University of Tehran Press

Comparative Law Review

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

Online ISSN: 2423-3404

Volume: 17, **Issue:** 1
Spring & Summer
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

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

The rapid expansion of digital technologies has exposed children to unprecedented data-driven risks. The particular vulnerability of this age group to the collection, processing, and commercial exploitation of personal data amplifies the need for specialized protective frameworks. Despite legislative efforts, Iran's legal system primarily focuses on protecting children from harmful content and suffers from the absence of a cohesive, data-centric regime. Using a comparative-legal analysis, this research examines leading international models, particularly the European Union's General Data Protection Regulation (GDPR) and the UK's Age Appropriate Design Code. The findings indicate that these models have adopted a preventive, design-based approach by introducing fundamental principles such as the "best interests of the child", "privacy by design", and practical mechanisms like "verifiable parental consent" and "Data Protection Impact Assessments". In contrast, an analysis of Iran's draft "Personal Data Protection Bill" reveals deep structural weaknesses and an insufficient approach to children's rights, notably by reducing protection to the traditional concept of "legal incapacity". Ultimately, by identifying existing gaps, this article presents a strategic legislative and executive roadmap. This roadmap is founded on the necessity of enacting a "Special Law for the Protection of Children's Data", which would recognize the "best interests of the child" as the governing principle and mandate operational mechanisms such as "verifiable parental consent" and the requirement for a "child-focused Data Protection Impact Assessment". Furthermore, while analyzing institutional challenges, the article proposes a model for establishing a specialized supervisory authority tailored to Iran's legal structure.

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

شاپا الکترونیکی: ۳۴۰۴-۲۴۲۳

دوره: ۱۷، شماره: ۱
بهار و تابستان ۱۴۰۵

مطالعات حقوق تطبیقی

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

University of Tehran Press

حفاظت از داده‌های شخصی کودکان در ایران: تحلیلی بر خلأهای تقنینی و ارائهٔ نقشهٔ راه استراتژیک با نگاهی به مقررات اتحادیهٔ اروپا و بریتانیا

محمد حاجعلی[۱]✉ | زهرا حسین‌پور[۲]

۱. نویسندهٔ مسئول؛ دانش‌آموختهٔ دکتری تخصصی مدیریت تکنولوژی، دانشگاه تهران، تهران، ایران. رایانامه: m.hajali@ut.ac.ir
۲. دانش‌آموخته کارشناسی ارشد حقوق خانواده، دانشکدهٔ رفاه، تهران، ایران. رایانامه: 0073209481@iau.ir

اطلاعات مقاله

نوع مقاله: پژوهشی

تاریخ دریافت:
۱۴۰۴/۰۶/۰۹

تاریخ بازنگری:
۱۴۰۴/۰۸/۰۵

تاریخ پذیرش:
۱۴۰۴/۰۹/۲۰

تاریخ انتشار برخط:
۱۴۰۵/۰۶/۰۱

کلیدواژه‌ها:
حریم خصوصی در طراحی، حفاظت از داده، حقوق کودک، رضایت قابل تأیید والدین، لایحهٔ حفاظت از داده‌های شخصی.

چکیده

گسترش روزافزون فناوری‌های دیجیتال، کودکان را در معرض مخاطرات داده‌محور بی‌سابقه‌ای قرار داده است. آسیب‌پذیری ویژهٔ این گروه سنی در برابر جمع‌آوری، پردازش و بهره‌برداری تجاری از داده‌های شخصی، ضرورت ایجاد چارچوب‌های حمایتی ویژه را دوچندان می‌کند. با وجود تلاش‌های تقنینی، نظام حقوقی ایران عمدتاً بر حفاظت از کودکان در برابر محتوای زیان‌بار متمرکز بوده، ولی دچار خلأ یک نظام منسجم و داده‌محور است. این پژوهش با روش تحلیل حقوقی- تطبیقی، به واکاوی الگوهای پیشرو بین‌المللی، به‌ویژه «مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا» و «آیین‌نامهٔ طراحی مناسب سن» بریتانیا می‌پردازد. یافته‌ها نشان می‌دهد این الگوها با معرفی اصولی بنیادین همچون «منافع عالیهٔ کودک»، «حریم خصوصی در طراحی» و سازوکارهای عملی مانند «رضایت قابل تأیید والدین» و «ارزیابی تأثیر حفاظت از داده»، رویکردی پیشگیرانه و طراحی‌محور اتخاذ کرده‌اند. در مقابل، تحلیل پیش‌نویس «لایحهٔ حفاظت از داده‌های شخصی» ایران، با تقلیل حمایت به مفهوم سنتی «محجوریت»، ضعف‌های ساختاری عمیق و رویکردی ناکافی به حقوق کودک را آشکار می‌سازد. در نهایت، در این مقاله با شناسایی خلأهای موجود، یک نقشهٔ راه استراتژیک تقنینی و اجرایی ارائه می‌شود. این نقشهٔ راه بر ضرورت تدوین «قانون اختصاصی حمایت از داده‌های کودکان» استوار است که اصل «منافع عالیهٔ کودک» را به‌عنوان قاعدهٔ حاکم به‌رسمیت شناخته و سازوکارهای عملیاتی مانند «رضایت قابل تأیید والدین» و «الزام به ارزیابی تأثیر حفاظت از دادهٔ متمرکز بر کودک» را پیش‌بینی می‌کند. همچنین، نگارندگان این مقاله ضمن تحلیل چالش‌های نهادی، الگویی متناسب با ساختار حقوقی ایران برای تأسیس یک نهاد ناظر تخصصی پیشنهاد می‌نماید.

استناد

حاجعلی، محمد؛ حسین‌پور، زهرا (۱۴۰۵). حفاظت از داده‌های شخصی کودکان در ایران: تحلیلی بر خلأهای تقنینی و ارائهٔ نقشهٔ راه استراتژیک با نگاهی به مقررات اتحادیهٔ اروپا و بریتانیا. *مطالعات حقوق تطبیقی*، ۱۷ (۱)، ۵۱- ۷۴.
DOI: https://doi.com/10.22059/jcl.2025.400961.634798

DOI 10.22059/jcl.2025.400961.634798

ناشر مؤسسه انتشارات دانشگاه تهران.

۱. مقدمه

عصر دیجیتال، زیست‌بوم کودکان را به‌طور بنیادین دگرگون کرده و آنان را در معرض مجموعه‌ای پیچیده از ریسک‌ها قرار داده است که ماهیت آنها از «محتوا» به «داده» تغییر یافته است (Hoseini & Hoseinpour, 1401: 96). تهدیدات مدرن لزوماً از جنس مواجهه با محتوای نامناسب نیستند، بلکه در قالب جمع‌آوری بی‌رویهٔ داده‌های رفتاری، مکانی و علایق کودک از طریق یک اپلیکیشن بازی و استفاده از آن برای پروفایل‌سازی تبلیغاتی و دست‌کاری رفتار او تجلی می‌یابند. این مدل کسب‌وکار که بر پایهٔ اقتصاد داده استوار است، یک تعارض ذاتی میان منافع تجاری پلتفرم‌ها و حقوق بنیادین کودکان ایجاد می‌کند. کودکان به دلیل آسیب‌پذیری‌های شناختی و رشدی، گروهی ویژه در مباحث حفاظت از داده محسوب می‌شوند؛ به همین دلیل مقررات عمومی حفاظت از دادهٔ اتحادیه اروپا[1] به‌صراحت آنان را «افراد آسیب‌پذیر»[2] تلقی کرده، بر لزوم «حمایت ویژه» از داده‌های شخصی آنان تأکید می‌نماید (European Union, 2016b: Recital 38).

با وجود این، مسئلهٔ اصلی این پژوهش آن است که نظام حقوقی ایران، علی‌رغم رویکرد حمایتی کلی نسبت به کودکان، در مواجهه با این مخاطرات نوظهور دچار یک غفلت بنیادین در بینش نسبت به موضوع است. قوانین و اسناد موجود، همچون «قانون حمایت از اطفال و نوجوانان» (Islamic Parliament of Iran, 1399:Art.10-19) و «سند صیانت از کودکان و نوجوانان در فضای مجازی» (Supreme Council of Cyberspace, 1400) عمدتاً رویکردی محتوامحور دارند و بر فیلترینگ و کنترل دسترسی متمرکز شده‌اند (Panahi, 2018: 16). این رویکرد «صیانت‌محور»، در برابر خطرهای ناملموس و ساختاری ناشی از پردازش داده‌ها، مانند بهره‌کشی تجاری از طریق پروفایل‌سازی، ناکارآمد است و یک خلأ تقنینی خطرناک ایجاد کرده است.

اهمیت و ضرورت این تحقیق از آنجا ناشی می‌شود که این خلأ قانونی صرفاً یک بحث نظری نیست، بلکه پیامدهای ملموسی در جامعهٔ ایران به‌دنبال داشته است. گزارش‌ها و پرونده‌های قضایی، ازجمله دستگیری پدری که فرزند شش‌سالهٔ خود را برای جذب دنبال‌کننده در اینستاگرام و کسب درآمد تبلیغاتی وادار به استفاده از الفاظ رکیک و تظاهر به شرب خمر می‌کرد، نشان‌دهندهٔ شکل‌گیری نوعی «کودک‌آزاری مدرن» و بهره‌کشی اقتصادی از کودکان در بستر دیجیتال است (Etemad, 1402). این پدیده که از آن با عنوان «کودکان کار اینستاگرامی» نیز یاد می‌شود، کودکان را به ابزاری برای تبلیغات و مدلینگ تبدیل کرده، حقوق بنیادین آنان، ازجمله حق بر حریم خصوصی و رشد سالم را نقض می‌کند. با

1. General Data Protection Regulation (GDPR)
2. vulnerable individuals

توجه به پیمایش ملی که نشان می‌دهد بیش از نیمی از کودکان ایرانی (۵۹.۱ درصد) اولین تجربهٔ استفاده از اینترنت را در سن ۱۰ سالگی یا کمتر داشته‌اند (Solgi, 1400)، با توجه به آمار بالای استفادهٔ کودکان ایرانی از اینترنت (OECD, 2025:14; UNICEF, 2017: 7)، این غفلت قانونی می‌تواند به آسیب‌های گستردهٔ رشدی، روانی و اجتماعی برای نسل آینده منجر شود. این پژوهش در پی پاسخ به این پرسش اصلی است: ارکان، اصول و سازوکارهای یک نظام حقوقی مؤثر برای حفاظت از داده‌های کودکان در ایران با توجه به استانداردهای بین‌المللی و الزامات بومی کدام‌اند؟

برای دستیابی به این هدف، پژوهش حاضر از روش تحلیل حقوقی- تطبیقی با رویکردی انتقادی بهره می‌گیرد. در این چارچوب، مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا (GDPR) و آیین‌نامهٔ طراحی مناسب سن بریتانیا (AADC)، نه به‌عنوان الگوهایی برای تقلید صرف، بلکه به‌مثابه مدل‌هایی مفهومی برای استخراج اصول بنیادین (مانند منافع عالیهٔ کودک و حریم خصوصی در طراحی) و سازوکارهای عملی (مانند رضایت قابل تأیید والدین) تحلیل می‌شوند. سپس، این اصول و سازوکارها با توجه به ظرفیت‌ها و موانع موجود در نظام حقوقی ایران، ازجمله مبانی قانون مدنی و چالش‌های نهادی، مورد ارزیابی قرار می‌گیرند. ساختار مقاله به این ترتیب سامان یافته است: در بخش دوم، مبانی نظری و الگوهای بین‌المللی پیشرو تشریح و تحلیل می‌شوند. بخش سوم به تحلیل وضعیت موجود در نظام حقوقی ایران اختصاص دارد؛ از قوانین عام حمایتی گرفته تا کالبدشکافی پیش‌نویس لایحهٔ حفاظت از داده‌های شخصی. در بخش چهارم، یک چارچوب پیشنهادی جامع برای ایران، شامل اصول بنیادین، سازوکارهای اجرایی و نقشهٔ راه تقنینی و نهادی ارائه می‌گردد و در نهایت، بخش پنجم به بحث و نتیجه‌گیری اختصاص یافته است.

۲. مبانی نظری و الگوهای بین‌المللی پیشرو

تحولات حقوقی در حوزهٔ حفاظت از داده، به‌ویژه در اتحادیهٔ اروپا، یک نقطهٔ عطف جهانی در این زمینه محسوب می‌شود. بررسی دو نمونهٔ برجسته، یعنی مقررات عمومی حفاظت از داده (GDPR) (European Union, 2016b) و آیین‌نامهٔ طراحی مناسب سن بریتانیا (AADC)، (European Commission, 2022) می‌تواند نقشهٔ راه ارزشمندی برای نظام‌های حقوقی در حال توسعه فراهم آورد.

۲. ۱. مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا: چارچوبی حق‌محور

GDPR که در سال ۲۰۱۸ لازم‌الاجرا شد، رویکردی جامع و حق‌محور به حریم خصوصی دارد و حمایت از داده‌های شخصی را به‌عنوان یک حق بنیادین به‌رسمیت می‌شناسد. این مقررات صرفاً مجموعه‌ای از قواعد فنی نیست، بلکه بر پایهٔ اصولی استوار است که حمایت ویژه‌ای را برای کودکان درنظر می‌گیرد.

(Data Protection Commission, 2021: 68). مبنای رویکرد GDPR به کودکان، شناسایی آنان به عنوان «افراد آسیب‌پذیر» است. مقدمهٔ ۳۸ این مقررات به‌صراحت بیان می‌کند که «کودکان، شایستهٔ حمایت ویژه‌ای در خصوص داده‌های شخصی خود هستند، زیرا ممکن است از خطرها، پیامدها و تضمین‌های مربوطه و حقوق خود در خصوص پردازش داده‌های شخصی آگاهی کمتری داشته باشند». این اصل، سنگ بنای فلسفی تمام الزامات خاصی است که GDPR برای پردازش داده‌های کودکان وضع کرده است (European Union, 2016c: Recital 38)

مهم‌ترین و صریح‌ترین مادهٔ GDPR در خصوص کودکان، مادهٔ ۸ است که شرایط رضایت کودک از «خدمات جامعهٔ اطلاعاتی»[1] را مشخص می‌کند (European Union, 2016a: Art.8). بر اساس بند ۱ این ماده، پردازش داده‌های شخصی کودکی که حداقل ۱۶ سال سن دارد، بر مبنای رضایت وی قانونی است. اما در صورتی که کودک زیر ۱۶ سال باشد، این پردازش تنها در صورتی قانونی خواهد بود که رضایت از سوی «دارندهٔ مسئولیت والدینی طفل»[2] داده یا تأیید شده باشد. این ماده به کشورهای عضو اجازه می‌دهد که سن رضایت را تا ۱۳ سال کاهش دهند. نکتهٔ حائز اهمیت در بند ۲ مادهٔ ۸، تکلیف کنترل‌کنندهٔ داده است که باید با درنظر گرفتن فناوری موجود، «تلاش‌های معقولی»[3] برای تأیید اینکه رضایت از سوی دارندهٔ مسئولیت والدینی داده شده، به‌عمل آورد. این الزام، کنترل‌کنندگان را از اکتفا به یک تیک ساده در وب‌سایت بازمی‌دارد و آن‌ها را به سمت استفاده از سازوکارهای تأیید سن و رضایت سوق می‌دهد و بار مسئولیت حفاظت را از کاربر به شرکت منتقل می‌کند. علاوه بر این، مادهٔ ۱۲ GDPR بر لزوم شفافیت تأکید دارد و کنترل‌کنندگان را موظف می‌کند اطلاعات مربوط به پردازش داده‌ها را به شکلی «مختصر، شفاف، قابل فهم و در دسترس» و «با استفاده از زبانی واضح و ساده» که برای کودک قابل درک باشد، ارائه دهند.

۲. ۲. آیین‌نامه طراحی مناسب سن بریتانیا: تحول بنیادین به الگوی طراحی‌محور

آیین‌نامهٔ طراحی مناسب سن[4] که به «کد کودکان»[5] نیز شهرت دارد، نمونه‌ای برجسته از تبدیل اصول کلی GDPR به استانداردهای عملی و قابل اجراست. این آیین‌نامه که در دفتر کمیسر اطلاعات[6] بریتانیا تدوین شده و از سپتامبر ۲۰۲۱ به‌طور کامل لازم‌الاجرا است، شامل ۱۵ استاندارد مشخص برای خدمات آنلاینی است که «احتمالاً از سوی کودکان (افراد زیر ۱۸ سال) مورد دسترسی قرار می‌گیرند». (ICO,

1. Information Society Services
2. holder of parental responsibility
3. reasonable efforts
4. Age Appropriate Design Code (AADC)
5. Children's Code
6. Information Commissioner's Office)ICO(

17 :2021) این حرکت از یک الگوی انطباق حقوقی صرف به یک الگوی مبتنی بر طراحی و اخلاق، تحولی کلیدی است. GDPR مشخص می‌کند که «چه» کاری باید انجام شود (مثلاً کسب رضایت والدین)، اما AADC توضیح می‌دهد که «چگونه» باید این کار در بطن طراحی یک محصول یا سرویس انجام شود. (Elvy, 2024: 958)

اولین و مهم‌ترین استاندارد AADC، اصل «منافع عالیهٔ کودک»[1] است. این اصل که مستقیماً از کنوانسیون حقوق کودک سازمان ملل اقتباس شده (United Nations, 1989: Art.3)، مقرر می‌دارد که منافع عالیهٔ کودک باید یک «ملاحظهٔ اولیه»[2] در تمام اقدامات مربوط به پردازش داده‌های کودکان باشد. این اصل، توازن قدرت را به نفع کودک تغییر می‌دهد و ایجاب می‌کند که منافع تجاری یک شرکت، همواره در اولویت دوم پس از حقوق و سلامت کودک قرار گیرد.

استانداردهای کلیدی دیگر این آیین‌نامه عبارت‌اند از:

حریم خصوصی به‌مثابه پیش‌فرض[3]: تنظیمات حریم خصوصی برای حساب‌های کاربری کودکان باید به‌طور پیش‌فرض روی بالاترین سطح حفاظت تنظیم شود.

به حداقل‌رسانی داده‌ها[4]: شرکت‌ها باید تنها حداقل داده‌های شخصی لازم برای ارائهٔ یک عنصر خاص از سرویس را که کودک به‌طور فعال در آن مشارکت دارد، جمع‌آوری و نگهداری کنند.

ممنوعیت استفادهٔ زیان‌بار از داده‌ها[5]: استفاده از داده‌های کودک به شیوه‌ای که ثابت شده برای سلامت جسمی یا روانی او «زیان‌آور» است، ممنوع می‌باشد.

ممنوعیت «تکنیک‌های اغواگر»[6]: استفاده از عناصر طراحی که کودکان را تشویق یا اغوا می‌کند تا تنظیمات حفاظتی خود را تضعیف کرده یا داده‌های شخصی غیرضروری را به اشتراک بگذارند، مجاز نیست.

این رویکرد پیشگیرانه، مسئولیت اصلی حفاظت را از دوش کاربران (والدین و کودکان) برداشته و برعهدهٔ طراحان و ارائه‌دهندگان خدمات قرار می‌دهد و نقطهٔ کانونی گذار از مقررات واکنشی به مقررات پیشگیرانه است.

قدرت و تأثیر این چارچوب‌های قانونی صرفاً در اصول نظری آنها خلاصه نمی‌شود، بلکه در ضمانت‌های اجرای سنگین و بازدارندهٔ آنها تجلی می‌یابد. مبنای حقوقی این جریمه‌ها در مادهٔ ۸۳ GDPR تبیین شده که مقرر می‌دارد ضمانت‌های اجرا باید «مؤثر، متناسب و بازدارنده» باشد. این سه

1. The best interests of the child
2. a primary consideration
3. Privacy by Default
4. Data Minimisation
5. Detrimental use of data
6. Nudge Techniques

اصل، به نهادهای ناظر اجازه می‌دهد تا در تعیین میزان جریمه، عواملی چون ماهیت و شدت تخلف، عمدی یا سهوی بودن آن، تعداد افراد متأثر و اقدامات شرکت برای کاهش خسارت را درنظر بگیرند. هدف از این رویکرد، نه صرفاً تنبیه، بلکه تغییر رفتار بازار و تبدیل حفاظت از داده به یک اولویت راهبردی برای کسب‌وکارها است. نهادهای ناظر اروپایی با استفاده از این اختیارات، جریمه‌های هنگفتی را علیه بزرگ‌ترین شرکت‌های فناوری جهان به دلیل نقض حقوق داده‌ای کودکان اعمال کرده‌اند.

این اقدامات نشان می‌دهد که حفاظت از داده‌های کودکان یک اولویت اجرایی است، نه یک توصیهٔ اخلاقی. برای مثال، در سپتامبر ۲۰۲۳، کمیسیون حفاظت از دادهٔ ایرلند، پلتفرم تیک‌تاک را به دلیل نقض‌های متعدد در پردازش داده‌های کودکان، ازجمله عمومی بودن پیش‌فرض حساب‌های کاربری نوجوانان، به پرداخت جریمهٔ ۳۴۵ میلیون یورویی محکوم کرد (The Guardian, 2023). پیش از آن نیز در سپتامبر ۲۰۲۲، همین نهاد شرکت متا (اینستاگرام) را به دلیل افشای اطلاعات تماس کودکان که از حساب‌های تجاری استفاده می‌کردند، با جریمه‌ای بالغ بر ۴۰۵ میلیون یورو مواجه ساخت (The Guardian, 2022). این جریمه‌ها که می‌تواند تا ۴ درصد از گردش مالی سالانهٔ جهانی شرکت‌ها را شامل شود، این پیام روشن را به بازار ارسال می‌کند که نادیده گرفتن منافع عالیهٔ کودک در طراحی خدمات دیجیتال، یک ریسک تجاری غیرقابل قبول است.

این رویکرد اجرایی، با وضعیت «سکوت و بی‌عملی» در نظام حقوقی ایران دارای تضاد کامل است که ریشه در سه عامل اصلی دارد: نخست، فقدان یک قانون جامع حفاظت از داده که مبنای حقوقی برای اعمال مجازات باشد؛ دوم، نبود یک نهاد ناظر مستقل و متخصص با اختیارات اجرایی؛ و سوم، سطح پایین آگاهی عمومی و قضایی نسبت به ماهیت آسیب‌های داده‌محور.

جدول ۱. نمونه‌ای از جریمه‌های برجستهٔ GDPR در حوزهٔ حفاظت از داده‌های کودکان (۲۰۲۲–۲۰۲۴)

شرکت متخلف	نهاد ناظر	مبلغ جریمه	ماهیت تخلف
متا پلتفرم (اینستاگرام)	کمیسیون حفاظت از دادهٔ ایرلند (DPC)	۴۰۵ میلیون یورو	افشای عمومی آدرس ایمیل و شمارهٔ تلفن کودکان از طریق حساب‌های کاربری تجاری.
تیک‌تاک	کمیسیون حفاظت از دادهٔ ایرلند (DPC)	۳۴۵ میلیون یورو	عمومی بودن پیش‌فرض حساب‌های کاربری کودکان و عدم شفافیت در پردازش داده‌ها.
تیک‌تاک	دفتر کمیسر اطلاعات بریتانیا(ICO)	۱۲.۷ میلیون پوند	پردازش داده‌های کودکان زیر ۱۳ سال بدون رضایت معتبر والدین (The Guardian, 2023a)

۲. ۳. چالش‌های بومی‌سازی و ارزیابی تطبیقی

با وجود پیشرو بودن الگوهای اروپایی، پیاده‌سازی مستقیم آنها در نظام حقوقی ایران با چالش‌های جدی مفهومی، فنی و نهادی روبه‌رو است. نخست، اصل «رضایت کودک» در GDPR بر مبنای مفهوم «ظرفیتِ درحال تحول کودک» و استقلال فردی او استوار است، درحالی که در حقوق ایران، مفهوم «ولایت» و «اهلیت» در قانون مدنی، چارچوب متفاوتی را ترسیم می‌کند که تمرکز آن بیشتر بر ادارهٔ امور مالی است تا تصمیم‌گیری در مورد حقوق بنیادین. این تفاوت مبنایی، بومی‌سازی مفهوم «سن رضایت دیجیتال» را پیچیده می‌سازد. دوم، الزامات فنی مانند «رضایت قابل تأیید والدین» نیازمند زیرساخت‌های فناورانه و پایگاه‌های دادهٔ ملی یکپارچه برای احراز هویت است که پیاده‌سازی آن در ایران مستلزم سرمایه‌گذاری و هماهنگیِ بین‌نهادی گسترده است. سوم، اثربخشی این مقررات در اروپا به‌شدت به وجود نهادهای ناظر مستقل و قدرتمند (DPA) وابسته است. همان‌طور که در ادامه بحث خواهد شد، ایجاد چنین نهادی در ساختار حکمرانی ایران با موانع سیاسی و حقوقی قابل‌توجهی مواجه است. بنابراین، تحلیل تطبیقی نباید به معنای تقلید صرف باشد، بلکه باید به‌مثابه یک فرایند «ترجمهٔ حقوقی» درنظر گرفته شود که در آن اصول جهان‌شمول با در مدنظر قرار دادن واقعیت‌های بومی، بازتفسیر و بازطراحی می‌شوند.

۳. تحلیل وضعیت موجود در نظام حقوقی ایران

نظام حقوقی ایران با وجود برخورداری از مبانی حمایتی قوی در قبال اطفال و نوجوانان، در حوزهٔ تخصصی حفاظت از داده‌های شخصی آنان با یک «پازل ناقص» روبه‌رو است (Khani Razgi et al., 1403: 29). قوانین موجود یا عام هستند و برای چالش‌های خاص این حوزه طراحی نشده‌اند، یا در صورت وجود، رویکردی محتوامحور دارند و از پرداختن به ابعاد داده‌محور غفلت کرده‌اند (Pourmasjedian & Ebrahimi, 1399: 84; Nikbeen & Raoofi, 1404: 715).

۳. ۱. قوانین حمایتی عام و خاص: ظرفیت‌ها و محدودیت‌ها

«قانون حمایت از اطفال و نوجوانان» مصوب ۱۳۹۹ (Islamic Parliament of Iran, 1399)، جامع‌ترین سند تقنینی ایران در حمایت از کودکان محسوب می‌شود. مادهٔ ۱ این قانون، تعاریف مهمی از «سوء رفتار» و «بهره‌کشی» ارائه می‌دهد و مادهٔ ۳، فهرستی از «وضعیت‌های مخاطره‌آمیز» را برمی‌شمارد. با این حال، تحلیل دقیق این قانون نشان می‌دهد که تمرکز اصلی آن بر آسیب‌های سنتی و ملموس است. جرائم پیش‌بینی‌شده در مواد ۱۰ تا ۱۹ عمدتاً ناظر بر تولید و انتشار محتوای مستهجن، آزار جنسی، معامله و قاچاق کودکان است. هیچ ماده‌ای به‌صراحت، جمع‌آوری بی‌رویهٔ داده‌های رفتاری یک کودک از سوی یک پلتفرم دیجیتال برای مقاصد تجاری (مانند پروفایل‌سازی و تبلیغات هدفمند) را به

عنوان «سوء رفتار» یا «وضعیت مخاطره‌آمیز» شناسایی نمی‌کند، در حالی کـه چنـین اقـداماتی می‌توانـد تأثیرات عمیق و مخربی بر رشد، استقلال و سلامت روانی کودک داشته باشد. با ایـن حـال، بایـد توجـه داشت که انتشار تصاویر کودکان در فضای مجازی، به دلیل ماندگاری و قابلیت انتشار گسترده، می‌توانـد مصادیق دیگری از نقض حقوق را نیز دربر گیرد. تعرض به حریم خصوصی، تحت تـأثیر قـرار دادن حـق تعیین سرنوشت، سوءاستفاده جنسی از تصاویر و آسیب‌های روحی و روانـی، همگـی ازجملـه آثـار سـوئی هسـتند کـه می‌تواننـد بـرخلاف مصـلحت کـودک باشـند و نیازمنـد توجـه ویـژۀ قانون‌گـذار هسـتند (Ghanizadeh Bafghi & Chaji, 1402: 267).

به همین ترتیب، «قانون تجـارت الکترونیکـی» مصـوب ۱۳۸۲، (Islamic Parliament of Iran, 1382) در مواد ۳۳ و ۳۴، تأمین‌کنندگان را به ارائۀ اطلاعات شفاف به مصرف‌کنندگان ملزم می‌کند، امـا این الزامات عمومی بوده، هیچ حمایت ویژه‌ای برای مصرف‌کنندگان کودک در نظر نگرفته است. «قانون جرائم رایانه‌ای» مصوب ۱۳۸۸ (Islamic Parliament of Iran, 1388) نیز بر جرائم کلاسیک در بستر سایبری مانند دسترسی غیرمجاز و کلاهبرداری متمرکز است و فاقـد نگـاه پیشـگیرانه و سـاختاری لازم برای حفاظت از داده‌های کودکان است. این درحالی است که برخی پژوهشگران بر این باورند کـه بـرای حمایت مؤثر از کودکان در فضای مجازی، باید راهکارهای اجتمـاعی، فرهنگـی، حقـوقی و آموزشـی بـه صورت یکپارچه درنظر گرفته شوند. این راهکارها شامل فرهنگ‌سازی، قانون‌گذاری دقیق، آموزش سـواد رسانه‌ای و تقویت تفکر انتقادی در کودکان و والدین است که فقدان چنین نگاه جامعی در قـوانین فعلـی ایران مشهود است (Faramarziani et al., 1401: 151).

۳. ۲. پیوند با قانون مدنی: تحلیل مفاهیم اهلیت، حجر و ولایت در بستر دیجیتال

قانون مدنی ایران به‌عنوان قانون مادر در حوزۀ روابط خصوصی، مبانی مهمی را در باب وضـعیت حقـوقی اطفال و نوجوانان پایه‌ریزی کرده است که تحلیل آن‌ها برای درک خلأهای موجـود در فضـای دیجیتـال ضروری است. مادۀ ۱۲۰۷ این قانون، اشخاص را از حیث توانایی برای اجرای حقـوق خـود بـه دو دسـتۀ دارای اهلیت و محجور تقسیم می‌کند. محجورین شامل صغار، اشخاص غیررشید و مجانین هستند.

صغیر به دو دستۀ ممیز و غیر ممیز تقسیم می‌شود. مادۀ ۱۲۱۲ قـانون مـدنی چنـین بیـان می‌کنـد کـه اعمال و اقوال صغیر تا حدی که مربوط به اموال و حقوق مالی او باشد باطل و بلااثر است، مگر در خصوص تملک بلاعوض از سوی صغیر ممیز (مانند قبول هبه) که صحیح تلقی می‌شود. سایر معاملات صغیر ممیـز، غیرنافذ بوده، صحت آن منوط به اجازۀ ولی یا قیم است. همچنین بر اساس مادۀ ۱۱۸۰ قـانون مـدنی، ادارۀ امور محجورین برعهدۀ ولی قهری (پدر و جد پدری) یا قیم منصوب از سوی دادگاه است.

این چارچوب سنتی که برای ادارهٔ اموال و امور مالی طراحی شده، برای پاسخگویی به چالش‌های عصر دیجیتال ناکارآمد است. «رضایت» به پردازش داده‌های شخصی، یک عمل حقوقی است که ماهیتی متفاوت با یک معاملهٔ مالی دارد (Takhshid, 2022: 1417). تحلیل این ناکارآمدی نیازمند فراتر رفتن از مفاهیم سنتی و بهره‌گیری از نظریه‌های حقوقی نوین است. بسیاری از حقوقدانان معتقدند که الگوی غالب «اطلاع و انتخاب»[1] که زیربنای رضایت در فضای آنلاین است، به‌ویژه برای کاربران آسیب‌پذیر، نوعی «توهم رضایت» ایجاد می‌کند. کاربران، به‌خصوص کودکان، در عمل با متون طولانی و پیچیدهٔ حقوقی مواجه می‌شوند که آن‌ها را بدون مطالعه می‌پذیرند. این پدیده که از آن با عنوان «آسیب‌شناسی رضایت دیجیتال» یاد می‌شود، نشان می‌دهد که مشکل صرفاً «حجر» یا عدم اهلیت کودک نیست، بلکه خودِ سازوکار أخذ رضایت، ماهیتی اجبارآمیز و غیرآگاهانه دارد.

این ابهام یک خلأ تفسیری جدی ایجاد می‌کند که برای رفع آن می‌توان دو راهکار ارائه داد: نخست، یک راهکار تفسیری؛ قضات می‌توانند با استفاده از اصول کلی حقوقی مانند قاعدهٔ «لاضرر» و اصل «منافع عالیهٔ کودک»، رضایت کودک به پردازش داده را نه یک عمل حقوقی مالی غیرنافذ، بلکه یک «إذن قابل رجوع» تفسیر کنند که هر زمان با مصلحت کودک در تعارض قرار گیرد، از سوی ولی یا دادگاه قابل فسخ است. دوم، یک راهکار تقنینی؛ قانون‌گذار باید در قانون آتی حفاظت از داده، به‌صراحت «رضایت دیجیتال» را از مفهوم «اهلیت» در قانون مدنی منفک کرده، برای آن یک نظام سنی و شرایط اعتبارسنجی مستقل (مانند آنچه در مادهٔ ۸ GDPR آمده) تعریف نماید. این ناتوانی در انطباق مفاهیم حقوق مدنی با واقعیت‌های دیجیتال، ضرورت قانون‌گذاری خاص و هدفمند را آشکار می‌سازد (Shudra, 2023: 1).

۳. ۳. اسناد سیاستی و رویهٔ قضایی: شکاف میان سیاست و اجرا

مهم‌ترین سند سیاستی در این حوزه، «سند صیانت از کودکان و نوجوانان در فضای مجازی» مصوب ۱۴۰۰ (Supreme Council of Cyberspace, 1400) است. این سند با تأکید بر «ایجاد محیط صیانت‌شده» و «کنترل دسترسی» (Shahsavari, 1402: 110)، تجسم عینی «نگرش کنترل‌محور» است. این رویکرد با اولویت دادن به فیلترینگ فنی، کودک را یک دریافت‌کنندهٔ منفعل فرض کرده، فرصت یادگیری مهارت‌های تاب‌آوری دیجیتال را از او سلب می‌کند (Taghizadegan, 1402: 14). مهم‌تر آنکه، این سند فاقد قدرت الزام‌آور مستقیم و ضمانت اجراهای حقوقی است.

در حوزهٔ رویهٔ قضایی نیز بررسی آرای موجود سکوتی معنادار را در خصوص نقض حریم خصوصی داده‌محور کودکان نشان می‌دهد. فقدان رویهٔ قضایی مشخص، معلول دو عامل اصلی است: اول، نبود

1. Notice and Choice

قوانین صریح که بتواند مبنای طرح دعوا قرار گیرد؛ و دوم، سطح پایین آگاهی عمومی و تخصصی نسبت به این نوع جدید از آسیب.

۳. ۴. کالبدشکافی لایحهٔ حفاظت از داده‌های شخصی: پاشنهٔ آشیل نظام حمایتی

ویرانگرترین خلأ نظام حقوقی ایران در این حوزه، در فلج مزمن فرایند قانون‌گذاری برای تصویب «لایحهٔ حفاظت از داده‌های شخصی» نمایان می‌شود. تحلیل این شکست، صرفاً بررسی یک خلأ قانونی نیست، بلکه کالبدشکافی یک ناتوانی ساختاری در پاسخ به مهم‌ترین چالش عصر دیجیتال است.

۳. ۴. ۱. تاریخچه‌ای از تعلل و بن‌بست تقنینی

مسیر پر فراز و نشیب این لایحه، خود گویای موانع عمیق سیاسی و نهادی است (Iran Newspaper, 1401). تدوین پیش‌نویس لایحه از سال ۱۳۹۶ در دولت دوازدهم آغاز شد و در مرداد ۱۳۹۷ رونمایی گردید. این اقدام که هم‌زمان با توجه جهانی به GDPR صورت گرفت، نشان از درک اولیهٔ اهمیت موضوع داشت (Shahsavari, 1402: 106). با این حال، لایحه برای سال‌ها در پیچ‌وخم‌های بوروکراتیک متوقف ماند. پس از تحرکی دیرهنگام در دولت سیزدهم و تصویب آن در کمیسیون حقوقی دولت در اردیبهشت ۱۴۰۳، امیدها برای تعیین تکلیف آن زنده شد (IRNA, 1403). اما بر اساس گزارش‌ها، طرحی جدید در مهر ۱۴۰۳ در مجلس اعلام وصول شد و لایحهٔ دولت همچنان در وضعیت نامشخصی قرار دارد (Fekraneh, 1403). این چرخهٔ «پیشرفت و سپس فلج»، عملاً به تداوم وضعیت عدم حمایت از داده‌های شهروندان، به‌ویژه کودکان، می‌انجامد. این تعلل در حالی رخ می‌دهد که نیاز به یک چارچوب قانونی جامع برای حفاظت از داده‌های کودکان، با توجه به افزایش روزافزون حضور آنان در فضای دیجیتال، بیش از پیش احساس می‌شود؛ مقرراتی که بتواند با تعیین سن رضایت قانونی، ساده‌سازی اطلاعات برای درک کودکان و تأکید بر حق حذف داده‌ها، به‌طور مؤثر از حقوق آنان حمایت کند (Shirvani & Isaei Tafreshi, 1404: 279).

این بن‌بست تقنینی در مهر ۱۴۰۳ با اعلام وصول «طرح حفاظت از داده‌های شخصی» در مجلس شورای اسلامی، وارد مرحلهٔ جدید و پیچیده‌تری شد. این طرح که با امضای ۴۱ نماینده ارائه گردید (Islamic Parliament of Iran, 1403)، عملاً یک مسیر موازی و بالقوهٔ رقیب برای لایحهٔ دولت که در اردیبهشت ۱۴۰۳ در کمیسیون حقوقی دولت تصویب شده بود، ایجاد کرد. این دوگانگی میان «لایحهٔ» دولت و «طرح» مجلس صرفاً یک تفاوت شکلی نیست، بلکه نشان‌دهندهٔ یک شکاف راهبردی و رقابت نهادی بر سر کنترل و راهبری یکی از مهم‌ترین حوزه‌های حکمرانی دیجیتال است. درحالی که لایحهٔ دولت محصول فرایندی کارشناسی و بوروکراتیک در قوهٔ مجریه است، طرح مجلس نمایانگر ارادهٔ

قوهٔ مقننه برای اعمال نفوذ مستقیم و احتمالاً با رویکردی متفاوت، بر این حوزهٔ حساس است. این وضعیت، چشم‌انداز تصویب یک قانون منسجم را بیش از پیش مبهم ساخته، تداوم خلأ حمایتی از داده‌های شهروندان، به‌ویژه کودکان را تضمین می‌کند.

این بن‌بست تقنینی را نباید یک تأخیر بوروکراتیک ساده تلقی کرد، بلکه باید آن را نمودی از یک تضاد راهبردی بنیادین و حل‌نشده در درون حاکمیت ایران بر سر حکمرانی داده تحلیل نمود. (Alizadeh & Nasiri, 1404: 89). وجود هم‌زمان یک «لایحهٔ» دولتی و یک «طرح» پارلمانی، نشان‌دهندهٔ اولویت‌های متعارض است. قوهٔ مجریه (دولت) اغلب بر توسعهٔ اقتصادی و یکپارچگی بین‌المللی متمرکز است، که یک قانون مدرن شبه GDPR می‌تواند آن را تسهیل کند. در مقابل، قوهٔ مقننه در سال‌های اخیر بیشتر تحت تأثیر اهداف امنیتی و کنترل فرهنگی بوده است (مانند طرح صیانت)؛ بنابراین، تقابل این دو پیش‌نویس صرفاً رویه‌ای نیست، بلکه نمایانگر یک نزاع عمیق ایدئولوژیک بر سر این است که آیا داده‌ها در درجهٔ اول یک منبع اقتصادی برای مدیریت هستند یا یک تهدید امنیتی برای کنترل. این فلج تقنینی، در عمل به یک سیاست حفظ وضع موجود تبدیل شده که با تداوم بی‌قانونی، به نفع بازیگران قدرتمند دولتی و خصوصی تمام می‌شود که می‌توانند بدون محدودیت از داده‌ها بهره‌برداری کنند.

۳. ۴. ۲. تحلیل انتقادی متن پیش‌نویس: رویکردی ناکافی به حقوق کودک

بررسی پیش‌نویس‌های موجود از لایحه نشان می‌دهد که حتی در صورت تصویب، این متن در مقایسه با استانداردهای جهانی، به‌ویژه در زمینهٔ حمایت از کودکان، دارای نواقص بنیادین است. ضعف اصلی پیش‌نویس، رویکرد آن به داده‌های کودکان است. این لایحه فاقد یک فصل یا بخش ویژه و اختصاصی برای کودکان است و حمایت از آنها را ذیل یک مفهوم کلی و ناکافی در بند ۲ مادهٔ ۳ قرار می‌دهد: «در صورت محجور بودن شخص موضوع داده، اجازهٔ ولی یا قیم قانونی او ضروری است».

این رویکرد دو خطای بنیادین دارد: ۱- خطای مفهومی «محجوریت». این عبارت، حمایت از کودکان را به مفهوم سنتی «حَجر» در قانون مدنی تقلیل می‌دهد. همان‌طور که پیش‌تر بحث شد، این مفهوم برای محافظت از دارایی‌های مالی طراحی شده و قادر به درک و مدیریت ریسک‌های هویتی، روانی و اجتماعی مرتبط با داده‌های شخصی نیست. گو اینکه گاه هویت والدین خود موجب تحدید حریم خصوصی کودکانشان می‌شود. برای مثال، در تعارض میان حق آزادی بیان رسانه‌ها و حق حریم خصوصی کودکان، خصوصاً برای والدین صاحب شهرت، این مصلحت و منافع عالیهٔ کودک است که باید در اولویت قرار گیرد. تقلیل حمایت به مفهوم «محجوریت» این واقعیت را نادیده می‌گیرد که کودکان، صرف نظر از وضعیت والدین خود، سزاوار حمایت ویژه هستند (Mirshkari et al., 1401: 109). ۲- فقدان الزامات مشخص. این بند کلی، هیچ‌یک از الزامات دقیق و عملیاتی که در استانداردهای جهانی

وجود دارد، مانند تعیین سن رضایت دیجیتال، الزام به تأیید رضایت والـدین، محـدودیت پروفایل‌سـازی و الزام به زبان ساده را مشخص نمی‌کند.

۳. ۴. ۳. ارزیابی تطبیقی ویرانگر: پیش‌نویس ایران در برابر استانداردهای جهانی

برای درک عمق این شکاف، مقایسهٔ مستقیم بندهای کلی لایحهٔ ایران با مقررات دقیق مـادهٔ ۸ GDPR ضروری است.

جدول ۲. مقایسهٔ حمایت از داده‌های کودکان در پیش‌نویس لایحه با GDPR

ویژگی حمایتی	پیش‌نویس لایحهٔ حفاظت از داده ایران	مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)
سن رضایت دیجیتال	نامشخص. به سن بلوغ عمومی در قانون مدنی ارجاع می‌دهد که برای اهداف دیجیتال ناکافی است.	مشخص و منعطف. سن پیش‌فرض ۱۶ سال است، اما به کشورهای عضو اجازه می‌دهد آن را تا ۱۳ سال کاهش دهند (مادهٔ ۸).
الزام رضایت والدین	کلی. صرفاً به «اجازهٔ ولی یا قیم» اشاره می‌کند.	صریح و قابل تأیید. نیازمند رضایت «داده‌شده یا تأییدشده از سوی صاحب مسئولیت والدین» است (مادهٔ ۸)
تأیید رضایت[1]	سکوت کامل. هیچ الزامی برای کنترل‌گر جهت تأیید صحت اجازهٔ والدین وجود ندارد.	الزام‌آور. کنترل‌گر باید «تلاش‌های معقولی» با توجه به فناوری موجود برای تأیید رضایت والدین انجام دهد (مادهٔ ۸)
محدودیت در پردازش	سکوت کامل. هیچ محدودیتی برای پروفایل‌سازی، بازاریابی یا تبلیغات هدفمند برای کودکان وجود ندارد.	حمایت ویژه. به‌صراحت بیان می‌کند که حمایت ویژه باید در مورد استفاده از داده‌های کودکان برای اهداف بازاریابی یا ایجاد پروفایل‌های شخصیتی اعمال شود. (مقدمهٔ ۳۸)
الزام به زبان ساده	سکوت کامل. هیچ الزامی برای ارائهٔ اطلاعات به زبان قابل فهم برای کودک وجود ندارد.	الزام‌آور. اطلاعات و ارتباطات مربوط به پردازش باید به زبانی واضح و ساده که برای کودک قابل درک باشد، ارائه شود (مادهٔ ۱۲)

منبع: تحلیل پژوهش بر اساس پیش‌نویس لایحه و متن GDPR

1. Verification

این مقایسه به‌وضوح نشان می‌دهد که بن‌بست قانونی در ایران بـه معنـای آن اسـت کـه داده‌هـای شخصی کودکان در برابر جمع‌آوری، پردازش و بهره‌برداری تجاری از سوی پلتفرم‌ها، فاقد هرگونه نظـام حمایتی مؤثر است (Taherabadi, 1401: 85).

۴. طراحی چارچوب پیشنهادی برای ایران: اصول و سازوکارها

برای رفع خلأهای شناسایی‌شده و حرکت به سمت یک نظام حمایتی کارآمد، لازم است چارچوب قـانونی پیشنهادی بر پایهٔ اصولی بنیادین و جهان‌شمول استوار گردد که هم با تعهدات بین‌المللـی ایـران سـازگار باشد و هم ظرفیت انطباق با الزامات بومی را داشته باشد (Farahmanad, 1403: 18)

۴. ۱. اصول بنیادین یک نظام داده‌محور

اصل «منافع عالیهٔ کودک» به‌مثابه قاعدهٔ حاکم. این اصل باید به‌عنوان ستون فقرات و قاعـدهٔ تفسـیری اصلی در قانون پیشنهادی گنجانده شود. اصل «منافع عالیهٔ کودک» کـه در مـادهٔ ۳ کنوانسـیون حقـوق کودک سازمان ملل (که ایران نیز به آن پیوسته است) تصریح شده، ایجاب می‌کند که در تمامی اقدامات مربوط به کودکان، منافع عالیهٔ آنان یک «ملاحظـهٔ اولیـه» باشـد (Abedini & Meshkibaf, 1400: 185). وارد کردن این اصل به حوزهٔ حفاظت از داده به این معناست که هرگاه تعارضی میان منافع تجاری یک ارائه‌دهندهٔ خدمات آنلاین و حق حریم خصوصی، سلامت و رفاه کودک وجـود داشـته باشـد، منـافع کودک باید برتری یابد (Meisami et al., 1399: 162). این اصل، به‌ویژه در فضای مجازی که کودکان با انواع محتواهای آسیب‌زا مواجه هستند، اهمیتی دوچندان می‌یابد. تربیت دینی و اخلاقی کودکان در این فضا، یکی از مصادیق بارز تأمین منافع عالیهٔ آنهاست که باید در هرگونه قانون‌گذاری مدنظر قرار گیرد تا از تضعیف باورهای دینی و القای شبهات جلوگیری شود (Badami et al., 1401: 465).

اصل «حریم خصوصی به‌مثابـه پیش‌فـرض و در طراحـی». ایـن دو اصـل مکمـل کـه در مـادهٔ ۲۵ GDPR به آنها اشاره شده و در AADC به یک الزام عملی تبدیل گشته اسـت، بایـد بـه صـورت یـک تکلیف قانونی صریح برای ارائه‌دهندگان خدمات آنلاین در ایران درآید. حریم خصوصی در طراحـی[1]، بـه این معناست که حفاظت از داده‌ها باید از همان ابتدای فرایند طراحی در آن تعبیه شود. حـریم خصوصـی به‌مثابه پیش‌فرض ایجاب می‌کند که تنظیمات اولیه یک سرویس، به‌طور خودکار بالاترین سطحِ حفاظـت از حریم خصوصی را ارائه دهد.

اصل «به‌حداقل رساندن داده‌ها». بر اساس این اصل، جمـع‌آوری، اسـتفاده و نگهـداری از داده‌هـای

1. Privacy by Design

شخصی کودکان باید به آنچه برای ارائهٔ یک سرویس یا ویژگی خاص که کودک به‌طور فعال از آن استفاده می‌کند، «کاملاً ضروری»[1] است، محدود شود. این اصل، منطق غالب اقتصاد داده را که مبتنی بر «جمع‌آوری حداکثری» است، معکوس می‌کند.

۴. ۲. سازوکارهای اجرایی کلیدی

۴. ۲. ۱. رضایت قابل تأیید والدین و تعیین سن رضایت دیجیتال

یک نظام حقوقی روشن نیازمند تعیین یک سن مشخص برای «رضایت دیجیتال» است (Pasquale et al., 2022: 1). پیشنهاد می‌شود این سن در ایران ۱۳ سال تمام شمسی تعیین گردد. این انتخاب با حداقل سن مجاز در مادهٔ ۸ GDPR و همچنین سن محوری در قانون حفاظت از حریم خصوصی آنلاین کودکان امریکا[2] هماهنگ است و با تقسیم‌بندی «قانون حمایت از اطفال و نوجوانان» به دو گروه «طفل» و «نوجوان» نیز سازگاری دارد. بنابراین، برای پردازش داده‌های شخصی افراد زیر ۱۳ سال، کسب رضایت قابل تأیید از والدین یا قیم قانونی آن‌ها الزامی خواهد بود (Hamidi, 1394: 41). مفهوم «تلاش معقول» برای تأیید رضایت، باید در قانون یا آیین‌نامه‌های اجرایی آن، به مصادیق عینی تبدیل شود. با الهام از روش‌های موردبحث در راهنمای کمیسیون تجارت فدرال امریکا[3] برای اجرای COPPA، می‌توان مجموعه‌ای از روش‌های قابل قبول را به صورت منعطف پیش‌بینی کرد:

- ارسال فرم رضایت‌نامهٔ امضاشده از طریق پست، فکس یا اسکن.
- استفاده از کارت اعتباری یا بانکی برای انجام یک تراکنش مالی (حتی با مبلغ بسیارکم).
- تماس تلفنی یا ویدئو کنفرانس با یک اپراتور آموزش‌دیده.
- احراز هویت از طریق سامانه‌های ملی (مانند سامانهٔ ثبت احوال یا دولت همراه).

۴. ۲. ۲. الزام به ارزیابی تأثیر حفاظت از دادهٔ متمرکز بر کودک

«ارزیابی تأثیر حفاظت از داده»[4] یک ابزار کلیدی برای عملیاتی کردن اصل «حریم خصوصی در طراحی» و مدیریت پیشگیرانهٔ ریسک است (Marelli, 2024: 65). پیشنهاد می‌شود انجام DPIA برای هر سرویس آنلاینی که «احتمالاً کودکان به آن دسترسی دارند» و پردازش داده‌های آن «می‌تواند ریسک بالایی برای حقوق و آزادی‌های کودکان ایجاد کند»، به یک الزام قانونی تبدیل شود

1. strictly necessary
2. Children's Online Privacy Protection Act (COPPA)
3. Federal Trade Commission (FTC)
4. Data Protection Impact Assessment (DPIA)

(Fekrizadeh & Dorodian, 1402: 42). یک DPIA متمرکز بر کودک، با الهام از راهنمای ICO، باید به‌طور خاص به پرسش‌های زیر پاسخ دهد:

- انطباق با اصل منافع عالیهٔ کودک: آیا طراحی سرویس، منافع عالیهٔ کودک را در اولویت قرار داده است؛ چگونه؟
- ارزیابی ریسک‌های خاص کودکان: ریسک‌های ناشی از پروفایل‌سازی، تصمیم‌گیری خودکار، ردیابی موقعیت مکانی، و استفاده از تکنیک‌های اغواگر چگونه شناسایی و مدیریت شده‌اند؟
- ارزیابی آسیب‌های احتمالی: آیا طراحی سرویس می‌تواند به سلامت روانی (مانند افزایش اضطراب) یا جسمی (مانند اختلال در خواب) کودک آسیب برساند؟
- شفافیت و فهم‌پذیری: آیا اطلاعات مربوط به حریم خصوصی به زبانی متناسب با سن و درک کودک ارائه شده است؛ چگونه؟

۴. ۲. ۳. شفافیت متناسب با سن و تضمین حقوق دسترسی

الزام قانونی به ارائهٔ اطلاعات به زبانی ساده و قابل فهم (موضوع مادهٔ ۱۲ GDPR) باید در قانون پیشنهادی ایران نیز گنجانده شود. شرکت‌ها باید فراتر از یک سیاست حریم خصوصی واحد و پیچیده حرکت کنند و اطلاعات کلیدی را در قالب‌های مختلف و متناسب با گروه‌های سنی متفاوت ارائه دهند. همچنین، قانون باید به‌صراحت حقوق زیر را برای والدین (به نمایندگی از کودک زیر ۱۳ سال) و خود نوجوانان (بالای ۱۳ سال) به‌رسمیت بشناسد: حق دسترسی، حق اصلاح، و حق حذف (حق فراموش شدن) (Faisal, 2022:120).

۴. ۳. نقشهٔ راه استراتژیک: الزامات تقنینی و نهادی

طراحی یک چارچوب حقوقی مؤثر، تنها نیمی از مسیر است. نیم دیگر، تبدیل این چارچوب به قوانین لازم‌الاجرا و ایجاد ساختارهای نهادی برای تضمین اجرای آن است.

۴. ۳. ۱. پیشنهادهای تقنینی: ضرورت تدوین قانون اختصاصی

با توجه به ماهیت فنی، پیچیده و پویای موضوع، تدوین یک قانون مستقل و اختصاصی، رویکرد ارجح به‌نظر می‌رسد (Wenxiao, 2024: 8). این رویکرد دارای مزایای متعددی است:

دقت و جامعیت فنی: یک قانون مستقل می‌تواند با جزئیات بیشتری به مسائل فنی بپردازد.

همسویی با تجارب جهانی: کشورهای پیشرو مانند امریکا (COPPA) و بریتانیا (AADC) نیز رویکردهای اختصاصی را برگزیده‌اند.

شفافیت و دسترسی‌پذیری: وجود یک قانون واحد و متمرکز، درک و اجرای آن را برای همهٔ ذی‌نفعان آسان‌تر می‌کند.

۴. ۳. ۲. الزامات نهادی: تأسیس سازمان مستقل حفاظت از داده

تصویب بهترین قانون نیز بدون وجود یک بازوی اجرایی و نظارتی قدرتمند، بی‌اثر خواهد بود. اجرای مؤثر مقررات پیچیده حفاظت از داده، نیازمند یک نهاد ناظر مستقل، متخصص و دارای اختیارات کافی[1] است (Greenleaf, 2012: 25). این نهاد که می‌تواند به‌عنوان «سازمان حفاظت از داده‌های شخصی» شکل گیرد، باید وظایف تدوین مقررات، نظارت و بازرسی، رسیدگی به شکایات، راهنمایی و آموزش، و اعمال ضمانت اجرا را برعهده داشته باشد.

البته باید توجه داشت که پیشنهاد تأسیس یک «سازمان حفاظت از داده‌های شخصی» مستقل، هرچند از منظر حقوقی و تطبیقی کاملاً صحیح است، اما در عمل با موانع ساختاری عمیقی در نظام حکمرانی ایران مواجه می‌شود (Pirnia & Abrishami Rad, 1402: 374). مفهوم «استقلال» یک نهاد نظارتی در نظام‌های حقوقی غربی، متکی بر تفکیک قوای روشن و وجود جامعهٔ مدنی قدرتمند است. در ساختار حقوقی ایران که در آن قوای سه‌گانه ذیل نظارت ولی فقیه فعالیت می‌کنند (اصل ۵۷ قانون اساسی) و نهادهای فراقوه‌ای متعددی مانند «شورای عالی فضای مجازی» با حکم رهبری تشکیل شده و مصوبات آن لازم‌الاجراست، ایجاد یک نهاد نظارتی که بتواند به صورت مستقل بر عملکرد دستگاه‌های اجرایی و امنیتی نظارت کند، با چالش‌های جدی روبه‌رو است (Qotbi & Habibzadeh, 1394: 341).

هرگونه سازمان حفاظت از داده که از سوی مجلس تأسیس شود، از نظر سلسله‌مراتب حقوقی، پایین‌تر از شورای عالی فضای مجازی قرار خواهد گرفت و مصوبات آن نمی‌تواند ناقض تصمیمات شورا باشد (Akbarzadeh et al., 2024: 3). علاوه بر این، تعدد نهادهای نظارتی موازی و بعضاً متعارض در ایران، خود یکی از معضلات ساختاری است که به‌جای کارآمدی، به تشتت و ناکارآمدی دامن زده است. بنابراین، موفقیت چنین نهادی، نه‌تنها به متن قانون، بلکه به ارادهٔ سیاسی برای اعطای استقلال واقعی و مصونیت آن از نفوذ سایر مراکز قدرت، به‌ویژه نهادهای امنیتی و اطلاعاتی، بستگی دارد؛ امری که با توجه به تجارب پیشین، با تردیدهای جدی همراه است. این تحلیل نشان می‌دهد که کپی‌برداری صرف از الگوی اروپایی بدون بومی‌سازی ساختاری، محکوم به شکست است.

از طرفی تأسیس این نهاد از جانب دولت نیز چندان صحیح به‌نظر نمی‌رسد. یک بُعد حیاتی که در تحلیل نظام حقوقی ایران باید مورد توجه قرار گیرد، «تعارض منافع نهادی» دولت است (Shahbik et

1. Data Protection Authority - DPA

al., 1401: 75). در نظریه‌های حکمرانی، وضعیتی که در آن یک نهاد (در اینجا دولت) هم‌زمان نقش بازیگر اصلی بازار (پردازشگر داده) و داور (ناظر بر حفاظت از داده) را ایفا می‌کند، به‌عنوان «اتحاد ناظر و منظور» شناخته می‌شود که به‌طور ذاتی ناکارآمدی و سوءاستفاده را تقویت می‌کند (Rose-Ackerman, 1999:69). دولت و نهادهای حاکمیتی در ایران، بزرگ‌ترین گردآورنده، پردازشگر و نگهدارندهٔ داده‌های شخصی شهروندان هستند. این داده‌ها برای اهداف متنوعی از ارائهٔ خدمات عمومی و تأمین اجتماعی گرفته تا اجرای قانون و حفظ امنیت ملی جمع‌آوری می‌شوند. در چنین شرایطی، سپردن وظیفهٔ نظارت بر حفاظت از داده‌ها به نهادی که خود بخشی از بدنهٔ دولت است یا تحت نفوذ مستقیم آن قرار دارد، مصداق بارز تعارض منافع است.

در این رویکرد، دولت هم‌زمان در جایگاه «پردازشگر داده»[1] و «ناظر»[2] قرار می‌گیرد که این دو نقش ذاتاً در تعارض هستند (EDPS, 2014: 3). منافع دولت در مقام پردازشگر ایجاب می‌کند که دسترسی گسترده‌تر و محدودیت‌های کمتری برای پردازش داده‌ها داشته باشد، درحالی که وظیفهٔ آن در مقام ناظر ایجاب می‌کند که محدودیت‌های سخت‌گیرانه‌ای را برای حفاظت از حقوق شهروندان اعمال کند.

بدون وجود یک نهاد ناظر و حقیقتاً مستقل که بتواند بدون واهمه از قوهٔ مجریه و نهادهای امنیتی، تخلفات آنها را بررسی و اعمال قانون کند، هر قانونی در زمینهٔ حفاظت از داده‌ها در برابر بزرگ‌ترین ناقض بالقوهٔ حریم خصوصی شهروندان، یعنی خود حاکمیت، بی‌اثر خواهد بود. این تعارض منافع، پاشنهٔ آشیل هرگونه تلاش برای اصلاحات در این حوزه است و باید در طراحی ساختار نهادی به صورت جدی مدنظر قرار گیرد.

۴. ۳. ۳. فراتر از کپی‌برداری: بررسی الگوهای حکمرانی جایگزین و متناسب با زمینه

تحلیل پیش‌گفته نشان می‌دهد که کپی‌برداری مستقیم از الگوی اروپایی یک «سازمان حفاظت از دادهٔ» کاملاً مستقل، به دلیل تفاوت‌های ساختاری در نظام حکمرانی ایران، احتمالاً به شکست یا تسخیر آن از سوی سایر مراکز قدرت منجر خواهد شد. بنابراین، به‌جای اصرار بر یک راه‌حل ایدئال اما غیرعملی، ضروری است که الگوهای حکمرانی جایگزین، ترکیبی یا «به قدر کفایت خوب» که ممکن است از نظر سیاسی در خصوص ایران عملی‌تر باشد، مورد بررسی قرار گیرند. برخی از این الگوها که می‌توانند مبنای بحث‌های آتی قانون‌گذاری قرار گیرند، عبارت‌اند از:

نهاد مستقر در قوهٔ قضاییه: استقرار یک نهاد نظارتی در درون قوهٔ قضاییه، به‌طور بالقوه می‌تواند آن را از نفوذ مستقیم قوهٔ مجریه و نهادهای امنیتی که بزرگ‌ترین پردازشگران داده هستند، مصون‌تر بدارد.

---

1. Data Controller/Processor
2. Regulator

کمیسیون چندذی‌نفعی: تشکیل نهادی متشکل از نمایندگان دولت، بخش خصوصی، دانشگاهیان و جامعهٔ مدنی (تا حد امکان) که با افزایش شفافیت و الزام به اجماع‌سازی، از تصمیم‌گیری یک‌جانبه جلوگیری کند.

الگوی «دیوان محاسباتی» برای داده: ایجاد نهادی با اختیارات قدرتمند تحقیقی و حسابرسی که مستقیماً به مجلس و افکار عمومی گزارش می‌دهد. تمرکز این رویکرد بیشتر بر شفافیت و پاسخگویی پسینی است تا اعمال مستقیم ضمانت اجرا که می‌تواند در صلاحیت دادگاه‌ها باقی بماند.

جدول ۳. تحلیل تطبیقی مدل‌های بالقوهٔ نظارت بر حفاظت از داده در ایران

الگو	درجه استقلال	تخصص فنی	قدرت اجرایی	شفافیت و پاسخگویی	امکان‌سنجی سیاسی در ایران
DPA مستقل (الگوی اروپایی)	بالا (در تئوری)	بالا	بالا	بالا	پایین
نهاد مستقر در قوهٔ قضاییه	متوسط تا بالا	متوسط	متوسط	متوسط	متوسط
کمیسیون چندذی‌نفعی	متوسط	بالا	پایین تا متوسط	بالا	متوسط تا بالا
الگوی دیوان محاسباتی	بالا	متوسط	پایین (نظارتی)	بسیار بالا	متوسط

۴. ۳. ۴. ضمانت اجراهای مؤثر: از جبران خسارت تا جرایم بازدارنده

برای اطمینان از بازدارندگی و اثربخشی قانون، باید یک الگوی ضمانت اجرای سه‌لایه پیش‌بینی شود. این چارچوب باید به صورت یکپارچه با نظام مسئولیت مدنی ایران عمل کند. نقض مقررات حفاظت از داده‌های کودکان باید به‌عنوان یک فعل زیان‌بار و مصداق تقصیر تلقی شود که بر اساس قواعد عمومی مسئولیت مدنی، ازجمله مادهٔ ۱ قانون مسئولیت مدنی و قواعد فقهی «تسبیب» و «لاضرر»، موجب الزام به جبران خسارت مادی و معنوی می‌شود.

ضمانت اجرای مدنی: به‌رسمیت شناختن حق افراد برای مطالبهٔ جبران خسارت مادی و معنوی ناشی از نقض مقررات این قانون.

ضمانت اجرای اداری: اعطای اختیار به نهاد ناظر برای اعمال جریمه‌های سنگین و بازدارنده، مشابه الگوی GDPR که می‌تواند درصدی از گردش مالی سالانه شرکت متخلف باشد.

ضمانت اجرای کیفری: برای موارد نقض شدید و عمدی که به آسیب جدی به کودک منجر می‌شود، می‌توان مجازات‌های کیفری متناسب را نیز درنظر گرفت.

۵. نتیجه‌گیری

این پژوهش با هدف طراحی یک نظام حقوقی جامع برای حفاظت از داده‌های کودکان در ایران، نشان داد که نظام حقوقی فعلی کشور در تحول بنیادین از الگوی «حفاظت محتوامحور» به «حمایت داده‌محور» دچار یک خلأ ساختاری است. یافته‌های کلیدی تحقیق نشان می‌دهد که رویکرد قوانین موجود در ایران برای مقابله با چالش‌های ناشی از اقتصاد داده ناکافی است؛ درحالی که الگوهای پیشرو بین‌المللی مانند GDPR و AADC با محور قرار دادن اصولی چون «منافع عالیهٔ کودک» و «حریم خصوصی در طراحی»، مسئولیت اصلی حفاظت را از دوش کاربر به سمت طراحان و ارائه‌دهندگان خدمات منتقل کرده‌اند. این گذار در مسئولیت، نقطهٔ کانونی تحولی است که نظام حقوقی ایران برای ارائهٔ حمایت مؤثر از کودکان به آن نیازمند است.

بر این اساس، نگارندگان این پژوهش استدلال می‌کنند که پر کردن خلأ قانونی موجود نیازمند تدوین یک «قانون اختصاصی حفاظت از داده‌های کودکان» است و چنین قانونی باید فراتر از ارجاع کلی به مفهوم «حجر» در قانون مدنی بوده، شامل ویژگی‌های مشخص زیر باشد:

تعیین سن رضایت دیجیتال: تعیین سن ۱۳ سال تمام شمسی به‌عنوان مبنای أخذ رضایت مستقیم از نوجوان، و الزام به کسب «رضایت قابل تأیید والدین» برای کودکان زیر این سن.

الزامات طراحی‌محور: تصریح قانونی به اصول «حریم خصوصی در طراحی» و «حریم خصوصی به‌مثابه پیش‌فرض» برای تمام سرویس‌هایی که احتمالاً از سوی کودکان استفاده می‌شوند.

محدودیت‌های پردازشی: ممنوعیت صریح پروفایل‌سازی از داده‌های کودکان برای اهداف بازاریابی و تبلیغات هدفمند و محدود کردن جمع‌آوری داده به «حداقل ضرورت».

شفافیت متناسب با سن: الزام ارائه‌دهندگان خدمات به استفاده از زبان ساده، شفاف و قابل فهم برای کودکان در سیاست‌های حریم خصوصی و اطلاع‌رسانی‌ها.

موفقیت چنین قانونی در گرو ایجاد یک نهاد ناظر متخصص و کارآمد است. با اذعان به چالش‌های ساختاری در ایجاد یک نهاد کاملاً مستقل به سبک اروپایی در ایران، باید به مدل‌های جایگزین اندیشید. گزینه‌هایی مانند استقرار یک کمیسیون تخصصی در درون قوهٔ قضائیه برای مصونیت از نفوذ قوهٔ مجریه، یا ایجاد یک نهاد نظارتی چندذی‌نفعی با حضور نمایندگان بخش خصوصی، جامعه مدنی و نهادهای حاکمیتی، می‌تواند از منظر امکان‌سنجی سیاسی واقع‌بینانه‌تر باشد. انتخاب هریک از این مدل‌ها نیازمند توازن میان استقلال، تخصص و قدرت اجرایی است.

در نهایت، تصویب چنین قانونی نه‌تنها یک نظام حمایتی ضروری برای نسل جدید ایران فراهم می‌آورد، بلکه با همسو کردن نظام حقوقی کشور با استانداردهای جهانی، شفافیت و قطعیت حقوقی لازم

را برای فعالیت کسب‌وکارهای ایرانی و نوآوری مسئولانه ایجاد می‌کند. غفلت از این امر، نه‌تنها کودکان را در برابر بهره‌کشی‌های تجاری بی‌دفاع می‌گذارد، بلکه در بلندمدت، اقتصاد دیجیتال کشور را نیز در معرض انزوا قرار خواهد داد. بنابراین، حرکت به سمت حمایت داده‌محور، یک سرمایه‌گذاری راهبردی برای آیندهٔ دیجیتال ایران است.

References

1. Abedini, A., & Meshkibaf, M. (2021). The position of welfare in the Convention on the Rights of the Child and Iranian family laws. *Comparative Research on Islamic and Western Law*, 8(4), 183-212. DOI: https://doi.org/10.22091/csiw.2021.4635.1625 (In Persian).
2. Akbarzadeh, S., Naeni, A., Yilmaz, I., & Bashirov, G. (2024). Cyber surveillance and digital authoritarianism in Iran. *Global Policy Journal*.
3. Alizadeh, P., & Nasiri, M. (2025). Governance structure of technology in Iran: Analysis of institutional challenges and policy requirements for improving efficiency based on content analysis of legal documents. *Scientific Quarterly of Governance Knowledge*, 3(6). DOI: https://doi.org/10.22034/jokog.2025.509483.1066 (In Persian).
4. Badami, M. A., Meqdadi, M. M., & Pilevar, M. (2022). Investigating the Impact of Cyberspace on the Abuse of the Right to Raise a Child with Emphasis on Religious Education. *Journal of Legal Research*, *21*(50), 457–494. DOI: https://doi.org/10.48300/jlr.2021.279730.1619 (In Persian).
5. Data Protection Commission. (2021). *Fundamentals for a Child-Oriented Approach to Data Processing*. Ireland: Data Protection Commission.
6. EDPS. (2014). EDPS issues guidelines on conflicts of interest in data protection. Retrieved from https://www.edps.europa.eu/press-publications/press-news/press-releases/2014/edps-guidelines-conflicts-interest-data-protection_en
7. Elvy, S. A. (2024). Age-Appropriate Design Code Mandates. *University of Pennsylvania Journal of International Law*, 45(4), 953. https://doi.org/10.58112/jil.45-4.3
8. Etemad. (2024, February 18). *The severity of child abuse in cyberspace*. Etemad Newspaper. (In Persian).
9. European Commission. (2022). *A digital decade for children and youth: the new European strategy for a better internet for kids (BIK+)*. Publications Office of the European Union.
10. European Union. (2016). Article 8 GDPR – Conditions applicable to child's consent in relation to information society services - General Data Protection Regulation (GDPR).
11. European Union. (2016). *General Data Protection Regulation*.
12. European Union. (2016). Recital 38 - Special protection of children's personal data - General Data Protection Regulation (GDPR).
13. Faisal, K. (2022). *Certain Legal Aspects of Children's Right to Protect Personal Data in the Context of AI under the European Union Data Protection Laws*. Social Science Research Network.
14. Farahmanad, F. (2024). Protection and safeguarding of personal data and information with comparative study of General Data Protection Regulation (GDPR). *Journal of New Technology Law*, 5(9), 17-25. DOI: https://doi.org/10.22133/mtlj.2023.383528.1164 (In Persian).

15. Faramarziani, P., Ansari, B., Soltanifar, M., & Mozaffari, A. (2022). Identifying and Evaluating Solutions for Protecting Children's Privacy in Cyberspace. *Scientific Quarterly of Culture Studies-Communication*, *23*(59), 151–171. DOI: https://doi.org/10.22083/jccs.2022.286237.3362 (In Persian).
16. Fekraneh, Z. (2024, October 21). "Personal Data Protection" bill received in parliament; government bill still under review. *Peyvast Monthly* (In Persian).
17. Fekrizadeh, H., & Dorodian, M. (2023). Analysis of cyberspace harms to children with an approach to Iran's legal system. *Children's Rights Quarterly*, 5(18), 41-53 (In Persian).
18. Ghanizadeh Bafghi, M., & Chaji, F. (2024). A Comparative Study of the Protection of Children's Image Rights in Cyberspace. *Journal of Legal Research*, *22*(56), 263–294. DOI: https://doi.org/10.48300/jlr.2022.325738.1929 (In Persian).
19. Greenleaf, G. (2012). Independence of data privacy authorities: International standards and Asia-Pacific experience. *Computer Law & Security Review*, 28(1-2), 1-49. https://doi.org/10.2139/ssrn.1971627
20. Guardian, The. (2022, September 5). Instagram owner Meta fined €405m over handling of teens' data.
21. Guardian, The. (2023a, April 4). TikTok fined for UK data protection law breaches.
22. Guardian, The. (2023b, September 15). TikTok fined €345m for breaking EU data law on children's accounts.
23. Hamidi, H. (2015). Ethics and protection of children's online privacy with parental consent. *Ethics in Science and Technology*, 10(3), 41-57 (In Persian).
24. Hoseini, F. S., & Hoseinpour, Z. (2022). Legal protections against risks facing children in cyberspace. *Journal of Jurisprudence and Media Law Studies*, 4(1), 95-116 (In Persian).
25. ICO. (2021). *Age appropriate design: A code of practice for online services (Children's Code)*.
26. Iran Newspaper. (2022, May 15). "Personal Data Protection" bill goes to parliament, p. 12 (In Persian).
27. IRNA. (2024, May 5). Approval of "Personal Data Protection" bill in government legal commission. *Islamic Republic News Agency* (In Persian).
28. Islamic Parliament of Iran. (2003). *Electronic Commerce Law* (In Persian).
29. Islamic Parliament of Iran. (2009). *Computer Crimes Law* (In Persian).
30. Islamic Parliament of Iran. (2020). *Law on Protection of Children and Adolescents*. (In Persian)
31. Islamic Parliament of Iran. (2024). *Personal Data Protection Bill* (In Persian).
32. Khani Razgi, B., Peyvandpour, S., Andi, H., & Ghaemi, A. H. (2024, March 15). Investigating the protection of law for children and adolescents in cyberspace in Iran's legal system. Paper presented at the Thirteenth International and National Conference on Management, Accounting and Law Studies, Tehran (In Persian).
33. Marelli, M. (Ed.). (2024). Data Protection Impact Assessments (DPIAs). In *Handbook on Data Protection in Humanitarian Action* (3rd ed., pp. 65-74). Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781009414630.009
34. Meisami, F., Aghajani Ronaghi, A., & Shahbazi, A. (2020). The best interests of the child in international human rights law and Iranian law: Reflections on practice and theory. *Comparative Law Research*, 24(2), 139-162. DOI: http://dorl.net/dor/20.1001.1.22516751.1399.24.2.1.1 (In Persian).

35. Mirshkari, A., Hosseini, S. M. A., & Chaji, F. (2022). Privacy of Children of Celebrities in the Age of Modern Media. *Modern Technologies Law*, *3*(5), 105-120. DOI: http://doi.org/10.22133/MTLJ.2022.340027.1092 (In Persian).
36. Nikbeen, M., & Raoofi, A. (2025). Protection of children's rights in cyberspace from the perspective of the United Nations system and Iranian law. *Public Law Studies Quarterly, University of Tehran*, 55(1), 697-718 (In Persian).
37. OECD. (2025). *How's Life for Children in the Digital Age?* OECD Publishing. https://doi.org/10.1787/0854b900-en
38. Panahi, R. (2018). *The COP National Framework IRAN's Children Cyber Space: Action Plan and Ecosystem*. International Telecommunication Union (ITU).
39. Pasquale, L., Zippo, P., Curley, C., O'Neill, B., & Mongiello, M. (2022). Digital age of consent and age verification: Can they protect children? *IEEE Software*, 39(3), 50-57. DOI: https://doi.org/10.1109/MS.2020.3044872
40. Pirnia, K., & Abrishami Rad, M. A. (2023). Supervision of the Supreme Council of Cyberspace resolutions in the legal system of the Islamic Republic of Iran. *Iranian Association of Administrative Law - Scientific Quarterly of New Administrative Law Research*, 5(17), 367-391. DOI: https://doi.org/10.22034/mral.2022.549602.1286 (In Persian).
41. Pourmojeddian, F., & Ebrahimi, S. N. (2020). Legal analysis of protecting children's privacy in cyberspace with a view to Iranian laws and international treaties. *Women and Family Studies, Al-Zahra University*, 8(4), 82-102. DOI: https://doi.org/10.22051/jwfs.2020.32749.2512 (In Persian).
42. Qotbi, M., & Habibzadeh, T. (2016). Analysis of the position of supra-parliamentary executive institutions approved by parliament in the system of the Islamic Republic of Iran and the framework of the principle of separation of powers. *Public Law Studies Quarterly, University of Tehran*, 45(3), 341-360 (In Persian).
43. Rose-Ackerman, S. (1999). *Corruption and Government: Causes, Consequences, and Reform*. Cambridge University Press. DOI: https://doi.org/10.1017/CBO9781139175098
44. Shahbik, H., Heydari, M. J., & Nouzari Fardosieh, M. (2022). Legal solution to resolve conflicts of interest in implementing environmental protection laws and regulations. *Scientific Quarterly of New Administrative Law Research*, 4(10), 75-100. DOI: https://doi.org/10.22034/mral.2021.538916.1188 (In Persian).
45. Shahsavari, E. (2023). Comparative study of the Iranian model "Protection of children and adolescents in cyberspace" and international child rights standards. *Comparative Law Research Journal*, 7(2), 105-124. DOI: https://doi.org/10.22080/lps.2023.25007.1471 (In Persian).
46. Shirvani, K., & 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. DOI: https://doi.org/10.22133/mtlj.2025.493734.1405 (In Persian).
47. Shudra, T. (2023). Children' personal data protection in digital environment with different expectations between parents and children. *Journal of Personal Data Protection Law*, 1, 1-23.
48. Solgi, M. (2021). *National survey of internet and children in Iran; Opportunities and*

threats. Research Institute of Culture, Art and Communications (In Persian).
49. Supreme Council of Cyberspace. (2021). *Protection of children and adolescents in cyberspace*. (In Persian)
50. Taghizadegan, M. (2023). Digital resilience of children in Iran: Considerations about digital security and safety of children. *Cultural and Social Research Journal of Children and Adolescents*, 1(3), 7-26. DOI: https://doi.org/10.22083/cssca.2024.433653.1007 (In Persian).
51. Taherabadi, M. (2022). Information privacy of children in Iran's domestic laws. *Children's Rights Quarterly*, 4(15), 75-87 (In Persian).
52. Takhshid, Z. (2022). *Children's Digital Privacy and the Case Against Parental Consent*. Social Science Research Network, 101.
53. UNICEF. (2017). *The State of the World's Children 2017: Children in a Digital World*.
54. United Nations. (1989). *Convention on the Rights of the Child*.
55. Wenxiao, Z. (2024). Research on legislation of special protection of children's privacy data. *The Frontiers of Society, Science and Technology*, 6(1). https://doi.org/10.25236/FSST.2024.060102