University of Tehran Press

Comparative Law Review

Online ISSN: 2423-3404

Volume: 17, Issue: 1
Spring & Summer
2026

Homepage: https://jcl.ut.ac.ir

Protecting Children's Personal Data in Iran: An Analysis of Legislative Gaps and a Strategic Roadmap with Comparative View on EU and UK Regulations

Mohammad Hajali[1]✉ | **Zahra Hoseinpour**[2]

1. Corresponding Author; Ph.D. in Technology Management, University of Tehran, Tehran, Iran. Email: m.hajali@ut.ac.ir
2. M.A. in Family Law, Refah University, Tehran, Iran. Email: 0073209481@iau.ir

Article Info

Article Type:
Research Article

Received:
2025/08/31
Received in revised form:
2025/10/27
Accepted:
2025/12/11
Published online:
2026/08/23

Keywords:
Children's Rights, Data Protection, Personal Data Protection Bill, Privacy by Design, Verifiable Parental Consent.

Abstract

1. Introduction: The Data-Driven Risk to Children

The digital environment has fundamentally altered children's lives, exposing them to a new category of risks that have evolved from "content" to "data". Modern threats are no longer just about inappropriate content, but about the pervasive collection of behavioral, location, and interest data by platforms for the purposes of commercial profiling and behavioral manipulation. This data-economy business model creates a foundational conflict between the commercial interests of platforms and the fundamental rights of children. Children are rightly classified as "vulnerable individuals" in data protection law, as noted by the EU's GDPR, because they may be less aware of the risks involved and thus require "special protection".

The central research problem is that Iran's legal system, while generally protective of children, exhibits a "fundamental negligence" in its understanding of these data-driven risks. Existing legislation, such as the "Law on Protection of Children and Adolescents" (1399) and the "Cyberspace Child Protection Document" (1400), is predominantly "content-centric", focusing on filtering and access control. This "protection-oriented" approach is ineffective against the intangible dangers of data processing, such as commercial exploitation, creating a dangerous legislative vacuum. This gap has tangible consequences, including the rise of "modern child abuse" and "Instagram child laborers". Given that 59.1% of Iranian children first use the internet at or before age 10, this legal gap poses a significant threat.

This study asks: What are the pillars, principles, and mechanisms of an effective legal system for protecting children's data in Iran, considering international standards and local requirements? It employs a critical comparative-legal analysis, examining the EU's GDPR and the UK's Age Appropriate Design Code (AADC) to extract core principles (e.g., best interests of the child, privacy by

Article Info

Abstract

design) and practical mechanisms (e.g., verifiable parental consent). These are then evaluated against the capacities and obstacles within Iran's legal system.

2. International Models: Principles and Enforcement

The research analyzes two leading international benchmarks:

2.1. The EU General Data Protection Regulation (GDPR)

The GDPR provides a comprehensive, rights-based approach. Its most critical provision for children is Article 8, which sets the default digital age of consent at 16. For children below this age (which member states can lower to 13), processing is lawful only if consent is "given or authorised by the holder of parental responsibility". Crucially, Article 8(2) mandates that the controller must make "reasonable efforts," using available technology, to verify this parental consent. Furthermore, Article 12 mandates transparency in "clear and plain language" that a child can understand.

2.2. The UK Age Appropriate Design Code (AADC)

The AADC translates the GDPR's principles into actionable standards for services "likely to be accessed by children". It marks a key shift from legal compliance to a design-based paradigm. Its first and most important standard is the "best interests of the child" (from the UNCRC), which must be a "primary consideration" in all data processing, superseding commercial interests. Other key standards include "privacy by default" (highest setting), "data minimisation," and prohibitions on "nudge techniques" that lure children into weakening their privacy settings. This preventive approach shifts the burden of protection from the user to the service provider.

The power of these frameworks is solidified by "effective, proportionate and dissuasive" sanctions. Major fines, such as the €405 million fine against Meta (Instagram) and the €345 million fine against TikTok, demonstrate that non-compliance is a significant business risk. This enforcement contrasts sharply with the "silence and inaction" in Iran, which stems from the lack of a comprehensive law and an independent regulator.

3. Analysis of the Existing Legal Situation in Iran

Iran's legal framework for child protection is an "incomplete puzzle".

3.1. Inadequacy of General Laws and the Civil Code

The "Law on Protection of Children and Adolescents" (1399) focuses on traditional, tangible harms (e.g., sexual abuse, trafficking) and fails to identify data-driven commercial exploitation as a "risk situation" or "ill-treatment". Similarly, the Civil Code's framework, designed for financial matters, is unfit for the digital age. The code's concepts of "Ahliyat" (capacity) and "Hajar" (interdiction) cannot properly govern "digital consent," which is a unique legal act, not a financial transaction. The standard "notice and choice" model is an

Article Info

Abstract

"illusion of consent", especially for children. The article argues that "digital consent" must be legislatively decoupled from the Civil Code's concept of capacity, and a new, independent regime must be established.

3.2. The Personal Data Protection Bill: Gridlock and Flaws

The most critical failure is the "chronic paralysis" in passing the "Personal Data Protection Bill". This legislative gridlock, marked by years of delay, has been complicated by the introduction of a competing "Tarh" in Parliament in Mehr 1403 (October 2024) alongside the government's "Layeheh" (bill). This duality signifies a deep "strategic rift and institutional competition" over digital governance, reflecting an ideological conflict on whether data is an economic resource to be managed or a security threat to be controlled.

Even if passed, the current draft is "fundamentally deficient" regarding children. It lacks any special chapter for children, reducing all protection to a single, inadequate clause: "In case the data subject is interdicted (mahjur), the permission of his legal guardian or custodian is necessary". This approach is flawed:

1. **Conceptual Error:** It wrongly equates data protection with the Civil Code's financial concept of "Mahjuriyat" (interdiction), which is incapable of addressing the psychological and social risks of data processing.
2. **Lack of Specificity:** The clause is silent on *all* essential operational mechanisms: it fails to set a digital age of consent, mandate *verification* of parental consent, limit profiling, or require child-friendly language.

4. A Proposed Strategic Framework for Iran

To address these gaps, the article proposes a framework built on new principles and practical mechanisms.

4.1. Fundamental Principles

1. **The "Best Interests of the Child" as the Governing Rule:** This principle, from the UNCRC which Iran ratified, must be the primary interpretive rule, dictating that children's welfare outweighs commercial interests in any conflict.
2. **"Privacy by Design and by Default":** These principles must become explicit legal obligations, embedding protection into services from the start and setting the highest privacy settings automatically.
3. **"Data Minimisation":** Data collection must be limited to what is "absolutely necessary" for the specific service element the child is actively using.

4.2. Key Executive Mechanisms

1. **A Digital Age of Consent:** The article proposes setting the "digital age of consent" at **13 full solar (Shamsi) years**. For children under 13, processing would require **"verifiable parental consent"**.

Article Info

Abstract

"Reasonable efforts" to verify this could include methods like signed forms, bank transactions, or national ID systems.

2. **Mandatory Child-Focused DPIA:** A Data Protection Impact Assessment (DPIA) must be legally required for any service "likely to be accessed by children" that poses a "high risk". This DPIA must specifically assess adherence to the child's best interests, risks from profiling and "nudge techniques," and potential for harm.

3. **Age-Appropriate Transparency and Data Rights:** The law must mandate plain language (per GDPR Art. 12) and explicitly grant rights of access, rectification, and erasure (the "right to be forgotten").

4.3. Legislative and Institutional Roadmap

The article argues that the most effective legislative path is enacting a "Special Law for the Protection of Children's Data". This allows for technical precision and clarity.

However, this law requires an expert "Personal Data Protection Organization" to enforce it. The article critically notes that the independent EU-model DPA faces structural hurdles in Iran. A deeper problem is the "institutional conflict of interest": the state is the *largest collector* of citizen data. Placing the regulator within the government creates an "alliance of the regulator and the regulated", where the state's interest as a data processor conflicts with its duty as a regulator.

Given that the EU model is likely unworkable, the article suggests exploring more politically feasible alternative models, such as a supervisory body **within the Judiciary** (to ensure independence from the Executive) or a **Multi-stakeholder Commission**. A three-tiered enforcement system (civil, administrative, and criminal) is also proposed.

5. Conclusion

This research demonstrates that Iran's legal system is trapped in an outdated, "content-centric" paradigm and faces a "structural gap" in transitioning to a "data-centric" model. The key finding is that international models have shifted the *burden of responsibility* from the user to the service provider, based on principles of "best interests of the child" and "privacy by design".

The article concludes that filling this gap requires a **"Special Law for the Protection of Children's Data"**. This law must include:

1) A **digital age of consent set at 13**, with "verifiable parental consent" for those younger;

2) Legal enforcement of **"privacy by design" and "by default"**;

3) A **ban on profiling children** for marketing and strict "data minimisation"; and

4) A requirement for **age-appropriate, transparent language**.

Acknowledging the institutional challenges, a realistic regulatory

Article Info	Abstract
	model must be developed. Adopting this data-centric approach is a "strategic investment". It not only protects children from commercial exploitation but also provides the legal certainty needed for responsible innovation, preventing the long-term "isolation" of Iran's digital economy.
How To Cite	Hajali, Mohammad; Hoseinpour, Zahra (2026). Protecting Children's Personal Data in Iran: An Analysis of Legislative Gaps and a Strategic Roadmap with Comparative View on EU and UK Regulations. *Comparative Law Review*, 17 (1), 51-74. DOI: https://doi.com/10.22059/jcl.2025.400961.634798
DOI	10.22059/jcl.2025.400961.634798
Publisher	