Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/mtlj.2025.493734.1405

Protection of Children's Personal Data under the General Data Protection Regulation (GDPR) of the European Union and its Absence in Iranian Law

Khadijeh Shirvani[1*] Mohammad Isaei Tafreshi[2]

[1] Assistant Prof. Department of Law, Faculty of Humanities, University of Damghan, Semnan, Iran.

[2] Professor of private law, University of Science and Culture, Tehran, Iran.

Article Info

Original Article

Received:
13-12-2024
Accepted:
22-02-2025

Key Words:
Child
Personal Data Protection
General Data Protection Regulation (GDPR)

Abstract

In today's digital era, where the internet and digital technologies play an integral role in children's lives, safeguarding their data has become critical. The General Data Protection Regulation (GDPR) of the European Union stands as one of the most comprehensive legal frameworks addressing this concern. It mandates parental consent for data processing, promotes the use of simple language for children's understanding, and upholds the right to data deletion. Additionally, the GDPR enforces strict limitations on processing children's data and ensures specific rights to them. However, Iran's legal system still lacks a structured and comprehensive regulatory framework for protecting children's data. Although initiatives like the "Personal Data Protection and Support Plan" have been introduced, they fail to explicitly prioritize children's data protection. The rapid growth of online platforms and services targeting children has raised serious concerns about privacy and data security. Social media, educational applications, and gaming platforms often collect and process children's data without adequate safeguards, exposing them to potential risks such as identity theft, unauthorized profiling, and targeted advertising. The GDPR has sought to address these concerns by introducing stringent measures that hold data controllers accountable for the lawful and transparent processing of children's data. Conversely, Iran's legal framework remains underdeveloped in this area, lacking clear guidelines and enforcement mechanisms to ensure children's data privacy.

***Corresponding author**
e-mail: kh.shirvani@du.ac.ir

How to Cite:
Shirvani, K.H., & Isaei Tafreshi, M. (2025). Protection of Children's Personal Data under the General Data Protection Regulation (GDPR) of the European Union and its Absence in Iranian Law. *Modern Technologies Law*, *6*(12), 275-292.

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

1. Introduction

Children are increasingly engaged in digital environments, making their data vulnerable to misuse and exploitation. The internet has revolutionized access to information, communication, and entertainment, allowing children to interact in virtual spaces that were previously inaccessible. However, this increased connectivity has also led to new challenges concerning privacy, security, and digital rights. With the expansion of digital technologies, children's data has become a valuable commodity for companies and organizations that seek to analyze user behavior, target advertisements, and develop consumer profiles. This commercialization of data has raised ethical and legal concerns, particularly regarding the extent to which children's information should be collected, stored, and processed.

While digital platforms provide numerous benefits, such as educational resources and social networking opportunities, they also expose children to potential risks. Cyberbullying, identity theft, and exploitation are just some of the dangers that children face in the online world. The lack of legal literacy among children, coupled with their limited understanding of privacy policies, makes them particularly vulnerable to data misuse. Consequently, there is an urgent need for governments and regulatory bodies to implement policies that protect children from these threats and ensure their digital rights are safeguarded.

The GDPR was introduced to address these challenges by establishing a legal framework that prioritizes the protection of children's data. By requiring companies to obtain parental consent before processing children's data, the GDPR aims to reduce unauthorized data collection and provide greater transparency in how data is used. Furthermore, the regulation emphasizes the need for child-friendly privacy policies that are easy to understand and accessible to younger audiences. These measures ensure that children and their guardians can make informed decisions about their digital presence and the data they share online.

Despite the advancements brought by the GDPR, many countries, including Iran, have yet to implement comparable regulations. Iran's current legal framework on data protection is fragmented and lacks specific provisions that address children's online privacy. While some legislative efforts have been made, such as the proposed "Personal Data Protection and Support Plan," they fail to comprehensively address children's digital rights. This gap in regulation leaves Iranian children exposed to potential data exploitation without adequate legal recourse.

The primary objective of this study is to compare GDPR's child data protection mechanisms with Iran's current legal framework and to highlight the gaps that necessitate legal reforms. By analyzing both legal systems, this research aims to provide insights into the challenges and opportunities associated with protecting children's online privacy in Iran. Additionally, the study explores the broader socio-cultural implications of implementing stricter data protection policies and the potential impact on businesses, education systems, and digital governance.

With the proliferation of digital technologies, children's data is often collected, processed, and stored without their informed consent. The absence of comprehensive regulations in Iran leaves children susceptible to online threats, including cyberbullying, unauthorized data sharing, and surveillance. Given these challenges, the study aims to provide a comparative legal analysis that will assist policymakers in formulating effective data protection strategies tailored to children's needs. By drawing lessons from the GDPR, Iran can develop a robust legal framework that prioritizes children's digital rights and ensures that their data remains secure in an increasingly connected world.

2. Methodology

This study employs a comparative legal analysis method, examining the GDPR's provisions on children's data protection alongside Iranian laws. Data is gathered from legislative documents, legal analyses, and international reports on children's digital privacy. The study also incorporates case studies and expert opinions to identify key areas where Iran's legal system requires improvement. The analysis further explores the socio-cultural implications of adopting stricter data protection policies in Iran.

A qualitative research approach is utilized, involving document analysis and expert interviews to assess the effectiveness of existing legal frameworks. Furthermore, international best practices are reviewed to propose policy recommendations that align with global standards. By adopting a multidisciplinary perspective, the study aims to bridge the legal and technological gaps in child data protection.

3. Results and Discussion

The study identifies several key differences between GDPR and Iranian laws regarding children's data protection:

1. Age of Consent: The GDPR sets the digital age of consent at 16, allowing member states to reduce it to 13. Iran, however, follows Islamic legal age definitions (9 years for girls, 15 for boys), which significantly undermines children's ability to make informed privacy decisions. The discrepancy between the legal age of consent in Iran and international norms exposes Iranian children to potential data exploitation.

2. Transparency and Language: The GDPR mandates that digital service providers use child-friendly, simple language in privacy policies. Iranian regulations lack explicit provisions requiring clear and understandable communication with children. Without accessible privacy policies, children in Iran are less likely to understand their digital rights and responsibilities.

3. Marketing and Data Use Restrictions: GDPR imposes strict limits on the use of children's data for marketing and profiling, whereas Iranian laws do not explicitly prohibit data exploitation for commercial purposes. As a result, children in Iran may be targeted by advertisers and data brokers without adequate legal protections.

4. Right to Data Deletion: Under the GDPR, children have the right to request data deletion, an essential safeguard against long-term privacy risks. Iran's legal system lacks explicit guarantees for such rights, leaving children's digital footprints unprotected. The absence of a "right to be forgotten" provision in Iran further complicates efforts to safeguard children's online privacy.

The findings highlight the need for urgent reforms in Iran’s legal framework to align with global best practices. Implementing child-specific data protection measures can reduce the risk of cyber exploitation and unauthorized data processing. Additionally, integrating privacy education into school curricula can empower children and parents to navigate digital environments safely.

A comprehensive policy shift is required to ensure that Iran adopts child-centric data protection laws. Legal reforms should be accompanied by technological solutions, such as age-verification mechanisms and parental control tools, to enhance the safety of children’s online experiences. Moreover, collaboration between government agencies, educational institutions, and the private sector is essential to developing an effective child data protection ecosystem.

4. Conclusions and Future Research

The study concludes that Iran must establish a legal framework similar to the GDPR to ensure children's online safety. Key recommendations include:

Raising the legal age of consent for data processing to 18 to align with international child protection standards.

Mandating the use of clear and comprehensible language in privacy policies for children to ensure transparency and informed decision-making.

Introducing strict regulations limiting the commercial use of children's data and prohibiting targeted advertising practices that exploit minors.

Recognizing and enforcing children's right to data deletion to protect them from potential digital harm.

Implementing digital literacy programs to educate children and parents about online privacy risks and responsible internet use.

Establishing an independent regulatory body dedicated to monitoring and enforcing child data protection laws.

Encouraging private sector compliance with ethical data handling practices through incentives and penalties.

Promoting cross-sectoral collaboration between government agencies, tech companies, and advocacy groups to ensure a holistic approach to child data protection.

Conducting periodic assessments and revisions of child data protection policies to keep pace with technological advancements and emerging threats.

Enhancing international cooperation to adopt best practices from global data protection frameworks and ensure seamless integration into Iran’s legal landscape.

By adopting these measures, Iran can create a safer digital landscape for children, ensuring their fundamental right to privacy is protected in the evolving digital age. Addressing legislative gaps and fostering a culture of data privacy awareness will ultimately empower children to navigate the digital world securely and responsibly.

حقوق فناوری‌های نوین

http://doi.org//10.22133/mtlj.2025.493734.1405

حمایت از داده‌های شخصی کودکان در مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا و جای خالی آن در حقوق ایران

خدیجه شیروانی[۱*]، محمد عیسائی تفرشی[۲]

[۱] استادیار، گروه حقوق، دانشکدهٔ علوم انسانی، دانشگاه دامغان، دامغان، سمنان، ایران.

[۲] استاد گروه حقوق خصوصی، دانشکدهٔ حقوق، دانشگاه علم و فرهنگ، تهران، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۹/۲۳

تاریخ پذیرش:
۱۴۰۳/۱۲/۰۴

واژگان کلیدی:
کودک
دادهٔ شخصی
حمایت
مقررات عمومی حفاظت از داده‌ها

چکیده

در دنیای امروز که اینترنت و فناوری‌های دیجیتال بخشی جدایی‌ناپذیر از زندگی کودکان شده است، حفاظت از داده‌های شخصی آنان اهمیتی ویژه دارد. مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا (GDPR) با وضع قواعدی مانند لزوم کسب رضایت قانونی از سرپرستان کودکان، ساده‌سازی اطلاعات برای درک کودکان و تأکید بر حق حذف داده‌ها، به‌طور مؤثر از حقوق کودکان در فضای دیجیتال حمایت می‌کند. در نظام حقوقی ایران، به‌منظور حفاظت از داده‌ها تلاش‌هایی شده است؛ مانند تهیهٔ طرح حمایت و حفاظت از داده‌های شخصی که هنوز به تصویب نرسیده است، اما مفاد طرح مذکور نیز به‌طور خاص و چشمگیر به حمایت از کودکان نمی‌پردازد؛ به‌ویژه کاستی‌هایی مانند بی‌توجهی به سن رضایت والدین برای پردازش داده‌های کودکان هم‌سو با قانون حمایت از اطفال و نوجوانان (۱۳۹۹) و مقررات بین‌المللی، نبود قوانین شفاف دربارهٔ محدودیت‌های بازاریابی هدفمند، تأکید نکردن بر زبان ساده و شفاف و کمبود آموزش و آگاهی‌بخشی در این زمینه مشاهده می‌شود. این مقاله با مقایسهٔ تطبیقی بین مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا و نظام حقوقی ایران، پیشنهادهایی ارائه کرده است؛ ازجمله افزایش سن قانونی رضایت به هجده سال، تدوین قوانینی برای محدودسازی پردازش داده‌های کودکان و اجرای برنامه‌های آموزشی برای کودکان و والدین. این اقدامات می‌توانند گامی مؤثر در راستای حفظ حریم خصوصی کودکان و پیشگیری از سوءاستفاده‌های احتمالی در فضای مجازی باشند.

***نویسندهٔ مسئول**

رایانامه: kh.shirvani@du.ac.ir

نحوهٔ استناددهی:

شیروانی، خدیجه، و عیسائی تفرشی، محمد (۱۴۰۴). حمایت از داده‌های شخصی کودکان در مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا و جای خالی آن در حقوق ایران. حقوق فناوری‌های نوین، ۶(۱۲)، ۲۷۵-۲۹۲.

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

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

فناوری اطلاعات و ارتباطات، فرصت‌های بی‌سابقه‌ای را برای اشخاص فراهم کرده است تا با هم ارتباط برقرار کنند، اطلاعات مفید به اشتراک بگذارند، یاد بگیرند، به اطلاعات دسترسی داشته باشند و نظرات خود را درمورد موضوعاتی بیان کنند که در زندگی و جوامع آن‌ها تأثیرگذار است. در اتحادیهٔ اروپا، منشور حقوق اساسی حق احترام به زندگی خصوصی به‌طورکلی و حفاظت از داده‌های شخصی به‌طور خاص را تضمین می‌کند. دیوان دادگستری اتحادیهٔ اروپا مدت‌هاست که بر اهمیت این حقوق تأکید کرده است. منشور حقوق اساسی به رسمیت شناختن و حفاظت از حقوق کودکان را افزایش داده است و اکنون این امر برای نظم حقوقی اتحادیهٔ اروپا بسیار مهم است[1].

از زمان تصویب مقررات عمومی حفاظت از داده‌ها، تغییرات درخور توجهی در چشم‌انداز حفاظت از داده‌ها ایجاد شده است. نخست پیشرفت‌های سریع فناوری در چند سال گذشته، مقیاس و اهمیت جمع‌آوری و اشتراک داده‌ها را افزایش داده و چالش‌های جدیدی در برابر حفاظت از داده‌های شخصی ایجاد کرده است؛ دوم مقام‌ها سازوکارهای تبادل اطلاعات بین خود را به‌منظور پردازش داده‌ها به‌منزلهٔ بخشی از مبارزه با جرایم فراملی و تروریسم معرفی کرده‌اند؛ بنابراین نیاز به قوانین واضح و منسجم درمورد حفاظت از داده‌ها در سطح اتحادیهٔ اروپا را افزایش می‌دهند. سومین مورد، که ارتباط نزدیکی با موارد فوق دارد، این است که آگاهی درمورد اهمیت داده‌های شخصی افزایش یافته و معاهدهٔ لیسبون حمایت از آن را به‌منزلهٔ حق اساسی براساس قوانین اتحادیهٔ اروپا[2] معرفی کرده است (Truli, 2018, pp. 3-4)؛ بنابراین جای تعجب نیست که نهادهای اتحادیهٔ اروپا اصلاح دستورالعمل حفاظت از داده‌ها را در دستور کار خود قرار دادند که فرایند آن از سال ۲۰۰۹ آغاز شد و پس از مشورت عمومی، کمیسیون اروپا در اواخر سال ۲۰۱۰ مکاتبهٔ مربوطه را منتشر کرد. متعاقباً همهٔ شرکت‌کنندگان عمده در این فرایند (شورا، پارلمان، ناظر حفاظت از داده‌های اروپا، و حزب کارگر) نظرات خود را هم درمورد مکاتبهٔ کمیسیون و هم با توجه به دیدگاه خود درمورد اصلاحات احتمالی برای دستورالعمل ارائه کردند (Truli, 2018, p. 4). درنهایت در آوریل ۲۰۱۶ نهادهای اتحادیهٔ اروپا بستهٔ اصلاحی را تهیه کردند که شامل موارد زیر است: الف) مقررات عمومی حفاظت از داده‌ها[3] و ب) دستورالعمل حفاظت از داده‌های شخصی[4] که به‌منظور اجرای قانون، یا همان‌طور که اغلب از آن یاد می‌شود، دستورالعمل پلیس و مقامات قضایی کیفری[5]، با هدف ایجاد سازوکار تبادل کارآمدتر اطلاعات بین مقام‌های مختلف قضایی استفاده می‌شود (Truli, 2018, pp. 4-5).

مقررات عمومی حفاظت از داده‌ها در ۲۵ مه ۲۰۱۸ اجرایی و از این تاریخ دستورالعمل EC/۴۶/۹۵ ملغی شد. به‌موجب آن بسیاری از مقررات (متعارض) قوانین ملی در این زمینه نیز ملغی شدند (Truli, 2018, p. 5) .

آنچه در این زمینه اهمیت دارد و نظر نگارندگان را جلب کرده است، تأکید مقررات عمومی حفاظت از داده‌ها بر کودکان و حفظ داده‌های ایشان است. درحقیقت در دوران جدید، زندگی «واقعی» کودکان بیش از هر زمان دیگری بر اینترنت متمرکز است[6]. آمارها می‌گویند که تخمین زده می‌شود از هر سه کاربر اینترنت در جهان امروز، یک نفر زیر ۱۸/۵ سال دارد (Livingstone et al., 2015, p. 1) و نیز از هر پنج کاربر

1. See Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (2012 OJ C 326/2) [hereafter CFR]; see also Article 16(1) of the Treaty on the Functioning of the European Union (2012 OJ C 326) [hereafter TFEU] and Article 39 of the Treaty on the European Union (2012 OJ C 326) (the full text of these Articles is set out in §§1–3 of Appendix I).
2. See Article 6(1) of the Treaty of the European Union, recognizing the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000 (as adapted in Strasbourg, on 12 December 2007), and Article 8 of the EU Charter of Fundamental Rights. See also Article 16 of the Treaty on the Functioning of the European Union and Article 8 of the European Convention on Human Rights.
3. General Data Protection Regulation (EU) 2016/679 of 27 April 2016 (GDPR)
4. Directive on the protection of personal data; Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/997/JHA, OJ L 119/89, 4 May 2016 (Police and Criminal Justice Data Protection Directive). The Directive must be transposed by member states by 6 May 2018.
5. Police and Criminal Justice Authorities Directive
6. A Brief History of Internet of Things, http://postscapes.com/internet-of-thingshistory, 21 June 2016.

اینترنت در اتحادیهٔ اروپا، یک نفر کودک است[1]؛ بنابراین این گرایش رایج که کودکان در اینترنت فقط از دریچهٔ خطرات مشاهده می‌شوند، باید به رویکردی واقع‌بینانه‌تر تغییر یابد که شامل همهٔ فرصت‌ها در طرف دیگر طیف است (Krivokapić & Adamović, 2016, p. 206). این واقعیت که حقوق کودکان و نیاز به حمایت ویژهٔ آن‌ها به‌صراحت در مقررات عمومی حفاظت از داده‌ها تأیید شده است و این‌که مقررات عمومی حفاظت از داده‌ها در مفاد مختلف خود به‌رسمیت می‌شناسد که کودکان گروهی از کاربران هستند که مستحق حمایت خاص‌اند، در اصل گامی بزرگ به جلوست (Fuster, 2016). همچنین مقررات مذکور صراحتاً موقعیت ویژهٔ کودکان و نیازهای آن‌ها را در محیط آنلاین ازطریق مرجعی خاص در مقدمه تأیید می‌کند و می‌گوید: «کودکان در رابطه با داده‌های شخصی خود مستحق حمایت خاصی هستند؛ زیرا ممکن است کمتر از خطرات، عواقب و حقوق خود در رابطه با پردازش داده‌های شخصی آگاه باشند.» به‌هرحال، پذیرفته شده است که ایمنی کودکان در اینترنت نگرانی عمده‌ای است؛ اما قبل از مقررات عمومی حفاظت از داده‌ها هیچ قانونی در سطح اروپا وجود نداشت که به‌طور مستقیم این موضوع را تنظیم کند (Krivokapić & Adamović, 2016, p. 214) .

در نظام حقوقی ایران، هنوز قانون واحدی که به‌طور خاص حفاظت از داده‌های شخصی را بررسی کند تصویب نشده است؛ بنابراین هدف از تحقیق حاضر، بررسی حمایت‌های قانونی مقررات عمومی حفاظت از داده‌ها در اتحادیهٔ اروپا از کودکان و تطبیق آن با نظام حقوقی ایران و درنهایت، ارائهٔ پیشنهادهایی در این زمینه به قانون‌گذار است. در این پژوهش، نخست به بررسی اصول و شرایط کلی داده‌ها در نظام حقوقی اتحادیهٔ اروپا و ایران می‌پردازیم و شرایط پردازش داده‌های کودکان را مطالعه می‌کنیم.

۱. اصول و شرایط کلی پردازش داده‌ها

درخصوص تفاوت اصول و شرایط، باید یادآور شد که اصول چهارچوب‌های کلی‌ای هستند که باید در تمام مراحل پردازش داده‌ها رعایت شوند. این اصول بیشتر جنبهٔ کلی و راهبردی دارند و به نحوهٔ رفتار با داده‌ها و حقوق افراد مربوط می‌شوند؛ اما شرایط مواردی هستند که در زمان پردازش داده‌ها باید وجود داشته باشند یا رعایت شوند. این شرایط بیشتر جنبهٔ عملیاتی و اجرایی دارند و به‌طور مستقیم به نحوهٔ اخذ رضایت، دسترسی به داده‌ها و موارد مجاز پردازش بدون رضایت مربوط می‌شوند. به‌هرحال، هر دوی این موارد در کنار هم، تضمین‌کنندهٔ حفاظت از داده‌های شخصی و حقوق افراد هستند.

۱-۲. اتحادیهٔ اروپا

۱-۱-۲. اصول

مقررات عمومی حفاظت از داده‌ها در مادهٔ ۵، قواعدی را درخصوص پردازش داده‌های شخصی[2] تنظیم و اصولی را مقرر می‌کند که پردازش‌کنندگان داده‌های شخصی ملزم به رعایت آن‌ها هستند (Feikert-Ahalt, 2021, p. 1). این اصول عبارت‌اند از:

الف) قانونی بودن، انصاف و شفافیت[3]: داده‌های شخصی باید به‌صورت قانونی، منصفانه و شفاف پردازش شوند. افراد باید از نحوه و هدف پردازش داده‌های خود مطلع شوند.

1. "When Free isn't", eNASCO Report, http://www.enacso.eu/wp-content/uploads/ 2015/12/free-isnt.pdf, 59.

۲. بند ۱ مادهٔ ٤ مقررات عمومی حفاظت از داده‌ها در تعریف دادهٔ شخصی مقرر می‌دارد: «دادهٔ شخصی عبارت است از هرگونه اطلاعات مرتبط با شخص حقیقی که در حال حاضر شناخته شده است یا قابلیت شناسایی داشته باشد. منظور از شخص حقیقی قابل شناسایی هر شخصی است که به‌طور مستقیم یا غیرمستقیم به‌خصوص، با استفاده از مواردی ازجمله نام، شمارهٔ شناسایی، اطلاعات مربوط به مکان، شناسهٔ برخط، یا با استفاده از یک یا چند ویژگی خاص مانند هویت فیزیکی، ویژگی‌های فیزیولوژی، ژنتیکی، روانی، اقتصادی، فرهنگی و اجتماعی شخص مذکور قابل شناسایی باشد.»

3. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

ب) محدودیت هدف[1]: داده‌های شخصی باید فقط برای اهداف مشخص، قانونی و از پیش تعیین شده، جمع‌آوری شوند و پردازش‌های بیشتر نباید با این اهداف مغایرت داشته باشد؛

ج) حداقل‌سازی داده‌ها[2]: داده‌های شخصی باید فقط به مقدار لازم و کافی برای تحقق اهداف پردازش جمع‌آوری شوند و نباید بیشتر از آنچه نیاز است ثبت شوند.

د) دقت: داده‌های شخصی باید دقیق و درصورت لزوم به‌روز باشند. برای اصلاح یا حذف داده‌های نادرست اقدامات لازم باید انجام شود[3].

ه) محدودیت نگهداری: داده‌های شخصی باید فقط به مدت لازم برای تحقق اهداف پردازش نگهداری شوند. پس از تحقق این اهداف، داده‌ها باید حذف یا به طور ایمن نگهداری شوند[4].

و) یکپارچگی و محرمانگی: پردازش داده‌های شخصی باید به‌گونه‌ای انجام شود که امنیتشان حفظ شود و در برابر پردازش غیرمجاز یا غیرقانونی و همچنین در برابر خسارت محافظت شوند[5].

۲-۱-۲. شرایط

بند ۱ مادهٔ ۶ شرایطی را بیان می‌کند که براساس آن پردازش داده‌ها قانونی است. شایع‌ترین شرط بحث رضایت موضوع داده است-Feikert). Ahalt, 2022, p. 1) براساس مادهٔ مذکور، پردازش داده‌های شخصی فقط درصورتی قانونی است که یکی از شرایط ذیل وجود داشته باشد:

الف) رضایت شخص: فرد موضوع داده باید به‌صراحت رضایت خود را برای پردازش داده‌های شخصی‌اش برای یک یا چند هدف خاص اعلام کرده باشد؛

ب) پردازش داده‌ها برای اجرای یک قرارداد، که شخص یکی از طرفین آن قرارداد است، یا برای انجام اقداماتی که به درخواست فرد پیش از انعقاد قرارداد انجام می‌شود، ضروری باشد؛

ج) تخلف از تعهدات قانونی: پردازش داده‌ها برای رعایت یک تعهد قانونی که بر عهدهٔ شخص کنترل‌کننده است، ضروری باشد؛

د) حفاظت از منافع حیاتی: پردازش داده‌ها برای حفاظت از منافع حیاتی شخص موضوع داده یا شخص حقیقی دیگری ضروری باشد؛

ه) پردازش داده‌ها برای انجام وظایف عمومی یا برای تحقق منافع عمومی ضروری باشد، به شرط این‌که پردازش مذکور قانونی باشد؛

و) فرایند پردازش به‌منظور انعقاد منافع مشروع پردازشگر یا شخص ثالث ضروری باشد، تا زمانی که منافع فردی و حقوق و آزادی‌های بنیادین او بر این منافع مشروع غلبه نکند.

این شرایط چهارچوبی برای پردازش داده‌های شخصی فراهم می‌کنند و هدف اصلی آن‌ها حفاظت از حقوق و آزادی‌های افراد در مقابل پردازش غیرقانونی و زیانبار داده‌های شخصی است. هر پردازشگر باید نشان دهد که چگونه و چرا شرایط قانونی پردازش داده‌ها را برقرار می‌کند.

1. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
2. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
3. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
4. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
5. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

۲-۲. حقوق ایران

در حقوق ایران، قانونی که به‌طور ویژه به حفاظت از داده‌ها پرداخته باشد به تصویب نرسیده است و درحال‌حاضر، طرحی تحت‌عنوان طرح حمایت و حفاظت از داده و اطلاعات شخصی به امضای چند تن از نمایندگان رسید؛ اما هنوز به تصویب نرسیده است. به همین دلیل، مبنای بررسی ما در این مقاله طرح مذکور است.

۲-۲-۱. اصول

الف) قانونی بودن، انصاف و شفافیت: براساس این اصول، پردازش داده‌ها باید بر مبنای پایه‌ای قانونی انجام شود. این مبنای قانونی مانند رضایت شخص موضوع داده، که در مادهٔ ۴ ذکر شده است، یا ضرورت‌های قانونی موجود برای پردازش داده‌ها که در مادهٔ ۵ آمده است. پردازش باید منصفانه باشد و لطمه‌ای به حقوق افراد وارد نکند. علاوه بر این‌ها، افراد باید به‌طور شفاف درمورد چگونگی و هدف پردازش داده‌هایشان اطلاع داشته باشند. برای مثال، مادهٔ ۴ که مقرر می‌دارد رضایت شخص موضوع داده باید بیانگر آگاهی او باشد، حاکی از اهمیت شفافیت در بحث پردازش داده‌هاست.

ب) محدودیت هدف (هدفمندی): براساس مادهٔ ۴ طرح، داده‌ها باید فقط برای اهداف مشخص، صریح و مشروع جمع‌آوری و پردازش شوند و استفاده از داده‌ها برای اهداف دیگر بدون رضایت مجدد فرد ممنوع است. این امر نشان‌دهندهٔ اصل محدودیت هدف در پردازش داده‌هاست.

ج) حداقل‌سازی داده (کمینه‌سازی داده): براساس این اصل، فقط داده‌هایی که برای دستیابی به اهداف مشخص ضروری هستند باید جمع‌آوری و پردازش شوند و جمع‌آوری داده‌های اضافی یا غیرمرتبط ممنوع است.

د) دقت: داده‌ها باید دقیق و به‌روز باشند و درصورت وجود خطا باید اقدامات لازم برای اصلاح یا حذف داده‌های نادرست انجام شود. براساس مادهٔ ٦ طرح، شخص موضوع داده حق دارد اگر داده‌ها نادرست باشند، عدم پردازش داده‌ها را تقاضا کند. این ماده بیانگر این است که داده‌ها باید با دقت پردازش شوند.

۲-۲-۲. شرایط

الف) رضایت: براساس مادهٔ ۴ طرح، پردازش داده‌های شخصی مربوط به وضعیت‌ها و موقعیت‌های غیرعمومی، منوط به رضایت شخص موضوع داده است. رضایت باید پیش از پردازش اخذ شود و بیانگر آگاهی شخص و استنادپذیر باشد؛

ب) حق حذف داده‌ها: براساس مادهٔ ۶ طرح، شخص موضوع داده هر زمان حق دارد مانع از پردازش داده‌های خود شود یا تقاضا کند داده‌ها حذف شوند؛ به‌ویژه زمانی که داده‌ها نادرست باشند یا پردازش خارج از محدودهٔ رضایت او باشند؛

ج) دسترسی به داده‌ها: براساس مادهٔ ۸ طرح، شخص موضوع داده حق دارد به داده‌های شخصی خود دسترسی داشته باشد؛ البته به شرط این‌که شامل اطلاعات طبقه‌بندی شدهٔ عمومی یا داده‌های دیگران نباشد و استنادناپذیری داده‌ها مخدوش نشود؛

د) گمنامی: براساس مادهٔ ۹ طرح، رضایت به پردازش داده‌ها به معنای آشکارسازی هویت شخص نیست و حق گمنامی وی باید در محدودهٔ رضایت رعایت شود. در چهارچوب این قانون، آشکاری هویت به معنای آگاهی اشخاص غیرمجاز از نام و نام خانوادگی شخص موضوع داده یا شناسه‌های تخصیص یافته و منتسب به آن‌هاست.

۳. حمایت از کودکان در مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا

۳-۱. تعریف کودک

در جامعهٔ امروزی، داده‌های شخصی ازطریق نهادهای دولتی و خصوصی، طی بسیاری از فعالیت‌ها، برای اهداف وسیع و به روش‌های مختلف پردازش می‌شوند. افراد اغلب ممکن است از نظر درک نحوهٔ پردازش داده‌های شخصی آن‌ها، ازجمله فناوری استفاده شده در یک مورد خاص، چه ازطریق نهادی خصوصی یا نهادی عمومی، در موقعیت نامطلوبی قرار گیرند. آن‌گونه که گفته شده است، یکی از مهم‌ترین نوآوری‌های مقررات عمومی حفاظت از داده‌ها، که از سال ۲۰۱۸ جایگزین دستورالعمل ۱۹۹۵[1] شد، این است که مقرراتی را شامل می‌شود که به طور خاص با حفاظت از داده‌های کودکان سروکار دارد؛ این مقررات چالش برانگیز است، اما یک نوآوری خوشایند است. به‌هرحال، قانون‌گذاران سابق اتحادیهٔ اروپا مستحق انتقاد هستند؛ زیرا دستورالعمل ۱۹۹۵ در این زمینه ساکت بوده است؛ بنابراین این امر که مقررات عمومی حفاظت از داده‌ها تشخیص داده که لازم است از کودکان حمایت‌های ویژه‌ای شود، شایستهٔ تقدیر است (Feikert-Ahalt, 2021, p. 1). به‌منظور حفاظت از داده‌های شخصی اشخاص حقیقی در این شرایط، مقررات عمومی حفاظت از داده‌ها، چهارچوبی قانونی و منسجم و قوی ایجاد کرده است که عموماً با توجه به انواع مختلف پردازش، ازجمله مقررات خاص مربوط به حقوق موضوع داده، قابل اعمال است (European Data Protection Board, 2023, p. 8).

مقررات عمومی حفاظت از داده‌ها واژهٔ کودک را تعریف نکرده است و همین امر باعث شده است که نویسندگان این نکته را جزء نقاط ضعف مقررات مذکور یاد کنند. یکی از نویسندگان در این زمینه بیان می‌کند که آستانهٔ سنی تعیین شده در بند ۱ مادهٔ ۸ مقررات عمومی حفاظت از داده‌ها فقط برای اهداف این ماده که عبارت است از قواعد مربوط به ارائهٔ خدمات جامعهٔ اطلاعاتی کاربرد دارد. وقتی مقررات دیگر ـ که حقوق کودکان را تنظیم می‌کند ـ در نظر می‌گیریم، باید بپرسیم آستانهٔ سنی تعریف شده در مقررات مذکور به چه معناست؟ ازآنجاکه تمام کشورهای عضو اتحادیهٔ اروپا کنوانسیون حقوق کودک سازمان ملل را پذیرفته‌اند، منطقی است به این نتیجه برسیم که باید از تعریفی که سند مذکور برای کودک بیان کرده در مقررات عمومی حفاظت از داده‌ها هم استفاده می‌شد و بهتر است که این موضوع به‌صراحت توسط قانون‌گذاران مقررات عمومی حفاظت از داده‌ها حل شود؛ البته لازم به ذکر است که در هیچ جای مقررات عمومی حفاظت از داده‌ها نامی از کنوانسیون حقوق کودک سازمان ملل متحد برده نشده است و اتحادیهٔ اروپا هم عضو آن نیست. بنابراین، حتی ممکن است که تفسیر شود که آستانهٔ سنی مذکور در بند ۱ مادهٔ ۸ درواقع شامل تعریف معتبر کودک برای تفسیر در سایر مقررات است. اگر کشورهای عضو ملزم باشند که از تعریف کنوانسیون حقوق کودک استفاده کنند، این بدان معناست که مقررات عمومی حفاظت از داده‌ها دارای دو جریان مؤثر نسبت به کودکان است: تمام مقرراتی که در آن از کودک نام برده می‌شود، منظور افراد زیر هجده سال است؛ درحالی‌که بند ۱ مادهٔ ۸ یک استثنا در این نظام به شمار می‌رود. این دوگانگی قوانین درمورد کودکان ممکن است به طور بالقوه باعث برخی سوءتفاهم‌ها و سوءاستفاده از مقررات عمومی حفاظت از داده‌ها شود (Krivokapić & Adamović, 2016, p. 208). گفتنی است که مطابق مادهٔ ۱ کنوانسیون حقوق کودک سازمان ملل متحد، «کودک به افراد زیر هجده سال اطلاق می‌گردد؛ مگر این‌که طبق قانون قابل اجرا دربارهٔ کودک، سن بلوغ کمتر تشخیص داده شود.» مقررات عمومی حفاظت از داده‌ها تصریح می‌کند که پردازش داده‌های شخصی کودکان زیر شانزده سال تمام ـ ممکن است هر کشوری در اتحادیهٔ اروپایی این سن را با توجه به مقررات خود کاهش دهد ـ فقط با رضایت والدین یا سرپرست قانونی مجاز است. مطابق بند ۱ مادهٔ ۸ مقررات عمومی حفاظت از داده‌ها، هرجا که بند (الف) مادهٔ ٦ (۱) صدق کند و مربوط به ارائهٔ خدمات اطلاعاتی[2] نسبت به کودک، آن‌هم به‌طور مستقیم باشد، پردازش داده‌های شخصی کودک زمانی قانونی است که کودک حداقل شانزده سال داشته باشد. اگر کودک زیر شانزده سال باشد، پردازش داده‌های وی

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

۲. مثل فروشگاه‌های آنلاین، پلتفرم‌های اشتراک ویدئو، سایت‌های شبکه‌های اجتماعی، موتورهای جست‌وجو و غیره.

درصورتی قانونی است که رضایت یا مجوز از سوی والدین یا سرپرستان کودک وجود داشته باشد. کشورهای عضو می‌توانند طبق قانون، سن کمتری را برای این اهداف تعیین کنند؛ مشروط بر این‌که کمتر از سیزده سال نباشد[1].

آستانهٔ سنی شانزده سال در آلمان و رومانی استفاده می‌شود. با توجه به این‌که مقررات عمومی حفاظت از داده‌ها به کشورها اجازه می‌دهد سن کمتری برای رضایت ارائه کنند، برخی از کشورها آستانهٔ سنی را کاهش داده‌اند. فرانسه و یونان برای کودکان زیر پانزده سال به رضایت سرپرست قانونی نیاز دارند. اسپانیا افراد زیر چهارده سال را در نظر می‌گیرد و دانمارک، پرتغال، سوئد و بریتانیا این سن را برای رضایت در سیزده‌سالگی تعیین کردند. این قابلیت انعطاف‌پذیری به کشورها اجازه می‌دهد با توجه به شرایط فرهنگی و اجتماعی خود، سیاست‌های مناسب‌تری را اتخاذ کنند.

۳-۲. اصول کسب رضایت از سرپرستان

درمورد توازن خطرات و فرصت‌های ناشی از خدمات جامعهٔ اطلاعاتی نظراتی وجود دارد که حق حریم خصوصی کودکان (که البته شامل اطلاعات شخصی آن‌ها نیز می‌شود) درحال‌حاضر به اندازه‌ای نیاز به حمایت دارد که باید بر سایر حقوق مقدم باشد (Keen, 2016). برهمین‌اساس، مادهٔ ۸ مقررات عمومی حفاظت از داده‌ها به‌وضوح بر اهمیت حفاظت از داده‌های کودکان تأکید دارد و تأمین رضایت سرپرستان را پیش‌نیازی ضروری برای پردازش داده‌های شخصی افراد زیر سن خاص مشخص می‌کند. این ممنوعیت باعث تدوین چهارچوبی امن‌تر برای کودکان در دنیای دیجیتال می‌شود و بر شفافیت و آگاهی از حقوق خود تأکید دارد.

۳-۲-۱. رضایت معتبر

مطابق بند ۲ مادهٔ ۸ مقررات عمومی حفاظت از داده‌ها، کنترل‌کننده باید به‌منظور اثبات این‌که والدین یا سرپرستان قانونی طفل رضایت داشته‌اند، تلاش متعارفی کند[2]. لازم به ذکر است که بند ۳ همین ماده بیان می‌کند که بند ۱ بر قوانین عمومی قراردادها ازجمله قوانین مربوط به اعتبار، تشکیل و آثار قرارداد دربارهٔ کودکان در کشورهای عضو تأثیرگذار نیست. در بریتانیا، کنترل‌کنندهٔ داده‌ها وظیفه دارد تأیید کند فردی که رضایت کودک را ارائه می‌کند مسئولیت والدین کودک را برعهده دارد. در پرتغال به مجوز از قیم قانونی نیاز دارد تا ازطریق ابزاری مطمئن برای احراز هویت به دست آید. آلمان و رومانی از کنترل‌کنندگان داده‌ها می‌خواهند برای تأیید این‌که شخصی با اختیارات والدین از طرف کودک رضایت داده است تلاش‌های معقولانه‌ای انجام دهند. بااین‌حال، هر دو کشور روش تشخیص این امر را مشخص نکرده‌اند و هیچ راهنمایی درمورد چگونگی تعیین سن کودکان صادر نکرده‌اند. تصمیم اخیر دادگاه آلمان نشان داده است مانعی که نیاز به وارد کردن گذرنامه یا شمارهٔ شناسایی یا شمارهٔ کارت اعتباری با حداقل مبلغ برداشت شده از حساب دارد کافی نیست و به‌جای آن، استفاده از سایر اقدامات فنی‌تر مانند اطلاعات بیومتریک توصیه می‌شود (Feikert-Ahalt, 2021, p. 2). گفتنی است براساس قسمت اخیر مادهٔ ۳۸ مقررات عمومی حفاظت از داده‌ها، رضایت والدین نباید به‌منزلهٔ ابزاری برای کنترل والدین بر اعمال کودکان در هنگام استفاده از برنامه‌ها و بازی‌ها در نظر گرفته شود. رضایت والدین اقدامی قانونی برای رضایت به پردازش داده‌ها به‌منظور هدفی خاص است که این پردازش‌ها را قانونی می‌کند. والدین باید این تصمیم را برای فرزندان خود، زمانی که زیر سن خاصی هستند، براساس این ایده اتخاذ کنند که کودکان عواقب و خطرات عملیات پردازش داده‌های خاص را درک نمی‌کنند. این امر مستلزم آن است که والدین درمورد چیستی، چگونگی و چرایی پردازش داده‌های خاص توسط ارائه‌دهندهٔ خدمات

1. Art. 8 GDPR: 1- Where point (a) of Article 6 (1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

دیجیتال اطلاعاتی کسب کنند. کنترل والدین طیفی از ابزارها یا راهبردها را برای تضمین ایمنی کودکان فراتر از پردازش داده‌ها دربر می‌گیرد و بنا به صلاحدید والدین، اما ترجیحاً در ارتباط آزاد با فرزندانشان، استفاده می‌شود (Hof & Ouburg, 2021, p. 7).

۳-۲-۲. لزوم استفاده از زبان واضح و مناسب برای کودکان (اصل شفافیت)

برای اخذ رضایت صحیح از سرپرستان قانونی کودک، ضروری است اطلاعات شفافی درمورد نوع داده‌های جمع‌آوری شده، هدف پردازش و غیره ارائه شود. تصور نادرست دربارهٔ مادهٔ ۸ مقررات عمومی حفاظت از داده‌ها این است که تنها مبنا و شرط پردازش داده‌های کودکان کسب رضایت از سرپرستان ایشان برای پردازش است؛ اما مادهٔ ۸ این فرض را رد می‌کند. درحقیقت یکی از مزایای مقررات مذکور این است که پردازشگرهای داده را مجبور می‌کند به‌طور شفاف اطلاعاتی دربارهٔ مبنای داده‌ها ارائه دهند. براساس بند (۱) مادهٔ ۱۲ مقررات عمومی حفاظت از داده‌ها، کنترل‌کننده باید اقدامات مقتضی را برای ارائهٔ هرگونه اطلاعات مندرج در ۱۳ و ۱۴ و هرگونه مکاتبه براساس مواد ۱۵ تا ۲۲ و ۳۴، مربوط به پردازش به شخص موضوع داده به‌صورت مختصر، شفاف و قابل فهم و با قابلیت دسترسی آسان فراهم کند؛ به‌ویژه زمانی که اطلاعات مربوط به یک کودک باشد. بنابراین، مقررات مذکور الزامی را تعیین می‌کند که هرگونه اطلاعات و ارتباطات باید به زبانی واضح و ساده بیان شود که کودک بتواند به‌راحتی آن را درک کند. اصل شفافیت، که به‌ویژه کودکان را هدف قرار می‌دهد، به‌دلیل نحوهٔ دسترسی کودکان به اینترنت، یعنی بیشتر زمانی که تنها هستند و همچنین به‌دلیل در دسترس بودن دستگاه‌هایی که به اینترنت دسترسی دارند (مانند تلفن‌ها و تبلت‌های شخصی کودکان) مهم است. هنوز مشخص نیست که اصل شفافیت چگونه عملاً اجرا خواهد شد؛ با توجه به این واقعیت که کنترل‌کننده‌ها تاکنون تمایل داشتند اقداماتشان با داده‌های جمع‌آوری‌شده را پنهان کنند، فشار مستقیم به آن‌ها برای افشای اقدامات خود باید به بهبود در این زمینه منجر شود. توجه به کودکان باید به تغییر در درک عمومی منجر شود؛ به‌طوری‌که دیگر با آن‌ها به‌عنوان تنها گروهی از مصرف‌کنندگان بالقوه رفتار نشود، بلکه بپذیریم که آن‌ها گروهی آسیب‌پذیر از کاربران اینترنت هستند (Krivokapić & Adamović, 2016, p. 216).

۳-۲-۳. حق دسترسی به داده‌ها

حق دسترسی به داده‌ها[1] در مادهٔ ۱۵ مقررات عمومی حفاظت از داده‌ها مطرح شده است. این حق به گونه‌ای طراحی شده است که افراد حقیقی را قادر می‌سازد بر داده‌های شخصی مربوط به خود کنترل داشته باشند و به آن‌ها اجازه می‌دهد «از قانونی بودن پردازش آگاه شوند و آن را تأیید کنند». به‌طور خاص، هدف از حق دسترسی آن است که اشخاص موضوع داده را قادر سازد تا نحوهٔ پردازش داده‌های شخصی خود و همچنین پیامدهای آن را درک کنند و صحت داده‌های پردازش شده را بدون نیاز به توجیه قصد آن‌ها تأیید کنند. به عبارت دیگر، هدف از حق دسترسی به داده‌ها، ارائهٔ آسان اطلاعات کافی و شفاف درمورد پردازش داده‌ها به شخص موضوع داده، بدون توجه به فناوری‌های استفاده شده و توانمندسازی آن‌ها برای تأیید جنبه‌های مختلف یک پردازش (مثل قانونمندی، دقت و ...) مطابق با مقررات عمومی حفاظت از داده‌هاست (European Data Protection Board, 2023, p. 10). براساس بند ۱ مادهٔ ۱۲ مقررات عمومی حفاظت از داده‌ها، کنترل‌کننده باید اقدامات مناسبی را به‌منظور دسترسی به داده‌ها، مطابق مادهٔ ۱۵، به‌صورت مختصر، شفاف، قابل فهم و سهولت دسترسی با استفاده از زبانی شفاف فراهم کند. الزامی که ارائهٔ دسترسی به موضوع داده باید به‌صورت مختصر و شفاف انجام شود به این معناست که کنترل‌کننده‌ها باید اطلاعات را به‌طور مؤثر و مختصر ارائه کنند تا به‌راحتی توسط موضوع داده قابل درک باشد؛ به‌ویژه اگر کودک باشد. کنترل‌کننده باید هنگام انتخاب ابزاری برای ارائهٔ دسترسی طبق هنر، کمیت و پیچیدگی داده‌ها را در نظر بگیرد (European Data Protection Board, 2023, p. 44). علاوه‌براین، گفته شده است که الزامات دقیق‌تر در زمینهٔ حق دسترسی به شرایط پردازش داده و همچنین توانایی موضوع داده در درک ارتباطات (برای مثال با در نظر گرفتن این‌که موضوع داده یک کودک یا فردی با نیازهای ویژه است) بستگی دارد. اگر داده‌ها از کدها یا سایر «داده‌های خام» تشکیل شده‌اند، ممکن است لازم باشد این موارد توضیح داده شوند تا برای موضوع داده معنا پیدا کنند (European Data Protection Board, 2023, p. 44).

1. Right of access by the data subject

زمانی که کودکان موضوع داده هستند، حق دسترسی هم متعلق به کودک است. بسته به بلوغ و اهلیت کودک، ممکن است نیاز به شخص ثالثی داشته باشد تا حق خود را اعمال کند؛ مانند سرپرست قانونی وی. در تمام تصمیماتی که دربارهٔ اعمال حق دسترسی برای کودکان اعمال می‌شود؛ به‌ویژه در مواردی که حق دسترسی از طرف کودک اعمال می‌شود، شخص دارندهٔ اختیارات والدین باید بهترین منافع کودک را مدنظر قرار دهد (European Data Protection Board, 2023, p. 30).

۳-۲-٤. حق اصلاح داده‌ها

براساس مادهٔ ۱۶ مقررات عمومی حفاظت از داده‌ها، اشخاص موضوع داده حق دارند از کنترل‌کننده تقاضا کنند داده‌های نادرست یا ناقصشان را اصلاح کنند[1]. کودکان از تمام حقوقی که مقررات عمومی حفاظت از داده‌ها برای بزرگ‌سالان پیش‌بینی کرده است بهره‌مندند. قانون به‌صراحت نگفته که این حقوق از جانب سرپرستان آن‌ها اعمال می‌شود؛ اما این حقوق ممکن است از جانب سرپرستان آن‌ها اعمال شود. درحقیقت، سرپرستان قانونی کودک می‌توانند درصورت نیاز، اطلاعات ناقص یا نادرست مربوط به فرزندان خود را اصلاح کنند.

۳-۲-۵. حق حذف داده‌ها

مادهٔ ۱۷ مقررات عمومی حفاظت از داده‌ها به‌صراحت بیان می‌کند که درصورت دریافت درخواست حذف، کنترل‌کننده موظف است داده‌ها را حذف کند؛ مگر این‌که دلیل قانونی معتبری برای ادامهٔ نگهداری آن داده وجود داشته باشد. به‌موجب مادهٔ مذکور، حق حذف داده‌ها در چهار حالت به شخص موضوع داده اعطا می‌شود: الف) درصورتی‌که داده‌ها به‌طور غیرقانونی پردازش شده باشند؛ ب) اگر پردازش داده‌ها مبتنی بر رضایت فرد باشد و وی به هر دلیلی رضایتش را پس بگیرد؛ ج) درصورتی‌که شخص موضوع داده درخواست کند فرد داده‌های شخصی‌اش را به‌دلیل عدم انطباق با قانون حذف کند؛ د) درصورتی‌که داده‌ها مورد نیاز شخص موضوع داده نباشند. قسمت (و) بند ۱ مادهٔ ۱۷ این مقررات به‌طور خاص بیان می‌کند یکی از دلایل درخواست پاک کردن داده‌ها زمانی است که «داده‌های شخصی در رابطه با ارائهٔ خدمات جامعهٔ اطلاعاتی[2] ذکر شده در مادهٔ ۸ (۱) جمع‌آوری شده باشد». بند ۱ مادهٔ ۸ هم مقرر می‌دارد: «در مواردی که قسمت الف از بند ۱ مادهٔ ۶ در رابطه با ارائهٔ خدمات جامعهٔ اطلاعاتی به‌طور مستقیم درمورد کودک اعمال گردد، پردازش داده‌های شخصی کودک، درصورتی‌که حداقل ۱۶ سال سن داشته باشد، قانونی خواهد بود....». بنابراین، چنین ماده‌ای موضع شورای اروپا را در این زمینه که در بیانیهٔ کمیتهٔ وزیران درمورد حمایت از کرامت، امنیت و حریم خصوصی کودکان در اینترنت بیان شده، در خود گنجانده است[3].

درحقیقت، حق حذف داده‌ها به افراد این امکان را می‌دهد که کنترل بیش‌تری بر داده‌ها و اطلاعات خود داشته باشند. درمورد کودکان این حق را والدین و سرپرستان قانونی اعمال می‌کنند. بنابراین، اگرچه مقررات مذکور به‌صراحت توضیح نمی‌دهد، باید گفته شود که حق حذف داده می‌تواند توسط (الف) کودکانی که داده‌های آن‌ها براساس رضایت والدین جمع‌آوری شده است، زمانی که به سن بالاتر از سیزده تا شانزده‌سالگی برسند و همچنین (ب) توسط والدینی که فرزندانشان درمورد سن خود دروغ گفته‌اند تا آزادانه از خدمات جامعهٔ اطلاعاتی استفاده کنند،

---

1. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

۲. بند (ب) مادهٔ ۱ (۱) دستورالعمل Directive (EU) 2015/1535 در تعریف خدمات جامعهٔ اطلاعاتی مقرر می‌دارد: «عبارت است از هر خدمتی که معمولاً با دستمزد، از راه دور، به وسیلهٔ وسایل الکترونیکی و بنا به درخواست فرد دریافت‌کنندهٔ خدمات ارائه می‌شود.» در این تعریف:

الف) «از راه دور» به این معناست که خدمات بدون حضور هم‌زمان طرفین ارائه می‌شود.

ب) «ازطریق وسایل الکترونیکی» به این معناست که سرویس ابتدا به‌وسیلهٔ تجهیزات الکترونیکی برای پردازش (ازجمله فشرده‌سازی دیجیتال) و ذخیره‌سازی داده‌ها و انتقال به‌طور کامل، به‌وسیلهٔ سیم، رادیو یا ابزار نوری یا هر وسیلهٔ الکترونیکی دیگر ارسال و دریافت می‌شود.

ج) «به درخواست فردی گیرندهٔ خدمات» به این معناست که خدمات انتقال داده‌ها، براساس درخواست فردی، ارائه می‌شود.

3. Council of Europe Explanatory memo, point 5; also Council of Europe, Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID =09000016805d3d2d.

درصورتی‌که قبل از رسیدن کودک به آستانهٔ سنی لازم، از این موضوع مطلع شوند، مورد تقاضا قرار بگیرد (Krivokapić & Adamović, 2016, p. 218).

۳-۳. تأثیر غیرمستقیم نوآوری‌های مقررات عمومی حفاظت از داده‌ها در کودکان

بخشی از مقررات مذکور به‌طورکلی نظام حفاظت از دادهٔ اروپا را در مقایسه با دستورالعمل ۱۹۹۵ بهبود بخشیده است. این مقررات غیرمستقیم اما به‌طور شایان توجهی به نفع کودکان است. یکی از آن‌ها گسترش تعریف داده‌های شخصی است که مشخص می‌کند داده‌های شخصی شامل چه مواردی می‌شود (برای مثال ارجاع واضح به ابرداده). چنین «گسترشی» در تعریف داده‌های شخصی، به‌ویژه درمورد داده‌های کودکان، به دلیل افزایش تعداد مواردی که به عنوان «داده» جمع‌آوری می‌شوند، اهمیت بیشتری می‌یابد. علاوه‌بر پیچیدگی بالقوهٔ مفهوم داده‌های شخصی برای جوانان، در درک مهوم اینترنت اشیا و خطرات ناشی از آن نیز با مشکلات بیشتری مواجه شوند (Krivokapić & Adamović, 2016, p. 216).

مقررات مذکور، همچنین استانداردهای بالاتری را برای کیفیت رضایت تعیین کرده و امکانات کنترل کننده را برای تکیه بر توجیه منافع قانونی محدود کرده است. نمایه‌سازی داده‌های شخصی نیز در مقایسه با دستورالعمل ۱۹۹۵ درحال‌حاضر سخت‌تر است. علاوه‌بر افزایش تعهدات کنترل‌کننده‌ها، مقررات عمومی حفاظت از داده‌ها نیز تعهدات خاصی را برای پردازشگرها تعیین می‌کند. اختیارات کمیسیون از نظر حوزهٔ قلمروی برنامهٔ مقررات عمومی حفاظت از داده‌ها و از نظر فرصت برای اعمال جریمه‌های درخور توجه افزایش یافته است.

۴. حمایت از کودکان در مقررات ایران

در نظام حقوقی ایران، با توجه به تحولات گسترده در فضای مجازی و افزایش حضور کودکان در این فضا، نیاز به حمایت از حقوق کودکان، به‌ویژه در زمینهٔ حفاظت از داده‌های شخصی، اهمیت زیادی یافته است. بااین‌حال، مقررات موجود در ایران نسبت به حمایت از کودکان در فضای دیجیتال و حفاظت از داده‌های آن‌ها، به‌طور کامل توسعه نیافته است و خلأهای حقوقی فراوانی در این حوزه وجود دارد.

۴-۱. تعریف کدک

در قوانین ما، سن بلوغ شرعی در تبصرهٔ ۱ مادهٔ ۱۲۱۰ قانون مدنی در پسر پانزده سال تمام قمری و در دختر نه سال تمام قمری اعلام شده است. مطابق بند (الف) و (ب) مادهٔ ۱ قانون حمایت از اطفال و نوجوانان (مصوب ۱۳۹۹/۲/۲۳) «طفل هر فردی است که به سن بلوغ شرعی نرسیده باشد و نوجوان عبارت است از هر فرد زیر هجده سال کامل شمسی که به سن بلوغ شرعی رسیده باشد.» با جمع این دو ماده، طفل کسی است که زیر نه و پانزده سال تمام قمری باشد و نوجوان کسی است که زیر هجده سال است. علاوه‌براین، در بند ۲ مادهٔ ۱ سند صیانت از کودکان و نوجوانان در فضای مجازی[1]، خردسالان، کودکان و نوجوانان عبارت‌اند از کلیهٔ افراد کمتر از هجده سال که در قلمرو حاکمیت جمهوری اسلامی ایران قرار دارند و در چهارچوب سند تحول بنیادین آموزش‌وپرورش رده‌بندی سنی می‌شوند.

۴-۲. شرایط پردازش داده‌های کودکان

مادهٔ ۴ طرح حمایت و حفاظت از داده‌های شخصی به‌طورکلی بیان می‌کند که «پردازش داده‌ها و اطلاعات شخصی مربوط به وضعیت‌ها و موقعیت‌های غیرعمومی منوط به رضایت شخص موضوع آن‌هاست. اعلام رضایت اشخاص موضوع داده باید با رعایت شرایط ذیل باشد: الف) پیش از پردازش باشد؛ ب) بیانگر آگاهی شخص موضوع داده باشد؛ ج) استنادپذیر باشد. نکتهٔ درخور توجه این است که در تبصرهٔ مادهٔ ۵

۱. مصوبهٔ شورای عالی فضای مجازی درخصوص صیانت از کودکان و نوجوانان در فضای مجازی، که در اجرای مادهٔ ۱۱ آیین‌نامهٔ داخلی شورای عالی فضای مجازی به تصویب رسیده است.

این طرح بیان شده است: «.... درصورت عدم اهلیت وی، رضایت ولی یا قیم او الزامی است.» درهرحال، اصول کلی این طرح به‌گونه‌ای است که می‌تواند شامل حمایت از کودکان و افراد آسیب‌پذیر نیز باشد. برای مثال موارد زیر را می‌توان از طرح مذکور برداشت کرد:

۱. رضایت در پردازش اطلاعات: این طرح بیان می‌کند که پردازش داده‌های شخصی مربوط به وضعیت‌های غیرعمومی نیازمند رضایت شخصی است که اطلاعات مربوط به اوست. همان‌طور که پیش‌تر گفته شد، این رضایت در افراد محجور برعهدهٔ ولی یا قیم است؛

۲. حق دسترسی و اصلاح اطلاعات: افراد حق دارند که به داده‌های خود دسترسی داشته و درخواست اصلاح یا توقف پردازش داده‌های نادرست را داشته باشند (مواد ۶ و ۸). این حقوق می‌تواند برای حفاظت از حریم خصوصی کودکان، در برابر سوءاستفاده‌های احتمالی از اطلاعات آها، اهمیت ویژه‌ای داشته باشد؛

۳. اولویت حقوق افراد آسیب‌پذیر: در این طرح در موارد تضاد منافع یا تعارض حقوقی، اولویت با افرادی است که به‌لحاظ سنی و شرایط اجتماعی، آسیب‌پذیر محسوب می‌شوند (مادهٔ ۱۲). این امر به‌صورت ضمنی حمایت از کودکان را هم شامل می‌شود؛

۴. حفظ گمنامی: افراد موضوع داده‌ها، از جمله کودکان، حق دارند هویتشان گمنام بماند؛ مگر در مواردی که شخصاً موافقت کنند (مادهٔ ۹). این امر می‌تواند از هویت کودکان در برابر شناسایی شدن بدون رضایت حفاظت کند.

۴-۳. چالش‌های طرح حمایت و حفاظت از داده‌های شخصی

در طرح حمایت و حفاظت از داده‌های شخصی، حقوق افراد ازجمله کودکان در زمینهٔ پردازش داده‌ها و اطلاعات شخصی بررسی شده است؛ اما به‌طور خاص و آن‌گونه که در مقررات عمومی حفاظت از داده‌ها در اروپا به‌طور دقیق به حقوق اشخاص زیر شانزده سال پرداخته، به کودکان توجهی نشده است. درحالی‌که این موضوع به‌قدری مهم است که نویسندگان اتحادیهٔ اروپا، قانون‌گذاران پیشین را شایستهٔ سرزنش دانسته‌اند و مقررات عمومی حفاظت از داده‌ها را، با وجود ایراداتی که دارد، به‌دلیل توجه به حقوق کودکان در زمینهٔ حفاظت از داده‌های شخصی‌شان، شایان تقدیر دانسته‌اند. به‌هرحال این طرح در مقایسه با استانداردهای جهانی، مانند مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، ضعف‌ها و کاستی‌هایی دارد؛ به‌ویژه در زمینهٔ حفاظت از حقوق کودکان؛ ازجملهٔ این ضعف‌ها به قرار ذیل است:

۴-۳-۱. سن رضایت

در تبصرهٔ مادهٔ ۵ طرح حمایت و حفاظت از داده‌های شخصی بیان شده است که «.... در صورت عدم اهلیت وی، رضایت ولی یا قیم او الزامی است» و در حقوق ما اشخاصی که اهلیت ندارند عبارت‌اند از: صغار، مجانین و سفها. بنابراین، اگر شخصی بخواهد داده‌های اشخاص را پردازش کند، اگر شخص موضوع داده، صغیر (زیر پانزده سال تمام برای پسران و زیر نه سال تمام برای دختران) باشد، لازم است از ولی یا قیم وی اجازه بگیرد. این درحالی است که قانون حمایت از اطفال و نوجوانان، تعریفی از واژه‌های «اطفال» و «نوجوانان» ارائه داده است و افراد زیر سن بلوغ را طفل نامیده و افراد بالای سن بلوغ تا هجده سال تمام را نوجوان نامیده است و تمام این دو گروه را مشمول حمایت از مقررات قانون مذکور کرده است و به‌نظر می‌رسد بهتر است طرح حمایت و حفاظت از داده‌های شخصی به این نکته توجه کند و مانند قانون حمایت از اطفال و نوجوانان در این زمینه عمل کند.

۴-۳-۲. کم‌توجهی به شفافیت و زبان ساده

این طرح بر ارائهٔ اطلاعات به زبان ساده و مفهوم برای کودکان تأکید خاصی ندارد. این درحالی است که مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، به‌صراحت بر این موضوع تأکید کرده است تا کودکان بتوانند از حقوق خود آگاه شوند و تصمیمات آگاهانه بگیرند.

۴-۳-۳. عدم محدودیت صریح در استفاده از داده‌های کودکان برای اهداف بازاریابی

طرح مذکور درمورد استفاده از داده‌های کودکان برای اهداف بازاریابی یا اهداف پروفایل‌های شخصی محدودیت‌های صریحی ندارد. درحالی‌که مادهٔ ۲۱ مقررات عمومی حفاظت از داده‌های شخصی اتحادیهٔ اروپا، استفاده از داده‌های کودکان برای چنین اهدافی را به‌شدت محدود می‌کند.

۴-۳-۴. عدم پیش‌بینی حق حذف

در مادهٔ ۱۷ مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا، حق حذف به‌طور خاص برای کودکان در نظر گرفته شده است. این حق به کودکان یا والدین آن‌ها اجازه می‌دهد تا حذف داده‌های شخصی کودکان را درخواست کنند؛ به‌ویژه اگر داده‌ها در زمانی جمع‌آوری شده باشند که کودک به سن قانونی تعیین شده در مقررات مذکور نرسیده باشد. این درحالی است که در طرح حمایت و حفاظت از داده و اطلاعات شخصی این حق به‌صراحت پیش‌بینی نشده است.

۴-۴. پیش‌نویس لایحهٔ حمایت از داده و حریم خصوصی در فضای مجازی

در این لایحه به اشخاص محجور اشاره کرده و در بند ۱ و ۲ مادهٔ ۳ بیان می‌کند:
بند ۱: «ایجاد، پردازش و استفاده از داده‌های شخصی باید مبتنی بر رضایت صریح یا ضمنی اشخاص موضوع آن باشد مگر به حکم قانون. اعلام رضایت حاصل از فریب یا تهدید یا اکراه معتبر نیست. ....» بند ۲: «درصورت محجور بودن شخص موضوع داده اجازهٔ ولی یا قیم قانونی او ضروری است.» درخصوص این بند، لازم است نکاتی مطرح شود: نخست این‌که مسلم است لفظ محجور مطابق قانون مدنی عبارت است از مجنون، سفیه و صغیر. مطابق تبصرهٔ ۱ مادهٔ ۱۲۱۰ قانون مدنی، صغیر هر فردی است که به سن نه سال تمام قمری برای دختران و پانزده سال تمام قمری برای پسران، نرسیده باشد. نکتهٔ دوم، که در قالب سؤال از نگارندگان این طرح پرسیده می‌شود، این است که آیا بهتر نیست همگام با قانون حمایت از کودکان و نوجوان و نیز سند صیانت از حقوق کودک، تمام افراد زیر هجده سال را زیر چتر حمایتی خود درآورد و بیان کند پردازش داده‌های کلیهٔ افراد زیر هجده سال ـ که در قانون حمایت از اطفال و نوجوانان به اشخاص بالای سن بلوغ و کمتر از هجده سال نوجوان اطلاق می‌شود ـ نیاز به رضایت صریح سرپرست قانونی وی دارد؟

نتیجه‌گیری

مقررات عمومی حفاظت از داده‌های اتحادیهٔ اروپا به‌منزلهٔ مقررات جامع و پیشرفته در زمینهٔ حفاظت از داده‌های شخصی شناخته می‌شود. یکی از ویژگی‌های مهم این مقررات، حفاظت از حقوق کودکان در فضای دیجیتال است و نیاز به حفاظت خاص از داده‌های آن‌ها را به‌رسمیت می‌شناسد. این مقررات با محدودیت‌های سنی برای رضایت قانونی، ساده‌سازی اطلاعات برای درک کودکان، تقویت حفاظت از آن‌ها در محیط‌های آنلاین و تأکید بر حق حذف داده‌ها تلاش می‌کند تا از آسیب‌پذیری کودکان در برابر سوءاستفاده از داده‌های شخصی جلوگیری کند. این حمایت‌ها، به‌ویژه در فضای دیجیتال که کودکان در معرض خطرات گوناگونی مثل سرقت هویت، تبلیغات هدفمند نادرست، یا سوء استفاده‌های اجتماعی قرار دارند، اهمیت بسزایی پیدا می‌کند. در نظام حقوقی ایران، هرچند هنوز به مقررات جامعی مانند مقررات اتحادیهٔ اروپا دست نیافته است، تلاش‌هایی در راستای تدوین مقررات مشابه دیده می‌شود. برای مثال، طرح حمایت و حفاظت از داده و اطلاعات شخصی، به تصویب نرسیده است، اما گام مهمی در راستای حمایت از داده‌های شخصی است. با وجود این‌که مقرراتی برای حمایت از کودکان در ایران وجود دارد؛ خلأهایی جدی در زمینهٔ حفاظت از داده‌های شخصی کودکان در فضای مجازی مشاهده می‌شود. برای رفع این خلأها، تصویب قوانین جدید و اجرای سیاست‌های حمایتی ویژه برای کودکان در فضای مجازی ضروری است. این اقدامات نه‌تنها به حفظ حریم خصوصی کودکان کمک می‌کند، بلکه از آن‌ها در برابر تهدیدات فضای مجازی محافظت خواهد کرد. پیشنهاد می‌شود که قانون‌گذاران ایرانی با الگوبرداری از مقررات عمومی حفاظت از داده‌ها، قانونی را تصویب کنند که به حفاظت از داده‌های کودکان در فضای مجازی توجه داشته و برای پردازش

داده‌های آن‌ها، رضایت والدین یا سرپرستان قانونی را الزامی کنند. در این راستا، لازم است محدودهٔ سنی برای کسب رضایت از سرپرستان، که درحال حاضر در قوانین ما همان سن بلوغ است، به هجده سال افزایش یابد و هماهنگ با قانون حمایت از اطفال و نوجوانان، محدودیت سنی در پردازش داده‌ها هم کودکان و هم نوجوانان را تحت پوشش قرار دهد. این امر باعث می‌شود که قانون مذکور با مقررات بین‌المللی ازجمله کنوانسیون حقوق کودک هم‌سو باشد. همچنین، در این قانون باید مقرراتی برای افزایش شفافیت، ساده‌سازی اطلاعات، حق حذف داده‌های کودکان به‌طور خاص و محدودیت استفاده از داده‌های کودکان برای اهداف بازاریابی وضع شود. این اقدام گامی مؤثر در راستای حفظ حریم خصوصی کودکان و جلوگیری از سوءاستفاده‌های احتمالی از داده‌های آنان است. علاوه‌براین، برای تقویت حمایت از حقوق کودکان در فضای دیجیتال و حفاظت از داده‌های شخصی آنان، لازم است برنامه‌های آموزشی و آگاهی‌بخشی برای والدین و کودکان درخصوص حفاظت از داده‌های شخصی در فضای مجازی تدوین شود. این آموزش‌ها می‌تواند شامل نحوهٔ استفادهٔ امن از اینترنت، اهمیت حفاظت از داده‌های شخصی و مخاطرات فضای مجازی باشد. همچنین، یکی از راهکارهای مهم در حفاظت از کودکان در فضای مجازی، ایجاد رده‌بندی سنی برای محتواها و خدمات ارائه شده در اینترنت است. این اقدام مانع دسترسی کودکان به محتواهای نامناسب می‌شود و همچنین جمع‌آوری داده‌های آن‌ها را محدود می‌کند. همان‌طور که ملاحظه شد، در قانون حمایت از اطفال و نوجوانان، تمام حمایت‌هایی که برای این قشر مقرر داشته است، شامل هر دو گروه «اطفال» و «نوجوانان» می‌شود. بنابراین، پیشنهاد می‌شود قانون‌گذار نیز با توجه به گسترش فضای مجازی و سهولت دسترسی کودکان به این فضا، مقررات خاصی را برای اشخاص زیر هجده سال، به‌ویژه به‌منظور صیانت از داده‌هایشان، مقرر دارد.

منابع

Council of Europe. (n.d.). Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet. Link

European Data Protection Board. (2023, March 28). Guidelines 01/2022 on data subject rights - Right of access (Version 2.1). Link

Feikert-Ahalt, C. (2021). Children's online privacy and data protection in selected European countries (Report for Congress). The Law Library of Congress. Link

Fuster, G. G. (2016). *GDPR: we all need to work at it!* Link

Hof, S. van der, & Ouburg, S. (2021). *D2.3 Methods for obtaining parental consent and maintaining children rights*. Leiden University. Link

Keen, A. (2016, February 6). Free speech shouldn't be more important than the safety of our children. The Next Web. Link

Krivokapić, Đ., & Adamović, J. (2016). impact of general data protection regulation on children's rights in digital environment. *Belgrade Law Review*, *LXIV*(3), 207-224. Link

Livingstone, S., Carr, J., & Byrne, J. (2015). *One in three: internet governance and children's rights* (The Global Commission on Internet Governance, Paper Series, 22/2015). Link

Truli, E. N. (2018). The General Data Protection and civil liability. In Mohr Backum et al. (Eds.), *Personal data in competition, consumer protection and intellectual property: Towards a holistic approach?* Springer Verlag. Link