Modern Technologies Law

University of Science and Culture

http://doi.org//10.22133/mtlj.2025.452918.1321

The Concept and Examples of Personal Data

Abbas Mirshekari[1], Hamed Abbasnia[2]*, Darya safari[3]

[1] Assistant Prof., Faculty of Law and Political Science, University of Tehran, Tehran, Iran.

[2] MA. in Private Law, Faculty of Law, University of Tehran, Tehran, Iran.

[3] MA. in Private Law, Faculty of Law, University of Tehran, Tehran, Iran.

Article Info

Original Article

Received:
17-04-2024
Accepted:
21-02-2025

Keywords:
Personal Data
Anonymous Data
General Data Protection Regulation (GDPR)
Sensitive Data
Data Protection Laws

Abstract

In our time, the use of virtual space has become inevitable. Legislation and protection of users' rights is also a necessity of virtual life. In the meantime, the definition of personal data as a standard for data subject to data protection laws has a great importance. As long as the data is not related to a specific person, it is as if privacy has not been violated and there is no need for protection. Now the question is, what data is considered personal? Can specific instances of personal data be specified? In response, it can be said that a case-by-case investigation must be done to determine personal data and cannot be satisfied with a general rule. Whether data is personal or anonymous varies depending on factors such as facilities, time, nature of data, cost of identification, technological developments and the purpose of data processing. In the case of definite cases, although there is no definite determination of a specific type of data as personal data; But some examples, such as surnames in addition to other identifiers and pseudonymous data, are highly possibility to be considered personal data in the legal systems of the European Union and the United States. In this article, the laws and judicial procedure of the European Union and the United States of America as effective and leading legal systems in the field of data protection have been examined in order to determine a standard for identifying personal data and its examples.

*Corresponding author
e-mail: hamed.abbasnia@ut.ac.ir

How to Cite:
Mirshekari, A., Abbasnia, H., & Safari, D. (2025). The Concept and Examples of Personal Data. *Modern Technologies Law*, *6*(12), 391-410.

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

1. Introduction

In the rapidly transitioning 'onlife' world, where technology integrates with all aspects of daily life, all phenomena are increasingly transformed into data. This data plays a critical role in power dynamics, enabling those who control it to influence markets, predict behavior, and potentially manipulate individuals .

Given this reality, the preservation, management, and protection of data have become critical concerns, prompting the global enactment of data protection laws. These regulations naturally raise a fundamental question: What type of data should be protected?

Across various legal systems, the key criterion for data protection is whether the data in question is classified as personal. Data not considered personal typically falls outside the scope of protection, exempting it from the legal rights and obligations associated with privacy laws. However, this distinction is not new. Early legal scholars, including Warren and Brandeis (1890), emphasized that privacy protections apply only to identifiable individuals. From this perspective, if data is not linked to a specific individual, privacy concerns do not arise, and thus, no legal protection is required.

The accepted definition of personal data serves as the gateway to data protection law. Understanding this definition is essential for determining legal obligations and the extent of data protection measures. However, defining personal data is complex due to its multifaceted nature. These developments raise fundamental questions about the scope of personal data. Specifically, what level of connection must exist between information and an individual for it to be considered personal? Who must have access to the data for it to retain its classification? To what extent does data anonymization remove information from legal protection?

A balanced definition of personal data is necessary. If it is too narrow, privacy protections become ineffective. Conversely, if defined too broadly, excessive compliance burdens may render enforcement impractical and disrupt normal digital activities. Scholars in Iran have recognized the importance of personal data (and have provided definitions. However, previous studies have largely neglected specific examples of personal data and how U.S. law classifies them. To address these gaps, this article examines criteria for distinguishing personal from anonymous data and identifies specific examples based on legal standards in the European Union and the United States.

2. Methodology

This study employs a comparative legal approach, analyzing the definitions of personal data, the criteria for anonymization, and the legal treatment of sensitive data under the GDPR, the CCPA, and relevant case law.

The research relies on laws, judicial decisions, regulatory guidelines, and academic literature. A qualitative methodology is applied, emphasizing legal interpretation, case analysis, and comparative evaluation.

By identifying ambiguities and inconsistencies in defining personal data, this study aims to contribute to a clearer and more effective regulatory framework for data protection. The first section analyzes the definitions and key elements of personal data under EU and U.S. regulations. The second section explores definitive and controversial examples of personal data. The final section discusses sensitive personal data as a distinct category requiring special protection.

3. Results and Discussion

Personal data is the cornerstone of data protection laws. Many legal systems define personal data flexibly, classifying any information that can directly or indirectly identify an individual as personal. However, defining

personal data requires a contextual approach rather than rigid classifications. The classification of certain data types—such as IP addresses, pseudonymous data, and anonymized data—remains a subject of legal debate.

A key observation is that the classification of data depends on contextual factors. Data that is personal under one set of circumstances may be considered anonymous under another. This makes it challenging to create exhaustive lists of personal data. Despite this, there is general consensus that certain data types, such as surnames combined with unique identifiers and pseudonymized data, are classified as personal data under EU and U.S. laws. In contrast, anonymized data and certain forms of metadata continue to spark legal controversy.

Furthermore, personal data varies in sensitivity. Some categories require stricter protections due to the potential harm associated with their exposure. However, the classification of sensitive data is also subject to legal interpretation and depends on specific factual contexts. Within the Iranian legal system, forthcoming legislation should adopt a careful and nuanced approach to defining personal data. Given the rapid advancement of re-identification techniques, definitions should be broad enough to account for evolving technological capabilities. The GDPR and other leading frameworks emphasize expansive definitions to ensure robust data protection.

Additionally, certain categories of information—such as court decisions and judicial opinions—necessitate regulated anonymization. A dedicated legal framework should be established to determine when data is truly anonymous. This framework should distinguish between anonymized and encrypted data, ensuring appropriate legal protections for each category. Clear guidelines will help service providers understand their obligations and reduce legal ambiguities.

4. Conclusions and Future Research

The definition of personal data is fundamental to data protection laws, yet it remains a flexible and evolving concept. Most legal frameworks classify any data capable of identifying an individual as personal, necessitating a contextual rather than rigid approach.

While there is consensus on some identifiers, debates persist regarding elements such as IP addresses, metadata, and anonymized data. Certain personal data types require heightened protection due to their sensitivity, but their classification depends on legal interpretation and contextual analysis.

For Iran, future data protection laws should adopt an analytical approach aligned with GDPR principles. Broad interpretations should be encouraged to address technological advancements. Additionally, clear anonymization guidelines should be established, particularly for public disclosures such as court rulings. A structured legal framework should differentiate anonymized data from encrypted data to prevent misinterpretation.

Sensitive personal data necessitates stricter safeguards. Future legal frameworks should impose more rigorous processing regulations, moving beyond predefined lists to a more dynamic classification system. Future research should focus on methodologies for determining personal data based on evolving technologies and regulatory developments. Comparative studies across different jurisdictions could refine global best practices and provide clearer guidance for policymakers and organizations handling sensitive personal information.

حقوق فناوری‌های نوین، ۱۴۰۴، ۶(۱۲) https://www.mtlj.usc.ac.ir

حقوق فناوری‌های نوین

http://doi.org//10.22133/mtlj.2025.452918.1321

مفهوم و مصادیق دادهٔ شخصی

عباس میرشکاری[۱]، حامد عباس‌نیا[۲*]، دریا صفری[۳]

[۱] استادیار گروه حقوق خصوصی و اسلامی، دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران.

[۲] دانش‌آموختهٔ کارشناسی‌ارشد حقوق خصوصی، دانشگاه تهران، تهران، ایران.

[۳] دانش‌آموختهٔ کارشناسی‌ارشد حقوق خصوصی، دانشگاه تهران، تهران، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۲/۲۹

تاریخ پذیرش:
۱۴۰۳/۱۲/۰۳

واژگان کلیدی:
دادهٔ شخصی
دادهٔ ناشناس
مقررات عمومی حفاظت از داده‌ها
دادهٔ حساس
قوانین حفاظت از داده‌ها

چکیده

در روزگار ما، استفاده از فضای مجازی گریزناپذیر شده است. قانون‌گذاری و حفاظت از حقوق کاربران نیز از ملزومات زیست مجازی است. در این میان، تعریف دادهٔ شخصی، به‌عنوان معیاری برای تعیین داده‌های مشمول قوانین حفاظت از داده‌ها، اهمیت ویژه‌ای دارد؛ زیرا تا زمانی که داده به شخصی خاص مربوط نباشد، گویی حریم شخصی نقض نشده است و در نتیجه، نیازی هم به حمایت نیست. حال سؤال این است که چه داده‌هایی شخصی به‌حساب می‌آیند؟ آیا می‌توان مصادیق قطعی دادهٔ شخصی را مشخص کرد؟ در پاسخ می‌توان گفت برای تعیین دادهٔ شخصی باید بررسی و تحلیل موردی انجام داد و نمی‌توان به وضع قاعده‌ای کلی بسنده کرد؛ زیرا بسته به عواملی نظیر امکانات، زمان، ماهیت داده، هزینهٔ شناسایی، پیشرفت‌های فناوری و هدف پردازش داده، شخصی یا ناشناس‌بودن داده تفاوت می‌کند. در باب تعیین مصادیق قطعی دادهٔ شخصی نیز، هرچند نمی‌توان به قطعیت حکم کرد، برخی موارد خاص، مانند نام خانوادگی به همراه شناسه‌های دیگر و دادهٔ مستعار با احتمال شناسایی بالا، اغلب در اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا دادهٔ شخصی به‌حساب می‌آیند. در این مقاله، قوانین و رویهٔ قضایی اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا، به‌عنوان سیستم‌های حقوقی مؤثر و پیشرو در حوزهٔ حفاظت از داده‌ها، در راستای تعیین معیاری برای تشخیص دادهٔ شخصی و مصادیق آن بررسی شده است.

***نویسندهٔ مسئول**

رایانامه: hamed.abbasnia@ut.ac.ir

نحوهٔ استناددهی:

میرشکاری، عباس، عباس‌نیا، حامد، و صفری، دریا (۱۴۰۴). مفهوم و مصادیق دادهٔ شخصی. حقوق فناوری‌های نوین، ۶(۱۲)، ۳۹۱-۴۱۰.

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

شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶

مقدمه

جهانِ پیرامون ما به‌شتاب راهِ «آن‌لایف»[1] شدن را می‌پیماید و محیطی می‌شود که در آن، تمامی عناصر زندگی روزمره با فناوری ترکیب شده است. در این محیط، همهٔ پدیدارها به داده تبدیل می‌شوند (Purtova, 2018, p. 42)، داده‌هایی با ارزش اقتصادی که نقش مهمی نیز در تعیین مناسبات قدرت دارند؛ زیرا کنترل‌کنندگان این داده‌ها توان آن را پیدا می‌کنند که با استفاده از اطلاعاتی که در دست دارند، آینده را تا حدی پیش‌بینی کنند (Mantelero, 2013, p. 234). در چنین جهانی، حفظ و نگهداری داده‌ها و شیوهٔ استفاده از آن‌ها اهمیتی حیاتی پیدا می‌کند. از این رو، قوانین بسیاری برای حفاظت از داده‌ها در سراسر جهان وضع شده است و ضرورت حفاظت از داده‌ها بالطبع این سؤال را پدید می‌آورد که از کدام داده‌ها باید حفاظت شود؟ به عبارت دیگر، حفاظت از چه داده‌هایی غایت و هدفِ قوانین تصویب‌شده در این باب است؟

در بسیاری از قوانین مربوط به حفاظت از داده‌ها، ملاکِ حفاظت، دادهٔ شخصی قرار گرفته است؛ بدین معنا که داده‌هایی که شخصی به‌حساب نیایند از قلمرو حفاظت و درنتیجه، حقوق و تکالیف مقررشده در این قوانین بیرون‌اند؛ البته این ملاک، معیار تازه‌ای نیست و در گذشته نیز حقوق‌دانانی که به مطالعهٔ حریم شخصی پرداخته‌اند، ملاکی مشابه مطرح کرده‌اند. برای مثال، در یکی از نخستین مقالاتی که پیرامون حق بر حریم شخصی منتشر شده است، نویسندگان نشان داده‌اند که مقررات حریم شخصی تنها در مورد اشخاصِ قابل‌شناسایی اعمال می‌شود (Warren & Brandeis, 1890). از این نکته می‌توان نتیجه گرفت که اگر اطلاعات موضوع بحث، شخصی (یعنی مربوط به شخصی خاص) نباشند، بحث حریم شخصی نیز در میان نخواهد بود، تا بتوان با تکیه بر آن از این اطلاعات حفاظت کرد.

به بیان دیگر، تعریفی که از دادهٔ شخصی پذیرفته می‌شود دروازهٔ ورود به قلمرو حفاظت از داده‌هاست و ازاین‌رو، برای شناخت وظایف قانونی مربوط به داده‌ها و حدود حمایت از آن‌ها گریزی از ارائهٔ تعریف دقیقی از دادهٔ شخصی و بحث دربارهٔ پاره‌ای از مصادیق آن نیست. بااین‌حال، باید پذیرفت که به‌رغم تعاریف متعددی که از دادهٔ شخصی ارائه کرده‌اند، هنوز دشواری‌های فراوانی در این راه باقی مانده است و این امر به ماهیت پیچیده و زوایای پنهان آن بازمی‌گردد. برای نمونه، پاسخ به این سؤال آسان نیست که چه ارتباطی باید میان اطلاعات و شخص معین باشد تا داده، شخصی تلقی شود؟ یا اینکه اطلاعات باید در اختیار چه اشخاصی قرار داشته باشد تا بتوان داده را شخصی به حساب آورد؟ یا اینکه ناشناس‌سازی داده‌ها، با چه روش و در چه حدودی، اطلاعات را از شمول قوانین حفاظت از داده‌ها خارج می‌کند؟

نکته‌ای که در این بحث اهمیت دارد و نباید از آن غفلت شود، لزوم رعایت تعادل در تعریف دادهٔ شخصی است؛ یعنی نباید دادهٔ شخصی را آن اندازه محدود و مضیّق تعریف کرد که قوانین در حفاظت از حریم شخصی شهروندان ناکام بمانند و تلاش قانون‌گذاران در این باب به‌کلی بیهوده شود. از سوی دیگر، نباید در این تعریف آن‌قدر گشاده‌دستی روا داشت که در عمل، تکالیف دشوار یا ناممکنی بر دوش شرکت‌ها گذاشته شود و درنهایت، اجرای قانون ناممکن شود یا قانون مزاحم جریان طبیعی فعالیت‌های مجازی شود (Schwartz & Solove, 2011, p. 1827).

حقوق‌دانان ما به اهمیت دادهٔ شخصی و ضرورت شناخت آن به‌خوبی آگاه بوده‌اند (Ghanad & Aligholi, 2020, p. 305) و به همین خاطر در آثار خود به تعریف دادهٔ شخصی پرداخته‌اند (Ahmadvand & Jahanshahi, 2023, p. 115)؛ بااین‌همه، در این نوشته‌ها از مطالعهٔ مصادیق قطعی و احتمالی دادهٔ شخصی غفلت شده است. گذشته از این، مفهوم دادهٔ شخصی در ایالات متحدهٔ آمریکا، به‌منزلهٔ یکی از بازیگران اصلی در حوزهٔ پردازش داده‌ها، مسکوت مانده است. برای رفع این خلأها، در این مقاله به مطالعهٔ معیارِ تشخیصِ شخصی یا ناشناس‌بودن داده‌ها و تعیین مصادیق قطعی و احتمالی دادهٔ شخصی با بررسی قوانین اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا پرداخته شده است.

---

۱. Onlife: این واژه را لوسیانو فلوریدی ابداع کرده است. مراد او از به‌کاربردن آن، اشاره به استفادهٔ روزافزون از فناوری‌های ارتباطی است؛ تا بدان‌جا که دیگر تفکیک میان جهان آنلاین و آفلاین ممکن نباشد (Floridi, 2015, p. 7)

در بخش نخست این مقاله، تعاریف و عناصر دادهٔ شخصی را در چهارچوب مقررات اتحادیهٔ اروپا و ایالات متحدهٔ آمریکا مطالعه خواهیم کرد و سپس، به بررسی قوانین کشورمان در این باب خواهیم پرداخت. پس از آن، در قسمت دوم مقاله، مصادیق قطعی و نیز چالش‌برانگیز و مورد اختلاف دادهٔ شخصی را برمی‌شماریم و درنهایت، دادهٔ شخصی حساس، به‌عنوان نوع خاصی از دادهٔ شخصی، موضوع مطالعه قرار خواهد گرفت.

۱. تعریف دادهٔ شخصی

اغلب یا شاید تمامی قوانین مربوط به حفاظت از داده‌ها با ارائهٔ تعریفی از دادهٔ شخصی آغاز می‌شوند تا بدین‌ترتیب، حدود قانون معین شود و تنها پس از ارائهٔ این تعریف است که قوانین به بیان حقوق و تکالیف شخص موضوع داده و کنترل‌کننده می‌پردازند. بااین‌همه، «دادهٔ شخصی» ترکیبی است سخت مبهم و نباید آن را مفهومی ثابت و روشن پنداشت. یکی به این منظر که هنوز حتی بر سر نام این مفهوم توافقی حاصل نشده است؛ چنان‌که برای مثال در قوانین ایالات متحدهٔ آمریکا، از «اطلاعات قابل‌شناسایی شخصی»[1] نام برده‌شده؛ درحالی‌که در مقررات اتحادیهٔ اروپا، سخن از «دادهٔ شخصی» در میان است (Voss & Houser, 2019, p. 299)؛ البته اختلاف در مفهوم دادهٔ شخصی یا اطلاعات قابل‌شناسایی فردی به همین مورد خلاصه نمی‌شود؛ بلکه ازآنجاکه داده‌ها به‌صورت‌های متنوعی به شخص موضوع داده ارتباط پیدا می‌کند و عوامل متعددی بر رابطهٔ میان داده و شخص تأثیر می‌گذارد (Ausloos, 2012, p. 14)، تعاریف گوناگونی از این مفهوم در قوانین کشورهای مختلف پذیرفته شده است[2].

بنابر آنچه گفته شد، در نگاه نخست، مطالعهٔ تطبیقی دربارهٔ دادهٔ شخصی ناممکن به نظر می‌رسد؛ زیرا کشورهای موضوع مطالعهٔ ما نه در اصطلاحات به‌کاررفته در این باب هم‌نظرند و نه در اجزای تعریف این داده با هم توافقی دارند. بااین‌حال، از چشم‌اندازی وسیع‌تر، می‌توان تعاریف عرضه‌شده از دادهٔ شخصی را در دو دستهٔ موضوعی و تحلیلی قرار داد تا بدین طریق، گام نخست برای مطالعهٔ تطبیقی برداشته شود. سپس می‌توان به مطالعهٔ اجزای این تعاریف در نظام‌های حقوقی مختلف پرداخت و کار مقایسه و تطبیق را به سرانجام رساند. براین‌اساس، در دو بخش زیر، به‌ترتیب به بررسی رویکردها در تعریف دادهٔ شخصی و سپس مطالعهٔ اجزای این تعاریف می‌پردازیم.

۱-۱. رویکردها در تعریف دادهٔ شخصی

در شماری از تعاریف ارائه‌شده از دادهٔ شخصی، دیدگاه موضوعی پذیرفته شده است؛ بدان معنا که در این تعاریف، نوع خاصی از داده‌ها شخصی به شمار آمده‌اند. این دیدگاه را می‌توان برای مثال در قانون اطلاع از نقض اطلاعات ایالت ماساچوست[3] ایالات متحدهٔ آمریکا به‌روشنی مشاهده کرد. براساس این قانون، اطلاعاتی که شامل نام و نام خانوادگی یا نام و نام خانوادگی و ترکیبی از شمارهٔ تأمین اجتماعی، گواهینامه، شماره‌حساب بانکی یا اعتباری فرد باشند، اطلاعات شخصی قابل‌شناسایی به‌حساب می‌آیند (Office of Consumer Affairs & Business Regulation, 2023). به نظر می‌رسد که در کشور ما نیز قانون انتشار و دسترسی آزاد به اطلاعات همین معیار را پذیرفته باشد[4]. البته در همین قانون مواردی نظیر نام‌خانوادگی، محل کار و محل سکونت از باب تمثیل آورده شده است و قانون‌گذار به دنبال محدودکردن داده‌های شخصی نبوده است. از دیگر مصوباتی که شیوه‌ای مشابه برگزیده است، شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی[5] است. این قانون فهرست کاملی از داده‌های شخصی را برشمرده است؛ اما در جهت احصا موارد تحت شمول

1. Personal Identifiable Information (PII)
2. GDPR. Art 4(1); California Civil Code §1798.135(o)(1); DIRECTIVE 95/46/EC. Art 2(a)
3. Massachusetts Data Breach Notification Law

٤. زیرا در بند «ب» مادهٔ ۱ آن می‌خوانیم: «اطلاعات شخصی: اطلاعات فردی نظیر نام و نام خانوادگی، نشانی محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره‌حساب بانکی و رمز عبور است».

۵. این شیوه‌نامه در تاریخ ۱۳۹۷/۰۷/۲۹ در کمیسیون انتشار و دسترسی آزاد به اطلاعات تصویب شده و در تاریخ ۱۳۹۸/۰۹/۰۲ به تأیید رئیس‌جمهور رسیده است.

داده شخصی نبوده است. این موضوع را می‌توان از عبارت «مهم‌ترین و رایج‌ترین مصادیق داده‌شخصی» که در تمامی بخش‌های این شیوه‌نامه دیده می‌شود، برداشت کرد. نکتهٔ دیگری که در این شیوه‌نامه دیده می‌شود و آن را از قوانینی مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا متمایز می‌کند، اهمیت ویژهٔ حریم شخصی و تفکیک اطلاعات عمومی از شخصی به‌عنوان معیاری برای تشخیص شخصی‌بودن داده‌هاست. برای مثال نام و نام خانوادگی اشخاص، عکس پرسنلی، آدرس محل کار و نتایج امتحانات با وجود اینکه سبب شناسایی شخص موضوع داده می‌شود و او را از دیگران متمایز می‌کند، با توجه به اینکه انتشار چنین اطلاعاتی معمولاً نقض حریم شخصی به حساب نمی‌آید، طبق این شیوه نامه داده‌شخصی نیستند.

رویکرد موضوعی البته از ایراد و اعتراض مصون نمانده است. ازجمله می‌توان بر آن خرده گرفت که این دیدگاه، دامنهٔ دادهٔ شخصی را به مواردی و مصادیقی خاص محدود می‌کند؛ درحالی‌که شناسایی اشخاص از راه‌های دیگری نظیر الگوی دیدن صفحات مجازی یا حتی پوشیدن لباسی خاص در مکانی مشخص نیز ممکن است. برای همین هم باید پذیرفت که نام‌بردن از چند شیوهٔ خاص برای شناسایی افراد، باتوجه‌به پیشرفت فناوری و گسترده‌شدن شیوه‌های شناسایی، کاری بیهوده یا کم‌فایده است.

به همین دلیل، امروزه در بسیاری از قوانین حفاظت از داده‌ها، هرگونه داده‌ای را که به شخص شناخته‌شده‌ای مربوط باشد یا بتوان با استفاده از آن شخصی را شناسایی کرد، دادهٔ شخصی به‌حساب می‌آورند. در این صورت، دامنهٔ دادهٔ شخصی دیگر به داده‌ای خاص محدود نمی‌شود؛ بلکه در هر مورد که شناسایی شخص موضوع داده ممکن باشد، دادهٔ شخصی نیز موضوع بحث قرار می‌گیرد. در این رویکرد، گرایش به‌سمت ارائهٔ تعریف گسترده‌ای از دادهٔ شخصی است؛ همان‌طور که برای مثال مسئول حفاظت از داده‌های کانادا در گزارش سالیانه به پارلمان گفته بود: «تعریف [دادهٔ شخصی] به‌عمد وسیع در نظر گرفته شده است و من نیز تمایل دارم، تا جایی که امکان دارد، آن را به‌طور موسّع تفسیر کنم... تمایل دارم درصورتی‌که کمترین احتمالی برای شناسایی فرد باقی باشد، داده را شخصی به‌حساب آورم» (Radwanski, 2003, p. 56). اشارهٔ مسئول حفاظت از داده‌های کانادا به قانون حفاظت از داده‌های شخصی و اطلاعات الکترونیکی این کشور است که تمامی اطلاعات مربوط به شخص قابل‌شناسایی را دادهٔ شخصی می‌شمارد[1]. با این حال، گروهی نیز بر این تعریف گسترده ایراد گرفته‌اند و آن رامدیریت‌ناپذیر خوانده‌اند (Tene & Polonetsky, 2012, p. 259).

در مقابل رویکرد موضوعی، می‌توان از رویکرد تحلیلی یاد کرد. براساس این رویکرد، در هر فرض باید جداگانه شرایط را تحلیل کرد و فقط درصورتی داده‌ای را شخصی به‌حساب آورد که به‌تنهایی یا به همراه داده‌های دیگر برای شناسایی شخص موضوع داده کافی باشد. مادهٔ ۴ مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، دادهٔ شخصی را براساس این رویکرد، چنین تعریف می‌کند: «هر اطلاعات مربوط به یک شخص حقیقی شناخته‌شده یا قابل‌شناسایی». در این تعریف که در واقع تکرار تعریف کنوانسیون اروپایی موسوم به ۱۰۸[2] و دستورالعمل حفاظت از حریم شخصی و جریان‌های فرامرزی داده‌های شخصی[3] است، برای این‌که بتوان اطلاعات و داده‌ای را به شخصی منتسب کند، شکل خاصی معین نشده است. از همین نکته می‌توان نتیجه گرفت که براساس این تعریف، در هر پرونده باید به‌صورت تحلیلی دربارهٔ شخصی‌بودن یا نبودن داده‌ای تصمیم‌گیری کرد.

یافتن رویکردی که ایالات متحدهٔ آمریکا درمورد تعریف دادهٔ شخصی در پیش گرفته آسان نیست؛ زیرا در این کشور، قانون جامعی برای حفاظت از داده‌ها وجود ندارد و تعریف دادهٔ شخصی را باید در قوانین پراکنده‌ای نظیر قانون حفاظت از حریم شخصی آنلاین کودکان[4] و قانون قابلیت انتقال و مسئولیت بیمهٔ سلامت[5] جُست. با استقرا در این قوانین می‌توان گفت که در اغلب آن‌ها، نوع خاصی یا ترکیبی از داده‌های مختلف

1. Personal Information Protection and Electronic Documents Act (PIPEDA). art2(1)
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. art2(a)
3. guidelines on the protection of privacy and transborder flows of personal data (OECD). Art.1(b)
https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last visited: 2023/12/20)
4. The Children's Online Privacy Protection Act (COPPA)
5. Health Insurance Portability and Accountability Act(HIPAA)

مانند نام خانوادگی یا سایر شناسه‌ها مانند تلفن همراه، آدرس و... دادهٔ شخصی با حساب می‌آید. البته برخی از ایالت‌ها، مانند کالیفرنیا که از ایالت‌های پیش‌گام در حوزهٔ حفاظت از داده‌ها در این کشور است، با الگوگرفتن از قوانین اروپایی، در قانون حفاظت از حریم شخصی مصرف‌کنندگان، هر اطلاعاتی را که مرتبط با مشتری یا خانوادهٔ خاص باشد شخصی می‌دانند. این تعریف بسیار وسیع است و مواردی نظیر داده‌های جغرافیایی، اطلاعات شغلی و الگوی رفتاری مشتریان را نیز دربر می‌گیرد؛ البته گفتنی است که در این قانون، اطلاعات صحیحی که به‌صورت قانونی به‌دست‌آمده باشند یا اطلاعاتی که در دسترس عموم قرار دارند شخصی تلقی نمی‌شوند[1].

به نظر می‌رسد که کشور ما همگام با کشورهای پیشرو در حوزهٔ حفاظت از داده‌ها، رویکرد تحلیلی را پذیرفته است؛ زیرا در بند «ر» مادهٔ ۲ قانون تجارت الکترونیکی، داده‌پیام شخصی[2] این‌گونه تعریف شده است: «داده‌پیام‌های مربوط به یک شخص حقیقی مشخص و معین». البته این تعریف فقط با بخشی از رویکرد تحلیلی انطباق دارد؛ چراکه فقط شامل اطلاعات مربوط به شخص شناخته‌شده می‌شود و برخلاف قوانین حفاظت از داده‌های اتحادیهٔ اروپا، فرضی را که شخصِ موضوعِ داده با استفاده از این اطلاعات قابل‌شناسایی باشد دربر نمی‌گیرد. شاید به همین دلیل است که در پیش‌نویس طرح حمایت و حفاظت از داده و اطلاعات شخصی آمده است که «دادهٔ شخصی عبارت است از داده‌ای که به وسیلهٔ آن یا به تنهایی یا به همراه داده‌های دیگر، به توان شخص موضوع آن را شناسایی کرد.»[3] تا بدین‌ترتیب، دادهٔ شخصی شامل هر دو فرض (شناخته‌شده و قابل‌شناسایی) شود. دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوهٔ جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی[4] نیز بر این نظر بوده و با پذیرش رویکرد تحلیلی، داده‌ای که مربوط به هویت و اطلاعات شخصی را کاربران که موجب شناسایی کاربر می‌شود شخصی می‌داند[5].

۱-۲. اجزای تعریف دادهٔ شخصی

بنابر آنچه در بند پیش گفته شد، می‌توان دادهٔ شخصی را در نخستین تحلیل، «هرگونه اطلاعات مرتبط با یک فرد حقیقی شناخته‌شده یا قابل‌شناسایی» دانست. جزء اول این تعریف، عبارت «هرگونه اطلاعات» است. این جزء از تعریف دادهٔ شخصی، به‌رغم اهمیتی که دارد، چندان موردتوجه قانون‌گذاران قرار نگرفته و معیاری برای شناسایی آن نیز ارائه نشده است. این غفلت ممکن است تبعات نامطلوب بسیاری در پی داشته باشد؛ ازجمله این‌که با فراگیرشدن محاسبات رایانه‌ای و تحلیل پیشرفتهٔ الگوریتم‌ها، می‌تواند سبب پیدایش اثر انفجاری در موارد تحت حمایت قوانین حفاظت از داده‌ها شود (Purtova, 2018, p. 49).

اطلاعات و داده ارتباطی نزدیک و استوار با هم دارند و همین امر سبب می‌شود که گاه این دو را یکسان بپندارند؛ اما در واقع با هم تفاوت دارند: «اطلاعات» از تحلیل «داده» به دست می‌آید. برای مثال، یک عکس خانوادگی داده است، درحالی‌که سن افراد حاضر در عکس اطلاعات به شمار می‌آید. داده‌ها بیان‌کنندهٔ واقعیت‌ها و پدیده‌های طبیعی هستند که در قالب اعداد، صفات یا تصاویر بیان می‌شوند (Ansari & Ansari, 2012, p. 3) و مواردی را توصیف می‌کنند که به ما اجازهٔ ضبط، تحلیل یا شناخته‌شدن را می‌دهد (Mayer-Schönberger & Cukier, 2013, p. 78). برخی نیز داده را تفاوت دو حالت فیزیکی (مانند بالاتر یا پایین‌بودن شارژ باتری) یا دو نماد (مانند حرف الف و ب، یا اعداد ۰ و ۱) دانسته‌اند (Floridi, 2009, p. 18) درحالی‌که اطلاعات ممکن است به هر فرمت و شکلی، نظیر حروف الفبا، اعداد، تصاویر، اصوات، به‌شکل فیزیکی یا در حافظه‌های رایانه‌ای (به‌صورت صفر و یک) ذخیره شوند. از تفاوت‌های میان داده و اطلاعات، آنچه به بحث ما مربوط می‌شود این است که صوت، فیلم و یا حتی نقاشی، و به‌صورت کلی هر «داده»‌ای، ممکن است حاوی «اطلاعات» شخصی باشد (Article 29 DataProtection Working Party, 2007, P. 8).

1. California Consumer Privacy Act (CCPA).1798.140. V (2)
2. Private Data
۳ . از طریق لینک زیر در دسترس است: https://media.dotic.ir/uploads/org/2021/10/09/163377045160152200.pdf (last visited: 2023/11/8)
٤. این دستورالعمل مصوب یکصدوبیست‌وهفتمین جلسهٔ مورخ ۱۱/۱۰/۱۴۰۲ کمیسیون عالی تنظیم مقررات فضای مجازی کشور است.
۵. بند ۱-۴ این دستورالعمل مقرر می‌کند: «داده‌های مربوط به هویت و اطلاعات شخصی کاربران که منجر به شناسایی هویت ایشان می‌شود...»

درمورد «هرگونه اطلاعات»، یعنی جزء نخست تعریف دادهٔ شخصی، نکتهٔ دیگری نیز باید ذکر شود و آن این‌که اطلاعات لزوماً نباید مربوط به زندگی شخصی فرد باشد، بلکه همان‌طور که دادگاه اروپایی حقوق بشر در پرونده‌ای مقرر کرده[1]، ممکن است اطلاعات مربوط به محیط کار و شغل نیز اطلاعات شخصی قلمداد شوند. بدین‌ترتیب کافی است که اطلاعات به شخصی مربوط باشد؛ البته این ارتباط نیز باید موسّع تفسیر شود؛ چنان‌که حقایقی درمورد اشیا و فرایندها نیز ممکن است به‌طور غیرمستقیم اطلاعات شخصی را افشا کنند (Ausloos, 2020, p. 129). برای نمونه، ممکن است قیمت یک ملک متضمن اطلاعاتی درمورد مالک آن باشد (Party, 2007, p. 9). به‌طورکلی، درمورد ارتباط اطلاعات با شخص موضوع داده، یکی از سه عامل زیر ممکن است تعیین‌کننده باشد (Article 29 DataProtection Working Party, 2007, p. 10)[2]:

۱. محتوای اطلاعات: اطلاعاتی که دربارهٔ فرد مشخصی است، مانند نتیجهٔ آزمایش پزشکی یا سوءپیشینه؛

۲. هدف جمع‌آوری اطلاعات: هدفی که داده‌ها برای رسیدن به آن جمع‌آوری می‌شوند، مانند وقتی که شرکتی آی‌پی‌آدرس‌های[3] کاربران اینترنت را با هدف شناسایی افرادی که محتوای غیرقانونی دانلود می‌کنند ذخیره می‌کند یا زمانی که ارزش یک ملک برای تعیین مالیات یا اجرای حکم دادگاه استفاده می‌شود (Korff, 2008, p. 44)؛

۳. نتیجه: وقتی پردازش اطلاعات سبب تغییر رفتار با شخص موضوع داده شود، مانند وقتی که اطلاعات نسخه‌های پزشکان در سراسر کشور گردآوری می‌شود و پردازش این اطلاعات ممکن است سبب رفتار متفاوت بیمه با پزشکانی شود که داروی‌های گران‌قیمت تجویز می‌کنند.

جزء بعدی تعریف این است که اطلاعات باید «مرتبط با یک فرد حقیقی» یا به تعبیر دیگر، «شخص حقیقی» باشد. طبق مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، اطلاعات مربوط به اشخاص حقوقی، دادهٔ شخصی محسوب نمی‌شود (Article 29 Data Protection Working Party, 2007, p. 22). بااین‌حال، اطلاعات اشخاص حقوقی، درصورتی‌که به شخص یا اشخاص حقیقی مرتبط باشند، ممکن است دادهٔ شخصی به‌حساب آید، مانند اطلاعات مربوط به ارزش یک شخص حقوقی که ممکن است شامل اطلاعات سهام‌داران آن نیز باشد؛ البته در فرضی که شمار سهام‌داران شخص حقوقی محدود باشد. بااین‌حال، در قوانین بعضی از کشورها، مثل مادهٔ ۳ قانون فدرال حفاظت از داده‌های سوئیس[4]، کشوری که از شمول مقررات عمومی حفاظت از داده‌ها خارج است، اطلاعات اشخاص حقوقی نیز دادهٔ موضوع حفاظت به حساب می‌آید. بعضی دیگر از کشورهای عضو اتحادیهٔ اروپا نیز، مثل ایتالیا، لوکزامبورگ و اتریش، با توجه به اختیاراتی که مقررات عمومی حفاظت از داده‌ها به آن‌ها اعطا کرده، دامنهٔ شمول دادهٔ شخصی را به اشخاص حقوقی نیز گسترش داده‌اند؛ بااین‌حال، حتی در این کشورها، دادگاه‌ها تمایلی ندارند که تمامی قواعد مربوط به حفاظت از داده‌های مربوط به اشخاص حقیقی را درمورد اشخاص حقوقی نیز اعمال کنند یا به تعبیر دیگر، از اطلاعات مربوط به اشخاص حقوقی مانند اطلاعات مربوط به اشخاص حقیقی حمایت کنند. برای مثال، دیوان عالی اتریش[5] شرکتی را که داده‌های مربوط به مشتری‌های خودش را پردازش می‌کرد، شخص موضوع داده به حساب نیاورد و درنتیجه، این شرکت نتوانست علیه شرکت رقیب، که همان داده‌ها را پردازش می‌کرد، اقامهٔ دعوا کند (Kuner, 2007, p. 79). گذشته از این، با توجه به توضیح ۲۷ مقررات عمومی اتحادیهٔ اروپا[6]، دادهٔ شخصی فقط شامل اشخاص زنده می‌شود و اطلاعات افراد فوت‌شده خارج از شمول این قانون است. در قانون تجارت الکترونیکی کشور ما نیز شخص موضوع داده پیام باید شخص حقیقی باشد و از همین نکته برمی‌آید که قانون مذکور، اشخاص حقوقی و احتمالاً، با توجه به ظهور واژهٔ فوق، اشخاص حقیقی فوت‌شده را دربر نمی‌گیرد (Ahmadvand & Jahanshahi, 2023, p. 119).

---

1. AMANN v. SWITZERLAND (2000). (https://hudoc.echr.coe.int/eng# {%22itemid%22: [%22001-58497%22]}) (last visited: 2024/12/1)

۲. این موضوع در رأی پروندهٔ Nowak پذیرفته شده است.

3. IP address

4. Federal Act on Data Protection
https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/1993/1945_1945_1945/20190301/en/pdf-a/fedlex-data-admin-ch-eli-cc-1993-1945_1945_1945-20190301-en-pdf-a-4.pdf (last visited: 2023/8/2)

5. Oberster Gerichtshof

6. GDPR.retical 27

شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی نیز مواردی نظیر داده‌های هویتی مربوط به اشخاص حقوقی و داده‌های مربوط به عضویت اشخاص در بنگاه‌های اقتصادی را از شمار داده‌های شخصی خارج کرده است؛ البته به‌جز موارد عنوان‌شده، می‌توان برخی از داده‌ها، که جنبه اقتصادی دارند، مانند داده‌های مربوط به قراردادهای خصوصی، حساب‌های بانکی و اطلاعات مالی اشخاص حقوقی را شخصی در نظر گرفت؛ به این علت که این شیوه‌نامه در این موارد تفکیکی بین اشخاص حقوقی و حقیقی قائل نشده است.

درنهایت، آخرین جزء تعریف این است که اطلاعات باید مربوط به «شخص شناخته‌شده یا قابل‌شناسایی» باشد. بر سر حدود و تعریف مفهوم «قابل‌شناسایی» اختلاف بسیار است؛ چنان‌که حتی تنی چند از محققان، باتوجه‌به تحلیل کلان‌داده‌ها، تفکیک میان داده‌های قابل‌شناسایی و غیرقابل‌شناسایی را بی‌معنا دانسته‌اند (Tene & Polonetsky, 2012, p. 258).

به‌هرحال این‌که کدام شناسه برای تمایز شخصی از دیگران کافی است، در هر مورد متفاوت است. مطابق مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، «شخص حقیقی قابل‌شناسایی» فردی است که بتوان به‌صورت مستقیم یا غیرمستقیم او را شناسایی کرد؛ خاصه با ارجاع به مواردی نظیر نام، شمارهٔ شناسایی، موقعیت مکانی، شناسهٔ آنلاین و یا یک یا چند مورد مربوط به جسم، روان، ژنتیک، ذهن، وضعیت اقتصادی، فرهنگی یا شناسه‌های مربوط به زندگی اجتماعی او[1]. همین موارد در مقررات سابق حفاظت از داده‌های اتحادیهٔ اروپا تکرار شده است. فقط با این تفاوت که هویت ژنتیکی نیز به شمار مواردی که ممکن است سبب شناسایی شخص موضوع داده شود اضافه شده است، امری که ممکن است ناشی از توسعهٔ فناوری‌های جدید مانند استفاده از تجزیه‌وتحلیل دی‌ان‌ای[2] و ترکیب با جی‌پی‌اس[3] و دیگر داده‌های مکانی در گوشی‌های هوشمند باشد (Voss & Houser, 2019, p. 315)؛ به‌خصوص با توجه به این نکته که در روزگار ما، ارزش اقتصادی فراوانی در تبدیل دادهٔ ناشناس به دادهٔ شخصی نهفته است و درصورتی‌که منابع مالی کافی خرج شود، این کار ممکن نیز هست (Finck & Pallas, 2020, p. 12). به‌هرحال، توجه به این نکته اهمیت دارد که قابلیت شناسایی شخص موضوع داده، امری مطلق نیست و احتمال شناسایی بسته به مورد متفاوت است؛ خاصه ازاین‌روی که ممکن است افراد را با استفاده از کمترین اطلاعات نیز شناسایی کرد؛ حتی اطلاعاتی که در نگاه نخست برای شناسایی کافی به نظر نمی‌رسد. برای مثال در سال ۲۰۰۰، برخلاف آنچه در نخستین تحلیل به نظر می‌رسد، ترکیبی از زیپ کد[4]، تاریخ تولد و جنسیت برای شناسایی ۸۷ درصد جمعیت ایالات متحدهٔ آمریکا کافی بود (Sweeney, 2000, p. 3).

در پایان، ناگفته نباید گذاشت که مفهوم «قابل‌شناسایی» در گذشت زمان ثابت نمانده است. تاریخچهٔ پردازش داده‌ها مملو از مثال‌هایی است که نخست داده‌ای را ناشناس به‌حساب می‌آوردند؛ اما درنهایت افراد موضوع داده‌ها شناسایی شدند؛ بنابراین بعید نیست اگر داده‌ای که زمانی شامل هیچ اطلاعاتی دربارهٔ یک شخص معین نبوده و درنتیجه شخصی به شمار نمی‌رفته، پس از مدتی با استفاده از روش‌های جدید یا براثر پیشرفت فناوری امکان شناسایی فرد را فراهم آورد (Van der Sloot, 2015, p. 36). برای همین هم مسئلهٔ زمانِ بررسیِ قابل‌شناسایی‌بودن نیز اهمیت ویژه‌ای دارد. مادهٔ ۲۶ مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا بر ضرورت توجه به توسعهٔ ابزارهای معقول، که برای شناسایی شخص موضوع داده استفاده می‌شود، تأکید کرده است[5]. بااین‌حال، این عبارت نیز به‌قدر کافی روشن نیست و مشخص نمی‌کند که آیا فناوری‌های در دست آزمایش، مانند کامپیوترهای کوانتومی، که احتمال بالایی در شکستن رمزگذاری دارند، مشمول این مقررات می‌شوند؟ (Finck & Pallas, 2020, p. 17). در همین مورد، کارگروه مادهٔ ۲۹ قانون حفاظت از داده‌ها مقرر کرده است که مراد، فناوری‌های زمان

1. GDPR.retical 26
2. Deoxyribonucleic acid (DNA)
3. Global Positioning System (GPS)
4. Zip code

۵. «...برای مشخص‌کردن اینکه شخص حقیقی قابل شناسایی می‌باشد یا خیر، باید تمامی ابزارهای احتمالی معقول را، مانند جداسازی که توسط کنترل‌کنندهٔ داده یا یک شخص حقیقی دیگر به‌صورت مستقیم یا غیرمستقیم مورد استفاده قرار می‌گیرد، مورد بررسی قرار داد. برای مشخص‌کردن ابزارهای معقول شناسایی شخص حقیقی باید تمامی عوامل نظیر هزینه و زمان مورد نیاز برای شناسایی، فناوری‌های زمان پردازش و توسعهٔ فناوری، مورد توجه قرار گیرد... .»

پردازش با درنظرگرفتن امکان توسعهٔ آنان در طول مدت پردازش است (Article 29 Data Protection Working Party, 2014, p. 9). درنتیجه وقتی داده‌ای برای ده سال نگهداری می‌شود، کنترل‌کننده باید تغییرات فناوری را هم، که در این مدت ممکن است امکان شناسایی افراد را فراهم کنند، در نظر داشته باشد و نباید فقط به این علت که در زمانِ جمع‌آوری داده‌ها، فناوری لازم برای شناسایی وجود نداشته، داده‌ها را تا مدت زمانی طولانی ناشناس تلقی کرده و شخص موضوع داده را از حقوق خود محروم کند.

۲. مصادیق داده شخصی

در بخش پیش، رویکردهای موجود در تعریف دادهٔ شخصی و اجزای این مفهوم را مطالعه کردیم و حالا وقت آن است که به بررسی بعضی از مصادیق دادهٔ شخصی بپردازیم که پاره‌ای از آن‌ها به‌صورت عمومی پذیرفته شده و بر سر بعضی دیگر نیز نزاع است؛ البته برشمردن تمامی مصادیق دادهٔ شخصی در اینجا ممکن نیست، به جهت اینکه شخصی‌بودن یک داده به شرایط، زمان و امکانات گوناگون بستگی دارد. برای نمونه، پوشش فرد در یک مهمانی ممکن است سبب شناسایی او شود؛ درحالی‌که شناسایی براساس نوع پوشش در مقیاس شهر یا کشور، بدون وجود شناسه‌های دیگر، ممکن نیست.

۲-۱. نام شخصی در ترکیب با سایر اطلاعات

یکی از مصادیقی که در اکثر موارد دادهٔ شخصی به‌حساب می‌آید، اشاره به نام شخص به همراه دست‌کم یک شناسهٔ دیگر است. به‌طور معمول، نام فرد، به‌جز در محیط کوچکی مانند کلاس درسی کوچک، سبب شناسایی شخص موضوع داده نمی‌شود؛ اما نام شخص در ترکیب با سایر شناسه‌های مربوط به او می‌تواند سبب تمایز فرد شود و درنتیجه، دادهٔ شخصی به‌حساب آید. در رویهٔ قضایی اتحادیهٔ اروپا، نام شخص در ترکیب با مواردی نظیر شماره تلفن[1]، اطلاعات مربوط به محل کار یا سرگرمی‌ها[2]، آدرس[3]، ساعت کار، استراحت و یا زمان‌های مربوط به وقفه‌ها و شروع کار[4]، مقدار درآمد مربوط به شغل یا سایر درآمدها و یا دارایی‌های فرد[5] به‌صراحت دادهٔ شخصی شمرده شده است.

ایالات متحدهٔ آمریکا، برخلاف اتحادیهٔ اروپا، قانون جامعی برای حفاظت از داده‌ها ندارد و هر ایالت، تعریفی مخصوص به خود از اطلاعات شخصی ارائه می‌دهد؛ بااین‌حال، می‌توان گفت که قوانین بیشتر ایالت‌ها، اطلاعات شخصی را ترکیبی از اطلاعات مختلف می‌دانند که هویت فرد را افشا می‌کند. برای مثال، ایالت نوادا اطلاعات شخصی را نام و نام خانوادگی یک شخص حقیقی در ترکیب با اطلاعات دیگری مانند شمارهٔ گواهینامه، شماره‌حساب بانکی و شناسهٔ بیمهٔ سلامت تعریف کرده است. همچنین بیشتر ایالت‌ها اطلاعاتی را که در دسترس عموم است از دایرهٔ اطلاعات شخصی خارج کرده‌اند (Bragg, 2017).

1. cases C-141/12 and C- 372/12 YS and M. and S. v Minister of Immigration, Integration and Asylum

این رأی در سال ۲۰۱۴ از سوی دیوان دادگستری اروپا صادر شده است و از طریق لینک زیر در دسترس است:

https://curia.europa.eu/juris/document/document.jsf?docid=155114&doclang=EN(last visited: 2023/12/20)

2. case C-101/01, Bodil Lindqvist v. Åklagarkammaren

این رأی در سال ۲۰۰۳ از سوی دیوان دادگستری اروپا صادر شده و با استفاده از لینک زیر قابل دسترسی است:

https://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1523195 (last visited 2023/12/20)

3. C-553/07 College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer

این رأی در سال ۲۰۰۹ از سوی دیوان دادگستری اروپا صادر شده و با استفاده از لینک زیر قابل دسترسی است:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62007CJ0553(last visited: 2023/12/20)

4. Case C-342/12 Worten Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho

این رأی در سال ۲۰۱۴ از سوی دیوان دادگستری اروپا صادر شده و با استفاده از لینک زیر قابل دسترسی است:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0342 (last visited: 2023/12/20)

5. Case C-73/07 Satakunnan Markkinapörssi and Satamedia

این رأی در سال ۲۰۰۸ از سوی دیوان دادگستری اروپا صادر شده و با استفاده از لینک زیر قابل دسترسی است:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62007CJ0073(last visited: 2023/12/20)

۲-۲. دادهٔ مستعار

تصور کنید درصورت انتشار آرای دادگاه‌ها، که حاوی اطلاعات شخصی افراد نظیر نام و نام خانوادگی، شماره‌تلفن، پلاک یا آدرس است، چه مشکلاتی پدید می‌آید؟ همچنین مطالعهٔ این آرا چنان فایده‌ای در تحقیقات و مطالعات علمی دارد که به نظر می‌رسد گریزی از انتشارشان نیست. در این فرض، برای حل این مشکل می‌توان از مستعارسازی[1] بهره گرفت، روشی که برای استفاده از داده‌ها در تحقیقات علمی مرسوم است. در این روش، کلیهٔ مواردی که ممکن است سبب شناسایی شخص شود، از دادنامه پاک می‌شود و به هر دادنامه یک کد داده می‌شود (Elliot et al., 2016, p. 13) و در سند دیگری، به‌صورت جداگانه، اطلاعاتی که نشان می‌دهد هر کد متعلق به کدام دادنامه است نگهداری می‌شود.

مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا مستعارسازی را چنین تعریف می‌کند: «پردازش دادهٔ شخصی به‌گونه‌ای که دیگر نتوان دادهٔ شخصی را بدون استفاده از اطلاعات اضافی به شخص موضوع داده نسبت داد؛ مشروط بر اینکه این اطلاعات اضافی جداگانه نگهداری شود و با استفاده از اقدامات فنی و سازمانی، اطمینان حاصل گردد که داده‌های شخصی به یک شخص حقیقی شناسایی‌شده یا قابل‌شناسایی نسبت داده نمی‌شود[2].» به‌عبارت‌دیگر، مستعارسازی احتمال شناسایی شخص موضوع داده را کاهش می‌دهد[3]. گروهی دیگر، مستعارسازی را روشی می‌دانند که شناسه‌های مستقیمی را که سبب شناسایی فرد می‌شود با نام یا کد ساختگی جایگزین می‌کند (Rubinstein & Hartzog, 2016, p. 710). با اینکه چنین داده‌هایی بدون اطلاعات اضافی سبب شناسایی فرد نمی‌شوند، هنوز هم شناسایی فرد ناممکن نیست و همچنان احتمال منطقی شناسایی باقی است. درنتیجه، همان‌طور که از تعریف مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا برمی‌آید، این داده‌ها هنوز شخصی به‌شمار می‌آیند و از حمایت مقررات مربوط به حفاظت از داده‌ها برخوردار خواهند بود (Mourby et al., 2018, p. 225).

مستعارسازی درجات مختلفی دارد که برحسب نوع شناسه‌های باقی‌مانده در داده طبقه‌بندی می‌شود. برخی از معیار «یکتایی»[4] برای درجه‌بندی استفاده کرده‌اند (De Montjoye et al., 2015, p. 5) و گفته‌اند که هرچه شناسنده افراد کمتری را دربر بگیرد، درجهٔ بالاتری دارد. برای مثال، شماره‌تلفن همراه یا کارت بانکی به این علت که ارتباط نزدیکی با مالک آن‌ها دارند، دارای ضریب بالایی از یکتایی شخص هستند. همین موضوع سبب می‌شود در داده مستعاری که شامل چنین داده‌هایی باشد، شناسایی شخص موضوع داده با احتمال بالاتری انجام شود. گفتنی است وجود چنین اطلاعاتی در داده سبب می‌شود که مستعارسازی با اطمینان‌پذیری کمتری انجام شود.

دادهٔ مستعار و داده‌ای که از فرایند ناشناس‌سازی گذشته است شباهت‌هایی به هم دارند: هر دو دستخوش تغییر شده‌اند و برای همین هم شناسایی شخص موضوع داده آسان نیست. تفاوت این دو داده در شدت تغییرات اعمال‌شده است: در فرایند ناشناس‌سازی، تغییرات به‌حدی است که دیگر امکان شناسایی شخص موضوع داده وجود ندارد؛ در حالی که امکان شناسایی شخص در دادهٔ مستعار وجود دارد و ابزار مورد نیاز برای شناسایی نیز در دسترس است؛ البته ممکن است همهٔ افراد این ابزار را در اختیار نداشته باشند.

اتحادیهٔ اروپا داده‌ای را که از فرایند ناشناس‌سازی گذشته از دادهٔ مستعار تفکیک کرده است و مورد اول را برخلاف دادهٔ مستعار، از شمول مقررات حفاظت از داده‌ها خارج کرده و چنین داده‌ای را شخصی ندانسته است (Article 29 Data Protection Working Party, 2014, p. 5). اشاره‌ای به مستعارسازی در قانون حفاظت از حریم شخصی مصرف‌کنندهٔ ایالت کالیفرنیای آمریکا دیده می‌شود. به حکم این قانون، مستعارسازی «پردازش دادهٔ شخصی [است] به‌گونه‌ای که بدون استفاده از اطلاعات اضافی، اطلاعات شخصی دیگر به یک مصرف‌کنندهٔ خاص قابل‌انتساب نباشد. اطلاعات اضافی نیز [باید] به صورت جداگانه نگهداری شوند و مشمول اقدامات فنی و سازمانی در جهت اطمینان از این موضوع که اطلاعات شخصی به یک مصرف‌کننده شناسایی شده یا قابل‌شناسایی مرتبط نیست، قرار گیرند[5].» این قانون تا حد زیادی از مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا الهام گرفته است؛ به‌گونه‌ای که آن را نسخهٔ کم‌حجم مقررات عمومی حفاظت از داده‌ها خوانده‌اند

1. pseudonymisation
2. GDPR.art 4(5)
3. GDPR.recital 28
4. unicity
5. California Civil Code §1798.140(r)

(Slefo, 2018) و تعریف عرضه‌شده در این ماده نیز تقریباً با تعریف مقررات عمومی حفاظت از داده‌ها یکسان است. همان‌طور که از ظاهر این تعریف برمی‌آید، در این قانون دادهٔ مستعار کماکان شخصی به شمار می‌رود و موضوع حقوق و تکالیف این قانون خواهد بود. بااین‌حال، در بعضی از قوانین حفاظت از داده‌های ایالات متحده به مستعارسازی اشاره‌ای نشده است[1] و قانونگذار تفکیکی میان دادهٔ ناشناس و مستعار قائل نشده است.

۲-۳. دادهٔ ناشناس

در مقابل دادهٔ شخصی، دادهٔ ناشناس قرار دارد و آن داده‌ای است که از ابتدا به شخص مشخص یا قابل‌شناسایی مربوط نیست یا طی فرایند ناشناس‌سازی از شخص موضوع داده به‌کلی جدا شده است[2]. بدین‌ترتیب، ناشناس‌سازی فرایندی است که در آن، با استفاده از روش‌هایی، دادهٔ شخصی را به‌گونه‌ای تغییر می‌دهند که دیگر به شخص موضوع داده مربوط نیست.

گروهی بر این باورند که ناشناس‌سازی داده‌ای که برای عموم منتشر می‌شود ممکن نیست (Rubinstein & Hartzog, 2016, p. 705). در مقابل، در دفاع از ناشناس‌سازی گفته‌اند، فارغ از جنبهٔ نظری بحث، امکان شناسایی بسیاری از داده‌های ناشناس‌سازی‌شده[3]، در کمترین حالت ممکن است و در عمل، حفاظت از حریم شخصی افراد پس از ناشناس‌سازی مقدور است (Yakowitz, 2011, p. 3). تحلیل این دو دیدگاه و پاسخ به این سؤال که آیا داده‌ای که از فرایند ناشناس‌سازی گذشته دادهٔ شخصی به‌حساب می‌آید یا نه، به معیار ناشناس‌بودن داده بستگی دارد. در این مورد، دو نظریهٔ مطلق و نسبی ابراز شده است. در نظریهٔ مطلق، در هیچ فرضی، نباید امکان شناسایی شخص موضوع داده وجود داشته باشد (Spindler & Schmechel, 2016, p. 165). به بیان دیگر، برای این‌که دادهٔ ناشناس‌سازی‌شده دیگر شخصی نباشد، نباید با صرف هر هزینه‌ای یا به‌کاربستن هر نوع امکانات و یا فناوری‌ای توان شناسایی شخص موضوع داده وجود داشته باشد؛ اما در نظریهٔ نسبی، همین که احتمال منطقی برای شناسایی شخص موضوع داده وجود نداشته باشد، برای این‌که داده‌ای ناشناس به شمار رود، کافی است. در این نظریه، احتمال ترکیب‌کردن دادهٔ ناشناس‌سازی‌شده با سایر اطلاعات، هزینه و فناوری‌های موجود بررسی می‌شود و درصورتی‌که احتمال شناسایی به‌حدی کم باشد که بتوان از آن چشم‌پوشی کرد، داده ناشناس تلقی می‌شود. به نظر می‌رسد نظریهٔ نسبی منطقی‌تر باشد و سبب حفظ تعادل در قوانین حفاظت از داده‌ها شود و از فروریختن نظام حفاظت از داده‌ها، به‌علت گستردگی انواع داده‌های حمایت‌شده، جلوگیری کند (Tene & Polonetsky, 2012, p. 256).

در مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، تمایل به هر دو نظریهٔ مطلق و نسبی دیده می‌شود. در توضیح شمارهٔ ۲۶ این مقررات[4] در مقام تعیین شخص قابل‌شناسایی از «ابزارهای معقول جداسازی» نام برده شده که به نظریهٔ نسبی نزدیک است و از طرف دیگر، به درنظرگرفتن ابزارهای معقول شناسایی از سوی هر شخص دیگری غیر از کنترل‌کننده تکلیف شده است و گویا مقررات بدین‌ترتیب به نظریهٔ مطلق نزدیک شده است؛ زیرا از این عبارات برمی‌آید که چنین امکاناتی نباید در اختیار هیچ شخصی در جهان باشد، تا داده ناشناس به شمار آید. البته ناگفته نباید گذاشت که چون ابزارهای معقول شناسایی باید قانونی باشند، شمار آن‌ها به‌طور چشمگیری کاهش می‌یابد (Campos Sanchez-Bordona, 2016). به‌هرحال، با توجه به ادامهٔ توضیح شمارهٔ ۲۶ که معیارهایی نظیر هزینه و زمان برای شناسایی را در تشخیص ابزار معقول مؤثر می‌داند و همچنین نظریهٔ کارگروه مادهٔ ۲۹ که به‌موجب آن: «برای قابل‌شناسایی‌بودن شخص، صرف وجود یک احتمال فرضی برای تمیز از دیگران کافی نیست» (Article 29 DataProtection Working Party, 2007, p. 22)، می‌توان چنین نتیجه گرفت که در اتحادیهٔ اروپا،

1. Florida Digital Bill of Rights (FDBR)
2. GDPR.retical26; DIRECTIVE 95/46/EC.recital 26
3. anonymized data
٤. «...برای مشخص‌کردن اینکه شخص حقیقی قابل شناسایی می‌باشد یا خیر، باید تمامی ابزار های احتمالی معقول مانند جداسازی که توسط کنترل‌کننده داده یا یک شخص حقیقی دیگر، به‌صورت مستقیم یا غیرمستقیم مورد استفاده قرار می‌گیرد را مورد بررسی قرار داد. برای مشخص‌کردن ابزارهای معقول شناسایی شخص حقیقی، باید تمامی عوامل نظیر هزینه و زمان مورد نیاز برای شناسایی، فناوری‌های زمان پردازش و توسعهٔ فناوری، مورد توجه قرار گیرد...»

نظریهٔ نسبی بر نظریهٔ مطلق ارجحیت دارد. بااین‌حال، براساس قوانین این اتحادیه، برای آن‌که داده‌های ناشناس‌سازی‌شده دیگر شخصی محسوب نشوند، فرایند ناشناس‌سازی باید بازگشت‌ناپذیر باشد. تأثیر قطعی‌نبودن قوانین حفاظت از داده‌های اتحادیهٔ اروپا در رد یا قبول نظریهٔ نسبی را می‌توان در قوانین ملی کشورهای این اتحادیه نیز دید. برای مثال، در فرانسه ناشناس‌سازی فرایندی قطعی است، ولی درعین‌حال داده هنگامی ناشناس به شمار می‌رود که در عمل، امکان شناسایی شخص موضوع داده وجود نداشته باشد (National Commission on Informatics and Liberty, 2019).

در قوانین متعددی در ایالات متحدهٔ آمریکا، ازجمله قانون قابلیت انتقال و مسئولیت بیمهٔ سلامت، قانون حریم شخصی راننده[1]، قانون فدرال حقوق تحصیلی و حریم شخصی[2] و مقررات فدرال مدیریت دارو[3]، اشاراتی به ناشناس‌سازی دیده می‌شود. نزد مؤسسهٔ ملی استاندارد و تکنولوژی[4] این کشور، ناشناس‌سازی «ابزاری است که سازمان‌ها می‌توانند برای حذف اطلاعات شخصی از داده‌های شخصی که جمع‌آوری، استفاده، بایگانی و اشتراک‌گذاری شده، استفاده کنند» (Garfinkel, 2015, p. 1). قانون قابلیت انتقال و مسئولیت بیمهٔ سلامت، دادهٔ ناشناس را داده‌ای می‌داند که هویت شخص موضوع داده را افشا نمی‌سازد و همچنین زمینهٔ معقولی برای شناسایی او فراهم نمی‌کند[5]. این قانون، با قبول دیدگاه نسبی، دو روش را برای ناشناس‌سازی می‌پذیرد: در روش نخست، ناشناس‌سازی به دست متخصص و با استفاده از اصول و روش‌های علمی و آماری ناشناس‌سازی انجام می‌شود؛ به‌گونه‌ای‌که احتمال شناسایی شخص موضوع داده، با استفاده از داده به‌تنهایی یا با ترکیب داده‌هایی که معمولاً در اختیار گیرنده است ناچیز باشد. روش دیگر، پاک‌کردن شناسه‌هایی نظیر نام، تاریخ وقایع، شمارهٔ‌تلفن، شمارهٔ پلاک، شمارهٔ پروندهٔ پزشکی، شناسه‌های زیستی مثل اثر انگشت و...، از داده‌هاست. همچنین سازمان مدنظر نباید از این نکته اطمینان داشته باشد که می‌توان با استفاده از این اطلاعات شخص موضوع داده را شناسایی کرد (Portability & Act, 2012, p. 7). در این قانون، داده‌های شخصی همچنان مشمول ضوابط خاصی مانند ذخیره به‌صورت رمزگذاری هستند؛ اما درصورتی‌که داده‌ای به‌طورکلی ناشناس‌سازی شود، دیگر دادهٔ حفاظت‌شده به شمار نخواهد رفت و نیازی به اعمال مقررات این قانون درمورد آن نیست. به‌عبارت‌دیگر، چنین داده‌ای دیگر شخصی به‌حساب نمی‌آید[6].

در کشور ما بند ۱-۴ دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوهٔ جمع آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی مصوب کمیسیون عالی تنظیم مقررات فضای مجازی کشور، ارائه‌دهندگان را موظف کرده است تا داده‌های شخصی کاربران را صرفاً به‌صورت رمزنگاری شده ذخیره کنند. رمزگذاری با ناشناس‌سازی در شیوهٔ اجرا و هدف دارای تفاوت‌هایی هستند. در رمزگذاری داده‌ها به‌گونه‌ای تغییر می‌کنند که تنها با استفاده از کلید مخصوص قابل دسترسی هستند؛ اما در ناشناس‌سازی داده‌ها قابل استفاده هستند و صرفاً به شخص خاصی مربوط نیستند. این مورد سبب تفاوت مقررات عمومی حفاظت از داده‌ها و دستورالعمل ذکرشده می‌شود؛ زیرا دادهٔ ناشناس به‌کلی از شمول قانون حفاظت از داده‌ها خارج است؛ درحالی که دادهٔ رمزگذاری شده چنین نیست. شایسته است در دستورالعمل‌های آتی نیز به ناشناس‌سازی توجه شود و ضوابط مربوطه نیز با درنظرگرفتن نظریهٔ نسبی، به‌تفصیل بررسی شود.

۲-۴. آی‌پی‌آدرس

اغلب کاربران در محیط اینترنت گمان می‌کنند که ناشناس هستند. گروهی از آنان نیز با برگزیدن نام مستعار تلاش می‌کنند از حریم شخصی خود محافظت کنند؛ در حالی که برخلاف آنچه می‌پندارند، شناسایی افراد در این محیط حتی در بعضی موارد آسان‌تر از محیط واقعی است. آی‌پی‌آدرس شناسهٔ یکتایی است که هر رایانهٔ متصل به اینترنت دارد (Shue & Gupta, 2010, p. 3235). شرکت‌های خدمات‌دهندهٔ اینترنت[7]،

1. Driver's Privacy Protection Act
2. Federal Education Rights and Privacy Act (FERPA)
3. Federal Drug Administration Regulations
4. National institute of standards and technology
5. CFR § 164.514 (a)
6. CFR § 164.502 (d) (2)
7. Internet service provider (ISP)

که آی‌پی را در اختیار کاربران خود قرار می‌دهند، معمولاً اطلاعات مربوط به آن را، که نشان‌دهندهٔ این است که هر آی‌پی به کدام رایانه و در اکثر موارد به کدام کاربر تعلق دارد، نگهداری می‌کنند (et al., 2001, p. 192). معنای این نگهداری این است که اگر هر شبکهٔ اجتماعی، سایت یا بلاگ اینترنتی که از آن استفاده می‌کنیم آی‌پی ما را ذخیره کند و موقعیت مکانی ما نیز برای آن‌ها معلوم باشد، شناسایی ما (افراد)، با استفاده از اطلاعاتی که شرکت‌های خدمات‌دهندهٔ اینترنت در اختیار دارند، کار پیچیده و پرهزینه‌ای برای آن‌ها نخواهد بود.

درمورد دادهٔ شخصی‌بودن آی‌پی، نظرات متفاوتی وجود دارد. اختلاف اساسی به این نکته بازمی‌گردد که اطلاعات مورد نیاز برای شناسایی شخص موضوع داده در اختیار عموم مردم نیست و برای همین هم، بنابر تعریف پذیرفته‌شده از دادهٔ شخصی، آی‌پی ممکن است دادهٔ شخصی یا ناشناس قلمداد شود. به‌عبارت‌دیگر، درصورتی‌که معیار شناسایی را صرفاً اطلاعات در اختیار کنترل‌کنندهٔ داده[1] در نظر بگیریم و کنترل‌کننده نیز فاقد اطلاعات لازم برای شناسایی شخص موضوع داده باشد، داده ناشناس تلقی می‌شود؛ اما اگر بپذیریم که اطلاعات لازم برای شناسایی نباید در اختیار هیچ شخصی، ازجمله شرکت‌های خدمات‌دهندهٔ اینترنت باشد، آی‌پی، دادهٔ شخصی به شمار می‌رود؛ زیرا چنین شرکت‌هایی، با توجه به اطلاعاتی که در اختیار دارند، می‌توانند شخص موضوع داده را از دیگران تمییز دهند. دیدگاه اول را دادگاه سوم تجدیدنظر ایالات متحده پذیرفته است؛ بدین‌ترتیب که این دادگاه رأیی را در سال ۲۰۱۶ تأیید کرده که در آن، شناسه‌های دیجیتال مانند مک‌آدرس[2] و آی‌پی‌آدرس، اطلاعات قابل‌شناسایی شخصی[3] محسوب نشده بودند و موضوع قانون حفاظت از حریم شخصی ویدئوها نیز قرار نمی‌گرفتند[4]؛ زیرا طبق تعریف این قانون، اطلاعات قابل شناسایی فقط شامل مواردی می‌شود که یک شخص معمولی قادر باشد آن را شناسایی کند؛ درحالی‌که آی‌پی در اختیار هر شخصی نیست و فقط ارائه‌دهندگان اینترنت از آن مطلع هستند.

دیدگاه دوم که براساس آن داده باید نسبت به همهٔ اشخاص غیرقابل‌شناسایی باشد، در پروندهٔ مشهور Breyer v Germany[5] در اتحادیهٔ اروپا پذیرفته شده است. در این پرونده، آقای بریر به چندین وب‌سایت دولتی برخورده بود که اطلاعات مربوط به نحوهٔ دسترسی را در بخش تاریخچهٔ دسترسی ذخیره می‌کردند. این اطلاعات شامل آی‌پی کاربر بود که پیوسته به‌روزرسانی می‌شد. در این پرونده، دادستان کل معتقد بود همین که احتمال منطقی برای شناسایی شخص موضوع داده وجود نداشته باشد، کافی است و در چنین مواردی ریسک شناسایی فرد پایین است؛ درنتیجه، آی‌پی پویا دادهٔ شخصی محسوب نمی‌شود؛ اما دادگاه، برخلاف نظر دادستان مقرر کرد که آی‌پی پویا[6] دادهٔ شخصی تلقی می‌شود؛ حتی در شرایطی که فقط شخص ثالثی (در این فرض شرکت‌های فراهم‌کننده سرویس اینترنت) با استفاده از اطلاعات اضافی امکان شناسایی شخص موضوع داده را داشته باشد. در نظر دادگاه، امکان ترکیب آی‌پی پویا با اطلاعات اضافی که شرکت‌های خدمات اینترنتی ارائه می‌کنند، یکی از نمونه‌های ابزار معقول شناسایی (موضوع توضیح ۲۶ مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا) است[7].

در کشور ما نیز بند ۴ مادهٔ ۹ شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی، آی‌پی رایانهٔ شخصی را از مصادیق دادهٔ شخصی دانسته است که به نظر به دیدگاه دوم نزدیک است.

---

۱. کنترل‌کننده به معنی شخص حقیقی یا حقوقی یا مقام عمومی، آژانس یا هر نهاد دیگری که به‌تنهایی یا مشترکاً با دیگران، هدف و ابزارهای پردازش داده‌های شخصی را مشخص می کند (GDPR. art4 (7)).

2. media access control (MAC)

۳. اصطلاحی که در قوانین ایالات متحده برای دادهٔ شخصی استفاده می‌شود.

٤. ACA INTERNATIONAL, ET AL v. FEDERAL COMMUNICATIONS COMMISSION AND UNITED STATES .

متن کامل رای ازطریق لینک زیر قابل دسترسی است:

https://epic.org/wp-content/uploads/amicus/vppa/nickelodeon/3111946001-Appellant-Brief.pdf (last visited: 2023/12/21)

5. این پرونده، که در سال ۲۰۲۰ در دادگاه حقوق بشر اروپا بررسی شد، ازطریق لینک زیر قابل دسترسی است:

https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN (last visited: 2023/12/21)

6. dynamic IP addresses

7. Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016]. Para 45.

۳. دادهٔ شخصی حساس

در میان داده‌های شخصی، حمایت از نوع خاصی از داده به‌سبب حساسیت‌هایی که برای شخص موضوع داده ایجاد می‌کند مستلزم وجود قوانین سخت‌گیرانه‌تری است. دادهٔ شخصی حساس[1] داده‌ای است که به شخصی‌ترین امور زندگی افراد مربوط است و اغلب مردم ابداً راضی به فاش‌شدن آن نیستند (Gutwirth et al., 2009, p. 4). نخستین بار دستورالعمل حفاظت از حریم شخصی و جریان‌های فرامرزی داده‌های شخصی[2] وجود نوع خاصی از دادهٔ شخصی با نام دادهٔ حساس را اعلام کرد. در این دستورالعمل، به کشورها توصیه شده بود که مفهوم دادهٔ حساس را وارد قوانین خود کنند؛ هرچند که در آن معیاری برای تعریف این نوع داده بیان نشده بود[3]. داده‌های حساس موضوع حفاظت‌ها و محدودیت‌های بیشتر در پردازش هستند؛ به‌طوری‌که اصل و قاعده، ممنوعیت پردازش این نوع داده‌ها[4] است. بااین‌حال چند استثنا، مانند رضایت صریح شخص موضوع داده[5] یا عمومی‌شدن داده‌ها از طریق شخص موضوع داده[6] در این باب پذیرفته شده است.

در تعیین معیار تفکیک دادهٔ حساس از سایر داده‌های شخصی، دیدگاه‌های مختلفی وجود دارد. مادهٔ ۹ قانون حفاظت از داده‌های اتحادیهٔ اروپا دیدگاه موضوعی را پذیرفته و براین‌اساس، داده‌هایی را دادهٔ حساس شمرده است که دربردارندهٔ اطلاعاتی در موضوعاتی خاص باشند. بنا بر این ماده، داده‌هایی که بیان‌کنندهٔ نژاد، ریشهٔ نژادی، گرایش سیاسی، باورهای مذهبی یا سیاسی، عضویت در اتحادیه‌های کارگری و پردازش داده‌های مرتبط با سلامتی و زندگی جنسی یا گرایش جنسی فرد باشند، دادهٔ حساس[7] تلقی می‌شوند. دیوان دادگستری اتحادیهٔ اروپا در رأیی در سال ۲۰۰۳ حتی از این هم فراتر رفته است و اشاره به این نکته را که پای فردی مجروح شده و او به همین دلیل مجبور شده تا نیمه‌وقت کار کند دادهٔ حساس شمرده است[8]؛ البته برخی بر این نظرند که با توجه به توضیح شمارهٔ ۵۱ مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا[9] به نظر می‌رسد حساس‌بودن داده امری مطلق نیست و تا حد زیادی به لحظهٔ ارزیابی داده بستگی دارد (Ausloos, 2020 , p. 137).

برخلاف اتحادیهٔ اروپا، قانونگذار آمریکایی تعریف جامعی از دادهٔ حساس ارائه نداده است و تنها در قوانینی مانند قانون قابلیت انتقال و مسئولیت بیمه سلامت[10]، قواعد ویژه‌ای برای پردازش انواع خاصی از داده‌ها مقرر شده است. اکثر فروضی که در سایر کشورها دادهٔ حساس تلقی می‌شوند و اقدامات خاصی برای حفاظت از آنها لازم است، در ایالات متحدهٔ آمریکا به عنوان دادهٔ حساس پذیرفته نشده است (Schwartz & Solove, 2014, p. 906).

درمورد تعیین معیاری برای حساس‌بودن داده‌ها، گروهی بر این باورند که هر داده، بسته به شرایط، می‌تواند حساس قلمداد شود و در هر مورد، باید عواملی نظیر منافع پردازش‌کنندهٔ داده، هدف از پردازش و شرایط و عواقب احتمالی پردازش را در نظر گرفته ود و سپس حساس‌بودن بررسی شود و درنتیجه، تعیین معیاری به‌صورت کلی ممکن نیست (Quinn & Malgieri, 2021. p. 1591). برهمین‌اساس، پذیرفتن تعریف ثابت و قبول رویکرد موضوعی نسبت به دادهٔ حساس خود می‌تواند سبب پدیدآمدن مشکلات دیگری شود؛ زیرا ممکن است بتوان با استفاده از سایر اطلاعات یا الگوریتم‌های رایانه‌ای، که به‌صورت روزافزون در دسترس قرار می‌گیرند، به دادهٔ حساس نیز دست یافت.

---

1. sensitive personal data
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1(last visted: 2024/12/1)

۳. در پاراگراف ۱۹ این دستورالعمل آمده است که احتمالاً غیرممکن است که مجموعه‌ای از داده‌ها را بیابیم که به‌صورت جهانی حساس در نظر گرفته شوند.

4. GDPR.art9 (1)
5. GDPR.art 9 (1)(a)
6. GDPR.art9 (1)(e)
7. البته این ماده از عبارت «نوع خاصی از دادهٔ شخصی» استفاده کرده است که با توجه به تاریخچهٔ این موضوع و موارد عنوان‌شده، مفهومی متفاوت از دادهٔ شخصی حساس ندارد.
8. Lindqvist (2003) Court of Justice of the European Union C- 101/ 01
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101 (last visited: 2023/12/1)

۹. در این ماده، عکس به ور مطلق دادهٔ حساس به‌شمار نمی‌آید و فقط زمانی حساس تلقی می‌شود که با استفاده از ابزارهایی خاص، که در لحظهٔ پردازش در دسترس است، شخصِ موضوعِ داده قابل‌شناسایی باشد.

10. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

در مادهٔ ۵۸ قانون تجارت الکترونیکی کشور ما بدون نام‌بردن از دادهٔ حساس، ذخیره و پردازش داده‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا جنسی بدون رضایت صریح اشخاص غیرقانونی اعلام شده است. البته در این قانون داده‌هایِ شخصیِ حساس محدود به موضوعات خاصی است و برای همین از پویایی لازم برخوردار نیست و این امر، با توجه به ثابت نبودن دو مفهوم «دادهٔ شخصی» و «حساسیت»، قابل‌انتقاد است.

نتیجه‌گیری

دادهٔ شخصی، به عنوان دروازهٔ ورود به قوانین حفاظت از داده‌ها، اهمیت ویژه‌ای دارد؛ چنان‌که در بسیاری از قوانین تعریفی از آن عرضه کرده‌اند و گاه نوعی خاص از داده را شخصی به حساب آورده‌اند. بااین‌حال در اکثر قوانین، هر داده‌ای را که با آن بتوان شخصی را شناسایی کرد، شخصی قلمداد کرده‌اند و بدین‌ترتیب، از مفهومی انعطاف‌پذیر بهره برده‌اند. نکته‌ای که از بررسی عناصر تعریف دادهٔ شخصی فهمیده می‌شود آن است که در هر مورد باید شرایط را در نظر گرفت و نمی‌توان حکمی مطلق و کلی دربارهٔ شخصی‌بودن یا نبودن نوعی از داده‌ها صادر کرد. ممکن است داده‌ای در شرایطی خاص شخصی به‌حساب آید؛ درحالی‌که همان داده در شرایط دیگری ناشناس محسوب شود. با توجه به این نکته، تعیین مصادیق قطعی دادهٔ شخصی دشوار است. بر سر شخصی‌بودن مواردی خاص نظیر نام خانوادگی به همراه شناسهٔ دیگر و داده مستعار در سیستم‌های حقوقی اروپا و اتحادیهٔ اروپا اتفاق نظر وجود دارد، درحالی‌که مواردی مانند آی‌پی‌آدرس و داده‌ای که از فرایند ناشناس‌سازی گذشته است اختلاف نظر باقی است. درنهایت، بعضی از داده‌های شخصی حساسیت بیشتری دارند و به‌تبع نیازمند حفاظت ویژه‌ای هستند. تعیین این نوع از داده‌های شخصی نیز به‌صورت کلی ممکن نیست و مصادیق دادهٔ حساس بسته به نظر قانون‌گذار و تحلیل موارد خاص است. دربارهٔ نظام حقوقی ایران پیشنهاد می‌شود در قوانین جامعی که برای حفاظت از داده‌های کاربران در دست تصویب است، دادهٔ شخصی، با درنظرداشتن و پذیرش رویکرد تحلیلی تعریف شود و با توجه به پیشرفت‌های روزافزون در عرصهٔ شناسایی داده‌های ناشناس، به‌صورت موسع تفسیر شود؛ شیوه‌ای که در مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا و سایر قوانین کشورهای پیشرو در حوزهٔ حفاظت از داده‌ها مورد پذیرش قرار گرفته است. همچنین با توجه به لزوم انتشار برخی اطلاعات نظیر آرای دادگاه‌ها، آیین‌نامه‌ای برای ناشناس‌سازی داده‌ها تصویب و معیاری منطقی برای تعیین دادهٔ ناشناس مشخص شود تا ضمن حفظ حریم شخصی، جامعه بتواند از مزایای انتشار اطلاعات ناشناس‌سازی‌شده بهره‌مند شود. همچنین به تفاوت دادهٔ ناشناس و دادهٔ رمزگذاری‌شده توجه شده و هرکدام در جای مخصوص به خود استفاده شود. جزئیات این فرایندها نیز به‌تفصیل تعیین شود تا ارائه‌دهندگان خدمات به‌خوبی از وظایف خود آگاه باشند و زمینهٔ تفسیر نادرست به حداقل برسد. به دادهٔ شخصی حساس در مصوبات و آیین‌نامه‌های کشور ما به‌ندرت پرداخته شده است. با توجه به این‌که چنین داده‌هایی از اهمیت ویژه‌ای برخوردار بوده و انتشار آن‌ها آسیب‌های جبران‌ناپذیری به شخص موضوع داده وارد می‌کند، تهیهٔ نظام ویژه‌ای برای پردازش چنین داده‌هایی ضروری است تا پردازش و ذخیرهٔ دادهٔ شخصی حساس با محدودیت‌های بیشتری به‌نسبت سایر داده‌های شخصی انجام شود. در تعیین دادهٔ شخصی حساس نیز رویکرد تحلیلی مورد توجه قرار گیرد و فقط به ذکر چند مورد بسنده نشود.

منابع

احمدوند بهناز، و جهانشاهی آرتین (۱٤۰۲). بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیهٔ اروپا و ایران. پژوهش‌های حقوق تطبیقی، ۲۷(۱)، ۱۰۵-۱۳۲. https://doi.org/20.1001.1.22516751.1402.27.1.6.5

انصاری، باقر و انصاری، اسماعیل (۱۳۹۱). حقوق اطلاعات از منظر تحلیل اقتصادی. مطالعات حقوق تطبیقی، ۳(۲)، ۱-۲۱. https://doi.org/10.22059/jcl.2012.32109

قناد، فاطمه، و علیقلی، امیره. (۱۳۹۹). مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی. حقوق فناوری‌های نوین، ۱(۱)، ۲۹۷- ۳۲۲. لینک

Ausloos, J. (2012). The ‘right to be forgotten’–worth remembering? Computer Law & Security Review, 28(2), 143-152. https://doi.org/10.1016/j.clsr.2012.01.006

Ausloos, J. (2020). The Right to Erasure in EU Data Protection Law. United Kingdom: Oxford University Press, USA. https://doi.org/10.1093/oso/9780198847977.001.0001

Bahadur, G., Weber, C., & Chan, W. (2001). Privacy defended: Protecting yourself online. Que Corp. Link

Bragg, C. (2017). Data Breach Notification: State Law Requirements. Link

De Montjoye, Y. A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. Science, 347(6221). https://doi.org/10.1126/science.1256297

Portability, I., & Act, A. (2012). Guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability act (HIPAA) privacy rule. Link

Elliot, Mark, Mackey, Elaine, O'Hara, Kieron and Tudor, Caroline (2016) The Anonymisation Decision-Making Framework, Manchester, GB. UKAN. Link

Floridi, L. (2009). Philosophical conceptions of information. In Formal theories of information: From Shannon to semantic information theory and general concepts of information (pp. 13-53). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-00659-3_2

Floridi, L. (2015). The onlife manifesto: Being human in a hyperconnected era (p. 264). Springer Nature. https://doi.org/10.1007/978-3-319-04093-6

Garfinkel, S. (2015). De-identification of Personal Information: (pp. 1-46). US Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8053

Slefo, G. P. (2018). Marketers and Tech Companies Confront California's Version of GDPR, ADAGE. Link

Radwanski, G. (2003). Office of the Privacy Commissioner of Canada, Annual Report to Parliament 2001–2002. Link

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., & Nouwt, S. (Eds.). (2009). Reinventing data protection? Springer Science & Business Media. https://doi.org/10.1007/978-1-4020-9498-9

Korff, D. (2008). The difficulties in Meeting the Challenges Posed by Global Social and Technical Developments. London Metropolitan University, European Commission Comparative Study. Working paper. Link

Kuner, C. (2007). European data protection law: Corporate compliance and regulation. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199289486.001.0001

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. Computer Law & Security Review, 29(3).229-235. Link

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt. Link

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., & Kaye, J. (2018). Are 'pseudonymised'data always personal data? Implications of the GDPR for administrative data research in the UK. Computer Law & Security Review, 34(2), 222-233. https://doi.org/10.1016/j.clsr.2017.11.004

National Commission on Informatics and Liberty. (2019). Comment prévenir les risques et organiser la sécurité de vos données. Link

Office of Consumer Affairs & Business Regulation. (2023). Massachusetts data breach notification law. Link

Sanchez-Bordona, C. (2016). Opinion of Advocate General Campos Sdnchez-Bordona, delivered on 12 May 2016, Case C-582/14 - Patrick Breyer v Bundesrepublik Deutschland. Link

Party, D. P. W. (2007). Opinion 4/2007 on the concept of personal data. Brussels, Belgium: European Commission. Link

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40-81. https://doi.org/10.1080/17579961.2018.1452176

Quinn, P., & Malgieri, G. (2021). The difficulty of defining sensitive data—The concept of sensitive data in the EU data protection framework. German Law Journal, 22(8), 1583-1612. https://doi.org/10.1017/glj.2021.84

Rubinstein, I. S., & Hartzog, W. (2016). Anonymization and risk. Wash. L. Rev., 91, 703-760. Link

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220. https://doi.org/10.2307/1321160

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. NYUL rev., 86.1814-1894. link

Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. Calif. L. Rev., 102, 877-916. https://doi.org/10.2139/ssrn.2271442

Spindler, G., & Schmechel, P. (2016). Personal data and encryption in the European general data protection regulation. J. Intell. Prop. Info. Tech. & Elec. Com. L., 7. 163-176. link

Sweeney, L. (2000). Simple demographics often identify people uniquely. Health (San Francisco), 671(2000). 1-34. link

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. Nw. J. Tech. & Intell. Prop., 11, 231-268. Link

van der Sloot, B. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system. Computer Law & Security Review, 31(1), 3-13. https://doi.org/10.1016/j.clsr.2014.11.002

Voss, W. G., & Houser, K. A. (2019). Personal data and the GDPR: Providing a competitive advantage for US companies. American Business Law Journal, 56(2), 313-350. https://doi.org/10.1111/ablj.12139

Working Party. (2014). Opinion 05/2014 on Anonymization Techniques (Apr. 10, 2014). Link

Yakowitz, J. (2011). Tragedy of the data commons. Harv. JL & Tech., 25, 1-49. Link

Shue, C. A., & Gupta, M. (2010). An Internet without the Internet protocol. Computer Networks, 54(18), 3232-3245. https://doi.org/10.1016/j.comnet.2010.06.009

[In Persian]

Ahmadvand, B., & Jahanshahi, A. (2023). A comparative study of the concept of personal data in the legal systems of the European Union and Iran. Comparative Legal Research, 27(1), 105-132. https://doi.org/20.1001.1.22516751.1402.27.1.6.5

Ansari, B., & Ansari, E. (2012). Information law from an economic analysis perspective. Comparative Law Studies, 3(2), 1-21. https://dor.isc.ac/dor/20.1001.1.1735496.1391.3.2.1.1

Ghanad, F., & Aligholi, A. (2020). The concept and importance of personal data and privacy and its various protections in cyberspace. New Technologies Law, 1(1), 297-322. Link