و ایجاد هماهنگی های لازم با سند یادشده، تغییراتی در متن نهایی قانونی که در خصوص حمایت از داده‌های شخصی، در کشور خود به تصویب رسانده‌اند، ایجاد کرده و حمایت از داده‌های اشخاص حقوقی را نیز در دستور کار خود قرار داده‌اند (قدمگاهی ۱۴۰۰: ۲۰).

مثلاً دولت آلمان به موجب قانون فدرال حمایت از دادهٔ ۳۰ ژوئن ۲۰۱۷ خود، که در ۲۰ نوامبر ۲۰۱۹ نیز متممی بر آن اضافه شد، حمایت خود را از اطلاعات نهادهای عمومی و خصوصی دولت فدرال آلمان اعلام کرد (Federal Data Protection Act of 30 June 2017)[3]. طبق بخش دوم (تعاریف) این سند، حمایت‌های مندرج در سند یادشده بر داده‌های نهادهای عمومی، که در اصل

1. individuation
2. identification
3. Federal Law Gazette I, p. 2097.

همان مؤسسات و مراکز دولتی آلمان هستند، و اطلاعات نهادهای خصوصی، که همان اشخاص حقیقی یا حقوقی بدون رابطهٔ استخدامی رسمی با دولت فدرال آلمان هستند، اعمال خواهد شد. از طرفی این سند در بند ٤ و ٥ خود و در توضیح نهادهای خصوصی یا نحوهٔ اعمال حمایت بر داده‌های اشخاص حقیقی یا حقوقی چنین شرح می‌دهد که نهادهای خصوصی در واقع اشخاص حقیقی و حقوقی، جوامع، و سایر انجمن‌هایی هستند که تحت قوانین خصوصی دولت آلمان تأسیس شده‌اند و همچنین اگر یک نهاد خصوصی وظایف حاکمیتی و اداری دولت را انجام دهد یک نهاد عمومی در نظر گرفته خواهد شد.[1]

ثالثاً، لفظ شناسایی‌شده خود دلالت قوی بر متمایز شدن شخص حقیقی از سایر اشخاص دارد. زیرا در صورت شناسایی شدن یک فرد حقیقی به وسیلهٔ داده‌ها و با استفاده از همان روش‌های متعارف که قبلاً به آن اشاره شد و پیدا نشدن مورد مشابه داده‌های به‌کاررفته به‌قطع شخصی خواهند بود. مثلاً قائل بودن به این تمایز، به‌ویژه هنگام ارزیابی اینکه آیا فناوری‌های تشخیص چهره[2] در محدودهٔ کاربرد GDPR قرار می‌گیرند، اهمیت دارد. زیرا تجزیه‌وتحلیل داده‌های مرتبط با این فناوری‌ها را امکان‌پذیر می‌کنند (Davis 2020: 365). البته گفتنی است این فناوری با مکانیسم شناسایی چهره[3] که ملازم با تشخیص هویت فرد نیز هست تفاوت دارد و بیشتر مربوط به نرم‌افزارهای امنیتی است که در مکان‌های عمومی با دریافت اطلاعات چهره و رفتار اشخاص به پیش‌بینی حرکات بعدی آنان و احتمال وجود خطر برای مردم حاضر در مجموعه‌های مختلف، از قبیل مکان‌های تفریحی یا بانک‌ها یا فستیوال‌های مذهبی، می‌پردازند. با توجه به این توضیح می‌توان دریافت که صرف شناسایی فرد حقیقی از بین سایر افراد توسط پردازش داده‌ها نیز آن‌ها را در دستهٔ شخصی طبقه‌بندی نمی‌کند، بلکه باید علاوه بر جداسازی وی از بقیه در تشخیص هویت او نیز مؤثر باشد.

رابعاً، به نظر می‌رسد عبارات «شناسایی‌شده» یا «قابل شناسایی» در ارتباط با هر پردازشگری که به داده‌ها دسترسی دارد بیان شده‌اند (Dalla Corte 2019: 6-8). زیرا متن ماده به طور خاص

1. https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0013, section 2, paras: 4-5.
2. facial detection
3. facial recognition

مشخص نکرده است که حتماً این عملیات شناسایی باید توسط شرکت‌ها یا نهادهای دولتی یا سایر مجموعه‌ها انجام شود یا به عبارت دیگر نهاد شناسایی‌کننده شخص حقیقی را معرفی نکرده است. پس می‌توان نتیجه گرفت که داده‌های این‌چنینی در دسترس هر شخصی (چه حقیقی چه حقوقی) که باشند، اگر قابلیت شناسایی هویت اشخاص حقیقی را با قید استفاده از ابزار و وسایل متعارف روز به وی بدهند، در دستهٔ داده‌های شخصی قرار داده می‌شوند و لزومی ندارد که حتماً داده‌ها در اختیار اشخاص حقوقی مانند شرکت‌ها یا سازمان‌ها باشند.

خامساً، تأکید تدوین‌کنندگان این سند بر استفاده از لوازم و ابزار معقول و منطقی برای شناخت و کشف هویت اشخاص حقیقی مرتبط با داده یا همان اشخاص موضوع داده نیز از اهمیت بالایی در طبقه‌بندی داده‌ها برخوردار است. زیرا در این صورت برای شناسایی شخص حقیقی همهٔ عوامل عینی و شرایط موجود- مانند هزینه‌ها، مقدار زمان مورد نیاز برای شناسایی، تکنولوژی موجود در زمان پردازش، و همچنین تحولات تکنولوژیکی در آیندهٔ نزدیک- باید در حد منطقی و عرفی در نظر گرفته شود. بنابراین پس از بررسی شرایط یادشده داده‌هایی که همچنان قابلیت شناسایی شخص حقیقی را نداشته باشند از شمول مقررات این سند خارج می‌شوند و طبق متن GDPR باید با استفاده از ابزار منطقی و متعارف بین داده‌ها و شخص حقیقی یک ارتباط واضح و روشن برقرار باشد یا قابلیت برقراری داشته باشد (Fink & Pallas 2020: 13). از طرفی با توجه به آنجه آمد اگر با استفاده از همهٔ ابزار و وسایل متعارف روز داده‌ای همچنان قابلیت شناسایی شخص حقیقی را به دست ندهد (گمنام باشد) دادهٔ شخصی نخواهد بود؛ حتی اگر در طول زمان و با پیشرفت تکنولوژی قابلیت شناسایی مالک آن در آینده فراهم شود.

نتیجه

در حال حاضر مقررات عمومی حفاظت از داده‌های شخصی اروپا مهم‌ترین سند حقوقی در زمینهٔ حمایت از داده‌های شخصی کاربران فضای سایبر است و با توجه به اینکه حمایت‌های این سند صرفاً در مورد داده‌های شخصی اشخاص حقیقی اعمال می‌شود روشن شدن این نکته که چه نوع داده‌هایی شخصی تلقی می‌شوند و وجه تمایز این داده‌ها با سایر اطلاعاتی که کاربران در فضای سایبر به اشتراک می‌گذارند چیست برای قانون‌گذاران و خدمات‌دهندگان و همچنین کاربران (به

منظور بهره‌مندی کامل از حقوق خود) ضروری است. از این رو، با تدقیق در مطالبی که بیان شد اعم از مفاهیم و مصادیق حریم خصوصی و داده‌های شخصی و همچنین ارتباط بین این مفاهیم و ویژگی‌های داده‌های شخصی، که توسط سند GDPR:2016 و اسناد ایرانی، نظیر قانون تجارت الکترونیک (۱۳۸۲)، قانون مبارزه با جرایم رایانه‌ای (۱۳۸۸) و پیش‌نویس لایحهٔ حمایت از داده‌های شخصی (۱۳۹۷) به آنها اشاره شده؛ می‌توان گفت مهم‌ترین تفاوت داده‌های شخصی با انواع دیگر داده‌ها قابلیت شناسایی اشخاص موضوع داده با کمک وسایل و لوازم متعارف توسط آن‌هاست.

این تعبیر بدان معناست که اولاً همهٔ داده‌های مربوط به اشخاص حقوقی از دایرهٔ شمول این سند خارج خواهند بود. ثانیاً عملیات شناسایی صرفاً باید با استفاده از ابزار متعارف توانایی شناسایی شخص موضوع داده (شخصی که مالک داده‌هاست و اطلاعات به او ارتباط دارد) را به دست بدهد. ثالثاً، داده‌های یادشده به هیچ شخص حقیقی دیگری نباید ارتباط پیدا کنند. زیرا در صورت بروز چنین حالتی نیز داده‌ها دیگر شخصی تلقی نخواهند شد. رابعاً، عملیات شناسایی می‌تواند توسط هر شخصی، اعم از حقیقی و حقوقی، صورت پذیرد و میان اینکه چه کسی با استفاده از داده‌های یادشده قابلیت دستیابی به هویت شخص موضوع داده را دارد تفاوتی وجود ندارد. خامساً، توانایی تمایز افراد از یک‌دیگر با استفاده از داده‌هایی نظیر داده‌های بیومتریک و ابزار پردازش این داده‌ها تا هنگامی که با استفاده از سایر داده‌ها به تشخیص هویت شخص حقیقی نینجامد تحت پوشش این مقررات قرار نمی‌گیرد. بنابراین، این داده‌ها در صورتی که با سایر اطلاعات هویتی همراه باشند در دستهٔ داده‌های شخصی قرار می‌گیرند و در نتیجه تحت حمایت اسناد حمایت از داده، نظیر GDPR، خواهند بود.

نتیجهٔ عملی آگاهی از مطالب بیان‌شده در این نوشتار و روشن شدن ویژگی‌های خاص داده‌های شخصی این است که خدمات‌دهندگان و سرویس‌دهندگان فعال در فضای سایبر، که با اتحادیهٔ اروپا در ارتباط‌اند، باید در صورت تشخیص داده‌های شخصی که در کنترل پردازشی آن‌هاست طبق منویات این مقررات عمومی با آن داده‌ها رفتار کنند. زیرا در غیر این صورت با جریمه‌های مندرج در این سند روبه‌رو خواهند بود.

در نهایت پیشنهاد می‌شود قوهٔ مقننهٔ جمهوری اسلامی ایران، با هدف به‌روزرسانی و بومی‌سازی قوانین و مقررات مرتبط با مقولهٔ داده‌های شخصی، ابتدا با بررسی تعاریف مختلف ارائه‌شده در سیستم‌های حقوقی گوناگون به تعریفی مناسب در این زمینه دست پیدا کند و سپس با توجه به پیشینه‌های اجتماعی و فرهنگی و مذهبی ایران اسلامی آن دسته از داده‌ها را که در طبقهٔ داده‌های شخصی قرار می‌گیرند به طور واضح و مشخص در مجموعه قوانینی مخصوص به این مقوله جمع‌آوری کند و به تصویب برساند تا برای همهٔ کاربران ایرانی و پردازندگانی که با داده‌های شخصی آنان سروکار دارند راهنمایی کاربردی باشد.

منابع

آستین، لورا؛ نیکیل سینا (۱۳۸۳). «رسانه‌های نوین و سیاست‌گذاری ارتباطات (نقش دولت در قرن ۲۱)»، مترجم: لیدا کاووسی، *رسانه*، س ۱۵، ش ۲.

اسکندری، مصطفی (۱۳۸۹). «ماهیت و اهمیت حریم خصوصی»، *حکومت اسلامی*، س ۱۵، ش ٤.

اعلامیهٔ حقوق بشر اسلامی قاهره (۱۹۹۰).

انصاری، باقر (۱۳۸٦). *حقوق ارتباط جمعی*، تهران، سازمان چاپ و انتشارات وزارت فرهنگ و ارشاد اسلامی.

پیش‌نویس لایحهٔ صیانت و حفاظت از داده‌های شخصی جمهوری اسلامی ایران (۱۳۹۷).

تقی‌زاد، مهرداد؛ زمردی؛ حاجیان (۱۳۹٦). «نقش اتحادیهٔ اروپا در قاعده‌مندسازی جرایم سایبری»، *مطالعات بین‌المللی پلیس*، د ۷، ش ۲۹.

حبیب‌زاده، طاهر (۱۳۹۰)، *حقوق فناوری اطلاعات، حقوق قراردادها در گسترهٔ قراردادهای الکترونیک (مطالعهٔ تطبیقی)*، تهران، دفتر مطالعات حقوقی مرکز پژوهش‌های مجلس شورای اسلامی، ج ۲.

حیدری، حسین، (۱۳۹٦)، حریم خصوصی در حقوق ایران و اسناد بین الملل، فصلنامه علمی ترویجی مطالعات بین الملل پلیس، سال هفتم، شماره ۲۹، ص:۳.

رئیسی، لیلا؛ فلور قاسم‌زادهٔ لیاسی (۱۳۹۹). «چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر»، *دادگستری*، ۸٤(۱۱۰): ص ۱۱۹ ـ ۱٤۲.

زرکلام، ستار (۱۳۸٦). «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیهٔ اروپا)»، *معارف اسلامی و حقوق*، س ۸، ش ۱.

سعادتی، سیده فهیمه (۱۳۹۲). «صیانت از حریم خصوصی در فضای مجازی بر اساس هنجارهای اسلامی»، *راهبرد*، ش ۲۳.

قانون تجارت الکترونیکی جمهوری اسلامی ایران (۱۳۸۲).

قانون جرایم رایانه‌ای جمهوری اسلامی ایران (۱۳۸۸).

قانون مدنی جمهوری اسلامی ایران.

قدمگاهی، محمدعلی (۱٤۰۰). «حق حفاظت از اطلاعات شخصی افراد در فضای سایبر، با تأکید بر مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا (GDPR: 2018)»، پایان‌نامهٔ کارشناسی‌ارشد، رشتهٔ

حقوق بین‌الملل، دانشکدهٔ حقوق، دانشکدگان فارابی دانشگاه تهران.

قناد، فاطمه؛ الهام شریف (۱٤۰۰). «مطالعهٔ اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا»، *حقوق فناوری‌های نوین*، ۲(۲)، ص ۱ ـ ۲۲.

قناد، فاطمه؛ امیره علی‌قلی (۱۳۹۹). «مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی»، *حقوق فناوری‌های نوین*، ۱(۱)، ص ۲۹۷ ـ ۳۲۲.

کدخدایی، عباس (۱۳۸۳). «شبکه‌های اطلاعاتی جهانی و نقض حقوق بشر با تأکید بر حریم خصوصی».

محسنی، فرید (۱۳۸۹). *حریم خصوصی اطلاعات (مطالعهٔ کیفری در حقوق ایران، ایالات متحدهٔ امریکا و فقه امامیه)*، تهران، انتشارات دانشگاه امام صادق(ع).

مصطفی‌زاده، فهیم (۱۳۸۵). «شناخت و بررسی حق خلوت به عنوان یکی از مصادیق حقوق شهروندی»، *مجموعه مقالات ستاد بزرگداشت هفتهٔ قوهٔ قضاییه*، تهران، مرکز مطبوعات و انتشارات قوهٔ قضاییه.

موسی‌زاده، ابراهیم؛ فهیم مصطفی‌زاده (۱۳۹۱). «نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی»، *بررسی‌های حقوق عمومی*، س ۱، ش ۲.

نخعی‌نیازی، غلامرضا (۱۳۹٤). *هویت و امنیت سایبر*، تهران، فرهنگ روز.

نوری، محمدعلی؛ رضا نخجوانی (۱۳۸۳). *حقوق حمایت داده‌ها*، تهران، انتشارات کتابخانهٔ گنج دانش.

واعظی، سید مجتبی؛ سید علی علی‌پور (۱۳۸۹). «بررسی موازین حقوقی حاکم بر حریم خصوصی و حمایت از آن در حقوق ایران»، *حقوق خصوصی*، س ۷، ش ۱۷.

وثیقی، عبدالهادی (۱۳۹۵). «حریم خصوصی در فقه مذاهب خمسهٔ اسلامی و قوانین کشور افغانستان»، پایان‌نامهٔ کارشناسی‌ارشد، رشتهٔ فقه و مبانی حقوق اسلامی، دانشکدهٔ الهیات و معارف اسلامی، دانشگاه شهید مطهری.

References

Ansari, B. (2008). *Mass Communication Law*, Tehran, Printing and Publishing Organization of the Ministry of Culture and Islamic Guidance. (in Persian)

----------. (2012). *Privacy Law*, Tehran, Samat Publications, (in Persian).

Austin, L. & Cena, N. (2004). "New Media and Communication Policy (The Role of Government in the 21st Century)", translated by Lida Kavousi, *Media Quarterly*, Vol. 15, No. 2.

Carlson, S. & Gisvold, G. (2003). *Practical Guide to the International Covenant on Civil and Political Rights*, McGill University.

COUNCIL OF THE EUROPEAN UNION, No. 2012/0011, DRAFT STATEMENT OF THE COUNCIL'S REASONS 3 (Mar. 31, 2016).

Dalla Corte, L. (2019). "Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law", *European Journal of Law and Technology*, 10(1).

Davis, P. A. (2020). "Facial Detection and Smart Billboards: Analysing the "Identified" Criterion of Personal Data in the GDPR", *European Data Protection Law Review*, 6(3).

DeCew, J. (1997). *In Persuit of Privacy: Law, Ethics, and Rise of technology*, Cornell University Press, London.

Douglas-Scott, S. (1993). Reviewed Work: Privacy, Intimacy and Isolation, by Julie Inness, Oxford University Press, (on behalf of the Mind Association), Vol. 102, No. 408.

Eskandari, M. (2010). "The Nature and Importance of Privacy", *Islamic Government*, Year 15, No. 4. (in Persian)

Finck, M. & Pallas, F. (2020). "They who must not be identified—distinguishing personal from non-personal data under the GDPR", *International Data Privacy Law*, Vol. 10, Issue 1, pp. 11–36.

Freedman, W. (1982). "The Right Of Privacy In The Age Of Computer Data And Processing", *Texas Tech Law Review*, Vol. 8, No. 4.

GDPR recitals, Available at: https://gdpr-info.eu/recitals/.

Ghadmagahi, M. A. (2020). "The right to protection of personal information of individuals in cyberspace, with emphasis on the EU Data Protection Guidelines (GDPR: 2018)", Master Thesis, International Law, Faculty of Law, Farabi Schools, University of Tehran. (in Persian)

Ghanad, F. & Sharif, E. (2020). "An Overview Of The Protection Of Personal Data In The Iranian Legal System And The Document Of The General Data Protection Regulation Of The European Union", *New Technologies Law*, 2(2), pp. 1-22. (in Persian)

Ghanad, F. & Aligoli, A. (2019). "The Concept And Importance Of Personal Data And Privacy And The Types Of Protection In Cyberspace", *New Technology Law*, 1(1), pp. 297-322.

Gregory, V. & Bouthinon-Dumas, H. (2021). EU GENERAL DATA PROTECTION REGULATION SANCTIONS IN THEORY AND IN PRACTICE, 37 Santa Clara High Tech. L.J.1.

Habibzadeh, T. (2011). *Information Technology Law, Contract Law in the Field of Electronic Contracts (Comparative Study)*, Office of Legal Studies, Research Center of the Islamic Consultative Assembly, Tehran, Vol. 2, (in Persian).

Heydari, Hossein, (2016), privacy in Iranian law and international documents, scientific quarterly for promotion of international police studies, 7th year, number 29, p: 3, (in Persian).

https://www.dlapiperdataprotection.com.

https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0013.
https://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf.
LG Feldkirch-57 Cg 30/19b–15.
Mohseni, F. (2010). *Information Privacy (Criminal Study in Iranian Law, USA and Imami Jurisprudence)*, Tehran, Imam Sadegh (AS) University Press. (in Persian)
Mostafazadeh, F. (2006). "Recognition And Study Of Privacy As One Of The Examples Of Citizenship Rights", *Collection Of Articles Of The Judiciary Week Commemoration Headquarters*, Tehran, Judiciary Press and Publications Centre. (in Persian)
Musazadeh, E. & Mostafazadeh, F. (2012). "A Look at the Concept and Principles of the Right to Privacy in the Customary Legal System", *Quarterly Journal of Public Law Studies*, First Year, No. 2. (in Persian)
N. Gruschka, V., Mavroeidis, V., & Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR, IEEE International Conference on Big Data (Big Data).
Nakhaei Niazi, G. (2015). *Identity and Cyber Security*, Tehran, Farhang Rooz Publications. (in Persian)
Nordic Conference of Jurists on the Right to Respect for Privacy (1976).
Nouri, M. A. & Nakhjavani, R. (2004). *Data Protection Law*, Tehran, Ganj-e-Danesh Library Publications. (in Persian)
Raisi, L. & Qasemzadeh Liasi, F. (2019). "Challenges of the Iranian legal system in the violation of personal data and privacy in cyberspace", *Journal of Justice Law*, 84(110), pp. 119-142. (in Persian)
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.
Saadati, S. F. (2013). "Protecting Privacy in Cyberspace Based on Islamic Norms", *Strategy Quarterly*, No. 23. (in Persian)
Safari, B. (2017). "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection", *Seton Hall Law Review*, Vol. 47, Issue. 3, Article 6.
Skopek, J. (2015). "Reasonable Expectations of Anonymity", *Virginia Law Review*, 101(3).
Stalla, S. & Knight, A. (2016). "Anonymous data v. personal data—a false debate: an EU perspective on anonymization, pseudonymization and personal data", *Wisconsin International Law Journal*.
Stalla-Bourdillon, S., Phillips, J., & Ryan, M. (2014). *Privacy vs security (Springer Briefs in Cybersecurity)*, London, GB. Springer.
Taghizad, M. & Zomordi, H. (2017). "The Role of the European Union in Regulating Cybercrime", *Quarterly Journal of International Police Studies*, Vol. 7, Issue: 29. (in Persian)
Vaezi, S. M. & Alipour, S. A. (2010). "A Study of Legal Standards Governing Privacy and Its Protection in Iranian Law", *Private Law Quarterly*, Year 7, No. 17. (in Persian)
Vaseighi, A.H. (2016). "Privacy in the jurisprudence of the five Islamic religions and the laws of Afghanistan", Master Thesis, Field of Jurisprudence and Fundamentals of

Islamic Law, Faculty of Theology and Islamic Studies, Shahid Motahari University. (in Persian)

Wachter, S. (2018). "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR", *Computer Law & Security Review*, Vol. 34, Issue 3.

Westin, A. (1968). *Privacy and Freedom*, New York, Athenaeum.

Zarkalam, S. (2007). "Internet Privacy (Study in Iranian and European Union Law)", *Islamic Education and Law*, Year 8, No. 1. (in Persian)