Journal Website

Legal Innovation Quarterly

Spring 2026

Volume 2, Issue 3

E-ISSN: 3115-8498

A Comparative Analysis of the Right to Privacy of Children in the Age of Artificial Intelligence and the Digital Environment in the Legal Systems of Iran and Canada

Mansooreh Hosseini* [1], Mojtaba Farahmand [2]

1. Ph.D. Student in Criminal Law and Criminology, Faculty of Law and Humanities, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran (Corresponding Author)*
2. Assistant Professor, Department of Criminal Law and Criminology, Faculty of Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.

***Corresponding author email address:** mansoureh.hosseini1404@gmail.com

Extended Abstract

1. Introduction

In the age of information technology, children are exposed to various risks, including unauthorized access to personal data, the dissemination of private images, and the commercial exploitation of personally identifiable information. The principal research question is how existing laws in Iran and Canada protect children's right to privacy in digital environments and which legal system adopts a more comprehensive approach. The protection of the privacy of children and adolescents is significant from the perspectives of criminal law and criminology, because violations of privacy may give rise to primary and secondary victimization of children. Furthermore, weaknesses in oversight mechanisms and the absence of specific criminal sanctions in this area have created a gap in criminal policy.

Received: December 31, 2025 - **Accepted:** February 6, 2026 - **Published:** March 21, 2026

Hosseini, Mansoureh; and Farahmand, Mojtaba. (2026). "A Comparative Analysis of Children's Right to Privacy in the Age of Artificial Intelligence and Digital Space under the Legal Systems of Iran and Canada." *Legal Innovation Quarterly*, 2(3), pp. 83–106.
Doi: https://doi.org/10.22034/lir.2026.2087769.1034

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

In other words, given the increase in cybercrime against children, the absence of specific legislation on the protection of children's data in Iran, and the diversity of protective legislation in Canada, including federal and provincial laws concerning the protection of personal information, alignment of Iran's criminal policy with the international standards established by the Convention on the Rights of the Child is essential.

2. Research Methodology

This study, conducted using a descriptive-analytical-comparative method, is grounded in theories such as the theory of protective victimology, which emphasizes the need for differentiated protection of children; the theory of data security and the right to control personal information, as reflected in Canadian legal instruments; and the principle of safeguarding human dignity in Iranian jurisprudence and law, as reflected in Articles 252 and 582 of the Islamic Penal Code, which has served as a basis for privacy protection under domestic law. The objectives pursued in this article are to identify the legal and criminological challenges arising from violations of children's privacy in Iran and Canada; to compare the legal policies of the two countries concerning the protection of children's personal data and digital content; and to put forward legislative reform proposals for drafting a law on the protection of children's data in Iran.

3. Research Findings

This study examines, from a comparative perspective, the legal safeguards for the protection of children's privacy under the legal systems of Iran and Canada. The findings indicate that the Canadian legal system has established a more effective framework for safeguarding children's data, drawing on comprehensive data protection laws, transparency requirements, parental consent, and a proactive approach to emerging technologies. By contrast, the Iranian legal system has yet to establish a coherent and dedicated framework for children's personal data, platform accountability, and oversight of artificial intelligence applications, while existing protections remain fragmented and lack a specialized focus. Through a comparative analysis of laws, criminal policies, international instruments, and relevant ethical standards, this study presents measures to strengthen criminal protection, regulate technology, and ensure children's privacy in the age of artificial intelligence and the digital environment.

Children and adolescents are among the victims of the use of cyberspace and artificial intelligence, have no awareness of privacy protection, and may readily be exploited by offenders. In other words, children may lack awareness or possess limited literacy skills that prevent them from fully understanding their right to privacy and the potential long-term risks and effects of data sharing and artificial intelligence processing. They therefore have a limited capacity to assess the associated risks. In this regard, the government should

implement protective and preventive measures through educating parents, children, and adolescents about the use of cyberspace, and appropriate legal action should be taken against offenders in this area.

A comparative analysis of the two legal systems concerning the protection of the privacy of children and adolescents in Iran and Canada led to the conclusion that Canada has a more advanced system of criminal protection and preventive regulations, whereas the establishment of a comprehensive data protection system remains on Iran's agenda. The principal differences between the two systems lie in the extent of their supervisory institutions, criminal sanctions, and data-driven policymaking. In other words, although artificial intelligence and the digital environment create opportunities, they may also pose a serious threat to children's privacy. The principal differences between Iran and Canada lie in the levels of legislative development, oversight, and public education; however, no country is immune to these challenges. Furthermore, to reduce the threats arising from the use of artificial intelligence and the digital environment and to protect children and adolescents, governments should cooperate in this area, technology companies should act with greater accountability, and families should increase their awareness and keep the online environment safe for their children and adolescents.

4. Recommendations

The proposals that may be advanced in this regard include drafting a comprehensive law in Iran on the "Protection of Children's Personal Data," drawing on the Canadian model; establishing a specialized unit within Iran's Cyber Police (FATA) to investigate offences involving violations of children's privacy; and formally acceding to the Optional Protocol, with the aim of taking more substantial steps towards improving children's circumstances in cyberspace and in connection with the use of artificial intelligence, and protecting their rights in this domain.

5. Conclusion

Measures that may be considered to address the challenges threatening children and adolescents who use artificial intelligence and cyberspace in Canada include restricting targeted advertising directed at children; exercising stricter control over facial recognition technology; strengthening regulations governing artificial intelligence in education; using privacy settings; teaching children the skill of saying "no" in digital environments; engaging in active, dialogue-based supervision; and using parental control tools. Furthermore, the drafting of a comprehensive law on the protection of children's data, the imposition of an obligation on platforms to ensure transparency in the use of data, the development of digital literacy education programmes, the establishment of an independent supervisory body, the use of privacy settings,

the teaching of the skill of saying “no” in digital environments to children, active and dialogue-based supervision, and the use of parental control tools are measures that may be considered in relation to the challenges that threaten children and adolescents who use artificial intelligence and cyberspace in Iran.

Keywords: Children’s privacy; digital environment; artificial intelligence; criminal protection; Iranian legal system; Canadian legal system; data protection.

Funding
This article has no financial support or funding.

Authors' Contributions
Mansooreh Hosseini: Methodology, formal analysis, writing – review & editing, investigation, writing – original draft.
Mojtaba Farahmand: Conceptualization, data curation, validation, project administration, and resources.

Conflict of Interest
According to the authors’ declaration, there is no conflict of interest regarding this article.

Ethical Considerations
This study was conducted based on the analysis of legal documents, statutes, judicial decisions, and library-based sources. It did not involve human participants, animals, or personal data; therefore, ethical approval from an institutional ethics committee was not required. Nevertheless, the authors adhered to the principles of academic integrity, research honesty, proper citation practices, and respect for intellectual property rights throughout all stages of the research.
Generative artificial intelligence (AI) tools were used solely to assist with language editing, improving the structure of the manuscript, and enhancing the readability of the text. These tools did not contribute to the study design, scientific analysis, interpretation of findings, drawing of conclusions, or any research-related decision-making. The author(s) assume full responsibility for the accuracy, originality, and final content of the manuscript.

Authors' Approval
All authors have reviewed and approved the final version of the manuscript and agree to its publication.

بهار ۱۴۰۵
دوره ۲، شمارهٔ ۳
شاپای الکترونیکی:
۳۱۱۵-۸۴۹۸

فصلنامه نوآوری حقوقی

وبسایت مجله

تحلیل تطبیقی حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام‌های حقوقی ایران و کانادا

منصوره حسینی [۱*]، مجتبی فرهمند [۲]

۱. دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق و علوم انسانی، واحد شهرکرد، دانشگاه آزاد اسلامی، شهرکرد، ایران (نویسندهٔ مسئول)
۲.استادیار گروه حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق، واحد خوراسگان اصفهان، دانشگاه آزاد اسلامی، اصفهان، ایران.

*ایمیل نویسندهٔ مسئول: mansoureh.hosseini1404@gmail.com

چکیده

رشد فزایندهٔ فناوری‌های ارتباطی، هوش مصنوعی و رسانه‌های اجتماعی، ابعاد نوینی از حریم خصوصی کودکان را در معرض تهدید قرار داده است. کودکان در فضای دیجیتال نه‌تنها به‌عنوان کاربران فعال، بلکه به‌عنوان بزه‌دیدگان بالقوه در برابر گردآوری بی‌رویهٔ داده‌ها، پروفایل‌سازی، ردیابی رفتاری و سوءاستفادهٔ احتمالی از اطلاعات شخصی قرار دارند. پژوهش حاضر با رویکرد تطبیقی به بررسی حمایت‌های قانونی در دو نظام حقوقی ایران و کانادا در زمینهٔ حفظ حریم خصوصی کودکان می‌پردازد. یافته‌ها نشان می‌دهد که نظام حقوقی کانادا، با تکیه بر قوانین جامع حفاظت از داده‌ها، الزامات شفافیت، رضایت والدین و رویکرد پیش‌دستانه در مواجهه با فناوری‌های نوپدید، ساختاری کارآمدتر برای صیانت از داده‌های کودکان ایجاد کرده است. در مقابل، در نظام حقوقی ایران هنوز چارچوب منسجم و ویژه‌ای برای داده‌های شخصی کودکان، مسئولیت‌پذیری پلتفرم‌ها و نظارت بر کاربردهای هوش مصنوعی شکل نگرفته و حمایت‌ها پراکنده و غیرتخصصی باقی مانده است. این مطالعه با تحلیل تطبیقی قوانین، سیاست‌های جنایی، اسناد بین‌المللی و معیارهای اخلاقی مرتبط، راهکارهایی برای تقویت حمایت کیفری، تنظیم‌گری فناوری و تضمین حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال ارائه می‌دهد.

واژگان کلیدی: حریم خصوصی کودکان، فضای دیجیتال، هوش مصنوعی، حمایت کیفری، نظام حقوقی ایران، نظام حقوقی کانادا، حفاظت از داده‌ها.

دریافت‌شده در تاریخ: ۱۰ دی ۱۴۰۴ - **پذیرش‌شده در تاریخ:** ۱۷ بهمن ۱۴۰۴- **منتشرشده در تاریخ:** ۱ فروردین ۱۴۰۵

حسینی، منصوره؛ فرهمند، مجتبی. (۱۴۰۵). «تحلیل تطبیقی حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام‌های حقوقی ایران و کانادا». فصلنامه نوآوری حقوقی، دوره ۲، شماره ۳، صص ۸۳- ۱۰۶.

Doi: https://doi.org/10.22034/lir.2026.2087769.1034

© 2026 The Authors. Published by Legal Innovation Research Institute, Tehran, Iran. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

مقدمه

نقشی که هوش مصنوعی در جامعه ایفا می‌کند، رو به افزایش است و تأثیر آن بر زندگی کودکان نیز رو به افزایش است. همه‌گیری کووید ـ ۱۹ این گذار دیجیتال را تسریع کرده است. از سال ۲۰۲۰ واقعیت‌های فاصله‌گذاری اجتماعی، فعالیت‌های برخط کودکان را از یادگیری گرفته تا بازی و مراقبت‌های بهداشتی، بیشتر از پیش تغییر داد و باعث پذیرش سریع و گستردهٔ فناوری‌های مبتنی بر هوش مصنوعی شد. این تغییرات قابل توجه هستند. ظهور هوش مصنوعی این پتانسیل را دارد که زندگی کودکان را راحت‌تر و در برخی موارد عادلانه‌تر کند. با این حال، هوش مصنوعی خطرات قابل توجهی را نیز برای حریم خصوصی کودکان ایجاد می‌کند، خطراتی که کمتر مورد بررسی کارشناسان و پژوهشگران قرار گرفته‌اند. برخی از تجربیات جدید کودکان که با هوش مصنوعی همراه هستند، کاملاً مشهود هستند. قابل توجه است که کودکان امروزه می‌توانند در کنار دوستان خیالی خود با اسباب‌بازی‌های هوشمند صحبت کنند. با این حال، برخی از مهم‌ترین پیامدهای آن در زیر سطح قرار دارند، به روش‌هایی که هوش مصنوعی داده‌های تولیدشده توسط روال‌های آشنا در زندگی روزمرهٔ کودکان ثبت، ذخیره و استفاده می‌کند. عکس‌های مدرسه که از طریق اینترنت، به جای پست، به اشتراک گذاشته می‌شوند، می‌توانند تجزیه و تحلیل شوند و از طریق فناوری تشخیص چهره برای شناسایی افراد استفاده شوند. کودکان کنجکاوی که به جای والدین، از یک بلندگوی هوشمند اطلاعات می‌خواهند، نه‌تنها به خودشان آموزش می‌دهند، بلکه به هوش مصنوعی نیز می‌آموزند که صدای آن‌ها را تشخیص دهد. نمره‌دهی الگوریتمی به این معنی است که نمرهٔ ضعیف در تنها یک آزمون ریاضی فقط یک بخش عادی از یادگیری نیست، بلکه می‌تواند به‌عنوان یک نقطهٔ داده برای پیش‌بینی عملکرد و فرصت‌های آیندهٔ کودک استفاده شود. هوش مصنوعی می‌تواند از اطلاعات کودکان برای تصمیم‌گیری درمورد آن‌ها استفاده کند که بر محتوایی که می‌بینند و فرصت‌هایی که می‌توانند به آن‌ها دسترسی داشته باشند، تأثیر می‌گذارند؛ علی‌رغم این خطرات، واکنش‌های سیاسی، عمدتاً بزرگ‌سالان‌محور بوده‌اند و توجه کمی به تأثیر عمیق و متمایز هوش مصنوعی بر کودکان داشته‌اند.

به عبارت دیگر در عصر فناوری اطلاعات، کودکان در معرض خطرات متنوعی چون دسترسی غیرمجاز به داده‌های شخصی، انتشار تصاویر خصوصی و بهره‌برداری تجاری از اطلاعات هویتی قرار گرفته‌اند. پرسش اصلی این است که چگونه قوانین موجود در ایران و کانادا از حق حریم

خصوصی کودکان در محیط‌های دیجیتال حمایت می‌کنند و کدام نظام حقوقی برخورد جامع‌تری دارد؟ بحث حفظ حریم خصوصی کودکان و نوجوانان از دیدگاه حقوق جزا و جرم‌شناسی اهمیت دارد، زیرا نقض حریم خصوصی می‌تواند زمینه‌ساز بزه‌دیدگی اولیه و بزه‌دیدگی ثانویه در کودکان شود. از سوی دیگر، ضعف سازوکارهای نظارتی و نبود ضمانت اجراهای کیفری مشخص در این حوزه، سیاست جنایی را با خلأ روبه‌رو کرده است. به عبارتی با افزایش بزهکاری سایبری علیه کودکان و نبود قانون اختصاصی حفاظت از داده‌های کودکان در ایران همچنین تنوع قوانین حمایتی در کانادا (مانند قوانین فدرال و استانی در زمینهٔ حفاظت از اطلاعات شخصی) همسویی سیاست جنایی ایران با استانداردهای جهانی کنوانسیون حقوق کودک ضروری است. این پژوهش که به روش تحلیلی ـ توصیفی ـ تطبیقی انجام شده بر پایهٔ نظریه‌هایی چون نظریهٔ بزه‌دیده‌شناسی حمایتی که بر ضرورت حمایت افتراقی از کودکان تأکید دارد، نظریهٔ امنیت داده‌ها و حق کنترل شخصی بر اطلاعات که در اسناد حقوقی کانادا نمود یافته است همچنین بر اصل صیانت از حیثیت انسانی در فقه و حقوق ایران طبق مواد ۲۵۲ و ۵۸۲ قانون مجازات اسلامی، که مبنای حریم خصوصی در قوانین داخلی بوده، استوار است. اهدافی که در این مقاله به دنبال آن هستیم عبارت‌اند از: شناسایی چالش‌های قانونی و جرم‌شناختی نقض حریم خصوصی کودکان در ایران و کانادا، مقایسهٔ سیاست‌های قانونی دو کشور در حفظ داده‌های شخصی و محتوای دیجیتال کودکان، ارائهٔ پیشنهادهای اصلاحی برای تدوین قانون حمایت از داده‌های کودکان در ایران.

۱. مفاهیم

۱ـ۱. مفهوم کودکان و نوجوانان در حقوق ایران و کانادا

صرف نظر از اختلاف عقایدی که درخصوص سن مسئولیت کیفری و به‌تبع در تعریف طفل وجود دارد،طبق قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹ مفهوم طفل در بند (الف) مادهٔ یک این‌گونه تعریف شده که: «طفل، هر فرد که به سن بلوغ شرعی نرسیده است» و سن بلوغ شرعی در کشور ایران برای دختر نه سال و برای پسر پانزده سال تمام هجری است.

براساس قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹ مفهوم نوجوان در بند (ب) مادهٔ یک بدین نحو تعریف شده است: «نوجوان فردی است که به بلوغ شرعی رسیده اما به سن هجده سال تمام نرسیده است». البته مطابق مادهٔ دو این قانون تمام افرادی که به سن هجده سال تمام شمسی

نرسیده‌اند مشمول این قانون هستند و به‌نظر می‌رسد این تقسیم‌بندی کودک و نوجوان محلی از اعراب نداشته باشد.

مطابق با مادهٔ یک کنوانسیون حقوق کودک سازمان ملل متحد (CRC, 1989)، عمداً از اصطلاح «کودک» هنگام اشاره به «هر انسانی که زیر هجده سال سن دارد، مگر اینکه طبق قانون قابل اجرا در مورد کودک، سن بلوغ زودتر حاصل شود» استفاده خواهم کرد. از آنجایی که کانادا کنوانسیون حقوق کودک را در سال ۱۹۹۲تصویب کرد و از آنجایی که در کانادا سن بلوغ زودتر حاصل نمی‌شود، سن قانونی که کودکان کانادایی از آن حمایت می‌شوند، هجده سال است. با این حال، اصطلاحات رایج مورد استفاده برای کودکان درگیر در سیستم عدالت کیفری، یعنی «نوجوان، جوان، خردسال» و همچنین اصطلاحات انگ‌زننده «نوجوان بزهکار و مجرم جوان»، کودکان را از حقوقی که هم تحت کنوانسیون حقوق کودک و هم قانون کانادا به آن‌ها اعطا شده است، محروم می‌کنند، در حالی که آن‌ها را از «حقوق بزرگسال» برخوردار نمی‌سازند. نام سه قانون اصلی عدالت کودکان کانادا در این زمینه گویاست: قانون بزهکاران نوجوان ۱۹۰۸، قانون جوانان قانون مجرمان ۱۹۸۵ و قانون عدالت کیفری جوانان ۲۰۰۲. این مبحث اصطلاح‌شناسی بین‌المللی، قوانینی که در سه قانون و دستورالعمل سازمان ملل متحد برای کودکان درگیر در دادرسی‌های قضائی مشهود است: قوانین حداقل استاندارد برای اجرای عدالت نوجوانان ۱۹۸۵، قوانین حمایت از نوجوانان محروم از آزادی ۱۹۹۰ و دستورالعمل‌های پیشگیری از بزهکاری نوجوانان۱۹۹۰ (Chapdelaine, 2007: 268).

۲-۱. مفهوم هوش مصنوعی

به‌طور کلی به یک سیستم مبتنی بر ماشین اشاره دارد که با توجه به مجموعه‌ای از اهداف تعریف‌شده، می‌تواند وظایفی را که معمولاً به هوش انسانی نیاز دارد، مانند پیش‌بینی‌ها و تصمیم‌گیری‌ها، انجام دهد. قابل توضیح است که هوش مصنوعی نقش بسیاری در زندگی کودکان ایفا می‌کند و اساساً تجربیات و مکان‌های روزمرهٔ آن‌ها را از خانه‌هایشان گرفته تا مدارسشان و سایر خدمات و فضاهای عمومی تغییر شکل می‌دهد. در حالی که کاربرد هوش مصنوعی به سرعت گسترش یافته است، ابزارهایی برای پرداختن به چالش‌هایی که هوش مصنوعی می‌تواند برای حریم خصوصی کودکان ایجاد کند، به سرعت پیشرفت نکرده‌اند (راهنمای متخصصان حریم خصوصی برای هوش مصنوعی و یادگیری ماشین (https://fpf.org).

۱-۳. مفهوم حق بر حریم خصوصی کودکان

حق بر حریم خصوصی یکی از شاخه‌های بنیادین حقوق بشر است که در اسناد بین‌المللی همچون مادهٔ ۱۲ اعلامیهٔ جهانی حقوق بشر و مادهٔ ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی مورد شناسایی قرار گرفته است. درخصوص کودکان، مادهٔ ۱۶ کنوانسیون حقوق کودک (CRC) به‌صراحت بر حق کودک نسبت به حریم خصوصی، مکاتبات و احترام به آبرو و حیثیت تأکید دارد. حریم خصوصی کودک، گستره‌ای از اطلاعات شخصی، رفتارهای برخط و داده‌های زیستی او را دربر می‌گیرد که امروزه با ورود هوش مصنوعی، امکان تحلیل، پردازش و حتی پیش‌بینی آن‌ها فراهم شده است.

۲. تهدیدات عصر هوش مصنوعی و فضای دیجیتال برای حریم خصوصی کودکان در ایران و کانادا

با توجه به اینکه امروزه رشد سریع تکنولوژی‌های دیجیتال، شبکه‌های اجتماعی و ابزارهای مبتنی بر هوش مصنوعی، فرصت‌های بی‌سابقه‌ای برای آموزش، سرگرمی و ارتباطات کودکان فراهم کرده، اما همین تکنولوژی تهدیدات جدی برای حریم خصوصی، امنیت داده‌ها و سلامت روانی کودکان به‌وجود آورده است.

به‌علت ناآگاهی کودکان از پیامدهای انتشار اطلاعات شخصی، در برابر سوءاستفاده‌های دیجیتال آسیب‌پذیرتر از بزرگسالان بوده و به همین دلیل این چالش در کشورهای مختلف، با توجه به سطح قوانین، زیرساخت‌ها و فرهنگ دیجیتال، ابعاد مختلفی را به دنبال دارد.

زمانی که کودکان و نوجوانان از هوش مصنوعی بدون رعایت چارچوب‌های اخلاقی استفاده کنند، حریم خصوصی‌شان نقض می‌شود، در نتیجهٔ این امر ممکن است به خطرات امنیتی و تبعیض در تصمیم‌گیری‌های آموزشی منجر شود. واضح است که تدوین سیاست‌های شفافی در زمینهٔ بحث مورد نظر توسط مسئولان، آموزش معلمان و دانش‌آموزان در راستای استفادهٔ درست از هوش مصنوعی و طراحی الگوریتم‌های منصفانه و امن بسیار اهمیت دارد (بویری منجی و زارعی، ۱۴۰۴: ۱).

تأثیر هوش مصنوعی در نقض یا تهدید حریم خصوصی کودکان را می‌توان در سه سطح، دسته‌بندی کرد: سطح اول که گردآوری گستردهٔ داده‌های کودکان است، هوش مصنوعی با پروفایل‌سازی و ردیابی دیجیتال، ریسک افشای اطلاعات زیستی و مکانی، حریم خصوصی کودکان و نوجوانان را تهدید می‌کند. در سطح مذکور داده‌ها را از طریق سامانه‌های هوشمند در بازی‌های

برخط، اپلیکیشن‌های آموزشی یا شبکه‌های اجتماعی داده‌های رفتاری، صوتی و چهرهٔ کودکان، ذخیره می‌کنند؛ در سطح دوم هوش مصنوعی از طریق تولید محتوای جعلی دست به اقدامات مخرب می‌زند که این کار را با استفاده از تصاویر جعلی از کودکان، شبیه‌سازی صدای کودکان و نوجوانان، ساخت هویت جعلی از آن‌ها انجام می‌دهد. این اقدام به هوش مصنوعی امکان می‌دهد تا بتواند از کودکان و نوجوانان یا خانواده‌های آنان باج‌گیری، آزار سایبری و سوءاستفاده کند یا از آن برای تبلیغات هدفمند یا پیش‌بینی رفتار استفاده می‌کند؛ در سطح سوم هوش مصنوعی با در اختیار داشتن اطلاعات شخصی و محرمانهٔ کودکان ریسک افشای اطلاعات زیستی و مکانی را برای کودکان و نوجوانان به‌وجود می‌آورد که این تهدید با استفاده از ابزارهای هوشمند خانگی مانند دستیارهای صوتی و دوربین‌های هوشمند، گاه بدون رضایت آگاهانهٔ والدین ذخیرهٔ اطلاعات محیطی و گفت‌وگوهای خانگی برایش مقدور می‌شود؛ در سطح چهارم هوش مصنوعی با استفاده از الگوریتم‌های اعتیادآور یا پلتفرم‌هایی که با استفاده از هوش مصنوعی ارائه می‌شود، محتوایی را نمایش می‌دهند که بیشترین زمان ماندگاری کودک را تضمین کند. درنتیجه برای کودک یا نوجوان وابستگی دیجیتال، کاهش تمرکز و آسیب‌های روانی ایجاد می‌کند؛ در سطح پنجم هوش مصنوعی به ردیابی آموزشی کودکان و نوجوانان می‌پردازد، به‌گونه‌ای که بسیاری از پلتفرم‌های ارائه‌شده در دوران آموزش برخط می‌تواند وسیله‌ای باشد که رفتار یادگیری، سرعت پاسخ‌دهی و میزان توجه کودکان و نوجوانان را ثبت و تحلیل می‌کند. هوش مصنوعی با این داده‌ها به طبقه‌بندی یا برچسب‌گذاری کودکان دست می‌زند.

به عبارت دیگر، کودکان و نوجوانان حق دارند تا از فضای مناسب در جهت آموزش و رشد استفاده کنند، با این حال استفاده از هوش مصنوعی در فضای پویای فناوری و اینترنت حریم خصوصی آن‌ها را به خطر می‌اندازد که با توجه حق آموزش و رعایت حریم خصوصی، آزادی بیان و منع تبعیض مسائل و حقوق مهمی برای کودکان توجه مسئولان و متولیان این امر، ضروری است.

> استفادهٔ نامناسب از هوش مصنوعی درحق بر آموزش کودکان به نقض حریم خصوصی و آسیب داده‌های کودکان منجر شده و موجب نگرانی‌های امنیتی می‌شود. همچنین نقض تعامل انسانی موجب کاهش ارتباطات انسانی و احساساتی کودکان است. افزایش نابرابری، تبعیض، محدودیت آزادی بیان کودکان ازجمله حقوقی است که در رابطه با حق برآموزش کودکان مورد نقض جدی قرار می‌گیرد (صفاری‌نیا، ۱۴۰۳: ۱).

به سخن دیگر،

> والدین نیز در کنار استقبال از امکانات آموزشی نوین، نسبت به کاهش مرزهای بین خانه و مدرسه، نامشخص بودن نحوهٔ ذخیره و تحلیل داده‌های فرزندان، ناامنی اطلاعاتی و تضعیف استقلال و هویت کودک در مواجهه با سیستم‌های هوشمند دغدغه‌های قابل توجهی بیان کرده‌اند. تحلیل پدیدارشناسانهٔ داده‌ها آشکار می‌سازد که چالش‌های اخلاقی ادراک‌شده، بیشتر به عدم شفافیت در کارکردهای هوش مصنوعی، ناآگاهی از پیامدهای بلندمدت آن بر فرایند جامعه‌پذیری کودکان، و محدودیت معلمان و والدین در مدیریت رفتار دیجیتال کودکان بازمی‌گردد. قلمرو کودکی در عصر هوش مصنوعی نیازمند بازتعریف اصول اخلاقی، اصلاح سازوکارهای حفظ حریم خصوصی، و توانمندسازی والدین و معلمان در استفادهٔ آگاهانه از فناوری‌های هوشمند است (خلیلی و سوادی، ۱۴۰۴: ۱).

در نظام حقوقی ایران، قانون جامع و اختصاصی برای حفاظت از داده‌های مربوط به کودکان و حفظ حریم خصوصی‌شان وضع نشده که این مسئله یک چالش قانونی در رابطه با تهدیدات عصر هوش مصنوعی و فضای دیجیتال محسوب می‌شود. چارچوب‌های قانونی موجود پراکنده و کلی و محدودیت‌هایی که در نظارت بر عملکرد پلتفرم‌های خارجی وجود دارد از دیگر چالش‌های این حیطه است. همچنین بخش زیادی از کودکان ایرانی از پلتفرم‌هایی استفاده می‌کنند که سرورهای آن‌ها خارج از کشور است که این مسئله به انتقال داده به خارج از کشور، نبود شفافیت دربارهٔ نحوهٔ استفاده از داده‌ها و دشواری پیگیری حقوقی منجر می‌شود. از مشکلات دیگر در ایران آگاهی پایین دیجیتال کودکان و نوجوانان در بسیاری از خانواده‌هاست، به گونه‌ای که سواد رسانه‌ای والدین محدود است و کنترل والدین بر روی استفاده از هوش مصنوعی و فضای دیجیتال به صورت نظام‌مند نیست، بنابراین کودکان بدون آموزش کافی وارد فضای مجازی می‌شوند.

در مقابل در نظام حقوقی کانادا، که یکی از کشورهایی است که در زمینهٔ حفاظت از داده پیشرو است و چارچوب‌های قوی‌تری داشته، قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی وضع شده است (Montgomery et al., 2017: 14). همچنین قانونگذار این کشور در ایالت‌های کانادا، قوانین استانی چون قانون حفظ حریم خصوصی کبک و تمرکز ویژه بر رضایت آگاهانه و حفاظت از کودکان کانادایی وضع کرده است. با وجود وضع قوانین قوی، همچنان مشکلاتی در این نظام حقوقی به‌چشم می‌خورد که از جملهٔ آن‌ها می‌توان به نفوذ شرکت‌های بزرگ فناوری به اطلاعات

شخصی کودکان و نوجوانان، تبلیغات هدفمند برای نوجوانان، چالش اجرای قوانین در برابر شرکت‌های فراملی اشاره کرد. در رابطه با رویکرد آموزشی در کشور کانادا، آموزش سواد دیجیتال در مدارس به صورت جدی‌تری نسبت به ایران صورت می‌پذیرد و همچنین کمپین‌های آگاهی‌بخشی برای والدین فعالیت می‌کنند و نهادهای ناظر مستقل در استفادهٔ کودکان و نوجوان از هوش مصنوعی وجود دارد (Barassi, 2020: 17).

استفادهٔ کودکان و نوجوانان از هوش مصنوعی و فضای مجازی پیامدهای اجتماعی و روانی به دنبال دارد. این پیامدها ممکن است شکل‌گیری ردپای دیجیتال دائمی از سنین پایین، تهدید هویت و امنیت شخصی، افزایش آزار سایبری و فشار روانی ناشی از مقایسهٔ اجتماعی را به دنبال داشته باشد. همچنین در بلندمدت، داده‌های جمع‌آوری‌شده می‌تواند بر فرصت‌های تحصیلی و شغلی آیندهٔ کودک تأثیر بگذارد.

۳. حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام حقوقی ایران

حمایت کیفری از حق حفظ حریم خصوصی کودکان از نظر حقوقی عبارت است از تدابیری که قانونگذار برای جلوگیری از تعرض به زندگی خصوصی کودکان و شخصیت معنوی آنان در قانون در نظر داشته و تجاوز به آن مستلزم حمایت از بزه‌دیده و اعمال مجازات بر فرد متجاوز بر حریم خصوصی است (انصاری، ۱۳۹۱: ۱۰). ضروری است تا با اقدامات تقنینی و با ابزارهایی چون فناوری‌های اطلاعات و ارتباطات، از کودکان و نوجوانان در فضای مجازی و در برابر هوش مصنوعی موجود در فضای مجازی، حمایت شود و با جرم‌انگاری رفتارهای بزهکارانه و جبران خسارات جسمی و روحی واردشده به کودکان و نوجوانان بزه‌دیده از هتک حیثیت این قشر جلوگیری شود (پورمسجدیان و ابراهیمی، ۱۳۹۹: ۸۲). قانون حمایت از کودکان و نوجوانان ۱۳۹۹ که حریم خصوصی دیجیتال را به‌طور مستقیم پوشش نمی‌دهد، قانون اساسی، قانون مجازات اسلامی، قانون آیین دادرسی کیفری، قانون احترام به آزادی‌های مشروع و حقوق شهروندی مصوب ۱۳۸۳، قانون جرائم رایانه‌ای اصلاحی سال ۱۳۹۹، قانون تجارت الکترونیک و مصوبات و بخشنامه‌های دیگر در زمرهٔ قوانین و مقرراتی هستند که مقنن گاه تلاش می‌کند تا به‌طور ضمنی و گاه صریحاً از برخی مصادیق حریم خصوصی حمایت نماید. در نظام حقوقی ایران به‌طور عمومی محل سکونت و سایر

ابعاد جسمانی و خانوادگی اشخاص در قانون مجازات اسلامی و سایر قوانین متفرقه از تعرض مصون مانده، اما ابعاد ذهنی مورد مصونیت قرار نگرفته است.

براساس اصل ۲۲ قانون اساسی، حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند. در توضیح اصل مذکور می‌توان گفت، کودکان و نوجوانان نیز به‌عنوان شهروندانی که دارای حقوق و آزادی‌های طبیعی و انسانی در جامعهٔ امروزی هستند، بایستی شرایط زندگی امن در جامعه به گونه‌ای برایشان فراهم شود تا نسبت به جان، مال، مسکن، تمام حقوق فردی خود و... هیچ گونه بیم و هراسی نداشته باشند یا به عبارتی قشر مذکور در امنیت کامل زندگی کنند. درواقع با استفاده از این اصل می‌توان از اتخاذ تدابیر و تصمیمات ضعیف توسط حکومت که زمینه هرگونه تعرض به جان، مال و حقوق و مسکن و شغل و... را فراهم کرده است، جلوگیری کرد.

همچنین براساس اصل ۲۵ قانون اساسی، بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون. در تشریح اصل فوق‌الذکر، در نظام حقوقی ایران، حریم خصوصی کودکان و نوجوانان را می‌توان در چهار عنوان مسکن و محل تحصیل خصوصی، اطلاعات جسمانی، اطلاعات شخصی و ارتباطات خصوصی معرفی کرد. بر این اساس، اطلاعات و اسرار شخصی قشر مورد بحث، اساساً باید از تعرض مصون باشد و هیچ شخصی مجوز دسترسی به آن‌ها را ندارد، این اصل مأموران دولتی و اشخاص دیگر را نیز شامل می‌شود. هیچ شخصی حق ندارد اطلاعات کودکان و نوجوانان را به مجرد وجود نفع برای خود، به دادگاه ارائه دهد مگر در زمان اضطراری اصل ۷۹ قانون اساسی و دیگری کشف و تعقیب جرائم. در عصر تکنولوژی کنونی، اصل مصونیت اطلاعات شخصی کودکان و نوجوانان با ظهور فضای مجازی و هوش مصنوعی با یک خطر جدی مواجه شده است، از این رو ضرورت دارد تا مقررات دقیقی از طرف دولت در رعایت اصل حفظ حریم خصوصی وضع شود. به‌طور کلی دو اصل ۲۲ و ۲۵ قانون اساسی به حمایت ضمنی از حریم خصوصی پرداخته است.

براساس مواد قانونی که در فصل پنجم قانون جرائم رایانه‌ای اصلاحی مصوب سال ۱۳۹۹، به‌عنوان هتک حیثیت و نشر اکاذیب، قانونگذار بیشتر بر محتوای مستهجن تمرکز دارد، نه حفاظت داده‌های کودکان. به گونه‌ای که در مادهٔ ۱۶ مقرر داشته، هرکس به وسیلهٔ سامانه‌های رایانه‌ای یا

مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. علاوه بر آن در تبصرهٔ همین ماده بیان داشته که چنانچه تغییر یا تحریف به صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

با بررسی مادهٔ فوق می‌توان گفت مادهٔ ۱۶ قانون جرائم رایانه‌ای وضع شد تا از حریم شخصی و حیات خصوصی افراد از سوی قانون گذاران حمایت شود؛ بنابراین اگر شخصی با سامانه‌های رایانه‌ای یا مخابراتی مرتکب تعرض به حریم خصوصی اشخاص شوند و اقدامات وی به نشر اطلاعات خانوادگی و شخصی طرف مقابل منجر شود، مستوجب مجازات می‌شود. در تحقق رفتار مادی جرائم مبتنی بر توزیع و انتشار، مالکیت مرتکب بر محتوا یا اشیای مستهجن شرط نیست؛ بنابراین واسطگان و اشخاصی که با انگیزهٔ تحصیل مال، عملیات توزیع یا فروش را محقق می‌سازند، مستوجب مسئولیت کیفری مباشرتی ناشی از مادهٔ فوق خواهند بود (میرکمالی و صالح احمدی، ۱۴۰۰: ۵۶).

همچنین بر اساس مادهٔ ۱۷ قانون جرائم رایانه‌ای، هر کس به وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که به ضرر یا عرفاً موجب هتک حیثیت او منجر شود، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

با نگاهی عمیق در مادهٔ ۱۷ قانون جرائم رایانه‌ای درمی‌یابیم که این ماده با هدف جرم‌انگاری در دسترس قرار دادن صوت، تصویر، فیلم‌های خصوصی یا خانوادگی و یا اسرار دیگری وضع شده است. عنصر مادی این جرم دارای دو بخش بوده که بخش اول آن، اظهار اکاذیب است. به‌طوری که مرتکب، مطالبی خلاف واقعیت را از عمد و دانسته (عامداً و عالماً) به اشخاصی نسبت دهد؛ در صورتی که عمل مرتکب به وارد شدن ضرر مادی یا معنوی به مجنی علیه منجر بشوند یا خیر. بخش دوم این جرم به نظر قانونگذار به جرم‌انگاری افشای اسرار مردم عادی بستگی دارد. با توجه به اینکه در جرم نشر اکاذیب توجه بر روی مقامات رسمی است، اما براساس مادهٔ فوق و با توجه به پیشرفته شدن و پیچیده‌تر شدن تکنولوژی وسایل الکترونیکی و رایانه‌ای، قانونگذار در مقام جرم‌انگاری

افشای حریم خصوصی اشخاص دیگر نیز آمده است. همچنین با توجه به اینکه افشای اطلاعات و داده‌های خصوصی اشخاص زیان‌های معنوی مختلفی را ممکن است به همراه داشته باشد، این گونه جرائم را در دستهٔ جرائم عمومی برشمرده‌اند که گذشت شاکی ممکن است صرفاً موجب تخفیف مجازات شود.

در مادهٔ ۱۸ قانون فوق‌الذکر نیز بیان داشته که هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به‌وسیلهٔ سامانهٔ رایانه‌ای یا مخابراتی اکاذیبی را منتشر کند یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأسا یا به‌عنوان نقل قول، به شخص حقیقی یا حقوقی به‌طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یادشده به نحوی از انحا ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعادهٔ حیثیت (در صورت امکان)، به حبس از ۹۱ روز تا دو سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۱۵۰ ریال یا هر دو مجازات محکوم خواهد شد.

با بررسی مادهٔ ۱۸ این برداشت می‌شود که با وجود اینکه جرم نشر اکاذیب قبلاً توسط قانونگذار جرم‌انگاری شده بود، اما از آنجایی که نشر اکاذیب به‌وسیلهٔ سامانه‌های رایانه‌ای یا مخابراتی یا استفاده از هوش مصنوعی در نظر گرفته نشده بود، قانونگذار با اختیار و قدرتی که در تعقیب و مجازات اشخاصی که از این طریق به نشر اکاذیب مبادرت می‌ورزند، به وضع مادهٔ ۱۸ قانون جرائم رایانه‌ای اقدام کردند. در صورتی که جرم نشر اکاذیب را می‌بایست جزء جرائم قابل گذشت درنظر گرفت، اما در رابطه با جرم نشر اکاذیب از طریق سامانه‌های رایانه‌ای و مخابراتی یا استفاده از هوش مصنوعی، به نظر برخی کارشناسان این حوزه باید جرم مذکور را دارای جنبهٔ عمومی دانسته و گذشت شاکی ممکن است فقط از جهات تخفیف محسوب شود. با توجه به موارد ذکرشده، فقدان حفاظت از داده‌های کودکان در قوانینی که در نظام حقوقی ایران قانونگذار وضع نموده به چشم می‌خورد.

علاوه بر قوانین فوق در مادهٔ ۹ قانون حمایت از اطفال و نوجوانان مصوب سال ۱۳۹۹، هرگونه دسترسی یا انتشار اطلاعات خصوصی کودک را بدون رضایت یا حکم قانونی، جرم‌انگاری کرده است. همچنین براساس سند سیاست‌های کلی شبکهٔ ملی اطلاعات مصوب سال ۱۳۹۵، نیز بر لزوم صیانت از کودکان در فضای مجازی تأکید دارد. با وجود این، هنوز در ایران قانون مستقل و جامع حمایت از داده‌های شخصی کودکان مشابه مقررات عمومی حفاظت از داده‌ها در اتحادیهٔ

اروپا وضع نشده است. بنابراین، نواقص حقوقی در حوزهٔ داده‌های دیجیتال، الگوریتم‌های هوش مصنوعی، و نظارت بر زیرساخت‌های کودک‌محور مشاهده می‌شود.

به جهت ارتقای سطح حمایت از حریم خصوصی کودکان و نوجوانان و حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال، اقداماتی چون تدوین قانون ویژهٔ حفظ داده‌های شخصی کودکان، تأسیس کمیسیون حفاظت از داده‌های کودکان در جهت نظارت بر شرکت‌ها و الگوریتم‌های هوش مصنوعی فعال در ایران، ترویج سواد رسانه‌ای و سواد داده‌ای خانواده‌ها، بومی‌سازی چارچوب‌های بین‌المللی، بایستی در دستور کار مسئولان این امر قرار گیرد.

۴. حق حفظ حریم خصوصی کودکان در عصر هوش مصنوعی و فضای دیجیتال در نظام حقوقی کانادا

حقوق بشر صرف نظر از سن، به‌طور مساوی برای همه اعمال می‌شود. با این حال، سازمان ملل متحد تصمیم گرفت که باید درمورد حقوق کودکان (افراد زیر هجده سال) دقیق‌تر عمل کند. این سازمان اذعان می‌کند که کودکان نیازها و موقعیت ویژه‌ای دارند که نسبت به بزرگسالان در برابر استثمار آسیب‌پذیرترند. بنابراین سازمان ملل متحد در سال ۱۹۵۹ سندی را به نام اعلامیهٔ جهانی «حقوق کودک» تصویب کرد که این سند ده حق مهم کودک (منظور از کودک، کودکان و نوجوانان هستند) مانند حق محافظت در برابر بی‌توجهی و ظلم، حق بقا، حق مراقبت، حق در امان ماندن از آسیب دیگران، حق مشارکت کامل در زندگی خانوادگی، فرهنگی و اجتماعی را فهرست می‌کند و کانادا ازجمله کشورهایی است که موافقت کرده است تا به مفاد این سند پای‌بند باشد. گفتنی است که این کنوانسیون در کانادا قانون نیست، اما سندی مهم است تا در راستای کمک به کودکان و نوجوانان مفید واقع شود. امروزه در قانون کانادا در راستای محافظت و حمایت از شهروندان خود ازجمله قشر آسیب‌پذیری چون کودکان و نوجوانان، عموماً در سه سطح دولتی قوانینی وضع کرده‌اند که عبارت‌اند از: قوانین فدرال، شهرداری و قوانین سرزمینی/ استانی. در کانادا قوانینی وجود دارد که از تعدادی از حقوق و آزادی‌ها محافظت می‌کند و به افراد ذی‌نفع اجازه می‌دهد که در صورت عدم رعایت این حقوق و آزادی‌ها، رسماً شکایت کنند.

وقتی به حقوق بشر در کانادا اشاره می‌شود، معمولاً منظور آن دسته حقوق و آزادی‌هایی است که توسط چندین قانون محافظت می‌شوند. اولین مورد منشور حقوق و آزادی‌های کانادا، که شامل

حمایت‌هایی در موارد، آزادی‌های اساسی مانند مذهب، حقوق دموکراتیک مانند حق رأی و نامزدی برای مناصب دولتی، حق حفظ حریم خصوصی اشخاص، حقوق قانونی مانند حق عدم بازداشت یا زندانی شدن خودسرانه و درنهایت حقوق برابری که اشخاص را در برابر قوانینی که به‌طور ناعادلانه علیه گروه خاصی از مردم تبعیض قائل می‌شوند. حقوق از جنبهٔ دیگری نیز مشروط هستند؛ حقوق فردی باید در برابر حقوق دیگران سنجیده شود. به‌طور مثال حق آزادی بیان شخص به این معنی نیست که می‌تواند مطالبی را منتشر کند که هدف آن نفرت‌پراکنی علیه گروه خاصی از مردم باشد. در چنین مواردی دولت می‌تواند حقوق و آزادی‌های اساسی را محدود کند، اما تنها در صورتی که بتواند ثابت کند که این محدودیت در یک جامعهٔ آزاد و دموکراتیک، منطقی و بنا به صلاح‌دید و حفظ و تضمین حقوق و آزادی‌های دیگر اشخاص جامعه است.

منشور حقوق بشر بخشی از قانون کاناداست؛ این بدان معناست که تمام قوانین دیگر کانادا باید به حقوق و آزادی‌هایی که در آن آمده است، احترام بگذارند. قوانین حقوق بشر نیز از حقوق اساسی حمایت می‌کند. در کانادا، قوانین حقوق بشر توسط دولت‌های استانی، منطقه‌ای و فدرال برای محافظت در برابر تبعیض تصویب شده‌اند (اخوان و همکاران، ۱٤۰۰: ٦٥).

از منظر دیگر باید درنظر داشت که کانادا یکی از پیشروترین کشورها در زمینهٔ حفاظت از اطلاعات شخصی و حقوق دیجیتال محسوب می‌شود. اما با گسترش هوش مصنوعی، یادگیری ماشین، و ابزارهای هوشمند، چالش‌های مرتبط با حریم خصوصی کودکان در این کشور نیز رو به افزایش است. کودکان کانادایی در مدرسه، فضای مجازی، بازی‌ها، شبکه‌های اجتماعی و حتی وسایل هوشمند خانگی با فناوری‌هایی تعامل دارند که حجم عظیمی از داده‌های رفتاری، زیستی، مکانی و تحلیلی آن‌ها را جمع‌آوری و پردازش می‌کند.

در این رابطه، نظام حقوقی کانادا تلاش کرده است با ترکیبی از قوانین فدرال، قوانین استانی، و چارچوب‌های اخلاقی نوین، از این حق بنیادین پشتیبانی کند. این گونه نیز می‌توان گفت که کانادا به‌جای یک قانون واحد، چندین قانون کلیدی برای حفاظت از اطلاعات شخصی دارد که کودکان نیز ذیل آن‌ها حمایت می‌شوند. همان‌گونه که قبلاً اشاره شد مهم‌ترین قانون فدرال در زمینهٔ حفاظت از اطلاعات شخصی در حوزهٔ خصوصی بوده و نکات مهمی در این زمینه ارائه داشته است. نکتهٔ اولی که در قانون مذکور به‌چشم می‌خورد رضایت باید «آگاهانه و معتبر» باشد، است؛ با این توضیح که برای کودکان، دریافت رضایت والدین الزامی است، مگر در مواردی که کودک قادر باشد اثرات

مثبت یا منفی جمع‌آوری داده را درک کند. نکتهٔ بعدی اینکه جمع‌آوری داده باید حداقلی و متناسب باشد، با این توضیح که شرکت‌ها موظف‌اند روش‌های شفاف برای اطلاع‌رسانی به والدین دربارهٔ نحوهٔ پردازش دادهٔ کودکان ارائه دهند (Teresa, 2020: 11).

در برخی از ایالات کانادا قوانین استانی مهم، جامع‌تر و سخت‌گیرانه‌تری نسبت به دیگر ایالات وضع شده است، مانند قانون حریم خصوصی در بریتیش کلمبیا، قانون حریم خصوصی در آلبرتا، قانون حفاظت از اطلاعات شخصی در انتاریو در بخش سلامت. همچنین قانون کبک صراحتاً پردازش داده‌های کودکان را حساس دانسته و محدودیت‌های بیشتری اعمال کرده است.

با وجود قوانین قوی همچون قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی[1] که یکی از مهم‌ترین قوانین فدرال کانادا در حوزهٔ حفاظت از داده‌های شخصی است و قوانین استانی برای عصر هوش مصنوعی، خلأهای قانونی‌ای در این حوزه به‌چشم می‌خورد. چالش‌هایی ازقبیل ناتوانی قوانین در مدیریت یادگیری الگوریتمی، نبود مقررات اختصاصی دربارهٔ داده‌های بیومتریک کودکان، پوشش ناکافی آموزش برخط و فناوری‌ها، محدودیت در مقابله با پروفایل‌سازی مبتنی بر هوش مصنوعی.

معضل دیگر در این زمینه، گستردگی داده‌هایی است که کودکان ناخواسته تولید می‌کنند. هوش مصنوعی سعی می‌کند تا تمام رفتارهای کودک به دادهٔ تحلیل‌پذیر تبدیل کند که این امر دولت کانادا را به‌شدت نگران کرده است. همچنین سازمان‌های کانادایی بارها از اینکه شرکت‌های فرامرزی از داده‌های کودکان سوءاستفاده می‌کنند، شکایت کرده‌اند، اما اعمال جریمه یا کنترل عملی دشوار است که این امر چالشی پیچیده برای رقابت با شرکت‌های فناوری بزرگ ایجاد کرده است.

کانادا در مواجهه با این شرایط اقدامات و رویکردهای اصلاحی خاصی را درنظر گرفته است. یکی از این اصلاحات قانون پیشنهادی C-27[2] است که این قانون با هدف اصلاح PIPEDA مطرح شده و شامل مواردی چون ایجاد قانون جدید[3]، ایجاد قانون داده و هوش مصنوعی[4] جهت تنظیم و کنترل بهتر هوش مصنوعی، افزایش شدید جریمه‌ها، تعریف دادهٔ کودکان به‌عنوان دادهٔ بسیار حساس

1. PIPEDA
2. Canada’s Digital Charter Implementation Act (2022–2024)
3. CPPA (Consumer Privacy Protection Act)
4. AI and Data Act

است. اگر قوانین فوق‌الذکر در کانادا به تصویب نهایی برسد، این کشور یکی از پیشروترین نظام‌های حفاظت از کودکان خواهد بود.

علاوه بر موارد ذکرشده دربارهٔ کودکان داده‌های کودکان که همیشه «حساس» محسوب می‌شود دفتر کمیسیونر حریم خصوصی کانادا،[1] که مسئول حفاظت از حریم خصوصی افراد و نظارت بر اجرای قوانین مرتبط با داده‌های شخصی بوده، دستورالعمل‌های خاصی ارائه کرده است که این دستورالعمل‌ها شامل موارد زیر است: جمع‌آوری نباید بیش از نیاز باشد، کودکان نباید هدف‌گذاری الگوریتمی شوند، پروفایل‌سازی پرخطر باید محدود شود (Valerie & Bailey, 2015: 15).

همچنین سیاستگذاران کشور کانادا در جهت بهبود وضعیت حریم خصوصی کودکان و نوجوانان در محیط‌ها و پلتفرم‌های آموزشی در حال تدوین الزامات جدید هستند تا نه‌تنها برای افزایش سطح امنیت اهداف آموزشی بلکه برای اهداف تجاری و نه برای آموزش الگوریتم‌های دیگر گامی مؤثر بردارند.

در کل می‌توان به این نتیجه دست یافت که حق حفظ حریم خصوصی کودکان در کانادا، به‌عنوان یکی از اصول بنیادین حقوق بشر دیجیتال، با تهدیدهای جدی عصر هوش مصنوعی روبه‌روست. اگرچه نظام حقوقی کانادا یکی از پیشرفته‌ترین و سختگیرانه‌ترین نظام‌ها در حوزهٔ حفاظت از داده است، سرعت پیشرفت فناوری‌های هوش مصنوعی باعث ایجاد خلأهای مهمی در حفاظت از کودکان شده است.

۵. حمایت قانون فدرال از کودکان و نوجوانان

قانون فدرال CVRA به قربانیان حق خاصی برای شنیده شدن در توافقات اقرار به جرم و همچنین حق عمومی برای مشورت با دادستان‌ها را می‌دهد. همچنین به قربانیان اجازه می‌دهد، در صورت نقض حق شنیده‌شدنشان از طریق ماندامو‌س،[2] درخواست بازگشایی مجدد توافق‌نامه را بدهند. اکثر

1. Office of the Privacy Commissioner of Canada (OPC)

۲. در نظام حقوقی کانادا، درخواست ماندامو‌س، نوعی درخواست به دادگاه فدرال است که از دادگاه می‌خواهد یک مقام یا ارگان دولتی را وادار کند تا به وظیفهٔ خود عمل کند و این امر باعث تسریع در روند رسیدگی به پرونده می‌گردد؛ به عبارت دیگر ماندامو‌س دستوری از یک مقام بالاتر به زیردستان است که آن‌ها را موظف می‌کند وظیفهٔ خود را در یک بازهٔ زمانی معین و به‌درستی انجام دهند.

ایالت‌ها به‌طور مشابه دارای یک قانون یا مادهٔ قانون اساسی هستند که به قربانیان حق عمومی مشورت یا مشاوره با دادستان (که مسلماً شامل توافقات اقرار به جرم نیز می‌شود) یا حق خاصی برای شنیده شدن قبل از پذیرش درخواست توسط دادگاه را می‌دهند. دادگاه‌ها برای رد توافقات اقرار به جرم یا بازگشایی غیررسمی جلسات رسیدگی به درخواست جرم، برای اطمینان از رعایت تمام حقوق قربانیان، آزاد بوده‌اند (Alan et al., 2021: 27).

۶. در معرض خطر قرار گرفتن حریم خصوصی کودکان و نوجوانان کانادایی در برابر هوش مصنوعی

ظرفیت و شرایط کودکان برای اعمال حریم خصوصی خود با بزرگ‌سالان متفاوت است. کودکان ممکن است فاقد آگاهی باشند یا مهارت‌های سوادآموزی محدودی داشته باشند که بتوانند حق خود برای حفظ حریم خصوصی را به‌طور کامل درک کنند و خطرات و تأثیرات بالقوهٔ بلندمدت اشتراک‌گذاری داده‌ها و پردازش هوش مصنوعی را درک کنند. در حالی که کودکان و نوجوانان عموماً از نظر فناوری ماهر هستند و می‌خواهند حریم خصوصی خود را حفظ کنند، تمایل دارند تصور محدودتر و کم‌انتقادتری از حریم خصوصی دیجیتال داشته باشد. کودکان تمایل دارند حریم خصوصی را به شیوه‌های بین فردی یا بین خود و سایر افراد یا گروه‌های درنظر بگیرند. آن‌ها (مانند اکثر بزرگ‌سالان) برای درک حریم خصوصی خود در قالب‌های انتزاعی‌تر، تجاری یا نهادی (مانند نحوهٔ ردیابی یا استنتاج داده‌هایشان توسط هوش مصنوعی) تلاش می‌کنند، بنابراین ظرفیت محدودی برای ارزیابی خطرات مرتبط دارند. جعبهٔ سیاه یا همان هوش مصنوعی ارتباطات را بیشتر مبهم می‌سازد و بین ورودی‌ها و نتایج، ارزیابی ریسک حریم خصوصی را برای کودکان دشوارتر می‌کند.

حریم خصوصی کودکان چند وجهی است؛ شامل توانایی آن‌ها در کنترل داده‌هایشان، حرکت در فضاها با استقلال، برقراری ارتباط بدون رهگیری و تصمیم‌گیری مستقل می‌شود. همچنین به زمینه و رابطه بسیار وابسته است؛ ترجیحات حریم خصوصی کودکان شامل ملاحظات متعددی است، ازجمله اینکه چه چیزی درمورد زندگی خصوصی آن‌ها شناخته شده است، توسط چه کسی، برای چه اهدافی و با چه عواقبی. هوش مصنوعی با جمع آوری داده‌های کودکان و وارد کردن اطلاعات به الگوریتم‌ها برای دستیابی به عملکردهای مختلف با نظارت محدود، ممکن است خطرات بالقوه‌ای را برای همهٔ این جنبه‌های حریم خصوصی کودکان ایجاد کند. سه دستهٔ اصلی از

خطرات مربوط به حریم خصوصی کودکان از جانب هوش مصنوعی وجود دارد: خطرات داده‌ای، خطرات عملکردی و خطرات نظارتی (Zon & Lipsey, 2020: 14).

نتیجه

کودکان و نوجوانان ازجمله قربانیان استفاده از فضای مجازی و هوش مصنوعی هستند و هیچ گونه اطلاعی از حفظ حریم خصوصی ندارند و به راحتی ابزار دست مجرمان می‌شوند. به عبارت دیگر، کودکان ممکن است فاقد آگاهی باشند یا مهارت‌های سوادآموزی محدودی داشته باشند که بتوانند حق خود برای حفظ حریم خصوصی را به‌طور کامل درک کنند و خطرات و تأثیرات بالقوهٔ بلندمدت اشتراک‌گذاری داده‌ها و پردازش هوش مصنوعی را درک کنند. بنابراین ظرفیت محدودی برای ارزیابی خطرات مرتبط دارند. در این رابطه نیز دولت بایستی تدابیر حمایتی و پیشگیرانه در قالب آموزش والدین و کودکان و نوجوانان در استفاده از فضای مجازی اعمال کنند و با مجرمان در این زمینه برخورد قانونی مناسب صورت گیرد.

با مقایسهٔ تطبیقی دو نظام حقوقی در رابطه با حفظ حریم خصوصی کودکان و نوجوانان در ایران و کانادا، این نتیجه حاصل شد که کانادا دارای نظام پیشرفته‌تری در زمینهٔ حمایت کیفری و مقررات پیشگیرانه است، در حالی که ایران هنوز راه‌اندازی نظام جامع حفاظت داده را در دستور کار دارد. تفاوت اصلی دو نظام در میزان نهادهای نظارتی، ضمانت اجراهای کیفری، و سیاست‌گذاری داده‌محور است. به عبارت دیگر هوش مصنوعی و فضای دیجیتال، همان‌قدر که فرصت‌ساز هستند، می‌توانند تهدیدی جدی برای حریم خصوصی کودکان باشند. تفاوت اصلی میان ایران و کانادا در سطح قانون‌گذاری، نظارت و آموزش عمومی است، اما هیچ کشوری از این چالش مصون نیست. همچنین در جهت کاهش تهدیدات استفاده از هوش مصنوعی و فضای دیجیتال و حفاظت از کودکان و نوجوانان بایستی دولت‌ها در این زمینه همکاری کنند، همچنین فعالیت شرکت‌های فناوری با مسئولیت‌پذیری بیشتری عمل کنند و نهایتاً خانواده‌ها با افزایش آگاهی خود، محیط مجازی را برای کودکان و نوجوانانشان امن نگه دارند.

پیشنهاداتی که در این زمینه می‌توان مطرح کرد این است که با تدوین قانون جامع در رابطه با «حمایت از داده‌های شخصی کودکان» در ایران با تکیه بر مدل کانادایی و همچنین با ایجاد واحد تخصصی در پلیس فتا برای رسیدگی به جرائم نقض حریم کودکان و علاوه بر آن با الحاق رسمی به

پروتکل اختیاری سعی شود که در بهبود شرایط کودکان در فضای مجازی و استفاده از هوش مصنوعی و حمایت از حقوق آنان در این حوزه گامی جدی‌تر برداشته شود.

راهکارهایی را که در رابطه با چالش‌هایی که کودکان و نوجوانانی که در کانادا از هوش مصنوعی و فضای مجازی استفاده می‌کنند، تهدید می‌کند، می‌توان به محدودسازی تبلیغات هدفمند برای کودکان، کنترل سخت‌گیرانه‌تر فناوری تشخیص چهره، تقویت مقررات مرتبط با هوش مصنوعی در آموزش، استفاده از تنظیمات حریم خصوصی، آموزش مهارت «نه گفتن دیجیتال» به کودک، نظارت فعال و گفت‌وگو محور، استفاده از ابزارهای کنترل والدین اشاره کرد. همچنین تدوین قانون جامع حفاظت از داده‌های کودکان، الزام پلتفرم‌ها به شفافیت در استفاده از داده، توسعهٔ برنامه‌های آموزش سواد دیجیتال، ایجاد نهاد نظارتی مستقل، استفاده از تنظیمات حریم خصوصی، آموزش مهارت «نه گفتن دیجیتال» به کودک، نظارت فعال و گفت‌وگومحور، استفاده از ابزارهای کنترل والدین راهکارهایی هستند که در رابطه با چالش‌هایی که کودکان و نوجوانانی را که در ایران از هوش مصنوعی و فضای مجازی استفاد می‌کنند، تهدید می‌کند، می‌توان درنظر داشت.

حامی مالی:

این مقاله هیچ حامی مالی ندارد.

مشارکت نویسندگان:

منصوره حسینی: روش‌شناسی، تحلیل، نوشتن بررسی و ویرایش، تحقیق و بررسی، پیش‌نویس اصلی.

مجتبی فرهمند: مفهوم‌سازی، نظارت بر داده‌ها، اعتبارسنجی، مدیریت پروژه، منابع.

تعارض منافع:

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

ملاحظات اخلاقی:

این پژوهش بر پایهٔ مطالعهٔ اسناد، قوانین، رویه‌های قضائی و منابع کتابخانه‌ای انجام شده و در آن هیچ‌گونه مطالعه‌ای بر روی انسان، حیوان یا داده‌های شخصی صورت نگرفته است؛ بنابراین، اخذ

تأییدیهٔ کمیتهٔ اخلاق برای این پژوهش ضروری نبوده است. با این حال، نویسنده اصول امانت‌داری علمی، صداقت پژوهشی، استناددهی صحیح و رعایت حقوق مالکیت فکری را در تمامی مراحل پژوهش رعایت کرده است.

در تهیهٔ این مقاله از ابزارهای هوش مصنوعی مولد صرفاً برای کمک به ویرایش زبانی، بهبود ساختار نگارش و ارتقای خوانایی متن استفاده شده است. این ابزارها در طراحی پژوهش، تحلیل علمی، تفسیر یافته‌ها، استنتاج نتایج یا تصمیم‌گیری‌های پژوهشی نقشی نداشته‌اند و مسئولیت کامل صحت، اصالت و محتوای نهایی مقاله بر عهده نویسنده/ نویسندگان است.

موافقت نویسندگان:

تمامی نویسندگان نسخهٔ نهایی مقاله را مطالعه و تأیید کرده‌اند و با انتشار آن موافقت دارند.

منابع

اخوان، بهار، بینا،احمد و گودرزی، ساناز (۱٤۰۰)، گور حقوق بشر در پرتوی منشور حقوق و آزادی‌های کانادا، تهران: مؤسسهٔ صیانت از حقوق زنان، چاپ اول.

انصاری، باقر (۱۳۹۱)، «مطالعهٔ تطبیقی مسئولیت مدنی ناشی از نقض حقوق مربوط به شخصیت در رسانه‌ها»، نشریهٔ حقوق خصوصی، ۲، ٦۷-۹۹.

بویری منجی، معصومه و زارعی، مریم (۱٤۰٤)، «چالش‌های اخلاقی استفاده از هوش مصنوعی در مدارس ـ حریم خصوصی،امنیت داده‌ها و خطرات و سوگیری الگوریتمی»، اولین همایش بین‌المللی معلمان پیشرو در عصر پژوهش‌های تحول‌آفرین.

پورمسجدیان، فاطمه و ابراهیمی، سیدنصراله (۱۳۹۹)، «واکاوی حقوقی حمایت از حریم خصوصی کودک در فضای مجازی با نگاهی به قوانین ایران و معاهدات بین‌المللی»، نشریهٔ مطالعات زن و خانواده، ٤، ۸۲.

خلیلی، فاطمه و سوادی، زهرا (۱٤۰٤)، «قلمرو کودکی در عصر هوش مصنوعی: از کلاس‌های هوشمند تا نگرانی‌های خانه؛ مطالعهٔ پدیدارشناسانهٔ چالش‌های حریم خصوصی و اخلاقی کودکان از دیدگاه معلمان و والدین»، همایش بین‌المللی آموزش و پرورش در قرن بیست و یکم.

صفاری‌نیا، مهزاد (۱۴۰۳)، «هوش مصنوعی و حق بر آموزش کودکان»، فصلنامهٔ مطالعات فقه و حقوق رسانه، ۱، ۱۳۳-۱۵۲.

میرکمالی، سیدعلیرضا و صالح احمدی، سحر (۱۴۰۰)، قانون مجازات اسلامی در نظم حقوقی کنونی، تهران: انتشارات گالوس، چاپ چهارم، جلد دوم.

قوانین

قانون اساسی ایران.

قانون حمایت از اطفال و نوجوان مصوب ۱۳۹۹.

قانون جرائم رایانه‌ای اصلاحی مصوب سال ۱۳۹۹.

قانون مجازات اسلامی.

قانون حمایت از کودکان و نوجوانان و خانواده‌ها کانادا، مصوب ۲۰۲۰.

منشور حقوق بشر و آزادی‌های کانادا ۲۰۲۵.

References

Young, A. N., & Dhanjal, K. (2021). *Victims' Rights in Canada in the 21st Century*. Ottawa: Department of Justice Canada.

Barassi, V. (2020), *Child Data Citizen: How Tech Companies Are Profiling Us from before Birth*, MIT Press.

Chapdelaine.C. (2007), Child Justice in Canada and The Four Ps: Protection, Prosection, Prevention and Participation, Springer Science+Business Media B.V, P.268.

Montgomery, K., Chester, J., & Milosevic, T. (2017), *Ensuring young people's digital privacy as a fundamental right*, International Data Privacy Law.

Teresa, S. (2020), "Privacy and the Open Internet in Canada", *Journal: Canadian Journal of Law and Technology*, vol18, no1, CanLIIDocs 4179.

Valerie, S., & Bailey, J. (2015), *Privacy and the Digital Generation*, Published in: University of Ottawa Press.

Zon, N., & Lipsey, A. (2020), STANDARDS RESEARCH Children's Safety and Privacy in the Digital Age, Springboard Policy, p.14.

https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf

United Nations, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, OHCHR - Convention on the Rights of the Child.