

Protecting Children's Privacy in the Digital Environment

حماية خصوصية الأطفال في البيئة الرقمية

Dahmani Fatima ¹, Abderrezzaq Brada ²

¹ M'sila University (Algeria), Fatima.dahmani@univ-msila.dz

² Relizane university (Algeria), abderrezzaq.brada@univ-relizane.dz

Received: 17/06 /2025

Accepted: 30/10 /2025

Published: December /2025

الملخص:

تتناول هذه الورقة البحثية موضوع حماية خصوصية الأطفال في البيئة الرقمية، بوصفه من القضايا الراهنة التي حظيت باهتمام متزايد في الدراسات الإنسانية والقانونية، نظراً لكون الأطفال يشكلون فئة هشة تتعرض بشكل متنامٍ لانتهاكات رقمية نتيجة للتطور التكنولوجي الذي امتد إلى مختلف مجالات الحياة الخاصة. وتكتسي هذه الفئة أهمية بالغة باعتبارها تمثل الجيل الذي تراهن عليه المجتمعات في تحقيق التنمية المستقبلية، ما استدعى من المشرعين والفقهاء بذل جهود مكثفة على المستويين الدولي والوطني من خلال الاتفاقيات والمواثيق الدولية وسن التشريعات الداخلية ذات الصلة. وقد اعتمدت الدراسة المنهج الوصفي التحليلي لوصف الظاهرة ومراجعة الأدبيات العلمية وتحديد أبعادها الأساسية، وانتهت إلى التوصية بضرورة إدراج حماية الخصوصية الرقمية للأطفال ضمن قانون حماية المعطيات الشخصية، من خلال نصوص قانونية مفصلة تضمن تعزيز الأمن السيبراني وحماية حقوق الطفل الرقمية.

الكلمات المفتاحية: الطفل، الخصوصية الرقمية، البيئة الرقمية، القانون، الأمن السيبراني.

Abstract:

This paper explores the issue of safeguarding children's privacy in the digital environment a contemporary and increasingly significant concern within both the humanities and legal scholarship. The growing exposure of children, as a particularly vulnerable social group, to digital violations resulting from rapid technological advancements affecting various aspects of private life underscores the urgency of this topic. Children occupy a crucial position as the generation upon which societies depend for sustainable future development, which has prompted concerted efforts by legislators and legal experts at both international and national levels. These efforts are reflected in the adoption of international agreements and conventions, as well as the enactment of national legislation aimed at regulating and ensuring digital protection.

The study employs a descriptive-analytical methodology to examine the phenomenon, review relevant scholarly literature, and delineate its fundamental dimensions. It concludes with a set of recommendations, most notably the incorporation of provisions dedicated to children's digital privacy within the Personal Data Protection Law. Such inclusion should be supported by detailed legal frameworks that reinforce cybersecurity measures and guarantee the protection of children's digital rights.

Key words: children, digital privacy, digital environment, legislation, cybersecurity.

Introduction:

The digital revolution has precipitated profound and rapid transformations across diverse domains of social, cultural, and economic life, fundamentally restructuring communication and media ecosystems. The repercussions of this transformation extend far beyond patterns of interaction and production; they have also generated complex challenges concerning the protection of vulnerable social groups, particularly children. (Abderrezzaq, 2024, p.31)

Given the early and increasing involvement of children in digital environments, the risks associated with the exploitation of their personal data have intensified especially within the sphere of digital advertising, which represents one of the most influential mechanisms shaping attitudes, preferences, and behaviors. This situation raises critical legal and ethical questions regarding the extent to which children's rights are safeguarded in digital contexts and how to reconcile those rights with the commercial interests driving data utilization.

Recent scholarly investigations converge on the alarming rise of violations targeting children's digital privacy, notably through smartphone applications, interactive video platforms, and online gaming environments. Such exposure renders children susceptible to recurring breaches of their privacy, thereby affecting their psychological well-being and social development. In response to these challenges, a range of international legal frameworks have been established to ensure stronger regulatory protection for children in the digital sphere. These include the Convention on the Rights of the Child (CRC) and General Comment No. 25 on children's rights in the digital environment, the General Data Protection Regulation (GDPR), and the Children's Online Privacy Protection Act (COPPA), in addition to the ethical and procedural guidelines formulated by organizations such as UNICEF and UNESCO (Livingstone et al., 2018; Montgomery et al., 2017; UNICEF, 2020).

However, despite the considerable progress achieved globally in the legislative and regulatory protection of children's digital privacy, many developing nations—Algeria included—continue to face substantial challenges in adapting and updating their national legal systems. Regular legislative reform remains essential for addressing emerging forms of deviant behavior in the digital realm and for integrating international norms into domestic frameworks. Such efforts are crucial for ensuring effective governance of institutions responsible for safeguarding children's privacy online. This need is particularly urgent given the accelerating pace of digital transformations, the novelty of the issue in the Algerian context, and the scarcity of empirical and analytical research on the subject. These realities underscore the necessity of conducting a critical assessment of international regulatory frameworks and comparing them with the national legislative landscape. (Dahmani & Brada, 2025, p.152).

Accordingly, this article undertakes a descriptive and analytical exploration of the protection of children's digital privacy. It begins by clarifying the conceptual foundations of digital privacy as they relate to children and outlining the key risks arising from privacy infringements. The second section examines the international frameworks that govern the protection of children's online privacy, with particular attention to global instruments such as the United Nations Convention on the Rights of the Child (CRC) and the European Union's

General Data Protection Regulation (GDPR). The third section analyzes the Algerian experience, focusing on the legal measures currently in place and the challenges confronting their implementation. It also compares Algeria's national legislation with international standards to determine the degree of alignment between them.

This study is therefore guided by the following central research question:

How is the protection of children's digital privacy regulated within the international legal framework, and to what extent does Algerian legislation conform to these standards?

From this central question, several sub-questions emerge:

1. What constitutes the conceptual framework of children's digital privacy?
2. What are the principal international frameworks and standards that regulate the protection of children's privacy in digital contexts?
3. What is the nature of Algeria's experience in protecting children's digital privacy, and what challenges does it face?
4. To what extent are Algerian legislative practices aligned with international ethical principles and legal norms?

1- The Methodological Framework of the Study

1.1-Significance of the Study

The protection of children's digital privacy has emerged as a critical subject of inquiry within contemporary academic discourse, reflecting the increasing prevalence of children's engagement with the internet and digital technologies. This growing digital participation has been accompanied by a parallel escalation in online risks and threats specifically targeting this demographic, primarily through their recurrent exposure to digital content that compromises their personal data and privacy.

Despite the existence of comprehensive international legal and ethical frameworks designed to safeguard children in digital spaces, the Algerian legislative landscape still necessitates a rigorous examination of its degree of alignment with these global standards. It equally requires a deeper analytical understanding of the Algerian experience and a clear identification of the principal challenges that impede effective implementation in this domain.

The significance of this study thus lies in its dual theoretical and practical contributions. Theoretically, it enriches the body of scientific literature by addressing a relatively underexplored yet increasingly pressing issue children's privacy in the digital environment from a modern sociotechnical and legal perspective. Practically, the research offers applied insights relevant to the fields of digital media studies and cyber legislation, thereby providing a framework that can inform policymakers, researchers, and institutions concerned with child protection in Algeria's evolving digital ecosystem.

1.2-Objectives of the Study

This study seeks to achieve the following objectives:

- A. To present the conceptual framework underpinning the notion of children's privacy in the digital environment.

- B. To analyze and critically review international frameworks and standards that regulate the protection of children's privacy in digital contexts.
- C. To explore the Algerian experience and identify the main challenges associated with protecting children's privacy online.
- D. To evaluate the extent of congruence between Algerian legislation and the guidelines of international legal frameworks governing member states' obligations in this field.
- E. To propose practical and policy-oriented recommendations aimed at strengthening the mechanisms for protecting children's digital privacy in Algeria.
- F.

1.3-Study Methodology

The study employs a descriptive and analytical research design, suitable for examining complex sociotechnical and legal phenomena such as the protection of children's digital privacy. This methodological approach enables both the systematic description of the issue under investigation and the analytical interpretation of relevant empirical and legislative data.

Accordingly, the study involved a comprehensive review and classification of the scientific literature, encompassing academic books, peer-reviewed journal articles, and international legal instruments. The sources were retrieved from reputable academic databases, including Web of Science, Scopus, ERIH PLUS, and ASJP.

The analysis focused on three principal dimensions:

- A. The conceptual and theoretical foundations of digital privacy as it pertains to children;
- B. The international frameworks and legal instruments that govern the protection of children's privacy in the digital environment; and
- C. The Algerian legislative context, assessing the degree of compliance with international standards and identifying existing gaps.

Through this framework, the study aims to provide a nuanced understanding of both global and national dynamics shaping the protection of children's digital privacy, offering an evidence-based foundation for future policy and academic initiatives.

2- Children's Digital Privacy

2.1-The Concept of Children's Digital Privacy

Children's digital privacy represents one of the most pressing contemporary concerns in cyberspace. Scholars and policymakers have become increasingly attentive to the mechanisms through which digital applications and online platforms collect, process, and disseminate children's personal data especially in light of the proliferation and diversity of digital content directed toward young audiences. This growing complexity necessitates a clear and comprehensive conceptualization of children's digital privacy grounded in academic literature and international legal standards. (Dahmani & Brada, 2025, p. 130)

In the scholarly context, children's digital privacy is often defined as a set of rights, safeguards, and regulatory controls that ensure the protection of children's personal and digital data during their interaction with technological tools and digital environments, including websites, mobile applications, and social media platforms. Its central objective is to prevent the unauthorized collection, processing, or dissemination of children's information

without the explicit and lawful consent of their parents or legal guardians, while upholding the child's right to digital safety, informational autonomy, and privacy of their electronic identity (Sun et al., 2023, p. 7).

The United Nations Children's Fund (UNICEF), in its General Comment No. 25 (2021), further clarifies that children's digital privacy encompasses "the right to the protection of personal data, the right not to be subjected to unauthorized digital surveillance or tracking, and the obligation to ensure that all processing of children's data is consistent with the principle of the best interests of the child" (UNICEF, 2021, p. 5).

Similarly, Medjkoune et al. (2023, p. 112) highlight that digital privacy extends beyond the mere protection of identifiable personal information such as name, address, or geographic location to include digital identity data, such as cookies, browsing history, and geolocation metadata. They emphasize that children should retain agency and control over their data within the digital ecosystem. In this regard, Steinberg (2023, p. 14) underscores that the essence of digital privacy lies in ensuring that children and their guardians can make informed decisions regarding data collection and sharing, supported by transparency in data-handling practices and mechanisms of accountability for service providers.

Furthermore, the Electronic Privacy Information Center (EPIC, 2022, p. 2) stresses that digital privacy should be understood as an inalienable child's right to safeguard their personal information from unauthorized collection, usage, or disclosure. This principle is particularly significant when considering international legal frameworks such as the Children's Online Privacy Protection Act (COPPA) which mandate verifiable parental consent prior to collecting personal data from children under the age of 13.

Given the exponential growth of digital targeting and data-driven advertising aimed at children, protecting digital privacy has become a policy imperative directly tied to the preservation of children's broader rights to freedom of expression, protection, and the formation of a secure digital identity. Consequently, contemporary research continues to highlight the necessity of developing an integrated legal and ethical framework that reconciles the opportunities offered by digital technologies with the imperative of safeguarding children's privacy and cybersecurity. This need is particularly urgent in developing societies, where legislative mechanisms and enforcement capacities remain limited, thereby exposing children to heightened digital vulnerabilities.

2.2-Risks Associated with Violations of Children's Digital Privacy

Over the past few decades, the digital environment has become an inseparable component of children's daily lives, permeating their educational, social, and recreational experiences. It has created unprecedented opportunities for communication, creativity, and cognitive development. However, this deep integration into the digital world has also introduced a wide spectrum of risks related to the violation of children's digital privacy. (Dahmani & Brada, 2025, p.115)

International organizations such as UNICEF and the OECD consistently highlight that children are not merely passive users of the internet; rather, they are active participants who face escalating threats to their privacy and personal data. These risks arise through the

pervasive collection and exploitation of information ranging from requests for geolocation permissions and the extensive use of data trackers to the extraction of unnecessary user permissions, behavioral analytics, and personalized advertising. In many cases, children engage with digital platforms that lack both ethical oversight and robust legal safeguards, prompting critical concerns about whether this vulnerable group is adequately protected from practices that harvest their data for commercial or marketing purposes without proper consent or regulatory supervision.

The main categories of these violations can be summarized as follows:

A-Exploitation of Children's Limited Cognitive Maturity

Empirical studies demonstrate that children's insufficient legal and cognitive awareness renders them particularly vulnerable to manipulative data collection practices. Digital advertising often capitalizes on this developmental vulnerability, as children are unable to recognize or fully comprehend the implications of consenting to data collection or engaging with persuasive commercial content (Medjkoune et al., 2023, p. 3).

B-Construction of Children's Digital Profiles

Early and continuous tracking of children's online activities results in the creation of what scholars describe as a "digital profile" a lasting data footprint that may compromise their privacy and autonomy in constructing an independent digital identity (Moti et al., 2023, p. 4). Research further warns that these practices extend beyond behavioral monitoring to include the exploitation of children's emotional and entertainment preferences, especially through seemingly innocuous games or multimedia content that covertly embed advertising strategies. This constitutes a dual violation: the erosion of digital privacy and the reinforcement of consumerist tendencies (Sun et al., 2023, p. 6).

C- Uneven Enforcement of Legal Frameworks

Although international conventions such as the Convention on the Rights of the Child (CRC) and legislative instruments like the Children's Online Privacy Protection Act (COPPA) and the General Data Protection Regulation (GDPR) impose clear restrictions on the exploitation of children's data, implementation remains inconsistent across jurisdictions. In many developing countries, including those with emerging digital infrastructures, national legal systems still lack specific provisions explicitly prohibiting the tracking and commercial exploitation of children's data (UNICEF, 2021; FTC, 2025).

D-Impact on Digital Identity Formation

Digital environments particularly interactive games and social media applications—play a significant role in shaping children's digital self-concept. The continuous exposure to personalized advertising content molds children's online identities around consumerist preferences and market-oriented values. Such processes risk fostering an early sense of self that is defined by material consumption and commercial validation, which may have enduring psychological and social consequences (Moti et al., 2023).

E-Behavioral and Psychological Consequences

A growing body of research links the excessive exposure of children to digital advertising with early consumerist orientations, heightened materialism, and greater brand attachment. These tendencies undermine the development of healthy consumer values and

distort children's self-image in the digital environment (Montgomery et al., 2022). Furthermore, by exploiting children's limited critical awareness, advertisements construct associations between happiness, success, and material possession ultimately contributing to psychological issues such as social anxiety, low self-esteem, and chronic dissatisfaction (Auxier et al., 2023).

F-Promotion of Unhealthy Consumer Behaviors

Repetitive exposure to targeted commercial content fosters impulsive and irrational consumption patterns. Children may develop persistent urges to acquire unnecessary goods or pressure their parents to purchase items linked to popular characters or interactive games used in marketing campaigns. Such dynamics not only encourage unsustainable consumer behaviors but also impose emotional and financial strain within families (Livingstone & Stoilova, 2021).

G- Reinforcement of Digital Social Inequalities

Targeted advertising algorithms frequently deepen digital and social disparities among children from different socioeconomic backgrounds. Premium or exclusive digital content is typically directed at children with higher purchasing power, reinforcing digital stratification and class-based differentiation (James et al., 2020, p. 43). These practices perpetuate the portrayal of children primarily as consumers rather than as rights-bearing individuals, raising serious ethical concerns related to digital socialization, equity, and digital citizenship (UNICEF, 2021).

In conclusion, protecting children from targeted digital advertising and invasive data practices transcends the domain of cyber privacy. It constitutes a multidimensional issue encompassing health, psychological well-being, social equity, and cultural development. Addressing these risks requires an integrated legislative and ethical approach that ensures a safe, just, and child-centered digital environment. In recognition of this necessity, recent international instruments such as the COPPA 2.0 Amendment (2025) have strengthened restrictions on data collection from minors and reaffirmed the requirement for explicit parental consent to safeguard the best interests of the child in cyberspace (Federal Trade Commission, 2025, p. 12).

3-International Frameworks for Protecting Children's Digital Privacy

In recent decades, there has been growing international concern about protecting children's privacy in the digital environment, particularly amid the unprecedented expansion of digital media use and the increasing instances of privacy violations targeting minors. Research indicates that children constitute a primary target group within digital content strategies, due to their high susceptibility to influence and their limited cognitive ability to distinguish between editorial and commercial content (Livingstone et al., 2018). Consequently, the international community has developed a range of legal and regulatory frameworks aimed at safeguarding children from digital risks especially concerning the collection, processing, and use of their personal data for advertising and commercial purposes.

3.1-The United Nations Convention on the Rights of the Child (CRC)

The Convention on the Rights of the Child (CRC), adopted by the United Nations General Assembly in 1989, constitutes a foundational legal instrument that establishes the

global framework for protecting children's rights in all dimensions, including the rights to privacy, dignity, and protection from exploitation. Article 16 of the Convention explicitly stipulates that “No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation,” thereby obliging States Parties to enact appropriate legislative and administrative measures to uphold this right.

With the rapid evolution of digital technologies, the online environment has become increasingly complex, presenting new challenges related to children's digital privacy, especially given the growing prevalence of digital content directed at minors and the commercial exploitation of their personal data. In this context, legal scholarship has consistently identified the CRC as the primary reference framework guiding national and international legislation on protecting children in digital media environments (UNICEF, 2020).

To reinforce this position, the United Nations Committee on the Rights of the Child issued General Comment No. 25 (2021) on children's rights in the digital environment, which updated the interpretation of the Convention to reflect digital realities. This Comment underscored the necessity of protecting children from exploitative online advertising practices, emphasizing that advertising directed at children whether through apps, social networks, or gaming platforms may constitute a violation of their rights to privacy and protection from commercial exploitation.

3.2-The General Data Protection Regulation (GDPR) in the European Union

The General Data Protection Regulation (GDPR), adopted by the European Union in 2016 and enforced as of May 25, 2018, represents one of the most comprehensive and stringent global legal frameworks for personal data protection in the digital era. The GDPR devotes particular attention to children's rights, recognizing them as a vulnerable group frequently targeted by digital tracking mechanisms and personalized advertising systems.

Article 8 of the GDPR explicitly safeguards children's privacy in relation to information society services such as social networks, gaming platforms, and mobile applications. It mandates that service providers obtain explicit parental consent before processing the personal data of children under 16 years of age, with Member States permitted to lower this threshold to 13 years (European Union, 2016).

Furthermore, the Regulation emphasizes several key obligations:

A-The design of clear and age-appropriate privacy policies aligned with children's cognitive capacities.

B-The prohibition of collecting sensitive data without legitimate legal grounds.

C-The restriction of behavioral advertising aimed at minors, including the use of tracking tools and personalized content derived from browsing behavior or inferred interests.

Regarding digital content, the GDPR mandates that all processing of children's personal data for commercial or marketing purposes must adhere to the principle of the best interests of the child, as articulated in the CRC. Behavioral advertising directed at minors is

considered a high-risk practice that requires parental authorization and ensures the child's right to withdraw consent at any time. (Brada & Dahmani, 2025)

Empirical assessments and comparative studies indicate that the GDPR has become a global legislative benchmark, inspiring numerous countries to integrate similar child-centered privacy protections within their national data protection laws (Livingstone et al., 2018).

3.3-The Children's Online Privacy Protection Act (COPPA 2.0)

The Children's Online Privacy Protection Act (COPPA), enacted by the United States Congress in 1998, represents the first global legislative initiative dedicated exclusively to regulating the collection and use of children's personal data in the digital environment. Recognizing the rapid pace of technological innovation and the proliferation of digital content directed at minors, the Act was substantially amended in 2025 through the introduction of COPPA 2.0, which aims to strengthen privacy protections in response to emerging digital practices.

The Act establishes a clear prohibition against the collection, processing, or dissemination of personal information from children under the age of 13 without obtaining verifiable parental consent. It also obliges websites, gaming applications, and social media platforms either directed toward children or likely to attract them, to provide clear, accessible, and age-appropriate privacy notices explaining how personal data are collected, stored, and used.

The 2025 amendment (COPPA 2.0) introduced several key innovations designed to address the complexities of the contemporary digital ecosystem:

A-Expanding the scope of personal data to encompass device identifiers, geolocation data, browsing patterns, and behavioral interactions within digital applications.

B-Restricting digital advertising aimed at children by prohibiting behavioral targeting technologies, including cookies and algorithmic profiling, unless explicit parental consent is obtained.

C-Mandating high default privacy settings for minors, thereby preventing the automatic sharing of personal data with third parties for advertising or analytics purposes.

D-Imposing significant financial penalties on non-compliant entities, reaching up to \$50,000 per individual violation.

E-Enhancing parental control tools, enabling guardians to monitor, manage, and restrict the collection and use of their children's personal information.

According to the 2025 Annual Report of the U.S. Federal Trade Commission (FTC), these amendments seek to address the growing challenges posed by personalized advertising and embedded commercial content in video games and streaming platforms identified as primary sources of cyber threats to children's digital privacy (FTC, 2025, p. 12).

In this regard, COPPA has evolved into a normative reference model for developing child-focused data protection policies worldwide. Scholars emphasize that its principles can foster greater legal and social awareness of the risks associated with digital content directed at minors particularly regarding privacy breaches, data exploitation, and the promotion of premature consumerist behaviors (James et al., 2020; Montgomery et al., 2022).

3.4-UNICEF and UNESCO Guidelines on Children's Digital Rights

Children's rights in the digital environment have become a central concern for international organizations. Among the most influential actors in this domain are the United Nations Children's Fund (UNICEF) and the United Nations Educational, Scientific and Cultural Organization (UNESCO), both of which have issued comprehensive guidelines and policy recommendations aimed at enhancing the protection of children's privacy and wellbeing online.

As digital ecosystems evolve, there has been a notable surge in digital content targeting children, often employing technologies that collect personal and behavioral data through interactive platforms, gaming environments, and algorithmic systems (UNICEF, 2017). In response, both UNICEF and UNESCO have intensified efforts to safeguard children's digital rights and mitigate the risks posed by exploitative advertising and data-driven content.

In 2021, UNESCO underscored the need to raise public and institutional awareness about the implications of data collection practices involving minors. It called upon families, educators, and policymakers to adopt proactive strategies for regulating interactive advertising and commercial content that targets children directly, citing its detrimental effects on children's privacy, autonomy, and consumer socialization.

These international guidelines advocate for a multilateral and collaborative approach that integrates the efforts of governments, private sector actors, and civil society organizations to ensure a safe, ethical, and inclusive digital environment for children. They emphasize alignment with the core principles of the Convention on the Rights of the Child and the standards of responsible digital governance, reinforcing the notion that protecting children's privacy online is a shared global responsibility (UNESCO, 2021).

4-The Algerian Experience and its Challenges in Protecting Children's Digital Privacy

4.1-The Algerian Experience in Protecting Children's Digital Privacy

Over the past decade, Algeria has undertaken notable legislative efforts to align its national frameworks with the evolving global standards for personal data protection in the digital environment. These efforts have emerged in response to the rapid expansion of internet access and the exponential growth of digital media use among children and adolescents. According to Statista (2024), the number of internet users in Algeria reached approximately 54.9 million in 2024, with children aged 0–17 years representing nearly 35% of the total population. This implies that millions of Algerian children are active participants in or at least exposed to digital environments and online advertising content.

At the same time, social media advertising expenditures in Algeria reached an estimated \$36.2 million in 2024, with projections indicating a rise to \$74.5 million by 2028. This significant and growing digital advertising activity underscores the legislative gap between the existing legal frameworks which lack explicit provisions concerning children's data privacy in digital advertising and the rapidly evolving digital practices targeting younger audiences.

The cornerstone of Algeria's data protection framework is Law No. 18-07 of June 10, 2018, concerning the protection of individuals in the processing of personal data. The law enshrines key principles such as consent, purpose limitation, data minimization, and security of processing, while also establishing the National Authority for the Protection of Personal Data. However, the legislation does not include specific provisions addressing children's data privacy, making only a general reference to "vulnerable groups." Consequently, the absence of child-specific safeguards leaves minors particularly exposed to online data collection and commercial exploitation.

Additionally, Executive Decree No. 20-229 of 2020, which regulates digital media activities, obliges service providers to block content harmful to minors, yet it does not extend its provisions to data privacy or digital advertising practices directed at children (Ben Ammar, 2021). Similarly, Law No. 09-04 of 2009 on cybercrime prevention includes measures to combat child exploitation and online pornography but omits any reference to data privacy or advertising-related violations.

From a media regulation perspective, Law No. 12-05 of 2012 establishes controls over media activity and prohibits content deemed offensive to children. However, it lacks specific mechanisms to monitor or restrict digital advertising and data-driven marketing aimed at minors. In the commercial domain, the Consumer Protection Law No. 09-03 of 2009 addresses misleading advertisements and unfair commercial practices targeting vulnerable populations but again fails to include explicit clauses concerning children's exposure to digital marketing and data profiling.

In light of the rapid digital transformation, the Ministry of Digitization and Statistics launched a draft Cybersecurity Law in 2022, which introduces provisions related to user data protection, including measures for children. Nevertheless, the draft remains under governmental review, and its implementation has yet to materialize.

Despite the establishment of the National Authority for the Protection of Personal Data, its operational capacity remains limited, and there are no comprehensive regulatory guidelines or enforcement mechanisms for digital content directed at children. Reports from consumer protection associations (2022) have documented a notable rise in unregulated advertisements within gaming applications and social media platforms, which frequently employ data-driven personalization techniques without adequate oversight (Boucharb, 2022).

In summary, Algeria's current legal framework for protecting children's digital privacy remains fragmented and largely reactive, characterized by general personal data protection principles without child-specific regulatory instruments. This legal vacuum, combined with the rapid growth of digital media and advertising, amplifies the risks of data exploitation, profiling, and commercial manipulation among Algerian children.

4.2-Current Challenges of Protecting Children's Digital Privacy in Algeria

The digital environment in Algeria, as in many developing countries, faces a complex array of challenges in protecting children's online privacy. These challenges have become more acute with the rapid growth of digital advertising technologies that rely on artificial intelligence (AI) and behavioral tracking mechanisms. The interaction between weak regulatory capacity and fast-paced technological development has created significant gaps

between legal intent and practical enforcement. These challenges can be analyzed across six interrelated dimensions: technical, legal, economic, political and institutional, social, and implementation levels.

A-Technical Challenges

The accelerated development of AI algorithms and user-targeting systems has made it increasingly difficult to monitor and control the use of children's personal data. Digital advertisements directed at children often rely on advanced tracking technologies that collect highly sensitive information such as geolocation, personal preferences, and browsing behavior frequently without parental knowledge or consent (Livingstone et al., 2019).

In the Algerian context, Ben Yamina (2022) highlights the limited adoption of technical safeguards by both local and international platforms operating in Algeria, as well as the absence of reliable mechanisms to verify the age and identity of minor users. Consequently, children's data remain vulnerable to unauthorized collection, profiling, and commercial exploitation through unregulated digital systems.

B-Legal Challenges

Although Law No. 18-07 (2018) represents a positive step toward data protection, its provisions remain generalized and insufficiently adapted to the unique vulnerabilities of children in the digital space. Bouchareb (2022) emphasizes that this legislative gap stands in contrast to international frameworks such as the General Data Protection Regulation (GDPR), which provides explicit protections for children and imposes restrictions on behavioral advertising (European Commission, 2023).

Furthermore, despite the establishment of the National Authority for the Protection of Personal Data, its oversight capacity remains limited. As Ben Ammar (2021) notes, the absence of operational enforcement mechanisms renders many legal provisions declarative rather than effective, weakening the deterrent power of Algeria's personal data legislation in the face of growing privacy violations.

C-Economic Challenges

From an economic standpoint, Algeria continues to struggle with limited investment in digital infrastructure and institutional capacity. According to OECD (2022) data, national spending on digital transformation does not exceed 0.5% of GDP, a figure significantly below international benchmarks. This underinvestment constrains the ability of relevant institutions to deploy advanced monitoring technologies or attract qualified technical experts specialized in cybersecurity and data protection.

Similarly, UNCTAD (2023) reports that Algeria counts only 18 skilled digital privacy professionals per million inhabitants, compared to a regional average of 64 professionals per million. This scarcity of human capital contributes to the slow implementation of digital laws and the absence of effective oversight mechanisms for digital advertising and child-targeted data collection.

D-Political and Institutional Challenges

At the political level, the lack of a clear national prioritization of digital privacy within Algeria's digital transformation agenda constitutes a major obstacle. Government strategies tend to emphasize administrative digitization and e-governance, rather than the protection of individual digital rights.

According to UNICEF (2023), effective protection of children's online privacy in North Africa requires integrating child protection strategies into national digital policies. Algeria has taken steps in this direction by working toward greater institutional independence and coordination among the Ministry of Digitization and Statistics, the Ministry of Communication, and the National Authority for the Protection of Personal Data. However, as noted by the World Bank (2023), coordination gaps and overlapping competencies continue to undermine the coherence and efficiency of policy implementation.

E-Socio-Cultural and Awareness Challenges

The lack of digital literacy and social awareness represents one of the most persistent barriers to protecting children in cyberspace. A study by Boumaaraf (2023) found that 71% of Algerian families lack sufficient knowledge about available privacy protection mechanisms and do not use parental control tools integrated into applications and platforms. Moreover, educational and media institutions have yet to develop systematic programs in media and digital literacy, leaving families and schools with limited capacity to guide children toward safe and responsible digital behavior.

This social deficit contributes to the normalization of risky online practices among minors and exacerbates their exposure to commercial exploitation and digital manipulation.

F-Implementation and Enforcement Challenges

Digital oversight mechanisms in Algeria remain weak and fragmented due to the limited technical and human resources of competent authorities. The country lacks a unified national monitoring system capable of tracking violations related to digital advertising targeting children. Field studies conducted by Boucharb (2022) and CNIL (2022) reveal that insufficient cooperation between the public and private sectors further weakens enforcement capacity, as no formal partnerships exist with technology companies to ensure compliance with child data protection standards.

5-Comparison between International Frameworks and Algerian Legislation on Protecting Children's Privacy in the Digital Environment

The data presented in Table (No. 1), which compares international frameworks and Algerian legislation concerning the protection of children's digital privacy, reveal limited areas of convergence alongside multiple gaps across three primary dimensions: criminal, procedural, and cooperative frameworks. These gaps stem from the rapidly evolving and complex nature of the digital environment, which necessitates the continuous adaptation of national laws to ensure effective protection for vulnerable groups, particularly children (Livingstone et al., 2021).

At the criminal level, Algerian legislation largely aligns with the main international legal reference in this field – the Budapest Convention on Cybercrime. Article (9) of the Convention explicitly criminalizes the production, distribution, possession, and dissemination of child pornographic material and obliges member states to incorporate these prohibitions into their domestic legislation. Similarly, the Convention on the Rights of the Child (CRC) and its General Comment No. 25 emphasize the protection of children in digital spaces, especially concerning the processing of their personal data. Complementing these instruments, the European General Data Protection Regulation (GDPR) establishes the principle of the “right to be digitally forgotten”, granting children and their families the ability to request the deletion of personal data or images shared online.

In contrast, Algerian legislation includes several complementary legal provisions. Law No. 04-15 amending the Penal Code and Law No. 09-04 on cybercrime criminalize the misuse of information and communication technologies, covering offenses such as cyberbullying, online sexual exploitation of minors, and the dissemination of pornographic material. Likewise, Law No. 15-12 on Child Protection (2015) underscores the state's obligation to protect minors from all forms of exploitation, including those facilitated by electronic media. Nevertheless, Algerian laws still require stronger enforcement mechanisms and more stringent oversight to achieve effective deterrence.

From a procedural standpoint, Algeria has undertaken significant reforms between 2017 and 2020, notably amending its Code of Criminal Procedure to include provisions related to digital evidence. These amendments authorize judicial authorities to collect, track, and preserve electronic data under specific legal conditions and judicial authorization, consistent with the procedural foundations set out in Articles 16–21 of the Budapest Convention. Additionally, Law No. 18-07 established the National Authority for the Protection of Personal Data, reflecting Algeria's efforts to align with international procedural standards. However, as Bencheneb (2022) notes, the Authority's operational role remains limited, requiring greater institutional empowerment to ensure the effective implementation of data protection laws.

Table No. 1: Comparison between International Frameworks and Algerian Legislation in Protecting Children’s Privacy in the Digital Environment

Aspect	International Law	Algerian Legislation
Criminal Framework	• The criminalization of child pornography is established under Article 9 of the Budapest Convention, which obliges States Parties to impose penalties for the production, distribution, possession, or dissemination of any pornographic material involving the sexual exploitation of children. • Similarly, the Convention on the Rights of the Child (CRC), together with its General Comment No. 25, and the General Data Protection Regulation (GDPR) of the European Union, prohibit the exploitation of children’s personal data in digital advertising and uphold their fundamental right to digital erasure, often referred to as the "right to be forgotten."	• The Algerian Penal Code, as amended by Laws No. 04-15 and 09-04, criminalizes the unlawful use of information and communication technologies, prescribing penalties for cyberbullying, online sexual exploitation of minors, and the dissemination of pornographic material involving children. • Law No. 15-12 on Child Protection (2015) establishes comprehensive safeguards to protect children from all forms of exploitation, including those perpetrated through electronic and digital media. • Law No. 09-04 of August 5, 2009, concerning cybercrime, explicitly criminalizes the processing or dissemination of a child’s personal data without prior consent, thereby reinforcing the protection of minors’ digital privacy.

Procedural Framework	- Articles 16 through 21 of the Budapest Convention set forth the legal framework governing the collection, preservation, and lawful seizure of digital evidence and electronic data. - The establishment of independent national authorities such as the Commission Nationale de l'Informatique et des Libertés (CNIL) in France and the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in Germany ensures effective regulatory oversight and the enforcement of sanctions in cases of non compliance.	- The Algerian Code of Criminal Procedure, as amended in 2017 and 2020, integrates provisions authorizing the collection of digital evidence, the prosecution of cybercrimes, and the judicial preservation of electronic data. - Law No. 09-04 on Cybercrime provides for the prosecution of individuals responsible for digital offenses, even when such acts are committed across national borders, thereby reinforcing the principle of extraterritorial jurisdiction. - Law No. 18-07 establishes the National Authority for the Protection of Personal Data, tasked with ensuring compliance with data protection standards and safeguarding individuals' digital privacy rights.
International and Cooperation Framework	- Articles 23 to 35 of the Budapest Convention delineate the mechanisms for international cooperation in criminal investigations and the provision of mutual legal assistance. - The establishment of permanent communication channels among States Parties facilitates the exchange of evidence and information concerning offenses committed against children. - Strengthening collaboration with international organizations, including INTERPOL and UNICEF, further enhances the digital protection of children and supports the global coordination of preventive and enforcement measures.	- In the judicial and security domains, Algeria is a signatory to several bilateral and regional agreements facilitating the exchange of information on cybercrime, notably through its cooperation with INTERPOL and AFRIPOL. - Algeria actively participates in programs led by the United Nations and the African Union aimed at enhancing the protection of children in online environments. - In the area of capacity building, Algeria collaborates with the International Telecommunication Union (ITU) to conduct joint training programs designed to strengthen the skills of investigators handling cases related to digital child protection.

Note: Table prepared by the researcher.

Regarding the cooperative dimension, international collaboration in the judicial and security fields remains one of the most effective mechanisms for safeguarding children's

digital privacy. Algeria participates in several bilateral and regional agreements focused on information exchange and the prosecution of cybercriminals and actively supports the programs of the United Nations and the African Union aimed at protecting children online. Furthermore, Algeria adheres to Articles 23–35 of the Budapest Convention, which detail mechanisms for inter-state cooperation in digital investigations, mutual judicial assistance, and the establishment of permanent communication channels for exchanging information and evidence related to cybercrimes against minors.

Nonetheless, Algeria must intensify efforts to enhance institutional coordination between national and international bodies and to strengthen the legal framework for digital judicial assistance, ensuring it can effectively respond to the rapid technical and legal developments in this field.

6- A Study on Violations of Children's Privacy in the Digital Environment

Breaches of personal data have become among the most pervasive phenomena in the digital age, affecting individuals broadly and children in particular, as they constitute the most vulnerable demographic in cyberspace. In this regard, numerous legislative instruments have been enacted to underscore the importance of personal data protection most notably, the Data Protection Act of 1998, which grants individuals the right to access information held about them. It also obliges institutions and data controllers to process such information appropriately, in compliance with the United Kingdom's privacy and electronic communications regulations, as mandated by the Information Commissioner's Office (ICO).

Nevertheless, the digital sphere continues to witness recurrent breaches of these regulatory frameworks by major international corporations, resulting in significant financial sanctions and legal consequences. Foremost among these entities are TikTok, YouTube Kids, and Facebook, which have been implicated in the unlawful exploitation of children's data and in violations of their digital privacy. The following section examines the most prominent cases of privacy violations involving these platforms.

6.1-TikTok

In April 2023, the United Kingdom's Information Commissioner's Office (ICO) imposed sanctions on TikTok following verified violations of children's data protection laws. Approximately 1.4 million children under the age of 13, who accessed the platform in 2020, were affected.

The company was found to have contravened the UK Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) by allowing underage users to access the platform without obtaining verifiable parental consent contradicting its own terms of service. (Information Commissioner's Office, 2023)

The principal infringements committed by TikTok, constituting a breach of the principles of lawful, fair, and transparent data processing stipulated in Article 5 of the GDPR, include:

- A.** Failure to implement effective age-verification mechanisms.
- B.** Absence of adequate procedures for identifying and removing underage users, despite prior knowledge of their activity.
- C.** Insufficient transparency regarding how user data were collected, processed, and shared.

6.2-YouTube Kids

YouTube, one of the world's leading producers and distributors of digital visual content, developed YouTube Kids as a platform specifically designed to provide children with a safe and age-appropriate online environment.

However, in March 2023, the ICO accused YouTube of unlawfully collecting data from children under 13, in direct contravention of the Children's Code adopted by the ICO in 2020. Investigations revealed that the platform gathered personal data including viewing histories, geographic locations, and device identifiers without obtaining parental consent, thereby breaching the principles of transparency and the protection of minors' privacy. (BBC News, 2023)

A report issued by the UK Communications Authority further exposed the magnitude of these violations, indicating that 89% of British children aged 3 to 17 had used YouTube in 2021. Moreover, similar violations have been observed globally. The company was previously fined by the U.S. Federal Trade Commission (FTC) for collecting data from children under 13 without parental consent, in violation of the Children's Online Privacy Protection Act (COPPA).

6.3-Facebook

Facebook, a global leader in technology and social networking, became embroiled between 2007 and 2014 in one of the most infamous data privacy scandals the unauthorized transfer of user data to Cambridge Analytica, a third-party company that exploited this information for illicit purposes, thereby constituting a grave violation of data protection laws.

In October 2018, the ICO imposed a £500,000 fine on Facebook under the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) for failing to safeguard users' personal information. (BBC News, 2018)

This breach affected approximately 87 million users worldwide, including over one million in the United Kingdom. User data were harvested through a psychological testing application to collect personal information, parts of which were subsequently transferred to Cambridge Analytica and used for targeted political advertising campaigns in the United States.

Finally, an examination of major privacy breaches perpetrated by leading technology and social media companies namely TikTok, YouTube, and Facebook reveals that children's privacy in the digital environment remains gravely endangered due to the unlawful processing of their personal data.

Findings indicate that these corporations have consistently failed to fully comply with the provisions of the UK Data Protection Act (2018) and the UK General Data Protection Regulation (UK GDPR). In the cases of TikTok and YouTube, this non compliance has manifested through ineffective age-verification systems and the blurring of distinctions between adult and child accounts. The Facebook case, in turn, highlights the ethical dimension of the issue, wherein personal data were exploited for political and commercial gain posing significant threats to children's privacy and potentially leading to adverse social and psychological consequences.

Although the principles of privacy by design and privacy by default upon which both the UK Data Protection Act and the Children's Code are founded seek to reinforce protections

against recurrent privacy violations, their practical effectiveness remains limited unless continuously updated to ensure robust, adaptive, and sustainable safeguards for children in the digital environment.

Conclusion:

This study concludes that the protection of children's digital privacy has become an increasingly complex and pressing challenge, both globally and nationally. International frameworks most notably the Convention on the Rights of the Child (CRC) and its General Comment No. 25 have made significant progress in developing detailed regulatory controls that prohibit exploitative advertising practices and uphold the best interests of the child alongside their right to digital security.

In contrast, the Algerian experience reveals evident limitations in the national legal framework both in terms of the comprehensiveness of existing legislation and the effectiveness of its implementation and monitoring mechanisms. Furthermore, the absence of consistent digital awareness programs targeting children and their guardians leaves them vulnerable to commercial exploitation and violations of privacy within the digital environment.

Children in Algeria are increasingly exposed to sophisticated forms of digital targeting, making the establishment of clear data-protection standards and ethical guidelines for respecting minors' online privacy an urgent priority. The lack of such safeguards directly threatens their psychological and social well-being and may distort the development of their digital identity. Consequently, the protection of children's privacy in Algeria's digital ecosystem represents a critical policy domain that demands immediate legislative, institutional, and societal intervention.

Based on the review and analysis of relevant literature, this study proposes the following recommendations to enhance the protection of children's privacy in the digital environment:

1. Strengthen the independence of the National Authority for the Protection of Personal Data and expand its powers in oversight, investigation, and preventive action.
2. Establish a multi-jurisdictional coordination unit bringing together key ministries (Justice, Interior, Education, Health, Communication, and Technology) to ensure integrated protection and monitoring of children's cyber privacy.
3. Support national awareness programs and initiatives to combat digital illiteracy targeting children, parents, and educational institutions, with a focus on mitigating exposure to harmful or extremist online content.
4. Enhance international cooperation with organizations such as UNICEF and the International Telecommunication Union (ITU) to exchange expertise and develop harmonized regulatory standards aligned with Algeria's cultural and social context.
5. Promote scientific research in the fields of cybersecurity, digital ethics, and child online protection to consolidate national digital sovereignty.
6. Incorporate explicit legal provisions on children's digital privacy into the Personal Data Protection Law, including a clear legal definition of "child," the requirement of parental consent, the activation of default privacy settings, the prohibition of targeted advertising directed at minors, and the guarantee of the right to data erasure.

References:

1. Abderrezzaq, B. (2024). The Impact of the School Environment on Deviant Behaviors: An Exploratory Study of the Impact of Feeling Safe, Adherence to Regulations, and Management Strategies. *Revista Universitară de Sociologie*, 10(2), 22-31.
2. Algerian Consumer Protection Association. (2022). *Report on digital advertising and its impact on children*. Algiers: Algerian Consumer Protection Association.
3. Auxier, B., et al. (2023). *Children's privacy and well-being in the digital world*. Pew Research Center. <https://www.pewresearch.org>
4. Ben Ammar, A. (2021). *The problematic of personal data protection in Algeria in light of digital transformations* [Master's thesis, University of Algiers]. Faculty of Law and Political Science.
5. Ben Yamina, M. (2022). *Protecting children's privacy in the digital environment: Technical challenges and legal mechanisms*. *Journal of Contemporary Media Studies*, 7(2), 145–160.
6. Bouchareb, K. (2022). *Algerian legislation and child protection in the digital environment*. *Journal of Legal Sciences*, 45, 123–145.
7. Boumaraf, M. (2023). *Algerian parents' awareness of internet risks to children and means of protection*. *Journal of New Media and Communication*, 12, 89–110.
8. BRADA, A., & DAHMANI, F. (2025). Criminal Behavior in the Digital Environment: Historical Foundations and a Sociological Perspective. *Revista Universitară de Sociologie*, 21(2).
9. Dahmani, F., & Brada, A. (2025). Cybersecurity Readiness in Algeria: An Assessment of Infrastructure, Legislation, and Crisis Management. *Rev. Universitara Sociologie*, 130.
10. Dahmani, F., & Brada, A. (2025). Media education and the challenges of the digital environment: towards enabling children to safely use social networking sites. *Annales de l'université d'Alger*, 39(2), 96-115.
11. Electronic Privacy Information Center. (2022). *Children's privacy*. <https://epic.org/issues/data-protection/childrens-privacy/>
12. Federal Trade Commission. (2023). *Children's online privacy protection rule (COPPA)*. <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
13. Federal Trade Commission. (2025). *Children's online privacy protection rule (COPPA) – Final amendments*. *Federal Register*.
14. Dahmani, F., & Brada, A. (2025). The Impact of Digital Transformation on Communication Officers in Algerian Institutions: An Analytical Approach to Skills Development and the Restructuring of Communication Roles. *Al Mieyar*, 29(4), 141-152.
15. James, C., et al. (2020). *The digital lives of children: Growing up in a connected world*. UNICEF Office of Research–Innocenti. <https://doi.org/10.18356/6d8d8f1e-en>
16. Livingstone, S., & Stoilova, M. (2021). *Children's data and privacy online: Growing up in a digital age*. *Media, Culture & Society*, 43(6), 1025–1040. <https://doi.org/10.1177/0163443720986195>

17. Livingstone, S., Stoilova, M., & Nandagiri, R. (2018). *Children's data and privacy online: Growing up in a digital age*. London School of Economics and Political Science.
18. Medjkoune, T., et al. (2023). *Marketing to children through online targeted advertising: Targeting mechanisms and legal aspects*. *International Journal of Child-Computer Interaction*, 36, 110–125. <https://doi.org/10.1016/j.ijcci.2023.100587>
19. Milkaite, I., & Lievens, E. (2020). *Children and data protection: Privacy by design and by default in the age of the GDPR*. *Information & Communications Technology Law*, 29(3), 257–273. <https://doi.org/10.1080/13600834.2020.1786602>
20. Montgomery, K. C., Chester, J., Grier, S. A., & Dorfman, L. (2017). *The new era of digital marketing to children: Protecting kids' privacy in the age of behavioral targeting and big data*. *Journal of Public Health Policy*, 38(2), 230–241. <https://doi.org/10.1057/s41271-016-0065-5>
21. Montgomery, K., Chester, J., & Nixon, L. (2022). *The harms of targeted food marketing to children: Policy implications for the digital age*. *Journal of Public Policy & Marketing*, 41(2), 232–245. <https://doi.org/10.1177/07439156211050480>
22. Moti, Z., et al. (2023). *Targeted and troublesome: Tracking and advertising on children's websites*. *arXiv preprint arXiv:2308.04887*. <https://doi.org/10.48550/arXiv.2308.04887>
23. Network Advertising Initiative. (2024). *COPPA 2.0 provides the opportunity to establish a new national standard for children's data privacy*. <https://thenai.org>
24. Regulatory Authority for Post and Electronic Communications. (2023). *Annual report on internet use and the digital space in Algeria*. Algiers: ARPCE.
25. Steinberg, S. (2023). *Children's data privacy in the digital economy: A legal analysis*. *Yale Journal of Law and Technology*, 25(1), 1–35. <https://yjolt.org>
26. Sun, R., et al. (2023). *Not seen, not heard in the digital world! Measuring privacy practices in children's apps*. *arXiv preprint arXiv:2303.09008*. <https://doi.org/10.48550/arXiv.2303.09008>
27. UN Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. United Nations Human Rights Office. <https://www.ohchr.org>
28. UNESCO. (2021). *Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information*. United Nations Educational, Scientific and Cultural Organization.
29. UNICEF. (2017). *Children in a digital world: The state of the world's children 2017*. United Nations Children's Fund. <https://www.unicef.org/reports/state-worlds-children-2017>
30. UNICEF. (2020). *The United Nations Convention on the Rights of the Child: A guide to the CRC and its implementation*. New York: UNICEF Publications.
31. BBC News. (2018, October 25). Facebook fined £500,000 for Cambridge Analytica scandal. <https://www.bbc.com/news/technology-45976300>
32. BBC News. (2023, March 1). YouTube accused of collecting UK children's data. <https://www.bbc.com/news/technology-64786968>
33. Information Commissioner's Office (ICO). (2023, April 4). ICO fines TikTok £12.7 million for misusing children's data. <https://ico.org.uk>