-- The Quarterly Journal of Public Law Research ------
Spring 2025, 26 (86), 235- 272
qjpl.atu.ac.ir
DOI: 10.22054/QJPL.2024.77452.2958

Original Research
Received: 30/Dec/2023
Accepted: 07/Oct/2024
ISSN:2345-6116
eISSN:2476-6216

Biometric Data Processing and Its Impact on Private Life: The Legislation of the European Union and the Council of Europe

Rezvaneh Mirzavand * LLM, Human Rights, Allameh Tabataba'i University, Tehran, Iran

Roya Motamednejad Associate Professor, Public Internaional Law, Allameh Tabataba'i University, Tehran, Iran

1. Introduction

Biometrics is derived from two Greek words: bios, meaning life, and metrikos, meaning measurement. Biometrics, or biocompatibility, refers to the practical method of identifying and authenticating individuals using biological, morphological, and behavioral characteristics. Biometric data can be categorized into the three types: biological data, morphological data, and behavioral data. Biological

* Corresponding Author: Rezvaneh_Mirzavand@atu.ac.ir
How to Cite: Mirzavand, R & Motamednejad, R., "Biometric Data Processing and Its Impact on Private Life: The Legislation of the European Union and the Council of Europe", The Quarterly Journal of Public Law Research, Vol. 26, No. 86, (2025), 235-272. Doi: 10.22054/QJPL.2024.77452.2958

data involves traits at the genetic and molecular levels. Examples include DNA properties or blood that can be examined through samples of bodily fluids such as blood, saliva, or urine. Morphological data pertains to an individual's physical structure. This includes features such as the eye (iris and retina), hand shape, fingers, fingerprint, vein patterns, and facial structure. Behavioral data varies based on unique patterns that differ from person to person. Examples include voice recognition, speech patterns, signature dynamics (e.g., speed, swiftness, and pressure), keyboard dynamics, typing patterns, interaction with objects, walking style, the sound of footsteps, and body movements. These patterns can also serve as indicators of individual identity.

Despite the sensitive nature of biometric data, there are currently very few international legal regulations specifically designed to protect it. Most existing legal texts address biometric data in a general sense, only within the broader context of personal data protection and privacy laws.

The current study aimed to explore the opportunities and challenges facing biometric technology, particularly in terms of privacy concerns. It proposed a conceptual framework focused on biometric technology, with an emphasis on European law (specifically those of the European Union and the Council of Europe). The goal was to analyze how legislation can evolve alongside technological advancements and determine which aspects of biometric data require more precise legal protections. European legislation is currently attempting to strike a balance between encouraging innovation in biometric technology and ensuring the protection and security of biometric data. To strengthen

privacy rights in Iran, the experiences and initiatives of the European Union and the Council of Europe can serve as valuable models for inspiration.

2. Literature Review

The approvals available on the European Union and Council of Europe websites allow for the examination of the impact of using biometric data. In this context, particular attention is given to the right to personal data protection and the growing need to strengthen it in the digital age, especially in Europe (Motamed-Nejad, 2019). The book Introduction to Biometrics (Jain et al., 2011) emphasized the importance of biometrics in its final chapter, highlighting the importance of data security and privacy. The edited volume titled Security and Privacy in Biometrics (Campisi, 2013) provided a comprehensive legal analysis of privacy concerns and the protection of biometric data. It also offered several recommendations for establishing a transnational surveillance framework. Another key text is Biometric Security and Privacy: Opportunities and Challenges in the Big Data Era (Jiang et al., 2013). The chapters discussed special biometric technologies, privacy and security issues (e.g., cancelable biometrics and soft biometrics), medical biometrics, healthcare, and human–robot interaction. Moreover, Biometrics in a Data Driven World: Trends, Technologies, and Challenges (Mitra & Gofman, 2017) explores the challenges of using biometric data in social networks, healthcare programs, mobile authentication, etc. The topic has been addressed—directly or indirectly—within the legal frameworks of the European Union and the Council of Europe.

Regulatory documents, including transition regulations in the field of data protection, are also relevant. While the relevant sources may be limited, they can be consulted indirectly.

3. Materials and Methods

The present study employed an analytical approach to examine the regulations of the European Union and the European Council. The library research was used to collect the data, relying on both internet resources and authentic publications such as books and journal articles.

4. Results and Discussion

Biometric data is increasingly used in health-related applications, such as biometric monitoring devices, telemedicine, and electronic health records. Moreover, biometric data plays a role in smart city initiatives, serving purposes like surveillance, public safety, and personalized services. The field of biometric data processing is rapidly evolving, along with its legal and regulatory landscape. New laws, regulations, and guidelines may be necessary to address emerging challenges and ensure the protection of privacy rights. It is thus crucial for organizations and individuals involved in biometric data processing to stay informed about these developments. Research and development in this field can further help reduce privacy risks. In today's digital age, data privacy is a critical concern. As more personal information is shared and stored online, the risks associated with its collection and use continue to grow. A major concern when processing biometric data is the potential for data breaches. Biometric data can also be misused for illegal activities such as fraud, theft, and impersonation.

To address these risks, it is essential that organizations and governments take serious measures to ensure privacy and security, protect civil rights, and prevent discrimination. This includes being transparent about how biometric data is collected and used, obtaining explicit consent from individuals, and enforcing strong security protocols to prevent data breaches. Additionally, biometric systems must be designed and tested to minimize bias and discrimination. It is equally important for individuals to understand the potential risks and consequences of biometric data processing and to take proactive steps to protect their privacy and data security.

5. Conclusion

The use of biometric data can have significant implications for civil freedoms and human rights. As such, legislators play a crucial role in formulating laws and regulations to safeguard the right to privacy and other fundamental rights, especially given the dynamic nature of biometric data processing. Judicial cases and legal procedures also contribute to shaping the legal framework surrounding privacy and biometric data processing. It is essential to offer educational materials and raise awareness about biometric data processing and privacy. Individuals must be informed about the risks, benefits, and their rights in relation to biometric data processing. It is also important to consider the ethical, legal, technological, and social dimensions of biometric technologies to ensure that individual rights and privacy are respected and protected. In an increasingly biometric-driven world, finding the right balance between the potential benefits and risks of these

technologies is critical. Above all, privacy must be upheld as a fundamental human right.

Keywords: Biometric Data, Private Life, Processing, European Union, Council of Europe

مقاله پژوهشی

تاریخ دریافت: ۱۴۰۲/۱۰/۱۹ تاریخ پذیرش: ۱۴۰۳/۰۷/۱۶

ISSN: ۲۳۴۵-۶۱۱۶ eISSN: ۲۴۷۶-۶۲۱۶

-- فصلنامه علمی پژوهش حقوق عمومی ---------

دوره ۲۶، شماره ۸۶، بهار ۱۴۰۴، ۲۳۵-۲۷۲

qjpl.atu.ac.ir

DOI: 10.22054/QJPL.2024.77452.2958

پردازش داده‌های بیومتریک و تاثیر آن بر زندگی خصوصی با تاکید بر قوانین اتحادیه اروپا و شورای اروپا

رضوانه میرزاوند * دانش‌آموخته کارشناسی ارشد حقوق بشر دانشگاه علامه طباطبائی، تهران، ایران

رویا معتمدنژاد دانشیار گروه حقوق عمومی و بین‌الملل دانشگاه علامه طباطبائی، تهران، ایران

چکیده

امروزه با وجود پیشرفت روزافزون فناوری‌ها و برنامه‌های کاربردی، زمینه پردازش داده‌های بیومتریک به طور مداوم در حال تحول است. در این میان به رسمیت شناختن حق بر حریم خصوصی در ارتباط با پردازش داده‌های بیومتریک جنبه مهمی از موضوع حفاظت از داده‌ها و حقوق بشر است. پرسش اصلی مقاله این است که استفاده از داده‌های بیومتریک که بعضا فراتر از هدف احراز هویت یا شناسایی می‌باشد، چه تاثیراتی بر زندگی خصوصی افراد دارد؟ و دیگر اینکه در وضعیتی که قانون ایران به‌طور صریح به داده‌های بیومتریک نپرداخته است؛ چه تدابیری را می‌توان اندیشید؟ یافته‌های پژوهش ناظر برآن است، به علت ماهیت خاص و بسیار حساس داده‌های بیومتریک، نیاز به وجود قوانینی متقن در راستای حفاظت از چارچوب زندگی خصوصی افراد بیش از پیش احساس می‌شود. ایجاد تعادل میان نیاز به امنیت عمومی و حقوق حریم خصوصی یک چالش پیچیده است. همچنین ایجاد چارچوب‌های قانونی روشن، مکانیسم‌های نظارتی و اقدامات پاسخگویی به منظور اطمینان از استفاده قانونی و مسئولانه از داده‌های بیومتریک بسیار حائز اهمیت خواهد بود.

واژگان کلیدی: داده‌های بیومتریک، زندگی خصوصی، پردازش، شورای اروپا، اتحادیه اروپا.

* نویسنده مسئول: Rezvaneh_Mirzavand@atu.ac.ir

مقدمه

بیومتریک از دو کلمه یونانی Bios به معنای زندگی و Metrikos به معنای اندازه‌گیری تشکیل شده است. بیومتریک یا زیست‌سنجی را می‌توان به‌عنوان روشی کاربردی برای شناسایی و احراز هویت افراد از طریق ویژگی‌های بیولوژیکی، مورفولوژیکی و رفتاری منحصر به فرد تعریف کرد. داده بیومتریک را می‌توان به صورت زیر دسته‌بندی نمود: داده بیولوژیکی: داده بیولوژیکی از صفات در سطح ژنتیکی و مولکولی استفاده می‌کند. مانند ویژگی‌های DNA یا خون که ممکن است از طریق نمونه‌ای از مایعات بدن فرد همچون خون، بزاق یا ادرار ارزیابی شود.

داده مورفولوژیکی: شامل ساختار بدن فرد می‌باشد مانند ویژگی‌های فیزیکی چشم (عنبیه، شبکیه)، شکل دست، انگشت، اثر انگشت، الگوی سیاهرگ یا شکل صورت افراد. داده رفتاری: بر اساس الگوهای منحصر به فرد برای هر فردی متفاوت است. از جمله این داده‌ها می‌توان به تشخیص صدا، نحوه صحبت کردن فرد، دینامیک امضا (سرعت حرکت قلم، شتاب‌ها، فشار اعمال شده)، دینامیک ضربه زدن به صفحه کلید، الگوی تایپ، نحوه استفاده از اشیاء، نحوه راه رفتن، صدای قدم‌ها، حرکات و غیره اشاره نمود که این داده‌ها نیز می‌توانند نشانه‌ای از هویت فرد باشند.

تکنولوژی بیومتریک در بخش‌های مختلف به منظور تأیید هویت افراد استفاده می‌شود. از جمله در اجرای قانون، خدمات بهداشتی و درمانی، امور مهاجرت و گمرک، خدمات مدنی، حفظ امنیت، انجام مبادلات تجاری و در نهایت هنگام دسترسی به رایانه و شبکه جهانی اینترنت.[1] با این حال به علت وجود مرزی باریک میان رشد، توسعه و بهره‌برداری از تکنولوژی‌های نوین و همچنین حفظ کرامت انسانی، حقوق بشر و آزادی‌های اساسی؛ همواره دغدغه این که چنین فناوری‌هایی باید مبتنی بر قانون و اخلاق باشند، مورد توجه بوده است و چالش‌های حقوقی بسیاری نیز در رابطه با تشخیص خودکار افراد بر اساس ویژگی‌های بیولوژیکی و رفتاری آنها در تبدیل اطلاعات آنالوگ (تصویر صورت، اثر انگشت، الگوی صدا) به اطلاعات دیجیتال (الگوها، جزئیات) وجود دارد. در این میان از

1. Eric Holder; Jr. Laurie O. Robinson & John H. Laub, *The Fingerprint: Sourcebook*, (New York: Create Space Publishing, 2014) P. 20.

جمله حقوقی که بیشتر در معرض نقض قرار می‌گیرند حق بر زندگی خصوصی افراد می‌باشد. این بدان معناست که ممکن است داده‌های بیومتریک مورد سرقت، سوءاستفاده همچون جعل هویت و در نهایت ابزاری برای دسترسی به اطلاعات حساس افراد شود. همچنین نگرانی‌هایی در مورد نحوه جمع‌آوری و ذخیره داده‌های بیومتریک توسط دولت‌ها و شرکت‌ها وجود دارد.

علاوه بر این از دیگر نگرانی‌ها، جمع‌آوری و استفاده پنهانی از داده‌های بیومتریک بدون در نظر گرفتن عنصر رضایت افراد خواهد بود. با وجود ویژگی بسیار حساس داده‌های بیومتریک، عملاً هیچ مقررات قانونی بین‌المللی برای حفاظت از این داده‌ها در سطح بین‌الملل وجود ندارد و متون حقوقی تنها بر مقررات مربوط به حفاظت از داده‌های شخصی و حریم خصوصی به معنای گسترده و کلی آن تکیه کرده‌اند.[1] در این مقاله تلاش می‌شود برخی از فرصت‌ها و چالش‌های پیش روی تکنولوژی بیومتریک در رابطه با ملاحظات حریم خصوصی افراد بررسی شود. به‌طور خاص این پژوهش چارچوبی مفهومی در قالب تکنولوژی بیومتریک با تاکید بر قوانین اروپا (شورای اروپا و اتحادیه اروپایی) ارائه می‌دهد به گونه‌ای که همگام با پیشرفت تکنولوژی، قوانین در دسترس تا چه اندازه مثمر ثمر می‌باشند و چه جنبه‌هایی نیاز به حفاظت بیشتر از طریق قانونگذاری دقیق‌تر دارند؟ در این میان قوانین اروپا (شورای اروپا و اتحادیه اروپایی) در حال حاضر تلاش می‌کند از یک سو میان قابلیت‌های نوآورانه‌ای که تکنولوژی بیومتریک فراهم می‌کند و از سوی دیگر جمع‌آوری مسئولانه این داده‌ها و ایمن نگه داشتن آنها تعادل ایجاد کند. در راستای حمایت هر چه بیشتر از حق زندگی خصوصی افراد در ایران می‌توان از تجربیات و اقدامات اتحادیه اروپایی و شورای اروپا الهام گرفت.

1. Jain, Anil K, Ross, Arun A. & Nandakumar, Karthik, *Introduction to Biometrics*, (New York: Springer, 2011) P. 302.

۱. مفهوم پردازش داده

در پردازش، داده به دانش و یا اطلاعات تبدیل می‌گردد. به دیگر بیان پردازش داده روشی برای جمع‌آوری داده‌های خام و تبدیل آن به اطلاعات قابل استفاده است. داده‌های خام جمع‌آوری، فیلتر، مرتب‌سازی، پردازش، تجزیه و تحلیل و در نهایت ذخیره می‌شوند و سپس در قالبی قابل خواندن ارائه می‌گردند. کل فرآیند به صورت چرخه‌ای تکرار می‌گردد، به‌گونه‌ای که خروجی اولین مرحله از چرخه پردازش را می‌توان به‌عنوان ورودی برای چرخه بعدی، ذخیره و استفاده نمود.

۲. مفهوم زندگی خصوصی و داده‌های شخصی

تفکیک میان این دو مفهوم در قوانین و اسناد اروپایی دیده می‌شود. ماده ۷ منشور حقوق اساسی اتحادیه اروپا[1] هر کس از حق احترام به زندگی خصوصی و خانوادگی، خانه و مراسلات خود برخوردار است. باید بیان داشت بر اساس بند ۳ ماده ۵۲ منشور حقوق اساسی اتحادیه اروپا[2] حقوق مطرح شده در ماده ۷ این منشور با حقوق تضمین شده در ماده ۸ کنوانسیون اروپایی حقوق بشر[3] (کنوانسیون حمایت از حقوق بشر و آزادی‌های اساسی) مطابقت دارد. حق بر زندگی خصوصی شامل استقلال شخصی، حق انتخاب در مورد زندگی خود بدون دخالت مقامات دولتی، پیشرفت و توسعه شخصیت خود و برقراری روابط با دیگران و نیز برقراری ارتباط است. جنبه‌های حق بر زندگی خصوصی شامل تمامیت جسمی و روانی یک فرد، زندگی جنسی و جنسیت، همچنین اطلاعات شخصی، شهرت، نام و تصاویر وی می‌باشد.

1. Charter of Fundamental Rights.

۲. این منشور حاوی حقوقی است که با حقوق تضمین شده توسط کنوانسیون حمایت از حقوق بشر و آزادی‌های اساسی مطابقت‌دار و نیز مفهوم و دامنه حقوق ذکر شده توسط کنوانسیون حمایت از حقوق بشر و آزادی‌های اساسی همان حقوقی است که در این منشور مقرر شده است.

3. European Convention on Human Rights (ECHR).

با بررسی رویه دادگاه اروپایی حقوق بشر[1] مشاهده می‌شود که محدودیت‌های برشمرده شده در مورد حقوق مندرج در ماده ۷ منشور حقوق اساسی اتحادیه اروپا و نیز ماده ۸ کنوانسیون اروپایی حقوق بشر با سختگیری فراوانی اعمال می‌شوند.[2] دو بعد حریم خصوصی را می‌توان اینگونه بیان نمود: یک بعد رابطه‌ای و یک بعد اطلاعاتی. اولی مربوط به رابطه فرد با افراد دیگر است و گاهی به‌عنوان حریم خصوصی سرزمینی و حریم خصوصی جسمی توصیف می‌شوند. بعد اطلاعاتی نیز به جمع‌آوری، ذخیره و پردازش داده‌های (شخصی) مربوط می‌شود. ویژگی مشترک هر دو بعد حریم خصوصی نیاز به حفظ کنترل بر فضای شخصی، تمامیت جسمی و اطلاعات شخصی است. ماده ۴ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا[3] GDPR در تعریف خود از داده‌های شخصی این‌گونه بیان می‌دارد که: داده‌های شخصی به معنای هرگونه اطلاعات مربوط به یک شخص حقیقی شناسایی شده یا قابل شناسایی (موضوع داده) است. یک شخص حقیقی قابل شناسایی، شخصی است که می‌تواند به طور مستقیم یا غیرمستقیم شناسایی شود، به‌ویژه با ارجاع به یک شناسه همانند نام، شماره شناسایی، داده‌های موقعیت مکانی، شناسه آنلاین یا یک یا چند عامل خاص فیزیکی، فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص حقیقی.[4] همچنین بر اساس ماده ۲ کنوانسیون حفاظت از اشخاص با توجه به پردازش داده‌های شخصی شورای اروپا موسوم به ۱۰۸+[5] داده شخصی عبارت است از: هرگونه اطلاعات مربوط به شخص شناسایی شده یا قابل شناسایی.

1. Paradiso and Campanelli V. Italy, European Court of Human Right. (24 January 2017). [GC] - 25358/12 Judgment 24.1.2017 [GC].

Case of M.L. and W.W. V. Germany, European Court of Human Right. (28 June 2018) (Applications nos. 60798/10 and 65599/10.

Liebscher V. Austria (application No. 5434/17) European Court of Human Right. (6 April 2021).

2. Axel Springer AG v. Germany, (Application no. 39954/08). European Court of Human Right. (7 February 2012).

3. General Data Protection Regulation, (2018).

4. GDPR Clause 1 Article 4.

5. Convention for the Protection of Individuals with Regard to the Processing of Personal Data Article 2.

باید توجه داشت بر اساس اسناد مذکور، این مفهوم، دامنه بسیار فراگیری دارد و شامل اطلاعات عینی مانند قد یک فرد و یا اطلاعات ذهنی مانند ارزیابی‌های شغلی، سابقه پزشکی یا سوابق کیفری است. علاوه بر این، سوابق مربوط به مصرف برق و آب نیز به‌عنوان اطلاعات شخصی در نظر گرفته می‌شود زیرا این اطلاعات برای تعیین الگوی رفتار مصرف یک فرد استفاده می‌شود. همچنین این مفهوم به هیچ قالب خاصی محدود نمی‌شود. داده‌های ویدئویی، صوتی، عددی، گرافیکی و تصاویر می‌توانند حاوی اطلاعات شخصی باشند. از آنجایی که این تعریف شامل هرگونه اطلاعات می‌شود، باید فرض کرد که اصطلاح داده‌های شخصی باید تا حد امکان به طور گسترده تفسیر شود. این امر در رویه قضایی دیوان عدالت اروپایی نیز پیشنهاد شده است. به‌عنوان مثال در برخی شرایط حتی اطلاعات مربوط به شغل، رنگ مو یا عقاید سیاسی یک فرد می‌تواند به‌عنوان داده‌های شخصی طبقه‌بندی شود.[1] معمولاً این به هدف و زمینه‌ای مربوط می‌شود که داده‌ها در آن جمع‌آوری شده‌اند و اینکه آیا موضوع داده می‌تواند به طور مستقیم یا غیرمستقیم قابل شناسایی باشد. گرچه در ادبیات روزمره اصطلاح داده‌های شخصی و داده‌های حساس اغلب برای توصیف یک نوع از داده به‌کار می‌روند، اما در کنوانسیون ۱۰۸+ و نیز GDPR تمایز واضحی میان این دو عبارت وجود دارد.

بر اساس ماده ۹ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا GDPR، داده‌های حساس مجموعه‌ای از دسته‌بندی‌های ویژه داده‌های شخصی هستند که باید با امنیت بیشتری مدیریت شوند و ارزش محافظت بیشتری دارند. بنابراین پردازش این دسته از داده‌ها می‌تواند خطرات قابل توجهی را برای حقوق و آزادی‌های اساسی افراد ایجاد نماید. این داده‌ها همانگونه که بیان شد در ماده ۹ GDPR تنظیم شده و شامل هشت دسته داده به شرح زیر است: داده‌ها با منشاء قومی یا نژادی، نظرات سیاسی، باورهای فلسفی یا مذهبی، عضویت در اتحادیه‌های کارگری، داده‌های بیومتریک و داده‌های ژنتیکی (که می‌تواند برای شناسایی منحصر به فرد شخص، مورد استفاده قرار گیرد) و همچنین داده‌های مربوط

1. Marcus, Smith, & Miller, Seumas, *Biometric Identification, Law and Ethics* (Springer Cham, 2021) P. 82.

به سلامت و داده‌های مربوط به زندگی جنسی یک فرد حقیقی و در نهایت داده‌های مربوط به جهت‌گیری جنسیتی.[۱]

۳. پیشینه حمایت از زندگی خصوصی و داده‌های شخصی در اروپا

محافظت از حریم خصوصی شهروندان، زندگی شخصی و خانوادگی آنها در بسیاری از اسناد و کنوانسیون‌های اروپایی مشاهده می‌گردد. امروزه با توسعه روزافزون فناوری اطلاعات، اهمیت حمایت از حریم خصوصی و داده‌های شخصی بیش از پیش نمایان می‌شود. حریم خصوصی و داده‌های شخصی با مقوله کرامت انسانی ارتباط مستقیمی دارند. بر همین اساس در بسیاری از اسناد، حق مصونیت داده‌های شخصی افراد از تعرض‌های غیرقانونی به‌عنوان حقی بشری و اساسی مدنظر می‌باشد و حمایت و نظارت جدی در رابطه با حفاظت از این حق صورت پذیرفته است. در عرصه حمایت از داده‌های شخصی، اروپا همواره پیشگام بوده و اقدامات کنوانسیون شورای اروپا در خصوص حمایت از داده‌های شخصی، با عنوان کنوانسیون حمایت از افراد در برابر پردازش خودکار داده‌های شخصی ۱۰۸+ مصوب ۱۹۸۱ از مهمترین اسنادی است که درباره داده‌های شخصی به تصویب رسیده و به‌عنوان الگویی برای سایر کشورها در رابطه با تهیه و تصویب مقررات حمایت از داده‌های شخصی افراد مدنظر قرار گرفته است. این کنوانسیون اولین معاهده بین‌المللی در مورد حفاظت از داده‌های شخصی و حریم خصوصی بود که اصول اولیه جمع‌آوری، پردازش و استفاده از داده‌های شخصی را تعیین نمود. این کنوانسیون از کشورهای امضا کننده می‌خواهد حقوق و آزادی‌های اساسی را در مورد پردازش خودکار داده‌های شخصی تضمین نمایند. در ادامه این مسیر، اتحادیه اروپا دستورالعمل حفاظت از داده‌ها (95/46/EC) را در سال ۱۹۹۵ به تصویب رسانید. این دستورالعمل چارچوبی را به منظور حفاظت از داده‌های شخصی در اتحادیه اروپا ایجاد نمود. دستورالعمل مذکور دولت‌های عضو را ملزم می‌سازد قوانین ملی حفاظت از داده‌ها را که از استانداردهای مشترک خاصی پیروی می‌کنند، وضع نمایند.

---

1. Tomas, Gomez-Arostegui, "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations", California Western International Law Journal, Vol. 35, No. 2, May, (2005), P. 176.

در سال ۲۰۱۶ اتحادیه اروپا به منظور یکپارچه‌سازی قوانین حفاظت از حریم خصوصی و داده‌های شخصی شهروندان مقررات حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR)، جایگزین دستورالعمل حفاظت از داده‌ها شد و مقررات حفاظت از داده‌های شخصی را در اتحادیه اروپا تقویت نمود. کنوانسیون ۱۰۸+ شورای اروپا و GDPR اتحادیه اروپا، هر دو اقدامات قانونی در زمینه حفاظت از داده‌ها وضع نموده‌اند، با این وجود در حالی که کنوانسیون تصویب شده توسط شورای اروپا اصول کلی را تعیین می‌کند، متون اتحادیه اروپا یک رژیم حقوقی دقیق به منظور حفاظت از داده‌ها را ارائه می‌دهد. با این حال متون تصویب شده هر دو طرف، پیوندهای اجتناب‌ناپذیری دارند و تأثیر متقابل دو نهاد بر یکدیگر را نشان می دهند.[1]

۱-۳. اقدامات شورای اروپا

شورای اروپا که در سال ۱۹۴۹ تاسیس شد از قدیمی‌ترین و بزرگترین سازمان‌های اروپایی است. امروزه ۴۶ کشور عضو را به منظور همکاری بین دولتی با هدف اصلی ایجاد منطقه دموکراتیک و قانونی مشترک در سراسر قاره اروپا با تضمین احترام به ارزش‌های مشترک حقوق بشر، دموکراسی و حاکمیت قانون متحد می‌سازد. اقدامات شورای اروپا شامل دسته اقدامات الزام‌آور و نیز اقدامات غیرالزام‌آور است. منظور از اقدامات الزام‌آور شورای اروپا، آن دسته از مصوباتی است که برای کشورهای عضوی که آنها را به تصویب رسانده‌اند و یا به این مصوبات ملحق شده‌اند، ایجاد وظیفه و تعهدات قانونی می‌نمایند. از طرفی منظور از اقدامات غیرالزام‌آور شورای اروپا، آن دسته اسنادی را شامل می‌شود که در برگیرنده توصیه‌ها، دستورالعمل‌ها، راهبردها و ... هستند و با وجود آنکه از لحاظ قوانین بین‌الملل الزام‌آور نبوده و موجبات مسئولیت بین‌المللی دولت‌ها نخواهند بود، اما موجب فرهنگ‌سازی و بالا بردن سطح اخلاق عمومی شده و کشورها نیز از راهنمایی‌های

1. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018) P. 25.

کاربردی این دسته از اقدامات غیرالزام‌آور نهایت استفاده را می‌برند.[1] در ادامه به دسته الزام‌آور پرداخته می‌شود.

۱-۱-۳. کنوانسیون حمایت از افراد در برابر پردازش خودکار داده‌های شخصی شورای اروپا

در سال ۱۹۸۱، کنوانسیون حمایت از افراد با توجه به پردازش خودکار داده‌های شخصی (کنوانسیون ۱۰۸) برای امضا باز شد. با گذشت زمان به منظور مقابله با چالش‌های ناشی از استفاده از فناوری‌های جدید اطلاعات و ارتباطات و نیز تقویت اجرای مؤثرتر، کنوانسیون ۱۰۸ تحت فرآیند مدرن‌سازی قرار گرفت. کار برای نوسازی کنوانسیون توسط کمیته مشورتی[2] ایجاد شده توسط کنوانسیون انجام شد و نیز توسط یک کمیته بین‌دولتی (کمیته ویژه حفاظت از داده‌ها CAHDATA)[3] ادامه یافت و در نهایت کنوانسیون مدرن ۱۰۸+ که منعکس کننده چالش‌های جدید حفاظت از داده‌ها در عصر دیجیتال است در سال ۲۰۱۸ به تصویب رسید. نسخه مدرن‌سازی شده کنوانسیون که شامل ۸ فصل و ۳۱ ماده می‌باشد. این کنوانسیون همچنین با پروتکل‌های اضافی تکمیل شده است. ماده ۶ به دسته‌های خاص داده‌ها پرداخته و بیان می‌دارد، پردازش داده‌های شخصی که منشأ نژادی یا قومیتی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی یا عضویت در اتحادیه‌های کارگری را آشکار می‌سازد و نیز پردازش داده‌های ژنتیکی، داده‌های بیومتریک به منظور شناسایی منحصر به فرد یک شخص حقیقی، همچنین داده‌های مربوط به سلامت یا داده‌های مربوط به گرایش جنسی یک شخص و نیز داده‌های مربوط به محکومیت‌های کیفری به صورت خودکار ممنوع است، مگر در شرایط خاص و اینکه قوانین داخلی ضمانت‌های مقتضی را

---

1. Cécile de Terwangne, "Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data", Computer Law & Security Review, Vol. 40, (2021).
2. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD).
3. Terms of Reference 2013 of the Ad hoc Committee on Data Protection, available at: https:// rm.coe. int/ CoERMPublic Common Search Services/ Display DCTMContent?documentId=090000168066d6af.
Information Document on the Ad hoc Committee on Data Protection, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066d0b6.

پیش‌بینی کرده باشند. همچنین پردازش دسته‌های خاص از داده‌های شخصی به منظور اهداف تحقیقاتی علمی یا تاریخی یا مقاصد آماری، مشروط به تدابیر مناسب به منظور صیانت از حقوق و آزادی‌های موضوع داده‌ها نیز ممکن است، مجاز باشد. کمیته ویژه حفاظت از داده‌ها CAHDATA نقش مهمی در توسعه استانداردهای حفاظت از داده‌ها و مسائل مربوط به حریم خصوصی دارد. این کمیته متشکل از کارشناسان مستقلی است که توسط کشورهای عضو شورای اروپا به منظور ارائه مشاوره و راهنمایی در مورد حفاظت از داده‌ها و مسائل مربوط به حریم خصوصی منصوب شده‌اند.

علاوه بر این، CAHDATA برای ارتقای آگاهی و درک مسائل مربوط به حفاظت از داده‌ها در میان عموم مردم تلاش می‌نماید. این سازمان مواد آموزشی و کمپین‌هایی را با هدف افزایش آگاهی از حقوق افراد در رابطه با پردازش داده‌های شخصی آنها ایجاد کرده است و برای ارتقای اهمیت حفاظت از داده‌های شخصی در عصر دیجیتال تلاش می‌کند. کمیته مشورتی کنوانسیون حمایت از افراد با توجه به پردازش خودکار داده‌های شخصی (T-PD) نیز متشکل از نمایندگان طرف‌های کنوانسیون، ناظرین دیگر کشورها (اعضا و غیر عضو، دولت یا مقامات حفاظت از داده‌ها)، سازمان‌های بین‌المللی و غیردولتی بوده و مسئول ترویج و نظارت بر اجرای کنوانسیون است. کمیته T-PD این کار را با انجام ارزیابی‌های منظم چارچوب‌های حفاظت از داده‌های ملی کشورهای عضو و ارائه توصیه‌هایی برای بهبود در صورت لزوم انجام می‌دهد. کمیته همچنین نقش مهمی در ارائه راهنمایی به کشورهای عضو در مورد تفسیر کنوانسیون و بهترین شیوه‌ها در زمینه حفاظت از داده‌ها ایفا می‌کند.

علاوه بر این، کمیته T-PD در توسعه استانداردهای بین‌المللی و بهترین شیوه‌ها در زمینه حفاظت از داده‌ها مشارکت دارد. کمیته T-PD همچنین نقش مهمی در ارتقای آگاهی و درک مسائل مربوط به حفاظت از داده در میان عموم مردم ایفا نموده و برای افزایش آگاهی از حقوق افراد در مورد پردازش داده‌های شخصی آنها و ترویج اهمیت حفاظت از داده‌های شخصی در عصر دیجیتال تلاش می‌کند. به‌طور کلی کمیته T-PD یک بازیگر کلیدی در توسعه و ارتقای استانداردها و نیز انتخاب بهترین شیوه‌های حفاظت از داده‌ها است. همچنین اجرای مؤثر قوانین حفاظت از داده‌ها توسط مقامات نظارتی

مستقل[1] در طرف‌های متعاهد، به منظور اجرای عملی کنوانسیون در نظر گرفته می‌شود. نقش مهم مقامات حفاظت از داده‌ها در حصول اطمینان از انطباق قوانین با کنوانسیون است. مقامات حفاظت از داده‌ها مسئول نظارت بر پردازش داده‌های شخصی و بررسی شکایات افراد هستند. آنها همچنین این قدرت را دارند که کنترل کننده‌های داده‌ای که اصول کنوانسیون را نقض می‌کنند را تحریم نمایند. به بیان دیگر افسران حفاظت از داده‌ها[2] (DPOs) افرادی هستند که در مورد رعایت قوانین حفاظت از داده‌ها در سازمان‌هایی که پردازش داده‌ها را انجام می‌دهند مشاوره داده و انطباق با مفاد کنوانسیون را تسهیل می‌نمایند و در عین حال به‌عنوان واسطه میان مقامات نظارتی، موضوعات داده‌ها و سازمانی که توسط آن منصوب شده‌اند عمل می‌نمایند. امروزه تعداد فزاینده‌ای از مشکلات نوظهور و سؤالات عملی به مقامات ملی حفاظت از داده‌ها ارائه می‌شود.

پیشتر بیان شد در اکثر کشورها کمیسر ملی حفاظت از داده‌ها مسئول پاسخگویی به این موارد است و این مقامات نظارتی مانند آمبودزمان[3] به بخشی جدایی‌ناپذیر از سیستم کنترل در یک جامعه دموکراتیک تبدیل شده‌اند که باید اصول کنوانسیون را تفسیر کرده و آنها را به منظور حل مشکلات و مسائل جدید به‌کار گیرند. افراد می‌توانند به مقامات نظارتی ملی مراجعه کنند تا اعتراض خود را در مورد عدم رعایت یکی از حقوق تضمین شده برای آنها اعمال کنند. این امر به‌ویژه در موقعیت‌های فرامرزی ارزشمند خواهد بود، جایی که موضوع داده در یک کشور اقامت دارد در حالی که کنترل کننده داده در کشور دیگری مستقر است.[4]

---

1. Independent Supervisory Authorities.
2. Data Protection Officers (DPOs).
۳. Ombudsman یا دادآوَر. این کلمه از زبان سوئدی وام گرفته شده است و به معنای نماینده است. به فرد یا دفتری غیرجانبدار و مستقل گفته می‌شود که وظیفه دارد به‌عنوان نماینده عموم مردم، موارد نقض حقوق افراد توسط دولت یا نهادها و شرکت‌های مختلف را بررسی و بازرسی کند. این وظیفه معمولاً توسط دولت یا پارلمان به آمبودزمان محول می‌شود و به وی استقلال عمل زیادی اعطا می‌گردد. سوئد اولین کشوری بود که یک مقام مستقل را به نام بازرس برای بررسی شکایات علیه مقامات و سازمان‌های دولتی منصوب کرد. از آن زمان کشورهای دیگر همچون فنلاند، دانمارک، و نیوزیلند و برخی از ایالت‌های کشور ایالات متحده آمریکا، مقامات مشابهی را منصوب نمودند.
4. Aden Hartmut, "Privacy and Security: German Perspectives, European Trends and Ethical Implications", Ethical Issues in Covert, Security and Surveillance Research Advances in Research Ethics and Integrity, Vol. 8, January, (2022), P.1.

۲-۳. اقدامات اتحادیه اروپا

اتحادیه اروپا پس از پایان جنگ جهانی دوم با هدف تقویت همکاری اقتصادی و ثبات سیاسی میان کشورهای عضو تأسیس شد. در سال ۱۹۹۳ معاهده ماستریخت[1] اتحادیه اروپا را به شکل امروزی تأسیس کرد. امروزه اتحادیه اروپا یک اتحادیه سیاسی و اقتصادی متشکل از ۲۷ کشور عضو است که عمدتا در اروپا قرار دارند و بر اساس سیستم نهادهای فراملی و تصمیم‌گیری بین دولتی عمل می‌کند.[2]

۱-۲-۳. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا GDPR ۲۰۱۸

مقررات عمومی حفاظت از داده‌ها GDPR، قانونی در مورد حفاظت از داده‌ها و حریم خصوصی در اتحادیه اروپا و منطقه اقتصادی اروپا[3] است. پیش از مقررات GDPR، دستورالعمل 95/46/EC برای بیش از دو دهه، اساس قانون حفاظت از داده‌ها در اتحادیه اروپا بود. با این حال با ادامه تکامل فناوری و گسترش استفاده از داده‌های شخصی، نگرانی‌های جدیدی به وجود آمد که این دستورالعمل دیگر قادر به محافظت از حقوق حریم خصوصی افراد در عصر دیجیتال نبود. در ۲۵ مه ۲۰۱۸، مقررات GDPR در ۱۱ فصل و شامل ۹۹ ماده است، لازم‌الاجرا گردید. GDPR قانونی است که واقعیت‌های عصر دیجیتال و ماهیت جهانی پردازش داده‌ها را منعکس نموده است و برخلاف دستورالعمل حفاظت از داده‌ها، دارای اثر فراسرزمینی است، بدین معنا که برای تمامی سازمان‌هایی که داده‌های شخصی ساکنان اتحادیه اروپا را پردازش می‌کنند، صرف‌نظر از اینکه سازمان مذکور در اتحادیه اروپا مستقر است یا نه، اعمال می‌گردد.

به‌طور کلی GDPR به دنبال تقویت حقوق افراد در رابطه با حفظ حریم خصوصی و حفاظت از داده‌های شخصی است و تعهدات مهمی را بر عهده سازمان‌ها می‌گذارد تا اطمینان حاصل نماید داده‌های شخصی به شیوه‌ای مسئولانه و شفاف جمع‌آوری، پردازش و ذخیره می‌شوند. مقررات GDPR، داده‌های بیومتریک را به‌عنوان یک دسته خاص از

---

1. Treaty on European Union (Maastricht Treaty).
2. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018) P. 81.
3. European Economic Area (EEA).

داده‌های شخصی در نظر می‌گیرد، به این معنا که باید تحت حمایت‌های اضافی قرار گیرند، چرا که زمینه پردازش آنها می‌تواند خطرات قابل توجهی را برای حقوق و آزادی‌های اساسی افراد ایجاد نماید.[1] ماده ۹ مقررات GDPR به پردازش دسته‌های خاص از داده‌های شخصی می‌پردازد و بیان می‌دارد: پردازش داده‌های شخصی مربوط به افشای مبدأ نژادی و قومی، عقاید مذهبی و فلسفی و پردازش داده ژنتیکی، داده بیومتریک با هدف شناسایی منحصر به فرد افراد، داده مربوط به سلامتی یا گرایش جنسی اشخاص باید ممنوع شود. جز در موارد زیر:

شخص موضوع داده، رضایت صریح خود را نسبت به پردازش داده‌های شخصی برای یک یا چند هدف خاص اظهار دارد، مگر اینکه بر اساس قانون کشور عضو یا اتحادیه موارد منع مطرح شده، توسط موضوع داده لغو گردد. پردازش با هدف انجام تعهدات و استفاده از حقوق خاص کنترلگر یا شخص موضوع داده در زمینه استخدام و امنیت اجتماعی ضروری باشد. اگر شخص موضوع داده توانایی فیزیکی و حقوقی برای دادن رضایت ندارد و پردازش برای حفظ منافع حیاتی شخص موضوع داده یا دیگر اشخاص حقیقی ضروری باشد. پردازش در قالب فعالیت‌های قانونی، ضمن حفظ ایمنی توسط مؤسسه یا دیگر نهادهای غیرانتفاعی که اهداف سیاسی، فلسفی، مذهبی یا تجاری اتحادیه اروپا را دنبال می‌کنند، انجام شود و داده‌های شخصی بدون رضایت شخص صاحب موضوع فاش نشود. پردازش داده‌های شخصی که توسط خود شخص موضوع داده به صورت عمومی منتشر شده است. زمانی که پردازش برای دفاع از دعوی حقوقی یا استفاده قضایی ضروری باشد.

پردازش با هدف حفظ منافع عمومی و بر مبنای قانون اتحادیه یا کشور عضو ضرورت داشته باشد و با احترام به حقوق حفاظت داده انجام پذیرد. پردازش برای داروهای پیشگیرانه و شغلی، به منظور ارزیابی ظرفیت کاری مستخدمین، بیماری‌ها، تأمین سلامت و مراقبت اجتماعی یا درمان و همچنین مدیریت سامانه‌های مراقبت بهداشتی و خدمات مربوطه و نیز مسئولیت پردازش این داده‌ها بر اساس قانون اتحادیه و کشورهای عضو یا پیرو قرارداد، باید توسط متخصصین سلامتی که متعهد به انجام قوانین اتحادیه و کشورهای عضو هستند، انجام شود. پردازش برای منافع عمومی در زمینه سلامت عمومی همانند

1. Suzanne Dibble, *GDPR for Dummies*, 1st Edition (New Jersey: For Dummies, 2020) P. 13.

حفاظت در مقابل تهدیدات فرامرزی سلامتی با حفظ استانداردهای کیفی و ایمنی سلامتی محصولات دارویی و ادوات پزشکی و بر اساس قانون اتحادیه یا کشور عضو ضروری باشد. پردازش برای دستیابی به اهداف مربوط به منافع عمومی، اهداف علمی و تحقیقات تاریخی یا اهداف آماری مطابق با ماده ۸۹ (۱)[۱] و بر اساس قانون اتحادیه یا کشور عضو ضروری بوده و در ضمن به حقوق حفاظت داده احترام گذاشته شود.

کشورهای عضو ممکن است شرایط بیشتری نظیر محدودیت نسبت به پردازش داده‌های ژنتیکی، بیومتریک یا سلامتی معرفی کنند. بر اساس این مقررات، سازمان‌ها نیز باید اقدامات فنی و سازمانی مناسب را به منظور محافظت از داده‌های بیومتریک در برابر دسترسی، افشا یا از دست دادن غیرمجاز اجرا کنند که شامل اقداماتی همچون رمزگذاری، کنترل‌های دسترسی، تست‌های امنیتی منظم و انتصاب یک افسر حفاظت از داده‌ها[۲] DPO در شرایط خاص است. علاوه بر این، سازمان‌ها باید هنگام پردازش داده‌های بیومتریک، ارزیابی تأثیر حفاظت از داده‌ها[۳] انجام دهند، به‌ویژه زمانی که پردازش در مقیاس بزرگ انجام می‌شود و یا شامل استفاده از فناوری‌های جدید خواهد بود.

شایان ذکر است که GDPR داده‌های بیومتریک را به طور گسترده تعریف نموده و نه تنها اثر انگشت و داده‌های تشخیص چهره، بلکه انواع دیگری از داده‌ها همچون اثر صوتی و نحوه راه رفتن افراد را نیز شامل می‌شود و این بدان معنا است، سازمان‌هایی که هر نوع داده بیومتریک را پردازش می‌کنند باید الزامات GDPR برای دسته‌های خاص، داده‌های شخصی را مراعات نمایند. البته باید در نظر داشت، پردازش تصاویر به طور سیستماتیک نباید به‌عنوان پردازش دسته‌های خاصی از داده‌های شخصی تلقی شود، زیرا تنها زمانی تحت پوشش تعریف داده‌های بیومتریک قرار می‌گیرند که از طریق ابزار فنی

---

۱. پردازش برای دستیابی به اهداف مربوط به منافع عمومی، اهداف تحقیقاتی علمی و تاریخی یا اهداف آماری باید تحت حفاظت‌های مناسب منطبق با این مقررات، در زمینه حقوق و آزادی شخص موضوع داده، قرار بگیرند. این حفاظت‌ها باید تضمین کنند که اقدام‌های فنی و سازمانی به صورت عملی و برای احترام به اصول حداقل‌سازی داده در نظر گرفته شده‌اند. این اقدام‌ها می‌توانند شامل مستعارسازی برای دستیابی به اهداف ذکر شده باشد. حتی اگر این اهداف با پردازش بیشتری قابل دستیابی باشند که امکان شناسایی اشخاص موضوع داده را فراهم نمی‌کند، این اهداف باید انجام شود.

2. Data Protection Officer (DPO).
3. Data Protection Impact Assessments (DPIAs).

خاصی که امکان شناسایی یا احراز هویت منحصر به فرد یک شخص حقیقی را فراهم نماید، پردازش شوند.

GDPR یک چارچوب نظارتی جامع به منظور حفاظت از داده‌های شخصی در اتحادیه اروپا ایجاد نموده که شامل نهادهای نظارتی مرکزی و ملی است و وظیفه اجرا و نظارت بر مقررات را بر عهده دارند. به دیگر بیان رگولاتوری[1] به سیستم قوانین و مقررات ایجاد شده توسط GDPR به منظور کنترل پردازش داده‌های شخصی در اتحادیه اروپا اشاره دارد. ماده ۶۸ GDPR، هیئت حفاظت از داده‌های اروپا[2] را به‌عنوان یک نهاد نظارتی مرکزی برای مقررات GDPR در اتحادیه اروپا معرفی و وظایف و مسئولیت‌های آن را مشخص می‌کند. بند ۲ ماده ۶۸ تصریح می‌کند که EDPB از روسا مراجع نظارتی ملی[3] در اتحادیه اروپا و همچنین ناظر حفاظت از داده اروپا[4] تشکیل شده است. بند ۱ ماده ۶۹ تصریح می کند، EDPB یک نهاد مستقل است، به این معنی که تحت تأثیر یا کنترل خارجی نیست و آزاد است، وظایف و مسئولیت‌های خود را بدون مداخله انجام دهد. ماده ۷۰ مقررات GDPR تصریح می کند که EDPB می تواند با مقامات نظارتی در کشورهای ثالث در مورد مسائل مربوط به حفاظت از داده‌های شخصی با رعایت پادمان‌ها و رویه‌های مناسب همکاری کند.

علاوه بر این، مواد ۵۷-۵۹ GDPR نقش مقامات نظارتی ملی را در اجرای مقررات در حوزه قضایی مربوطه خود تعیین می کند. مقامات نظارتی ملی مسئول اجرای مقررات GDPR در حوزه قضایی مربوطه خود هستند، از جمله انجام تحقیقات، اعمال جریمه و سایر تحریم‌ها برای نقض GDPR و نیز ارائه راهنمایی و مشاوره به سازمان‌ها در مورد تعهدات مربوط به GDPR. EDPS در هیئت حفاظت از داده‌های اروپا، در فرآیند تصمیم گیری مشارکت نموده و اطلاعاتی را در مورد راهنمایی‌ها و تصمیمات به EDPB ارائه می‌دهد. همچنین ناظر حفاظت از داده‌های اروپا EDPS یک مرجع مستقل می‌باشد و مسئول نظارت بر اجرای قوانین حفاظت از داده‌ها در نهادها و ارگان‌های اتحادیه اروپا

1. Regulatory.
2. European Data Protection Board (EDPB).
3. National Supervisory Authorities.
4. European Data Protection Supervisor (EDPS).

و ترویج قوانین حفاظت از داده‌ها در سراسر اتحادیه اروپا است. به‌طور کلی EDPS نقشی حیاتی در ترویج قوانین حفاظت از داده‌ها در سراسر اتحادیه اروپا، در رابطه با حفاظت از حریم خصوصی و داده‌های شخصی افراد در اتحادیه اروپا ایفا می‌نماید.[۱]

۴. تاثیر پردازش داده‌های بیومتریک بر زندگی خصوصی

۴-۱. اصول حاکم بر پردازش داده‌های بیومتریک

اصول حاکم بر پردازش داده‌های بیومتریک به معنای قواعد حمایت کننده داده‌ها و حقوق افراد موضوع داده است که شامل اصل قانونی بودن، اصل تحصیل مرتبط و مضیق داده‌ها، اصل صحت، اصل امنیت، اصل شفافیت، اصل دسترسی، اصل ممنوعیت افشا، اصل امحا، اصل ممنوعیت انتقال غیرمجاز داده‌ها، دسته‌های خاص داده‌ها می‌باشد.[۲]

۴-۲. تهدیدات علیه داده‌های بیومتریک

در حالی که استفاده از داده‌های بیومتریک مزایای متعددی از نظر امنیت و راحتی ارائه می‌دهند، با این حال استفاده از داده‌های بیومتریک خطرات و تهدیداتی را نیز به همراه دارد. از جمله این خطرات می‌توان به نفوذ و دسترسی غیرمجاز داده‌ها، تحصیل غیرمجاز داده‌ها، تخریب و تغییر غیرمجاز داده‌ها، سرقت هویت، انتقال غیرمجاز داده‌ها، افشای غیرمجاز داده‌ها همچنین نگرانی‌های مربوط به حریم خصوصی، فقدان استانداردها در برخی سیستم‌ها، بروز فناوری‌های نوین همچون Deepfake،[۳] دستکاری پایگاه داده، انواع حملات و دستکاری‌ها نیز از مواردی است که می‌توان به آنها اشاره نمود.[۴]

---

1. Sanjay Sharma, *Data Privacy and GDPR Handbook*, 1st Edition (New Jersey: Wiley, 2019) P. 251.

2. Els Kindt, *Privacy and Data Protection Issues of Biometric Applications a Comparative Legal Analysis* (Dordrecht: Springer, 2013) P. 278.

۳. این فناوری شامل ایجاد ویدیوها یا تصاویر دستکاری شده بسیار واقعی است که می‌تواند سیستم‌های بیومتریک را فریب دهد. برای مثال سیستم‌های تشخیص چهره را می‌توان با استفاده از ویدیوها یا تصاویر عمیق‌فیک برای جعل هویت شخص دیگری فریب داد. پیشرفت فناوری دیپ‌فیک تهدیدی رو به رشد برای یکپارچگی احراز هویت بیومتریک خواهد بود.

4. Richard Jiang, *Biometric Security and Privacy Opportunities & Challenges in the Big Data Era* (Paris: Springer, 2017) P. 305.

۳-۴. حقوق افراد در ارتباط با پردازش داده‌های بیومتریک آنان

حقوق افراد در رابطه با پردازش داده‌های بیومتریک می‌تواند بسته به حوزه قضایی و قوانین مربوط به حفاظت از داده‌ها متفاوت باشد. با این حال برخی از اصول و حقوق اساسی وجود دارد که به‌طور کلی به رسمیت شناخته شده و مورد حمایت قرار می‌گیرد. حقوقی همچون حق اطلاع از پردازش، حق انتخاب، حق دسترسی، حق منع پردازش، حق اصلاح و در نهایت حق برخورداری از ضمانت اجراهای مناسب و جبران خسارت.[1] با توجه به ماهیت بسیار حساس داده‌های بیومتریک، چشم‌انداز قانونی پیرامون این داده‌ها در حال تحول است و ممکن است مقررات و دستورالعمل‌های جدیدی در طول زمان نگاشته شوند و حقوق بیشتری را برای افراد موضوع داده در نظر گیرند. علاوه بر حقوق کلی که ذکر شد، افراد ممکن است حقوق خاصی در مورد داده‌های بیومتریک خود داشته باشند.

۵. نقش قانونگذار در حمایت از داده‌های بیومتریک

قانونگذاران مسئول وضع قوانین و مقرراتی هستند که چارچوب‌های حریم خصوصی و حفاظت از داده‌ها را ایجاد می‌کنند و شرایطی را تعریف می‌نمایند که تحت آن داده‌های بیومتریک جمع‌آوری، ذخیره، پردازش و به اشتراک گذاشته شوند. قانونگذاران، استانداردها و الزاماتی را برای امنیت و حفاظت از داده‌های بیومتریک تعیین می‌کنند. همچنین دستورالعمل‌هایی را برای نگهداری و حذف داده‌های بیومتریک تعیین می‌کنند. قانونگذاران مکانیسم‌های اجرایی و مجازات‌های نقض قوانین حفاظت از داده‌های بیومتریک را تعریف می‌کنند و به مقامات نظارتی قدرت می‌دهند تا بر رعایت قوانین حفاظت از داده‌ها نظارت داشته باشند. قانونگذاران ممکن است در بحث‌ها و توافقات بین‌المللی برای هماهنگ کردن استانداردهای حفاظت از داده‌های بیومتریک در سراسر کشورها شرکت کنند. این امر به‌ویژه در عصر جهانی شدن و جریان‌های داده‌های فرامرزی مهم است. به‌طور کلی قانونگذاران نقشی محوری در ایجاد چارچوب قانونی و پادمان‌های لازم به منظور حفاظت از داده‌های بیومتریک ایفا می‌کنند و مزایای استفاده از فناوری

1. Mitra Sinjini & Mikhail Gofman, *Biometrics in a Data Driven World: Trends, Technologies, and Challenges*, 1st Edition (NewYork: Boca Raton: CRC Press, 2017) P. 17.

بیومتریک را با حقوق حریم خصوصی متعادل می‌نمایند. فناوری بیومتریک به طور مداوم در حال تکامل بوده و تکنیک‌های جدیدی برای جمع‌آوری و استفاده از داده‌های بیومتریک در حال ظهور است. به همین علت قوانین و سیاست‌ها باید بروزرسانی شوند تا با این پیشرفت‌ها همگام شده و خطرات و چالش‌های مرتبط را برطرف نمایند. همچنین قوانین و سیاست‌ها باید آسیب‌پذیری‌های خاص جمعیت‌های خاصی همچون کودکان، سالمندان یا افراد دارای معلولیت را در هنگام جمع‌آوری و استفاده از داده‌های بیومتریک در نظر بگیرند. چرا که ممکن است برای اطمینان از رعایت حقوق خصوصی آنها و جلوگیری از آسیب یا تبعیض احتمالی، حمایت‌های ویژه‌ای لازم باشد.[۱]

۶. نقش کنترل کنندگان داده در حمایت از داده‌های بیومتریک

کنترل‌کننده‌های داده نقش مهمی در پشتیبانی از داده‌های بیومتریک با اطمینان از پردازش قانونی و مسئولانه آن ایفا می‌کنند. آنها باید اطمینان حاصل نمایند، جمع‌آوری، ذخیره و پردازش داده‌های بیومتریک با شرایطی که در قانون ذکر شده مطابق است. به طور خلاصه اینکه کنترل کننده داده باید اطلاعات واضح و قابل درک در مورد هدف پردازش، انواع داده‌های بیومتریک جمع‌آوری شده، دوره نگهداری و هر شخص ثالثی که ممکن است داده‌ها با آنها به اشتراک گذاشته شود، ارائه دهند. کنترل‌کنندگان داده‌ها باید ارزیابی ریسک را به صورت کامل به منظور شناسایی و ارزیابی ریسک‌های بالقوه مرتبط با پردازش داده‌های بیومتریک انجام دهند. این ارزیابی به تعیین تدابیر امنیتی مناسب و نیز تدابیر حفاظتی برای کاهش موثر این خطرات کمک می‌کند. در حوزه‌های قضایی خاص یا به دلیل وجود فعالیت‌های پردازشی پرخطر، ممکن است از کنترل‌کنندگان داده‌ها خواسته شود که ارزیابی تأثیر حریم خصوصی[۲] انجام دهند.

PIA تأثیر پردازش داده‌ها را بر حریم خصوصی افراد ارزیابی نموده و به شناسایی اقداماتی برای به حداقل رساندن خطرات جمع‌آوری و پردازش داده‌های بیومتریک در ارتباط با حریم خصوصی کمک می‌کند. کنترل‌کنندگان داده‌ها باید برنامه‌های آموزشی

---

۱. رویا معتمد نژاد، «قانونگذاری در عرصه دیجیتال و برنامه توسعه پایدار (با تأکید بر «جمهوری دیجیتال»)»، نشریه علمی مطالعات فرهنگی و ارتباطات، سال ۱۳، شماره ۴۹، (۱۳۹۶)، ص ۲۱۸.

2. Privacy Impact Assessment (PIA).

و آگاهی‌رسانی منظمی را برای کارکنان درگیر در پردازش داده‌های بیومتریک ارائه دهند تا اطمینان حاصل گردد پرسنلی که چنین داده‌هایی را مدیریت می‌نمایند، مسئولیت‌های خود را درک نموده و از اصول حفاظت از داده‌ها آگاه هستند و نیز بهترین شیوه‌ها را برای حفظ امنیت و حریم خصوصی داده‌ها دنبال می‌کنند. کنترل‌کنندگان داده‌ها باید برنامه‌های آموزشی و آگاهی‌رسانی منظمی را برای کارکنان درگیر در پردازش داده‌های بیومتریک ارائه دهند. تا اطمینان حاصل گردد پرسنلی که چنین داده‌هایی را مدیریت می‌نمایند، مسئولیت‌های خود را درک نموده و از اصول حفاظت از داده‌ها آگاه هستند و نیز بهترین شیوه‌ها را برای حفظ امنیت و حریم خصوصی داده‌ها دنبال می‌کنند. کنترل‌کنندگان داده‌ها باید از فناوری‌های نوظهور مرتبط با پردازش داده‌های بیومتریک، همچون سیستم‌های تشخیص چهره یا تجزیه و تحلیل نحوه راه رفتن مطلع باشند. با تکامل این فناوری‌ها، کنترل‌کنندگان داده‌ها باید تأثیر بالقوه آنها را بر حقوق حریم خصوصی افراد ارزیابی نموده و پیامدهای اخلاقی مرتبط با استفاده از آنها را در نظر گیرند. کنترل کننده‌های داده باید ممیزی‌ها و ارزیابی‌های منظم در رابطه با شیوه‌های پردازش داده‌های بیومتریک را انجام دهند تا از انطباق مداوم با مقررات و نیز انتخاب بهترین شیوه‌ها اطمینان حاصل نمایند. این ممیزی‌ها ممکن است شامل ارزیابی‌های داخلی یا ممیزی‌های خارجی توسط کارشناسان مستقل باشد. ارزیابی‌های منظم به شناسایی زمینه‌های بهبود، اطمینان از مؤثر بودن اقدامات حفاظتی داده‌ها و نشان دادن تعهد به مدیریت مسئولانه داده‌ها کمک می‌نماید. کنترل کنندگان داده باید ارتباط و همکاری مؤثری با مقامات حفاظت از داده‌ها در حوزه قضایی مربوطه خود برقرار کنند که می‌تواند شامل مشاوره با مقامات در مورد مسائل مربوط به انطباق، جستجوی راهنمایی در هنگام رسیدگی به فعالیت‌های پیچیده پردازش داده‌های بیومتریک و همکاری در تحقیقات یا ممیزی‌های مربوط به داده‌های بیومتریک باشد. به‌طور کلی کنترل‌کننده‌های داده نقش مهمی در حصول اطمینان از پردازش مسئولانه و قانونی داده‌های بیومتریک، حفاظت از حقوق حریم خصوصی افراد و حفظ امنیت و یکپارچگی داده‌ها دارند.[۱]

---

۱. رویا معتمدنژاد، «وظایف دولت‌ها در عرصه تکنولوژی‌های دیجیتال از دولت انحصارطلب تا دولت رگولاتور»، فصلنامه علوم خبری، دوره ۷، شماره ۲۸، (۱۳۹۷)، ص ۱۰.

۷. صنعت و حمایت از داده‌های بیومتریک

پشتیبانی از داده‌های بیومتریک در صنعت شامل جنبه‌های مختلفی است که می‌تواند شامل تأمین مالی پروژه‌های تحقیقاتی، همکاری با مؤسسات دانشگاهی و ایجاد مشارکت با شرکت‌های فناوری متخصص در بیومتریک باشد. ترویج توسعه و پذیرش استانداردهای صنعتی برای داده‌های بیومتریک به منظور اطمینان از قابلیت همکاری و سازگاری میان سیستم‌ها و دستگاه‌های مختلف مورد دیگری است. همچنین ارائه برنامه‌ها، منابع آموزشی و کارگاه‌ها به متخصصان صنعت، توسعه‌دهندگان و کاربران باعث افزایش درک آنها از فناوری‌های بیومتریک و نیز انتخاب بهترین شیوه‌ها می‌باشد. این کار سبب می‌شود از مدیریت صحیح، استفاده و حفاظت از داده‌های بیومتریک اطمینان حاصل گردد. تسهیل همکاری میان ذینفعان صنعت از جمله ارائه دهندگان فناوری، محققان و کاربران نهایی نیز مورد دیگری است. در این میان باید مواردی چون ارزیابی تأثیر حریم خصوصی، ملاحظات اخلاقی نیز بیش از پیش مدنظر قرار گیرد. با ارائه پشتیبانی جامع در این زمینه‌ها، ذینفعان صنعت می‌توانند اجرای مسئولانه و ایمن فناوری‌های داده‌های بیومتریک را تقویت نموده و در عین حال از حریم خصوصی افراد و داده‌های شخصی آنها همچون داده‌های بیومتریک محافظت نمایند.

Privacy by Design حریم خصوصی از طریق طراحی و پیش‌فرض، مفهومی است که از ملاحظات حفظ حریم خصوصی حمایت می‌کند تا از ابتدا در طراحی و توسعه سیستم‌ها، فناوری‌ها و فرآیندها گنجانده شود. با ادغام اقدامات حفظ حریم خصوصی در طراحی و ساخت سیستم‌های بیومتریک، سازمان‌ها می‌توانند خطرات حریم خصوصی را به حداقل برسانند و حفاظت از داده‌ها را افزایش دهند. ویژگی اصلی مفهوم Privacy by Design این است که به طور فعالانه به ملاحظات حفظ حریم خصوصی در کل چرخه عمر یک پروژه پرداخته شود. انجام ارزیابی‌های تأثیر حریم خصوصی یاPIA یک عمل توصیه شده قبل از اجرای سیستم‌ها یا پروژه‌های پردازش داده‌های بیومتریک است. PIA به سازمان‌ها کمک می‌کند تا خطرات بالقوه حریم خصوصی را شناسایی و به آنها رسیدگی نموده، ضرورت و تناسب فعالیت‌های پردازش داده‌ها را ارزیابی کنند و تدابیر حفاظتی مناسب را برای حفاظت از حقوق حریم خصوصی افراد اجرا نمایند.

پردازش داده‌های بیومتریک اغلب شامل استفاده از الگوریتم‌ها و فناوری‌های هوش مصنوعی (AI) است. بنابراین ملاحظات اخلاقی در هوش مصنوعی همچون شفافیت، مسئولیت‌پذیری و انصاف به پردازش داده‌های بیومتریک مربوط می‌شود. حصول اطمینان از اینکه سیستم‌های هوش مصنوعی مورد استفاده به منظور تجزیه و تحلیل داده‌های بیومتریک بی‌طرفانه و مشمول نظارت انسانی هستند، برای محافظت از حقوق حریم خصوصی مهم خواهد بود.

Privacy by Design باعث می‌شود تا حریم خصوصی به تنظیمات پیش‌فرض تبدیل شود، به این معنی که اقدامات افزایش حریم خصوصی باید به صورت پیش‌فرض در سیستم‌ها و محصولات تعبیه شود. به طوری که کاربران ملزم به انجام اقدامات اضافی برای محافظت از حریم خصوصی خود نباشند و در عوض، حفاظت از حریم خصوصی باید به صورت خودکار و ذاتی باشد. به‌طور کلی با اتخاذ اصل مذکور، سازمان‌ها می توانند حفاظت از حریم خصوصی را در عملیات، سیستم‌ها و محصولات خود تعبیه نموده و خطرات حریم خصوصی را به حداقل برسانند و از رعایت قوانین و مقررات حریم خصوصی اطمینان حاصل نمایند.

Privacy by Design سازمان‌ها را قادر می‌سازد تا تعهد خود را به حفظ حریم خصوصی نشان دهند و محصولات و خدماتی با حفظ حریم خصوصی بسازند که انتظارات در حال تکامل کاربران را برآورده سازد. علاوه بر آن رمزگذاری بیومتریک تکنیکی است که داده‌های بیومتریک و الگوریتم‌های رمزگذاری را به منظور محافظت از اطلاعات حساس ترکیب می‌نماید. با ترکیب داده‌های بیومتریک به منظور رمزگذاری، رمزگذاری بیومتریک یک لایه امنیتی اضافی را فراهم نموده و تضمین می‌کند که حتی اگر داده‌های رمزگذاری شده به خطر بیفتد، بدون الگوی بیومتریک صحیح و کلید رمزگشایی غیرقابل خواندن و بی‌فایده باقی می مانند.[1]

به‌طور کلی رمزگذاری بیومتریک رویکرد امیدوارکننده‌ای است که نقاط قوت احراز هویت بیومتریک و تکنیک‌های رمزگذاری را ترکیب می‌کند تا امنیت و حفاظت از حریم

1. Dan, Remenyi & Paul Griffiths, "Data: Its Nature and Management a Short Note on Some of the Complexity Behind the Concept of Data", The Electronic Journal of Business Research Methods, Vol. 20, No. 3, (2022), PP. 133-141,

خصوصی را برای داده‌های حساس فراهم نماید. با این حال ذکر این نکته ضروری است که رمزگذاری بیومتریک بدون چالش نیست و برخی ملاحظات همچون آسیب‌پذیری قالب‌های بیومتریک در برابر حملات، نیاز به ذخیره‌سازی امن کلیدهای رمزگذاری و ... همواره وجود خواهند داشت.

۸. قوانین ایران در رابطه با حفاظت از داده‌های بیومتریک

در نظام حقوقی ایران مقررات منسجمی در خصوص حفاظت از داده‌های شخصی وجود ندارد و طرحی که اخیراً با عنوان طرح حمایت و حفاظت از داده و اطلاعات شخصی تدوین شده تاکنون به تصویب مجلس نرسیده است. به همین دلیل حفاظت از حریم خصوصی را باید در مقررات مختلفی همچون قانون اساسی، قانون مجازات اسلامی، قانون تجارت الکترونیک و قانون انتشار و دسترسی آزاد به اطلاعات جستجو نمود. به دیگر بیان حفاظت از حریم خصوصی توسط قوانین سنتی ارائه می‌شود، گرچه داده‌های شخصی با وجود شرایط منحصر به فرد خود به قوانین جدید و به‌روز نیاز دارند. کشور ایران ابتدا قوانین پراکنده‌ای را در خصوص حفاظت از داده‌های شخصی وضع کرده و سپس به تدریج به سمت رویکرد اروپایی رفته و قانون جامع حفاظت از داده‌ها را تدوین نموده است.

بر اساس اصل ۲۵ قانون اساسی[۱]، هرگونه تجسس ممنوع است. با توجه به مفهوم جاسوسی، بسیاری از موارد تجاوز به حریم خصوصی را می‌توان جاسوسی دانست که بر اساس اصل مذکور ممنوع است. حریم خصوصی یکی از مهمترین اجزای حقوق انسانی

۱. بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون.

است که در اصل ۱۴[۱] و ۲۰[۲] قانون اساسی بر رعایت حقوق انسانی همه افراد تاکید شده است.

قانونگذاران ایران در ماده ۶۴۸ قانون مجازات اسلامی[۳] که به موضوع افشای اسرار پرداخته‌اند. این ماده به نوعی تشابهاتی با ماده ۹۰ مقررات GDPR دارد. ماده ۱۲ قانون جرائم رایانه‌ای به حریم خصوصی و حفاظت از داده‌های شخصی می‌پردازد. ماده ۷۲۹ قانون مجازات اسلامی به دسترسی غیرمجاز می‌پردازد. علاوه بر این بر اساس ماده ۱ قانون جرائم رایانه‌ای، هرگونه دسترسی غیرمجاز به داده‌های حفاظت شده اعم از مستقیم یا غیرمستقیم، جرم محسوب می‌شود. بر اساس ماده ۱۷ این قانون، تخلف از اصول مربوط به افشا و مخابره داده‌ها نیز جرم محسوب می‌شود. همچنین بر اساس ماده ۵۹ قانون تجارت الکترونیکی، برای ذخیره و پردازش داده‌های شخصی، رضایت لازم است. اما باید دقت داشت این ماده به طور مطلق از حریم خصوصی محافظت نمی‌کند، بلکه تنها زمانی که نقض حریم خصوصی باعث آسیب به موضوع داده شده باشد، در مقام حفاظت از آن قرار می‌گیرد. بر اساس ماده ۵۸ قانون تجارت الکترونیک؛ نگهداری، پردازش یا انتشار داده‌های شخصی که قومیت، نژاد، عقاید، مذهبی، ویژگی‌های اخلاقی یا وضعیت جسمی، روانی و یا جنسی افراد را بدون رضایت صریح آنها آشکار می‌کند، غیرقانونی است. از چند جهت می‌توان اصل ۵۸ قانون تجارت الکترونیک را نقد نمود. در واقع ماده مذکور برخلاف ماده ۶۶۹ قانون مجازات اسلامی[۴] هیچ گونه حمایتی از اطلاعات خصوصی غیرشخصی نمی‌کند.

---

۱. به حکم آیه شریفه «لا ینهاکم الله عن الذین لم یقاتلوکم فی الدین و لم یخرجوکم من دیارکم ان تبروهم و تقسطوا الیهم ان الله یحب المقسطین» دولت جمهوری اسلامی ایران و مسلمانان موظفند نسبت به افراد غیرمسلمان با اخلاق حسنه و قسط و عدل اسلامی عمل نمایند و حقوق انسانی آنان را رعایت کنند.

۲. همه افراد ملت اعم از زن و مرد یکسان در حمایت قانون قرار دارند و از همه حقوق انسانی، سیاسی، اقتصادی، اجتماعی و فرهنگی با رعایت موازین اسلام برخوردارند.

۳. اطبا و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند، هرگاه در غیر از موارد قانونی، اسرار مردم را افشاء کنند، به سه ماه و یک روز تا یک سال و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می‌شود.

۴. تهدید به قتل یا ضررهای نفسی یا شرفی یا مالی یا افشای سری نسبت به خود یا بستگان از موضوعات تهدید تلقی شده است. ضررهای نفسی شامل هرگونه آسیب به سلامتی و نفس شخص می‌گردد و در مورد ضرر شرفی هر موردی که بتوان به شرافت، آبروی شخص یا بستگانش مربوط کرد تهدید به آن، تهدید به ضرر شرفی است.

علاوه بر این، ماده ۵۸ قانون تجارت الکترونیک تنها به سه عمل ذخیره، پردازش و توزیع اطلاعات حساس دیگران اشاره داشته و جمع‌آوری غیرمجاز داده‌ها را که اهمیت بیشتری نسبت به ذخیره، پردازش یا توزیع داده‌ها دارد، جرم تلقی نمی‌کند.

ماده ۵۹ قانون تجارت الکترونیک، ذخیره، پردازش و یا انتشار داده‌های شخصی را مشمول شرایط خاصی می‌داند. ضرورت دسترسی آزاد به اطلاعات سبب تصویب قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ در ایران گردید. محدوده قانون مذکور تنها به دسترسی داده‌ها و انتشار می‌پردازد و در مورد جمع‌آوری و پردازش داده‌های شخصی اظهارنظر نمی‌کند. فصل چهارم این قانون به استثنائات دسترسی به اطلاعات از جمله اسرار دولتی، حفاظت از حریم خصوصی، حفاظت از سلامت و اطلاعات تجاری و امنیت ملی می‌پردازد. تعدادی از مصوبات شورای عالی فضای مجازی ایران به موضوع پردازش داده‌های عمومی و شخصی به‌طور خاص اشاره دارد. با وجود اینکه این مصوبات خط‌مشی کلی جمهوری اسلامی ایران در حوزه فضای سایبری را تشکیل می‌دهد، اما مستقیماً قابل اجرا نبوده و بخش قابل توجهی از آنها رعایت نمی‌شود. قانون اینترنت اشیا در تاریخ ۳۰ مهر ۱۳۹۷ با عنوان الزامات حاکم بر اینترنت اشیا در شبکه ملی اطلاعات به تصویب شورای عالی فضای مجازی رسید. در این قانون بر نقش اینترنت اشیا در توسعه جامعه و فناوری تاکید شده است. علاوه بر لزوم حفظ حریم خصوصی افراد، بر اقدامات لازم به منظور حفظ امنیت کاربران نیز تاکید شده است.[1]

بر اساس آیین‌نامه دفاتر خدمات اینترنت، این دفاتر از نقض حریم خصوصی شهروندان، استراق سمع و دسترسی غیرمجاز به داده‌های خصوصی آنها منع شده‌اند. بر اساس ماده ۶۵۸ قانون آیین دادرسی کیفری، قوه قضائیه موظف است به منظور حفظ حریم خصوصی و امنیت اطلاعات شخصی افراد، کلیه اقدامات فنی و قانونی لازم را به‌عمل آورد. بر اساس ماده ۶۷۵ قانون آیین دادرسی کیفری بررسی و ثبت داده‌ها باید متناسب با کشف جرم باشد. در صورت لزوم بررسی بخشی از اطلاعات به منظور کشف جرم و شناسایی متهم، نباید کل اطلاعات مورد بررسی و ثبت قرار گیرد، چرا که در غیر این‌صورت بررسی اسنادی که به موجب ماده ۸ قانون رعایت آزادی‌های مشروع و حقوق

---

۱. ماده ۲ الزامات حاکم بر اینترنت اشیا در شبکه ملی اطلاعات، ۱۳۹۷.

شهروندی[۱] مرتبط با جرم نباشد ممنوع است. ماده ۶۷۵، قانون آیین دادرسی کیفری ایران، اصل به حداقل رساندن داده‌ها را بیان می‌کند. بر اساس مواد ۶۶۰[۲] و ۶۶۱[۳]، قانون آیین دادرسی کیفری ایران، تعرض به حفاظت از داده‌ها، حبس یا جزای نقدی و انفصال از خدمت را به دنبال دارد. هر چند قانون آیین دادرسی کیفری بر ممنوعیت بررسی و ثبت اطلاعات افراد مگر در مواردی که قانونگذار اجازه بررسی اطلاعات شخصی را داده است بنا شده، با این حال مرز استثناء برای بررسی داده‌های شخصی به خوبی مشخص نگردیده است. همچنین از اصطلاحات کلی همچون لزوم کشف جرم استفاده گردیده که سبب سوء استفاده و تجاوز به حریم خصوصی موضوع داده می‌شود. ماده ۳۱[۴] منشور حقوق شهروندی بیان می‌دارد، موضوع داده دارای حقوق خاصی از جمله حق دسترسی و تصحیح

---

۱. بازرسی‌ها و معاینات محلی، جهت دستگیری متهمان فراری یا کشف آلات و ادوات جرم بر اساس مقررات قانونی و بدون مزاحمت و در کمال احتیاط انجام شود و از تعرض نسبت به اسناد و مدارک و اشیایی که ارتباطی به جرم نداشته و یا به متهم تعلق ندارد و افشای مضمون نامه‌ها، نوشته‌ها و عکس‌های فامیلی و فیلم‌های خانوادگی و ضبط بی‌مورد آنها خودداری گردد.

۲. چنانچه اشخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد یا محرمانگی اطلاعات را فراهم آورند یا به‌طور غیرمجاز آنها را افشاء کرده یا در دسترس اشخاص فاقد صلاحیت قرار دهند، به حبس از دو تا پنج سال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از خدمت از دو تا ده سال محکوم خواهند شد.

۳. چنانچه اشخاصی که مسئول حفظ امنیت مراکز، سامانه‌های رایانه‌ای و مخابراتی و اطلاعات موضوع این بخش هستند یا داده‌ها یا سامانه (سیستم)های مذکور در اختیار آنان قرار گرفته است بر اثر بی‌احتیاطی یا بی‌مبالاتی یا عدم مهارت یا عدم رعایت تدابیر متعارف امنیتی موجبات ارتکاب جرائم رایانه‌ای به‌وسیله یا علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را فراهم آورند، به حبس از شش ماه تا دو سال یا انفصال از خدمت تا پنج سال یا جزای نقدی از ده تا صدمیلیون ریال محکوم خواهند شد.

۴. حق شهروندان است که به اطلاعات شخصی خود که توسط اشخاص و موسسات ارائه دهنده خدمات عمومی جمع‌آوری و نگهداری می‌شود دسترسی داشته باشند و در صورت مشاهده اشتباه، خواستار اصلاح این اطلاعات گردند. اطلاعات خصوصی مربوط به افراد را نمی‌توان در اختیار دیگران قرار داد، مگر به موجب قانون یا با رضایت خود افراد.

اطلاعات است مواد ۳۵[۱] و ۳۶[۲] منشور، شهروندان حق دارند از اطلاعات شخصی و حریم خصوصی خود محافظت نمایند و دولت باید تمام اقدامات لازم را به منظور محافظت از این داده‌ها انجام دهد. همچنین بر اساس مواد ۳۷[۳]، ۳۸[۴] و ۳۹[۵] منشور حقوق شهروندی، حق بر حریم خصوصی شهروندان محترم شمرده می‌شود. با این وجود اما، مهم‌ترین پرسش این است که منشور حقوق شهروندی در نظام حقوقی داخلی ایران چه جایگاهی دارد. با توجه به بررسی‌ها و نحوه تنظیم و ابلاغ، اساسنامه نمی‌تواند بیش از یک برنامه اخلاقی برای دولت، همانگونه که در مقدمه منشور مطرح شده است باشد. در همین راستا طرح حمایت و حفاظت از داده و اطلاعات شخصی در جلسه علنی ۲۴ شهریور ۱۴۰۰ مجلس اعلام وصول گردید، اما هنوز به تصویب نرسیده است هدف اصلی این طرح رفع شکاف حقوقی مرتبط با داده ها است. این طرح، مکمل اقدامات مرتبط با حمایت از داده‌ها از جمله قانون مجازات اسلامی، قانون تجارت الکترونیک و قانون انتشار و دسترسی آزاد به اطلاعات می‌باشد. از دیگر اهداف این طرح، حمایت از موضوع داده‌ها است که به روش‌های زیر تحقق می‌یابد. شفاف‌سازی حقوق موضوع‌های داده، قانونی‌سازی پردازش داده‌های شخصی، مسئولیت‌پذیری کنترل‌کنندگان و پردازش‌کنندگان داده‌های شخصی و جبران خسارات ناشی از پردازش داده‌های شخصی.[۶] بر اساس ماده ۳، مشمولان این طرح

---

۱. حق شهروندان است که از امنیت سایبری و فناوری‌های ارتباطی و اطلاع‌رسانی، حفاظت از داده‌های شخصی و حریم خصوصی برخوردار باشند.

۲. حق هر شهروند است که حریم خصوصی او محترم شناخته شود. محل سکونت، اماکن و اشیاء خصوصی و وسایل نقلیه شخصی از تفتیش و بازرسی مصون است، مگر به حکم قانون.

۳. تفتیش، گردآوری، پردازش، به‌کارگیری و افشای نامه‌ها اعم از الکترونیکی و غیرالکترونیکی، اطلاعات و داده‌های شخصی و نیز سایر مراسلات پستی و ارتباطات از راه دور نظیر ارتباطات تلفنی، نمابر، بی‌سیم و ارتباطات اینترنتی خصوصی و مانند اینها ممنوع است مگر به موجب قانون.

۴. گردآوری و انتشار اطلاعات خصوصی شهروندان جز با رضایت آگاهانه یا به حکم قانون ممنوع است.

۵. حق شهروندان است که از اطلاعات شخصی آنها که نزد دستگاه‌ها و اشخاص حقیقی و حقوقی است، حفاظت و حراست شود. در اختیار قرار دادن و افشای اطلاعات شخصی افراد ممنوع است و در صورت لزوم به درخواست نهادهای قضایی و اداری صالح منحصراً در اختیار آنها قرار می‌گیرد. هیچ مقام و مسئولی حق ندارد بدون مجوز صریح قانونی، اطلاعات شخصی افراد را در اختیار دیگری قرار داده یا آنها را افشا کند.

۶. ماده ۱ طرح حمایت و حفاظت از داده و اطلاعات شخصی.

اتباع ایرانی هستند که اطلاعات شخصی آنها در داخل و یا خارج از ایران و نیز اتباع خارجی که اطلاعات شخصی آنها توسط کنترل کننده یا پردازشگر ایرانی پردازش می‌گردد. بر اساس این طرح، رضایت موضوع داده‌ها شرط پردازش داده‌های شخصی است. رضایت باید قبل از پردازش داده ها اخذ شود و باید بتوان رضایت را به فرد نسبت داد.[۱] اگر خود شخص، داده‌ها را در معرض دید عموم قرار داده باشد و پردازش آنها را منع نکرده باشد، پردازش داده‌های شخصی مربوط به موقعیت‌های عمومی بدون رضایت موضوع داده‌ها امکانپذیر است.[۲] موضوع داده این حق را دارد هر زمانی که بخواهد درخواست تعلیق بخش یا کل پردازش داده‌های خود را در صورتی که داده‌ها نادرست و یا منجر به نتایج نادرست می‌شود و نیز زمانی که داده‌ها خارج از محدوده رضایت او پردازش می‌شوند، داشته باشد.[۳] موضوع داده حق دسترسی به داده‌های خود را تحت شرایط خاص دارد، مشروط بر اینکه داده‌ها شامل داده‌های مهم عمومی یا شخصی دیگران نباشد و به آنها آسیبی نرساند.[۴]

طبق ماده ۹، رضایت شخص از پردازش اطلاعات شخصی به معنای افشای هویت او نیست. افشای هویت به معنای دسترسی غیرمجاز به داده‌های خصوصی افراد همچون نام و نام خانوادگی است. بر اساس ماده ۱۰، پردازش داده‌های شخصی در مواردی بدون رضایت شخص مجاز است که برای حفاظت از جان یا مال موضوع داده‌ها، امنیت عمومی، کشف جرائم، حفاظت از جان یا مال شخص دیگری ضروری باشد یا جلوگیری از متحمل شدن ضررهای مالی جدی، شناسایی متهم و اجرای دستورات قضایی ضروری است. مقامات زیر مسئول تنظیم و نظارت بر پردازش داده‌های شخصی هستند: کمیسیون حفاظت از داده‌های شخصی، گروه‌های تخصصی و شورای نظارت و در آخر دبیرخانه کمیسیون.[۵] در مواردی مانند پردازش اطلاعات حساس شخصی و بزرگ ناظر ویژه انتخاب می‌شود.[۶] کسب مجوز

---

۱. همان، ماده ۴.

۲. همان، ماده ۵.

۳. همان، ماده ۶.

۴. همان، ماده ۹.

۵. همان، ماده ۱۳.

۶. همان، ماده ۲۳.

از یک مرجع ذیصلاح، پیش‌نیاز و کلید پردازش داده‌های شخصی است.[۱] کنترل کننده یا پردازشگر موظف است هدف، نوع و نحوه پردازش، هویت و فعالیت‌های کنترل کننده یا پردازشگر، منابع پردازش، ویژگی و شرایط فنی پردازش، مجوزهای دریافت شده از مقامات ذیصلاح، سطح امنیتی پردازش و هزینه‌های آن، حقوق افراد موضوع داده در مورد پردازش داده‌های خصوصی خود و مرجعی که می‌توانند برای شکایت به آنها مراجعه کنند را در اختیار موضوع داده‌ها قرار دهد. لازم است کنترل کننده یا پردازشگر ظرف مدت یک ماه از تاریخ دریافت اطلاعات شخصی، مطابق این ماده اطلاع‌رسانی نماید.[۲]

با توجه به ضمانت‌های اجرای کیفری ماده ۵۱ این طرح، در صورت پردازش داده‌های شخصی بدون رضایت موضوع داده، مرتکب به اتهامات درجه ۵ محکوم می‌شود. قوانین ایران اطلاعات دقیقی در مورد حفاظت از داده‌های شخصی از جمله دامنه این حفاظت ارائه نمی‌دهد. تعدادی از اصطلاحات از جمله پردازش داده‌های شخصی، کنترل‌کننده و پردازش‌گر که مهمترین مفاهیم مربوط به حفاظت از داده‌های شخصی و حقوق موضوع داده‌ها هستند، تعریف نشده‌اند و منابع حقوقی ایران شرحی از آن ارائه نکرده‌اند.[۳]

به‌طور کلی در ایران قانون جامع حفاظت از داده‌ها به‌عنوان بخشی از نظام حقوقی تصویب نشده است که به نوعی می‌توان گفت، عدم تصویب قانونی جامع در این رابطه سبب ایجاد شکاف در نظام حقوقی می‌شود. قوانین متعددی با هدف حفاظت از حریم خصوصی وجود دارد که مهمترین آنها قانون تجارت الکترونیک و قانون جرائم رایانه‌ای است، با این وجود هیچ یک از این قوانین علی‌رغم اینکه در نظام حقوقی ایران نوآوری محسوب می‌شوند، حمایت همه جانبه‌ای از داده‌های شخصی ارائه نمی‌کنند.

نتیجه‌گیری

استفاده از داده‌های بیومتریک می‌تواند پیامدهایی برای آزادی‌های مدنی و حقوق بشر داشته باشد. بنابراین نقش قانونگذار در اینکه قوانین و مقررات را به نحوی تنظیم نماید تا

---

۱. همان، ماده ۳۰.

۲. همان، ماده ۳۳.

3. Mohammad Mustafa Mohiqi, “Personal Data Protection in the Iranian Legal System”, Journal of Politics and Law, Vol. 16, No. 3, (2023), P. 10.

همواره حق بر حریم خصوصی و حقوق بنیادین افراد مراعات گردد، بسیار مهم می‌نماید. چرا که زمینه پردازش داده‌های بیومتریک پویا است. پرونده‌های قضایی و رویه‌های حقوقی نقش مهمی در شکل دادن به فضای حقوقی مربوط به حق بر حریم خصوصی و پردازش داده‌های بیومتریک دارند.

تصمیمات قضایی به روشن شدن تفسیر و کاربرد حقوق حریم خصوصی، ارائه راهنمایی به سازمان‌ها و تأثیرگذاری بر تحولات قانونی کمک می‌کند. تعامل با حامیان حریم خصوصی، دانشگاه‌ها، کارشناسان صنعت و عموم مردم می‌تواند به شکل‌گیری سیاست‌ها، مقررات و بهترین شیوه‌های صیانت از حق حریم خصوصی کمک نموده و در عین حال امکان استفاده مفید از داده‌های بیومتریک را فراهم نماید. مکانیسم‌های جبران خسارت قوی باید برای رسیدگی به نقض حریم خصوصی یا نقض‌های مربوط به پردازش داده‌های بیومتریک وجود داشته باشد.

افراد باید راه‌های در دسترس برای طرح شکایت، جستجوی راه حل و دریافت غرامت در صورت نقض حریم خصوصی داشته باشند. ترویج آموزش و آگاهی در مورد پردازش داده‌های بیومتریک و حفظ حریم خصوصی حیاتی است. افراد باید در مورد خطرات، مزایا و حقوق خود در ارتباط با پردازش داده‌های بیومتریک مطلع شوند. در نظر گرفتن ابعاد اخلاقی، قانونی، تکنولوژیکی و اجتماعی به منظور اطمینان از حفاظت از حریم خصوصی و رعایت حقوق افراد در دنیایی که به طور فزاینده‌ای مبتنی بر بیومتریک است و نیز ایجاد تعادل میان مزایا و خطرات بالقوه مرتبط با فناوری‌های بیومتریک و در عین حال حفظ حریم خصوصی به‌عنوان یک حق اساسی، ضروری است.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID

Rezvaneh Mirzavand https://orcid.org/0009-0005-6467-608X

Roya Motamednejad https://orcid.org/0009-0003-4160-3377

منابع

مقاله‌ها

- داشاب، مهریار، «بخش اسناد حقوقی بین‌المللی، منشور حقوق اساسی اتحادیه اروپایی»، فصلنامه پژوهش حقوق عمومی، دوره ۶، شماره ۱۳، (۱۳۸۳).
- معتمدنژاد، رویا، «قانونگذاری در عرصه دیجیتال و برنامه توسعه پایدار (با تأکید بر «جمهوری دیجیتال»)»، نشریه علمی مطالعات فرهنگی و ارتباطات، سال ۱۳، شماره ۴۹، زمستان (۱۳۹۶).
- معتمدنژاد، رویا، «وظایف دولت‌ها در عرصه تکنولوژی‌های دیجیتال از دولت انحصارطلب تا دولت رگولاتور»، فصلنامه علوم خبری، دوره ۷، شماره ۲۸، (۱۳۹۷).

References

Books

- Anil K, Jain & Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics* (New York: Springer, 2011).
- Dibble, Suzanne, *GDPR for Dummies*, 1st Edition (New Jersey: For Dummies, 2020).
- European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018).
- Holder, Eric, Jr. Laurie O. Robinson, John H. Laub, *The Fingerprint: Sourcebook* (New York: Create Space Publishing, 2014).
- Jiang, Richard, *Biometric Security and Privacy Opportunities & Challenges in The Big Data Era* (Paris: Springer, 2017).
- Kindt, Els, *Privacy and Data Protection Issues Of Biometric Applications a Comparative Legal Analysis* (Dordrecht: Springer, 2013).
- Kuner, Christopher (ed), Drechsler, Laura (ed), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford: Oxford University Press, 2020).
- Sharma, Sanjay, *Data Privacy and GDPR Handbook*, 1st Edition (New Jersey: Wiley, 2019).

- Sinjini, Mitra & Gofman, Mikhail, *Biometrics in a Data Driven World: Trends, Technologies, and Challenges,* 1st Edition (Chapman and Hall/CRC, 2017).

- Smith, Marcus & Seumas, Miller, *Biometric Identification, Law and Ethics,* (Switzerland: Springer, 2021).

Articles

- Anil K. Jaina, Karthik Nandakumar, Arun Ross, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities", Pattern Recognition Letters, Vol. 79, (2016).

- Anil K. Jain, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, (2004).

- De Terwangne, Cécile, "Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data", Computer Law & Security Review, Vol. 40, (2021).

- Fierrez, Julian, Aythami, Morales, Ruben, Vera-Rodriguez, David, Camacho, "Multiple Classifiers in Biometrics. part 1: Fundamentals and Review", Information Fusion, Vol. 44, (2018).

- Gomez-Arostegui, Tomas, "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations", California Western International Law Journal, Vol. 35, No. 2, (2005).

- Hartmut, Aden, "Privacy and Security: German Perspectives, European Trends and Ethical Implications", Ethical Issues in Covert, Security and Surveillance Research Advances in Research Ethics and Integrity, Vol. 8, (2022).

- Hert, Paul & Vagelis Papakonstantinou, "The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on Its Global Ambition", Computer Law & Security Review, Vol. 30, (2014).

- Janelle, Mason, Rushit, Dave, Prosenjit, Chatterjee, Ieschecia, Graham-Allen, Albert, Esterline, Kaushik, Roy, "An Investigation of Biometric Authentication in the Healthcare Environment", Array, Vol. 8, (2020).

- Mohiqi, Mohammad Mustafa, "Personal Data Protection in the Iranian Legal System", Journal of Politics and Law, Vol. 16, No. 3, (2023).

- Prabhakar, Salil & Anil Kumar Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine, Vol. 1, (2003).

- Ratha Nalini K, Jonathan Connell, R. M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems", IBM Systems Journal, Vol. 40, No. 3, (2001).

- Remenyi Dan & Paul Griffiths, "Data: Its Nature and Management a Short Note on Some of the Complexity Behind the Concept of Data", The Electronic Journal of Business Research Methods, Vol. 20, No. 3, (2022).

- Sanchez-Reillo, Raul, Ines Ortega-Fernandez, Wendy Ponce-Hernandez, Helga C. Quiros-Sandoval, "How to Implement EU Data Protection Regulation for R&D in Biometrics", Computer Standards & Interfaces, Vol. 61, (2018).

In Persian

Articles

- Dashab, Mehriar, "International Legal Documents Section, Charter of Fundamental Rights of the European Union", Public Law Research Quarterly, Vol. 6, No. 13, (2013). [In Persian]

- Motamed Nejad, Roya, "Legislation in the Digital Arena and Sustainable Development Program (With an Emphasis on "Digital Republic")", Scientific Journal of Cultural and Communication Studies, Year 13, No. 49, (2016). [In Persian]

- Motamedenjad, Roya, "Duties of Governments in the Field of Digital Technologies, from the Monopolistic Government to the Regulatory Government", News Science Quarterly, Vol. 7, No. 28, (2017). [In Persian]

استناد به این مقاله: میرزاوند، رضوانه و معتمدنژاد، رویا، «پردازش داده‌های بیومتریک و تاثیر آن بر زندگی خصوصی با تاکید بر قوانین اتحادیه اروپا و شورای اروپا»، پژوهش حقوق عمومی، دوره ۲۶، شماره ۸۶، (۱۴۰۴)، ۲۷۲-۲۳۵.

Doi: 10.22054/QJPL.2024.77452.2958