Nusantara: Journal of Law Studies
Vol. 5 No. 1, 2026: 205-228
E-ISSN: 2964-3384
https://doi.org/10.66325/nusantaralaw.v5i1.222

Preventive Legislative Approaches to Child Protection in the Digital Environment: A Comparative Study of Australia, France, and Egypt

Tarek El-Sayed Mahmod Abu Okeal[1]*, Hisham Al-Kasasbeh[2], Hanaa Ibrahiem Abdullah[3], Salaheldin Ragab Fathelbab[4]

[1,4]College of Law, University of Al Maarif, Iraq
[2]Faculty of Law, Al-Zaytouna University, Jordan
[3]Faculty of Law, Cairo University, Khartoum Branch, Egypt

DOI: doi.org/10.66325/nusantaralaw.v5i1.222
*Corresponding Author: tarek.mahmoud@uoa.edu.iq

Received: 18-09-2025 | *Revised: 24-12-2025* | *Accepted: 08-03-2026* | *Published On: 14-03-2026*

Abstract: The rapid expansion of the digital environment has significantly increased children's exposure to various online risks, including sexual exploitation, cyberbullying, digital extortion, and violations of privacy and image rights. This study examines the effectiveness of preventive legislative frameworks in protecting minors in the digital sphere by comparing regulatory approaches in Australia, France, and Egypt. Specifically, it aims to analyse how preventive legal models in Australia and France address digital harms affecting children and to evaluate the extent to which these models can inform legislative reform within the Egyptian legal system. The research employs a qualitative approach using descriptive–analytical and comparative legal methods, focusing on statutory provisions, regulatory mechanisms, and institutional enforcement structures across the three jurisdictions. The findings reveal that Australia and France have gradually shifted from reactive criminalisation toward a proactive preventive governance model. These frameworks impose legally binding obligations on digital platforms, including age verification systems, algorithmic accountability, enhanced content moderation, and digital literacy initiatives to strengthen child safety online. Australia prioritises strict minimum-age requirements and corporate liability mechanisms, while France adopts a dual-track model combining technological verification, parental consent, and preventive educational policies alongside criminal sanctions. In contrast, Egypt's legal framework remains predominantly reactive, with regulatory provisions dispersed across the Child Law and the Cybercrime Law, and lacking comprehensive preventive obligations for digital platforms. This study contributes to the literature by providing an early comparative analysis of recent preventive legislative reforms (2024–

Copyright (c) 2026 Tarek El-Sayed Mahmod Abu Okeal et. al.
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

2026) and by identifying structural gaps in Egypt's digital child protection regime. It further proposes policy-oriented recommendations for developing a modernised preventive framework aligned with international standards, thereby strengthening the protection of children's rights in an increasingly digitalised society.

Keywords: Cyber Risks; Digital Child Protection; Preventive Legislation; Platform Liability.

Introduction

The rapid acceleration of technological innovation has produced a borderless digital environment whose risks transcend geographical boundaries and traditional notions of state sovereignty. Within this evolving cyber ecosystem, children have emerged as one of the most vulnerable categories of rights-holders.[1] The digital space has facilitated new patterns of abuse, including online child sexual exploitation, cyberbullying, digital extortion, and violations of the child's right to image and dignity.[2] As has been observed, technological development has intensified criminal assaults on children's personal rights by transforming the digital sphere into a platform capable of amplifying harm beyond physical and territorial limitations.[3]

Unlike traditional forms of criminality, digital offences targeting minors are not confined by physical proximity or national jurisdiction. They are characterised by anonymity, algorithmic amplification, rapid dissemination, and the persistence of harmful content. Consequently, protecting children in digital environments has become a matter of both international and domestic urgency.[4] Contemporary policy scholarship emphasises that online ecosystems, particularly social media and interactive gaming platforms, generate structural risks that require regulatory intervention rather than reliance solely on post-crime punishment.[5]

---

[1] Kirsty Robertson and Alison McLuckie, 'Social Protection for Children: Global Landscape and Domestic Provision in the UK', *Paediatrics and Child Health (United Kingdom)* 36, no. 2 (2026): 45–49, https://doi.org/10.1016/j.paed.2025.11.007.

[2] Nhat Dinh Quang Vo et al., 'Parents Protect Their Children When Travelling: Exploring Traffic Safety Behavioral Intentions through the Lens of Cognitive Appraisal and Protection Motivation Theories', *Accident Analysis and Prevention* 228 (2026), https://doi.org/10.1016/j.aap.2026.108421.

[3] Tariq Al-Sayed Mahmoud Abu Aqil, "Criminal Confrontation of Exploiting Technical Development in Assault on the Child's Right to the Picture: Comparative Study," *Journal of Legal Studies*, no. 9 (February 2026): 389–395, https://www.nuwab.bh/wp-content/uploads/2026/02/d8a7d984d8b9d8afd8af-d8a7d984d8aad8a7d8b3d8b9.pdf.

[4] Siti Nurjanah et al., 'Children's Rights in Islamic Law: A Contemporary Study of Family Practices', *MILRev: Metro Islamic Law Review* 4, no. 2 (July 2025): 933–953, https://doi.org/10.32332/milrev.v4i2.10077.

[5] Hala A. M. Al-Ahmadi, 'Real Risks of Digital Gameplay: A Policy Perspective on Protecting Children and Adolescents in Online Gaming Environments', *Doha International Family Institute Journal* 2025, no. 2 (December 2025): 13, https://doi.org/10.5339/difi.2025.13.

This evolving reality has generated profound academic and legislative anxiety. Classical criminal law has historically operated through deterrence and retribution after the commission of an offence. However, digital harms frequently materialise in environments shaped by platform design, automated recommendation systems, and monetisation algorithms. In such settings, responsibility cannot be confined to the individual perpetrator alone. Instead, the architecture of digital platforms themselves may facilitate exposure to harmful content, grooming behaviours, exploitative targeting, or reputational harm. The result has been a paradigmatic shift in contemporary legislative philosophy from reactive criminalisation toward proactive preventive governance. Preventive regulation seeks to intervene before harm occurs by imposing affirmative obligations upon digital intermediaries. These include age-verification requirements, safety-by-design standards, algorithmic accountability, rapid content removal protocols, and reinforced parental oversight mechanisms.

A leading example of this preventive turn is the Australian reform embodied in the Online Safety Amendment (social media Minimum Age) Act 2024.[6] This legislation establishes a legally binding minimum age for access to social media platforms and shifts the compliance burden from families to technology companies. By mandating enforceable age-verification systems and empowering regulatory oversight, the Australian model represents a structural reconfiguration of platform responsibility. It institutionalises what may be termed "preventive digital guardianship," in which platforms are no longer passive hosts but regulated actors charged with protecting minors within their ecosystems.[7]

Similarly, France has adopted a preventive regulatory approach by codifying the concept of the digital majority and strengthening technical verification requirements for parental consent. These reforms align with broader European regulatory instruments, particularly the Digital Services Act, which establishes due diligence obligations for online platforms and enhances enforcement capacity against unlawful content. The French model combines preventive access restrictions with enhanced criminal liability and strengthened data protection safeguards, thereby integrating child protection into the broader framework of digital constitutionalism.

Despite the growing body of interdisciplinary literature addressing digital child safety, much of the existing scholarship concentrates on sociological, psychological, or technological dimensions of risk. For instance, Hardianto Djanggih (2018) analysed the various ways in which children become victims of cybercrime, documented the psychological and social impacts, and identified legal and regulatory gaps that leave children exposed.[8] The study emphasised technological interventions, legislative reform, and parental guidance as mechanisms to enhance protection. Topan and Uzuntarla

[6] Online Safety Amendment (social media Minimum Age) Act 2024 (Australia), https://www.legislation.gov.au/C2024A00127/asmade/text.

[7] Marjun, Saroji, and Farhan Farhan, 'Cyberbullying and Legal Protection for Victims in the Digital Era: A Case Study on Social Media Platforms', *Hakim: Jurnal Ilmu Hukum Dan Sosial* 3, no. 1 (February 2025): 955–973, https://doi.org/10.51903/hakim.v3i1.2290.

[8] Hardianto Djanggih, 'The Phenomenon of Cyber Crimes Which Impact Children as Victims in Indonesia', *Yuridika* 33, no. 2 (May 2018): 212–231, https://doi.org/10.20473/ydk.v33i2.7536.

Güney (2025) examined parental digital literacy and found that parents with greater awareness of digital risks were better able to supervise their children's online activities effectively, thereby mitigating exposure to cyber harms.[9] Osório de Barros et al. (2025) explored the complex influence of artificial intelligence on children's educational and social environments, highlighting both developmental opportunities and risks, including reduced human interaction, privacy concerns, and ethical implications of AI deployment in daily learning and play.[10]

While these contributions significantly advance understanding of digital vulnerability, they often treat legal reform as a secondary dimension rather than the primary analytical focus. Moreover, there remains a scarcity of comprehensive comparative legal analyses that evaluate the newly enacted Australian and French preventive frameworks in juxtaposition with Middle Eastern legal systems.[11] The present research addresses this gap. To the best of the author's knowledge, it constitutes one of the earliest doctrinal and comparative examinations of the 2024–2026 preventive legislative developments in Australia and France, analysed against the existing Egyptian legal framework. Unlike prior studies that emphasise risk typologies or parental mediation strategies, this research focuses on the juridical architecture of prevention. It interrogates how the concepts of digital majority, platform liability, algorithmic governance, and institutional oversight are normatively constructed and legally operationalised. The Egyptian legislative approach, by contrast, remains predominantly anchored in reactive criminalisation through the Cybercrime Law No. 175 of 2018 and the Child Law No. 12 of 1996 (as amended). While these statutes provide punitive mechanisms against offenders, they do not establish an integrated preventive regulatory framework imposing systematic safety obligations upon platforms. The absence of binding age-verification mandates, algorithmic accountability provisions, and unified digital child protection legislation reflects a structural gap between traditional deterrence-based models and contemporary preventive governance paradigms.

Accordingly, the central problem addressed in this study concerns the extent to which preventive legislative models, particularly those adopted in Australia and France, offer a more effective and coherent framework for mitigating digital harms against children. It further examines whether such models can be adapted within the Egyptian legal system without undermining constitutional guarantees of privacy, access to information, and freedom of expression. Methodologically, the research employs a descriptive-analytical approach to examine statutory texts, regulatory mechanisms, and

[9] Aysel Topan et al., 'The Relationship Between Parents' Digital Parenting Awareness, Their Social Media Parenting Practices, and The Social Media Usage Levels of Their Children Aged 6–18', *Child and Adolescent Social Work Journal*, ahead of print, 16 November 2025, https://doi.org/10.1007/s10560-025-01059-1.

[10] Kleopatra Nikolopoulou, 'Child-Centered Integration of Generative AI in Early Learning: Balancing Promises and Challenges', *AI, Brain and Child* 1, no. 1 (December 2025): 21, https://doi.org/10.1007/s44436-025-00023-1.

[11] S. Bhalla et al., "Child Victimization in Cybercrime Environments," 2025; A. Topan and Uzuntarla Güney, "Parental Digital Literacy and Social Media Supervision," 2025; Osório de Barros et al., "Artificial Intelligence and Child Development: Ethical and Privacy Implications," 2025.

enforcement structures in Australia and France. It further utilises the comparative method to assess normative convergence and divergence between these systems and the Egyptian framework. Through this analysis, the study seeks to identify structural deficiencies, evaluate proportionality between child protection and digital freedoms, and formulate legislative recommendations grounded in preventive legal theory. Ultimately, this research is situated at the intersection of criminal law, regulatory governance, and digital rights jurisprudence. It responds to an urgent normative question: how can legal systems reconcile technological innovation with the paramount principle of the best interests of the child? By advancing a structured comparative analysis and articulating targeted reform proposals, the study contributes to the development of a coherent preventive paradigm capable of addressing the evolving threats of the digital age.

Method

This research adopts a qualitative legal research design, using a descriptive–analytical and comparative legal approach to examine preventive legislative mechanisms for child protection in the digital environment. The descriptive–analytical method is employed to systematically identify and interpret the normative structures embedded in contemporary digital child protection regulations, particularly those enacted in Australia, France, and Egypt. Through this approach, the study analyses the legal frameworks governing digital safety, including statutory provisions, regulatory obligations for digital platforms, and institutional enforcement mechanisms. The research specifically examines the legislative configuration of Australia's online safety regime, France's digital child protection policies, and Egypt's legal framework, including Cybercrime Law No. 175 of 2018, Child Law No. 12 of 1996 (as amended), and related personal data protection regulations. By applying a comparative legal analysis, the study aims to evaluate similarities, differences, and normative orientations among these jurisdictions in establishing preventive legal safeguards for children in cyberspace.

Data for this research are collected through documentary and library research, focusing on primary legal materials such as statutes, governmental regulations, policy documents, and international standards related to child protection in the digital sphere, as well as secondary sources including academic journals, books, and policy reports. The collected data are analysed using qualitative legal analysis and comparative interpretation, which involves a close textual examination of legal provisions, institutional responsibilities, and preventive regulatory strategies implemented in each jurisdiction. To ensure the reliability and validity of the findings, the study employs data triangulation and cross-checks legal texts with scholarly interpretations and international policy frameworks, including global child protection standards in digital governance. This validation process enhances the analytical accuracy of the study and enables a comprehensive evaluation of how preventive legislative approaches can contribute to developing a more effective, child-centred digital safety framework.

Results and Discussion

The Risks Posed by the Digital Environment to Children

The digital environment imposes "complex risks" (health-related, psychological, and criminal) that surpass the traditional frameworks for child protection, necessitating a legislative

shift from "ex-post criminalisation" to "proactive preventive classification."[12] A precise legal characterisation of these emerging violations and organised assaults constitutes the fundamental basis for formulating a national strategy that ensures "digital safety" for minors and limits the technical liability of platforms.[13] The most significant risks can be summarised as follows:

1. Health and Psychological Risks

Excessive digital engagement among children constitutes a direct violation of the rights to health and proper development enshrined in international conventions and child protection law.[14] It gives rise to organic and developmental disorders such as digital eye strain, obesity, and sleep disturbances, which are structural harms with systemic effects on public health.[15] These risks necessitate a legislative transition from "technical regulation" to "biological regulation" by imposing legal obligations on digital platforms, including mandatory time restrictions, to ensure a balance between the right to knowledge and the right to physical well-being.

Regarding psychological well-being and emotional development, the risks of excessive digital consumption manifest in highly complex dimensions.[16] Compulsive digital use by minors constitutes a structural violation of the right to psychological integrity and holistic development, converting anxiety, depression, and behavioural addiction from mere psychological disorders into legally recognised harms requiring protection.[17] According to General Comment No. 25 of the United Nations Committee on the Rights of the Child, these effects impose shared tortious responsibilities on states and technology companies.[18] Consequently, they are mandated to implement preventive design standards that limit algorithms encouraging compulsive usage, thus securing the child's inherent right to emotional stability and self-esteem, free from coercive comparison pressures and excessive digital attachment.[19]

---

[12] Alex Paradise, 'Child Sexual Abuse Material, Progression to Contact Offending and the Evolution of Technology', in *Rethinking the Police for a Better Future : Navigating Policing Challenges with Accountability and Trust*, ed. Baidya Nath Mukherjee et al. (Cham: Springer Nature Switzerland, 2025), 259–273, https://doi.org/10.1007/978-3-031-83173-7_17.

[13] OECD. Children in the digital environment, 2020.

[14] John Tobin& Nicolá Brando& Cynthia Chamberlain& Jonathan Collinson& Louise Forde& The UN Convention on the Rights of the Child: A Commentary, The International Journal of Children'sRights XX, ISSN: 0927 – 5568, (2024) 1-11

[15] Andrea Fuentes-González et al., 'Profiles of Protection Trajectories among Children in Residential Care', *Children and Youth Services Review* 183 (2026), https://doi.org/10.1016/j.childyouth.2026.108790.

[16] Muhammad Fitri Adi, 'Hadhonah Rights of Children (Not Mumayyis) Based on Compilation of Islamic Law and Child Protection Act', *NUSANTARA: Journal of Law Studies* 2, no. 1 (March 2023): 9–22, https://doi.org/10.5281/zenodo.17388734.

[17] Youli Wang et al., 'From Family to School: The Dual Protection of Father-Child Relationship and Teacher-Student Relationship on Children's Mental Health Problems', *BMC Psychology* 14, no. 1 (2026), https://doi.org/10.1186/s40359-025-03793-8.

[18] UNICEF. Feeding Profit: How food environments are failing children - 2025 Child Nutrition Report, September 2025.

[19] Sonia Livingstone, Realising children's rights in relation to the digital environment, UN Committee on the Rights of the Child (CRC/C/GC/25), 2021, Paragraph 84.

2. Behavioural and Social Risks in the Context of Digital Exposure

In addition to physical threats, the issue of inappropriate digital content emerges as a core factor influencing the behavioural formation of minors. The negative impact of the digital environment does not stop at violent content, which renders platforms a "criminal risk source" undermining the behavioural development of children, but extends to compulsive digital withdrawal, isolating the child from their real-world environment. This constitutes a dual breach of emotional safety according to paragraphs 54 and 83 of the previously cited General Comment No. 25/2021 and the child's right to holistic social development under Article 27 of the Convention on the Rights of the Child.

This interplay between "corrupt content" and "consumer isolation" necessitates a shift from optional parental supervision to mandatory regulatory obligations, through the imposition of safety by design standards as both technical and legal prerequisites for content licensing and usage time restrictions. Such measures are essential to restore the balance between the advantages of digital knowledge and the child's innate need for social integration.[20]

3. Exposure to Digital Assaults

Cyberattacks represent some of the most severe threats facing minors and are classified as grave crimes, encompassing child sexual exploitation, grooming, cyber extortion, and cyberbullying. All these acts require criminal prosecution due to their violation of the child's physical and psychological integrity by exploiting their vulnerability in the digital environment.[21]

- Online Child Sexual Exploitation

Online child sexual exploitation is an escalating global threat targeting the innocence of minors through digital spaces. This exploitation manifests in multiple forms, often beginning with grooming, where the perpetrator establishes a deceptive relationship of trust with the child, and extending to sextortion, involving threats to release private images or videos. With technological advancements, new risks have emerged, such as the use of generative AI to produce exploitative content, resulting in a significant surge in reported cases.[22] Studies indicate that nearly 1 in 12 children worldwide fall victim to this type of abuse. To address this phenomenon, experts emphasise the importance of digital literacy for parents, the activation of parental control tools, and the establishment of open communication channels with children to encourage reporting of suspicious interactions without fear of blame[3]. Protecting children, therefore, is not merely a technical responsibility but a societal obligation, requiring coordinated efforts between governments and technology companies to ensure a safe digital environment.[23]

---

https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

[20] United Nations, Committee on the Rights of the Child. General Comment No. 25 on the rights of the child in the digital environment, 2021.

[21] Romil Rawat, Sanjaya Kumar Sarangi, A. Samson Arun Raj, Janet Olivia Richmond, Purvee Bhardwaj, Child Protection Laws and Crime in the Digital Era, IGI Global, July 2025, 5:8. https://www.igi-global.com/book/child-protection-laws-crime-digital/381315

[22] Chauviré-Geib, K., Haag, AC., Gerke, J. et al. Associations between online child sexual solicitation and abuse and offline child maltreatment: A latent class analysis. Eur Child Adolesc Psychiatry (2025). https://doi.org/10.1007/s00787-025-02885-5

[23] Kathryn C Seigfried-Spellar, Marcus K Rogers, Nina L Matulis, Jacob S Heasley, Testing a hybrid risk assessment model: Predicting CSAM offender risk from digital forensic

- Grooming

Cyber grooming of minors is defined as a deliberate criminal act conducted by an adult through digital means, aiming to establish false trust and artificial intimacy with the child for sexual exploitation. This offence is characterised by a gradual behavioural component, where the perpetrator employs an escalating strategy: initiating emotional approaches, simulating the victim's interests, and offering virtual or emotional incentives to satisfy psychological needs. The process escalates from trust-building to obtaining sensitive information or sexualised material, ultimately culminating in inducement for physical meetings, making it a complex crime combining emotional deception with imminent physical abuse.[24]

Furthermore, such criminal practices exploit the structural characteristics of the digital environment, including social media networks, multiplayer gaming platforms, and instant messaging applications, which allow perpetrators to mask their identities using pseudonyms, deceiving victims. Offenders take advantage of minors' cognitive immaturity, young age, and gaps in digital protection mechanisms. The legal consequences of this crime extend beyond the material act, resulting in severe psychological trauma, behavioural disorders, and social trust disruption, necessitating an integrated legislative and technological approach to ensure proactive criminal protection for vulnerable groups in virtual environments.[25]

- Cyber Extortion:

Cyber extortion is among the most serious digital offences, classified as a threat-based crime with a demand component. Perpetrators intimidate minors by threatening to disclose sensitive materials (data, images, or videos) obtained through hacking or deception, coercing the victim into providing financial or sexual concessions. The severity of this crime is heightened by Dark Web technologies, creating fertile ground for illicit activities beyond conventional security oversight. Given the transnational nature of these offences, combating them requires activating international cooperation frameworks and modernising legislation to track offenders and provide preventive legal protection for children.[26]

- Cyberbullying:

Cyberbullying is a complex behavioural crime defined by intent and repetition to harm minors through digital means. Its legal and social danger lies in its extensive dissemination,

artifacts, Elsevier Forensic Science International: Digital Investigation, Volume 50, Issue Supplement, 2024, 301712.

[24] L. Alfies Sihombing, Yeni Nuraeni, Wahyudi, Loso Judijanto, Abidah Abdul Ghafar, Sexual Grooming of Children Mode through Live Streaming: Legal Gaps in the Face of Anonymity of Online Transactions, Lex Scientia Law Review, Vol. 9, Issue 2, 2025, 1791. https://garuda.kemdiktisaintek.go.id/documents/detail/5797102

[25] Chazizah Gusnita, Lucky Nurhadiyanto, Suyatno Ladiq, Patterns of Child Grooming and Sexual Harassment in Online Games, Jurnal Perempuan dan Anak, Volume7, Issue 2, Dec 31, 2023, 208. https://discovery.researcher.life/article/patterns-of-child-grooming-and-sexual-harassment-in-online-games/e8d910aa51623fec96c1cefd5a6d6c31

[26] Catherine C. Siegfried-Spiller, Marcus K. Rogers, Nina L. Matulis, Jacob S. Hesley, testing a Hybrid Risk Assessment Model: Predicting the Risk of Child Sexual Exploitation Offenders from Digital Forensics, op. cit., p. 301712

which makes mitigating its effects particularly challenging and leads to severe psychological consequences for victims.[27]

Emerging Policies in Australian and French Legislation

Recent legislative developments in France and Australia carry significant legal importance, as they represent a radical shift in punitive philosophy, moving from "ex-post criminal protection" (intervention after the crime has occurred) to "proactive prevention." This legislative model is grounded in the principle of shared responsibility, which does not confine liability to the individual perpetrator but extends direct legal obligations to digital platforms and service providers, requiring them to adopt Safety by Design standards. Undoubtedly, this legislative evolution aims to address the legal gaps created by the rapid pace of digital transformation, positioning the French and Australian experiences as pioneering models in formulating comprehensive legal frameworks that ensure a safe digital environment for minors.

1. Preventive Policy in Australian Law, 2024

The Online Safety Amendment (Minimum Age for social media) Act 2024 in Australia represents an unprecedented legislative breakthrough, affecting a fundamental shift in the philosophy of legal responsibility by transferring the burden of protecting minors from individual families to institutional responsibility assigned to technology companies.[28] Upon receiving Royal Assent in December 2024, the law enshrined a "preventive and deterrent" approach, imposing strict restrictions on digital access for individuals under sixteen years of age. Technology companies were granted until December 2025 to implement the necessary systems for age verification before punitive measures could be enforced.[29] This legislation has redefined the concept of state and corporate responsibility toward children in the digital environment and laid the foundations for proactive protection, as evidenced by provisions targeting:

a. Age-Use Restrictions

1. The Australian legislator established the minimum legal age for access to social media platforms and interactive games at 16 years,[30] prohibiting account creation below this threshold, with conditional exceptions subject to stringent safeguards, including:
2. Supervisory Authority: Mandatory explicit written consent from a parent or legal guardian.
3. Technical Verification: Implementation of age verification protocols to ensure compliance.
4. Parental Linkage: Creation of a technical connection between the child's account and the guardian's account to enable effective parental oversight.

[27] Sameer Hinduja and Justin W. Patchin, 'The Role of Hope in Bullying and Cyberbullying Prevention', *Frontiers in Sociology* 10 (July 2025), https://doi.org/10.3389/fsoc.2025.1576372.

[28] Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth). (2025 implementation)

[29] age-restricted user means an Australian child who has not reached 16 years., https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284

This framework aims to provide proactive protection from harmful content, reduce digital alienation, and safeguard the psychological and social well-being of children during critical developmental stages.[31]

b. Preventive Technical Obligations for Service Providers

Under the Online Safety Act, technology companies are subject to a set of legal and technical obligations to maintain a safe digital environment, [32]including:

1. Preventive Design Standards: Development of user interfaces tailored to age-specific characteristics, minimising exposure to potential risks. The law also mandates algorithmic governance, prohibiting recommendation systems from promoting content deemed harmful or age inappropriate. Additionally, it empowers parental oversight by providing technical tools to control digital access, set usage time limits, and monitor activities.
2. Rapid Response Protocols: Implementation of streamlined procedures for reporting violations, with a legal obligation for immediate removal of harmful content to ensure the effectiveness of civil and criminal protection mechanisms.[33]

To enforce these obligations, the legislature established deterrent sanctions for serious or systemic violations, with fines reaching AUD 50 million (or up to 5% of annual revenue), reinforcing the principle of direct corporate responsibilityfor deficiencies in protective systems.[34]

c. Strengthening the Role of the eSafety Commissioner

The Act enhances the powers of the eSafety Commissioner, granting broad regulatory and administrative authority to ensure rapid enforcement and compliance, including:

1. Mandatory removal of harmful content, with providers required to comply with the law.
2. Authority to impose direct administrative and financial penalties on platforms and companies in cases of safety violations, without affecting civil or criminal liability.
3. Provisions for institutional collaboration, enabling coordination with law enforcement agencies to pursue serious cybercrimes, bring perpetrators to justice, and track cross-border criminal activity.[35]

d. Legislative Obligations to Promote Digital Citizenship and Preventive Awareness

The legislature also established state-level responsibilities to develop a comprehensive preventive framework, including:

---

[31] Kim Osman, Michael Dezuanni, Lynrose Jane Genon, Young Australians' perspectives on the social media minimum age legislation, Digital Media Research Centre, 2025, 5. https://apo.org.au/node/332901

[31] Social media age restrictions, at: https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

[32] Social media age restrictions, at: https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions

[33]Kim Osman, Michael Dezwani, Lenrose Jane Ginnon, Australian youth views on minimum age legislation for social media use, op. cit., 10.

[34] Section 48A, Federal Register of Legislation, Online Safety Amendment (social media Minimum Age) Act 2024 (Cth). 2025

[35] esafety Commissioner, Social media age restrictions hub,

1. Mandatory awareness programs targeting the educational triad of child, guardian, and educational institution.[36]
2. Institutionalising the concept of "safe digital citizenship" within curricula or official activities to equip minors with tools for responsible engagement with cyber threats.
3. Promoting a transition from external supervision to self-protection by providing children with the skills to recognise digital risks and report incidents, enhancing the practical effectiveness of the law.[37]

2. Emerging Approaches in French Law for the Protection of Minors in the Digital Space

Recently, the French legislature adopted a "dual track" legislative strategy to establish a comprehensive protection framework for minors in cyberspace.[38] This strategy integrates proactive regulatory measures with ex-post criminal enforcement. On one hand, French laws, most notably the July 7, 2023, Act, impose preemptive technical obligations on service providers to ensure the safety of minors, such as mandatory age verification. On the other hand, the legislation strengthens post-crime criminalisation by updating the Penal Code to cover emerging forms of digital assaults. Furthermore, the French legislator introduced provisions protecting children's image rights[39], aiming to create a digital environment characterised by platform self-regulation under the threat of civil and criminal liability, thereby safeguarding children's fundamental rights against the risks of the virtual space.[40]

Based on the draft French law, the key mechanisms adopted to reduce cyber risks for children include:

a. Digital Eligibility and Access Restrictions in French Law

The French legislator set the age of majority for the digital age at 15, prohibiting minors under this age from accessing social media platforms without explicit parental or guardian consent. The National Assembly reinforced this policy through legislative amendments on January 26, 2026, shifting from mere formal acknowledgement of consent to mandatory technical verification.[41]

---

[36] Catherine Page Jeffery, ""Trust Us! We Know What We Are Doing!" Parent-Adolescent Digital Conflict in Australian Families', *Journal of Children and Media* 18, no. 4 (October 2024): 472–488, https://doi.org/10.1080/17482798.2024.2358947.

[37] Terry Flow, Timothy Kosky, Agata Stepnick, Digital Politics as a Problem Space: Shaping Policy, Public Opinion, and the Online Safety Amendment (social media Minimum Age) Act of 2024, op. cit, 6 Section 16 & 17. Federal Register of Legislation, Online Safety Amendment (Social Media Minimum Age) Act 2024 (Cth). (2025).

[38] Tariq Al-Sayyid Mahmoud Abu Aqil, previous reference, 403-404

[39] Magalie Dansac Le Clerc and Juliette Leportois , France introduces new law to enhance the protection of children's rights in France, March 19, 2024, at: https://connectontech.bakermckenzie.com/france-introduces-new-law-to-enhance-the-protection-of-childrens-rights-in-france/

[40] Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne. Journal officiel de la République française, 8 juillet 2023, disponible sur Légifrance. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533

[41] Armandin Goetz, Les réseaux sociaux seront-ils bientôt interdits aux moins de 15 ans ?, un sujet suggéré par l'équipe éditoriale de Village of Justice, article, 13 février 2026. https://www.village-justice.com/articles/les-reseaux-sociaux-bientot-interdits-aux-moins-ans-reserve-reserve,56008.html

Under these updates, digital platforms are legally required to adopt technical mechanisms approved by the Regulatory Authority for Digital Communications (ARCOM) to verify parental identity and consent.[42] Noncompliance entails both civil and criminal liability, aiming to close technical loopholes that allow circumvention of age restrictions and to ensure effective parental oversight in the virtual environment. To reinforce compliance, the French legislature introduced strict financial penalties: platforms that fail to implement ARCOM-approved verification mechanisms are subject to substantial fines.[43]

b. Procedural Obligations for Service Providers and Liability for Unlawful Content

The French legislator established a strict, rapid-response framework, obliging digital service providers and interactive platforms to remove or block access to content constituting a legal offence, including:

1. Pornographic and sexual abuse material: child sexual exploitation content requiring immediate removal.
2. Hate speech and incitement: content promoting violence, discrimination, or racial hatred.
3. Personal assaults: systematic cyberbullying and extortion targeting the child's psychological well-being.[44]

Short timelines are specified, ranging from one hour for severe offences (e.g., terrorism, sexual exploitation) to 24 hours for other content, with failure to comply triggering civil and criminal liability, substantial fines, and administrative measures restricting digital operations within French territory.[45]

c. Governance of Minors' Personal Data and Exploitative Restrictions

French law establishes a special legal regime for the protection of minors' personal data, based on the principle of "preemptive prohibition of exploitative processing." Companies and digital platforms are prohibited from collecting or processing minors' personal data for advertising profiling or commercial exploitation without explicit and informed consent from a parent or guardian, in coordination with the minor who has reached the digital age of majority.[46]

This approach is grounded in the "digital age of majority" provisions,[47] preventing platforms from using commercial targeting algorithms that exploit minors' vulnerabilities or

[42]ARCOM, *About Us: Discover the Institution*, accessed February 27, 2026, https://www.arcom.fr/en/about-us/discover-institution.

[43] Arcom. Rapport sur la mise en œuvre des obligations de vérification de l'âge et sanctions financières applicables. Autorité de régulation de la communication audiovisuelle et numérique, 2026 . https://www.arcom.fr/presse/lutte-contre-lexposition-des-mineurs-la-pornographie-larcom-met-en-demeure-deux-nouveaux-sites-pornographiques

[44] see at: https://www.theguardian.com/world/2026/jan/27/france-social-media-ban-under-15s ; https://www.vie-publique.fr/loi/301799-proteger-les-mineurs-risques-des-reseaux-sociaux-proposition-de-loi

[45] République Française, Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN), Article 15. Consulté via Légifrance (vigueur en 2026). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

[46] https://www.assemblee-nationale.fr/dyn/17/textes/l17b2107_proposition-loi

[47] Loi no 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne

track their online behaviour for promotional purposes. Violations incur severe administrative and financial penalties imposed by the National Commission on Informatics and Liberties (CNIL), including fines calculated as a percentage of global annual revenue, emphasising the primacy of digital privacy rights over platform economic interests.[48]

d. Digital Education as a Legislative Preventive Obligation

The French legislator mandated the integration of "digital education and cyber-prevention" into the formal curricula at all educational levels. Educational institutions are required to provide specialised content aimed at fostering critical awareness among minors regarding digital risks, equipping them with technical and legal skills to navigate virtual threats safely.[49] This approach constitutes a cornerstone of the national preventive strategy, transitioning schools from traditional education to digital resilience by teaching minors their rights and responsibilities online, as well as reporting mechanisms for violations, thereby fostering a generation with sufficient digital literacy to confront the challenges of the digital age.

Table 1. Comparative Overview of Legislative Approaches to Digital Child Protection

Dimension	Australia (2024)	France (2023–2026)	Egypt (Current & Draft)
Minimum Digital Age / Access Restrictions	16 years; parental consent required for underage accounts	15 years; mandatory parental consent with technical verification	No comprehensive age restriction: draft law under review aims to establish thresholds
Preventive Obligations for Platforms	Safety by Design; algorithm governance; time restrictions; content moderation	Technical verification (ARCOM-approved); content removal within 1–24 hours; Safe by Design standards	Limited preventive obligations: the National Telecom Regulatory Authority can block harmful websites; draft law seeks proactive measures
Criminal Liability Scope	Shared responsibility: state, guardians, and platforms; fines up to AUD 50M	Platforms liable for noncompliance; civil and criminal sanctions; CNIL oversight	Focus on individual offenders; some provisions for platform liability; draft law aims to expand scope.
Digital Literacy / Awareness Programs	Mandatory awareness programs for children, guardians, and schools; digital citizenship education	Integration of digital education into curricula; cyber-prevention awareness	Limited; draft law proposes digital literacy initiatives in schools.

[48] CNIL. Directives sur le traitement des données des mineurs à des fins publicitaires, 2026. https://www.cnil.fr/fr/transmission-de-donnees-un-reseau-social-des-fins-publicitaires-sanction

[49] Ministère de l'Éducation Nationale, Décret relatif à l'enseignement de la citoyenneté numérique et de la sécurité en ligne dans les établissements scolaires, Bulletin Officiel de l'Éducation Nationale, 2026.

Rapid Response / Content Removal Timelines	Immediate removal of harmful content; reporting protocols enforced by the eSafety Commissioner	1 hour for severe offences; up to 24 hours for other content; civil/criminal sanctions	No standardised timeline; content removal via judicial authorisation; draft law proposes structured timelines
Emerging Technology Provisions (AI / Deepfake)	Legislation encourages platform monitoring; AI risks are addressed indirectly.	Provisions anticipate new digital forms; personal data protection is emphasised.	Current law insufficient for AI-generated abuse; draft law seeks explicit criminalisation.

Source: Author's Interpretation

Table 1 provides a comparative overview of the legislative approaches adopted by Australia, France, and Egypt in regulating digital child protection, highlighting key regulatory dimensions such as age restrictions, preventive obligations for digital platforms, criminal liability, digital literacy initiatives, rapid response mechanisms, and provisions addressing emerging technologies. The comparison demonstrates that Australia and France have adopted more comprehensive and preventive regulatory frameworks, particularly through the establishment of minimum digital age requirements, strong obligations imposed on digital platforms, and clear mechanisms for rapid removal of harmful content. Australia emphasises a stricter preventive model through the "Safety by Design" principle, algorithmic governance, and strong corporate liability supported by the authority of the eSafety Commissioner. France, meanwhile, combines technical age verification, parental consent mechanisms, and strong regulatory oversight by institutions such as ARCOM and CNIL, alongside strict timelines for content removal and the integration of digital literacy into educational curricula.

In contrast, the table shows that Egypt's current legal framework remains comparatively limited and largely reactive, with regulatory provisions scattered across existing laws and lacking a unified preventive structure. While authorities such as the National Telecom Regulatory Authority may block harmful websites, the system does not yet establish comprehensive obligations for digital platforms or standardised procedures for content moderation and removal. However, the draft legislative reforms currently under discussion signal a gradual shift toward a more preventive model, including proposals for clearer age thresholds, expanded platform liability, structured timelines for content removal, and the integration of digital literacy programs in schools. Overall, the table illustrates the evolving global trend toward preventive digital governance while highlighting the regulatory gaps that remain in Egypt's legal system.

The Approach of Egyptian Law in Addressing the Risks of the Digital Environment to Children

Egypt's criminal policy in confronting digital risks to children is characterised as a "reactive deterrent" rather than a "preventive prohibitive" model. The current legislative framework, primarily embodied in the Child Law No. 12 of 1996 (as amended by Law No. 126 of 2008)[50]

[50] Law No. 12 of 1996, *Official Gazette*, Issue No. 13 (Supplement), 28 March 1996; as amended by Law No. 126 of 2008, *Official Gazette*, Issue No. 24 (bis), 15 June 2008; and further amended by Law No. 186 of 2023, *Official Gazette*, Issue No. 49 (bis), 10 December 2023.

and the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018,[51] is grounded in a philosophy of criminalisation and punishment, without establishing a comprehensive proactive procedural framework tailored to the technical specificities of the digital environment. Unlike the Australian and French experiences, Egypt does not yet have a specialised, comprehensive statute dedicated to protecting children in the digital sphere through a preventive approach. Instead, relevant provisions are dispersed across multiple laws, resulting in fragmented regulation and limited legislative integration.

By February 2026, the Egyptian House of Representatives had begun reviewing a new and comprehensive draft law to regulate minors' digital space, seeking to address procedural gaps revealed by the practical application of existing traditional provisions. This anticipated legislative trajectory aims to align with contemporary international standards, drawing inspiration from the stringent approaches adopted in Australia and France, particularly regarding robust age-verification mechanisms and the prohibition of commercial profiling, to establish a national legal framework capable of keeping pace with rapid digital transformations and ensuring optimal child protection.

The principal provisions currently relied upon within Egyptian legislation to protect children in the digital environment may be summarised as follows: First, predominance of Criminal Deterrence: The Egyptian legislator primarily relies on criminal deterrence as the foundation for child protection in the digital sphere. Nevertheless, certain provisions of the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 introduce minimum preventive mechanisms. Notably, the law empowers the National Telecommunications Regulatory Authority to order the blocking of websites or links that disseminate content threatening national security or endangering children's safety, upon judicial authorisation, as a preventive measure to halt ongoing harm.[52] Second, Public Prosecution Monitoring Mechanism: The Egyptian Public Prosecution has established a specialised Monitoring and Analysis Unit, functioning as a proactive protective mechanism by tracking trending content involving child exploitation or cyberbullying, and taking immediate action to remove such content and secure victim protection before the violation escalates.[53]

Criminal Protection Mechanisms for Minors in Egyptian Legislation

Criminal protection for minors in Egyptian law is structured around a network of punitive provisions designed to deter offenders and achieve both specific and general deterrence. These mechanisms operate at two principal levels:

First, Protection under the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018. This law extends beyond traditional offences to encompass emerging digital crimes. Article (25) imposes aggravated penalties (imprisonment and fines) on anyone who violates family principles or infringes upon a minor's right to private life. Penalties are further intensified

[51] Law No. 175 of 2018, *Official Gazette*, Issue No. 32 (bis A), 14 August 2018.

[52] Article 7 of Law No. 175 of 2018 (Anti-Cyber and Information Technology Crimes Law).

[53] Public Prosecutor Decree No. 2376 of 2019, Establishing the Department of Media, Guidance, and Social Communication at the Office of the Public Prosecutor (Egypt).

https://doi.org/10.66325/nusantaralaw.v5i1.222

when the offence involves extortion, threats, or harm to the child's personal dignity, reflecting the legislature's intent to confront digital offenders decisively. [54]

Second, Protection under the Child Law No. 12 of 1996 and its Amendments. The Child Law serves as the overarching framework for protecting minors. Article (116 bis) provides for sentence enhancement when crimes are committed against a child. Its strength lies in its broad coverage of all forms of exploitation, including sexual or commercial exploitation perpetrated through electronic means, considering the use of technology in committing the offence as an aggravating circumstance, warranting maximum penalties.[55]

Legislative Challenges in the Age of Artificial Intelligence

Despite the vitality of Egypt's punitive framework, it faces significant legislative challenges in addressing emerging technologies such as "deepfake" manipulation and generative artificial intelligence. Existing provisions may prove insufficient to encompass crimes that do not rely on authentic images of the child[56], but rather on entirely fabricated digital content. This raises complex legal questions regarding the qualification of the offence as a violation of privacy rights in the absence of tangible victim-generated material.

Accordingly, scholars[57] advocate for explicit legislative intervention to criminalise the digital simulation of child sexual exploitation, without conditioning punishment on the authenticity of the content, so long as it results in the degradation of the child's dignity or the virtual exploitation of their innocence. Such reform would align Egyptian law with contemporary technological realities and reinforce substantive child protection in the evolving digital landscape.

Table 2. Digital Risks to Minors and Legislative Measures Across Selected Jurisdictions

Type of Risk	Description	Australia (Preventive Measures)	France (Preventive Measures)	Egypt (Preventive / Reactive Measures)
Health & Psychological Risks	Eye strain, obesity, sleep disturbances, anxiety, depression, behavioural addiction	Mandatory time restrictions; Safe by Design interface; algorithmic controls	Curriculum-based digital literacy; parental consent for access; Safe by Design standards	Limited preventive measures; draft law proposes platform obligations to monitor

[54] Mohamed Shehata Ibrahim, Criminal Protection of Children Against Electronic Sexual Exploitation, Journal of Legal and Economic Studies, Volume Eleven, Issue Three, September 2025, 233-248, https://jdl.journals.ekb.eg/article_451107_5bf4a8b2695527c38d73acc77ad45872.pdf

[55] Mona El-Sayed El-Tohamy, Criminal Protection of Children in Egyptian and Emirati Legislation.Journal of Legal Research, Faculty of Law, Mansoura University, Volume 15, Issue 94, 2025, 7-36,; https://doi.org/10.21608/mjle.2025.484287

[56] United Nations Office at Geneva, "From Deepfakes to Luring, UN Warnings of Growing AI Risks to Children," January 26, 2026, https://www.ungeneva.org/ar/news-media/news/2026/01/115236/mn-altzyyf-almyq-aly-alastdraj-thdhyrat-ammyt-mn-mkhatr-aldhka.

[57] A. Paradise, "Child Sexual Abuse Material, Progression to Contact Offending and the Evolution of Technology," in *Rethinking the Police for a Better Future*, ed. B. N. Mukherjee et al. (Cham: Springer, 2025), https://doi.org/10.1007/978-3-031-83173-7_17.

				usage; current law is mainly reactive
Behavioural & Social Risks	Exposure to violent/inappropriate content; digital withdrawal; social isolation	Content moderation, age restrictions, and parental oversight via eSafety tools	Age verification, content removal within strict timelines; digital education	No standardised preventive framework; judicial blocking of harmful sites; draft law proposes structured content regulation
Online Sexual Exploitation & Grooming	Cyber grooming, sextortion, and child sexual abuse content	Mandatory reporting; rapid removal protocols; corporate liability; fines up to AUD 50M	Immediate content removal (1–24 hours); civil & criminal liability for platforms; ARCOM oversight	Current focus on punishing offenders; some preventive mechanisms via NTCA blocking; draft law seeks explicit AI/deepfake protections
Cyber Extortion & Cyberbullying	Threats, harassment, coercion, repeated online abuse	Algorithmic monitoring; rapid-response reporting; parental involvement	Mandatory removal of harmful content; CNIL oversight; Safe by Design measures	Reactive criminal prosecution; monitoring units for trending content; draft law proposes formal preventive obligations
Emerging AI / Deepfake Exploitation	Fabricated images, deepfake abuse targeting minors	Platform monitoring encouraged; legal liability for negligence	Strict personal data governance; preemptive prohibition of exploitative processing	Current law is inadequate; the draft law proposes criminalisation of simulated exploitation

Source: Author's Interpretation

Table 2 presents a comparative overview of the digital risks faced by minors and the legislative measures adopted in Australia, France, and Egypt to address these challenges. Overall, the table illustrates that Australia and France have developed proactive and preventive legislative approaches, placing primary responsibility on digital service providers through mechanisms such as age verification, content moderation, algorithmic controls, rapid removal of harmful content, and strengthened digital literacy programs supported by institutional oversight. Australia tends to emphasise strict technical regulation and strong corporate liability, whereas France adopts a more balanced model that combines technical verification, parental consent mechanisms, and digital education within an integrated regulatory framework. In contrast, Egypt's legal framework remains largely reactive, focusing on criminal enforcement after violations occur, with preventive mechanisms still limited and dispersed across different legal instruments. Although a draft law proposes new obligations for digital platforms and stronger protections against emerging threats, such as AI-based exploitation, the current system has yet to establish a comprehensive, integrated preventive framework to protect children in the digital environment.

Conclusion

This study demonstrates that contemporary child protection policies in the digital environment are increasingly characterised by a shift from reactive criminalisation toward preventive legislative governance. Through a comparative analysis of Australia and France, the research reveals that both jurisdictions have developed more proactive regulatory frameworks that impose legally binding obligations on digital platforms. Australia adopts a stricter "protective prohibition" model by establishing a firm minimum age for access to social media and emphasising preventive blocking mechanisms supported by strong institutional oversight through the eSafety Commissioner. In contrast, France employs a more balanced approach by combining minimum age requirements with parental consent mechanisms and digital literacy initiatives, thereby seeking to reconcile children's rights to digital participation with the imperative of protection. In both systems, responsibility for preventing online harm has shifted from individual users to digital service providers, supported by regulatory oversight and graduated sanctions. Compared with these models, the Egyptian legal framework remains largely reactive and fragmented, with regulatory provisions dispersed across existing laws and lacking an integrated preventive structure capable of addressing the evolving risks of the digital ecosystem.

From an academic perspective, this research contributes to the growing literature on digital child protection by providing an early comparative legal analysis of preventive legislative developments between 2024 and 2026. It highlights structural gaps in Egypt's regulatory framework, particularly the absence of comprehensive preventive obligations for digital platforms, a clearly defined minimum digital age, and a coordinated institutional oversight mechanism. These findings suggest the importance of developing a more integrated legal framework that balances children's rights to digital access with effective safeguards against online harm. Future research should therefore move beyond normative legal analysis to examine the practical implementation and enforcement of preventive regulations, including the effectiveness of age verification systems, platform accountability mechanisms, and digital literacy programs. Such empirical, interdisciplinary studies will be essential for evaluating the real impact of preventive legislation and for designing more adaptive, context-sensitive child protection policies in the evolving digital environment.

Acknowledgement

The author would like to express sincere gratitude to the College of Law, University of Al Maarif**,** Iraq, for its academic support and institutional encouragement that contributed to the completion of this research. The author also appreciates the constructive scholarly environment and intellectual resources provided by the institution, which greatly facilitated the development and refinement of this study. The support and commitment of the academic community at the College of Law have been invaluable in advancing research on contemporary legal issues, particularly in the field of digital child protection.

Author Contributions Statement

Tarek El-Sayed Mahmod Abu Okeal conceptualised the study, developed the main research framework, and supervised the overall research process. Hisham Alkasasbeh contributed to the comparative legal analysis and the examination of legislative frameworks

across the selected jurisdictions. Hanaa Ibrahiem Abdullah was responsible for data collection and the analysis of statutory and regulatory materials related to digital child protection. Salaheldin Ragab Fathelbab contributed to the interpretation of findings, drafting, and critical revision of the manuscript to ensure academic rigour and coherence. All authors reviewed and approved the final version of the manuscript and agreed to be accountable for the content of the work.

AI Usage Statement

The authors declare that artificial intelligence (AI)–assisted tools were used only to support language refinement, grammar correction, and general editing during the preparation of this manuscript. The use of such tools did not influence the research design, data analysis, interpretation of results, or the development of the study's arguments and conclusions. All intellectual content, analysis, and scholarly interpretations presented in this article are the sole responsibility of the authors, who have carefully reviewed and validated the final manuscript to ensure its academic integrity and originality.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article. The research was conducted independently without any financial, commercial, or personal relationships that could be construed as a potential conflict of interest. The authors affirm that the study was carried out with full academic integrity and objectivity.

References

Adi, Muhammad Fitri. 'Hadhonah Rights of Children (Not Mumayyis) Based on Compilation of Islamic Law and Child Protection Act'. *NUSANTARA: Journal Of Law Studies* 2, no. 1 (March 2023): 9–22. https://doi.org/10.5281/zenodo.17388734.

Al-Ahmadi, Hala A. M. 'Real Risks of Digital Gameplay: A Policy Perspective on Protecting Children and Adolescents in Online Gaming Environments'. *Doha International Family Institute Journal* 2025, no. 2 (December 2025): 13. https://doi.org/10.5339/difi.2025.13.

A. Topan and E. Uzuntarla Güney, "Parental Digital Literacy and Social Media Supervision," 2025.

ARCOM, About Us: Discover the Institution, accessed February 27, 2026, https://www.arcom.fr/en/about-us/discover-institution.

ARCOM, Rapport sur la Mise en Œuvre des Obligations de Vérification de l'Âge et Sanctions Financières Applicables, Autorité de régulation de la communication audiovisuelle et numérique, 2026, https://www.arcom.fr/presse/lutte-contre-lexposition-des-mineurs-la-pornographie-larcom-met-en-demeure-deux-nouveaux-sites-pornographiques.

Armandin Goetz, "Les Réseaux Sociaux Seront-ils Bientôt Interdits aux Moins de 15 Ans?," Village of Justice, February 13, 2026, https://www.village-justice.com/articles/les-reseaux-sociaux-bientot-interdits-aux-moins-ans-reserve-reserve,56008.html.

Australian Government, Online Safety Act 2021 as amended 2025, Office of the eSafety Commissioner, Canberra, 2021, https://www.esafety.gov.au/about-us/industry-regulation.

Chazizah Gusnita, Lucky Nurhadiyanto, Suyatno Ladiq, "Patterns of Child Grooming and Sexual Harassment in Online Games," Jurnal Perempuan dan Anak 7, no. 2 (2023): 208, https://discovery.researcher.life/article/patterns-of-child-grooming-and-sexual-harassment-in-online-games/e8d910aa51623fec96c1cefd5a6d6c31.

CNIL, Directives sur le Traitement des Données des Mineurs à des Fins Publicitaires, 2026, https://www.cnil.fr/fr/transmission-de-donnees-un-reseau-social-des-fins-publicitaires-sanction.

Djanggih, Hardianto. 'The Phenomenon of Cyber Crimes Which Impact Children as Victims in Indonesia'. *Yuridika* 33, no. 2 (May 2018): 212–231. https://doi.org/10.20473/ydk.v33i2.7536.

Fuentes-González, Andrea, Jesús Palacios, Rosa Rosnati, and Maite Román. 'Profiles of Protection Trajectories among Children in Residential Care'. *Children and Youth Services Review* 183 (2026). https://doi.org/10.1016/j.childyouth.2026.108790.

Hinduja, Sameer, and Justin W. Patchin. 'The Role of Hope in Bullying and Cyberbullying Prevention'. *Frontiers in Sociology* 10 (July 2025). https://doi.org/10.3389/fsoc.2025.1576372.

HAM Al-Ahmadi, "Real Risks of Digital Gameplay: A Policy Perspective on Protecting Children and Adolescents in Online Gaming Environments," Doha International Family Institute Journal 2025, no. 2 (2025): 13, https://doi.org/10.5339/difi.2025.13.

John Tobin, Nicolá Brando, Cynthia Chamberlain, Jonathan Collinson, Louise Forde, The UN Convention on the Rights of the Child: A Commentary, The International Journal of Children's Rights XX (2024): 1–11, 5, https://www.researchgate.net/publication/378854493_The_UN_Convention_on_the_Rights_of_the_Child_-_A_Commentary_edited_by_John_Tobin.

K. Chauviré-Geib, AC. Haag, J. Gerke et al., "Associations Between Online Child Sexual Solicitation and Abuse and Offline Child Maltreatment: A Latent Class

Analysis," Eur Child Adolesc Psychiatry, 2025, https://doi.org/10.1007/s00787-025-02885-5.

K. Nikolopoulou, "Child-centred Integration of Generative AI in Early Learning: Balancing Promises and Challenges," AI Brain Child 1 (2025): 21, https://doi.org/10.1007/s44436-025-00023-1.

Kathryn C. Seigfried-Spellar, Marcus K. Rogers, Nina L. Matulis, Jacob S. Heasley, "Testing a Hybrid Risk Assessment Model: Predicting CSAM Offender Risk from Digital Forensic Artefacts," Forensic Science International: Digital Investigation 50, Issue Supplement (2024): 301712.

Kim Osman, Michael Dezuanni, Lynrose Jane Genon, Young Australians' Perspectives on the Social Media Minimum Age Legislation, Digital Media Research Centre, 2025, 5, https://apo.org.au/node/332901.

L. Alfies Sihombing, Yeni Nuraeni, Wahyudi, Loso Judijanto, Abidah Abdul Ghafar, "Sexual Grooming of Children Mode through Live Streaming: Legal Gaps in the Face of Anonymity of Online Transactions," Lex Scientia Law Review 9, no. 2 (2025): 1791, https://garuda.kemdiktisaintek.go.id/documents/detail/5797102.

Law No. 12 of 1996, Official Gazette, Issue No. 13 (Supplement), March 28 1996; as amended by Law No. 126 of 2008, Issue No. 24 (bis), June 15 2008; and further amended by Law No. 186 of 2023, Issue No. 49 (bis), December 10 2023.

Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, Journal officiel de la République française, 8 July 2023, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533.

Marjun, Saroji, and Farhan Farhan. 'Cyberbullying and Legal Protection for Victims in the Digital Era: A Case Study on Social Media Platforms'. *Hakim: Jurnal Ilmu Hukum Dan Sosial* 3, no. 1 (February 2025): 955–973. https://doi.org/10.51903/hakim.v3i1.2290.

Magalie Dansac Le Clerc and Juliette Leportois, "France Introduces New Law to Enhance the Protection of Children's Rights in France," March 19, 2024, https://connectontech.bakermckenzie.com/france-introduces-new-law-to-enhance-the-protection-of-childrens-rights-in-france/.

Ministère de l'Éducation Nationale, Décret relatif à l'enseignement de la citoyenneté numérique et de la sécurité en ligne dans les établissements scolaires, Bulletin Officiel de l'Éducation Nationale, 2026.

Mohamed Shehata Ibrahim, "Criminal Protection of Children Against Electronic Sexual Exploitation," Journal of Legal and Economic Studies 11, no. 3 (September 2025): 233–248, https://jdl.journals.ekb.eg/article_451107_5bf4a8b2695527c38d73acc77ad45872.pdf.

Mona El-Sayed El-Tohamy, "Criminal Protection of Children in Egyptian and Emirati Legislation," Journal of Legal Research, Faculty of Law, Mansoura University 15, no. 94 (2025): 7–36, https://doi.org/10.21608/mjle.2025.484287.

Muhammad Al-Saeed Al-Qaz'a, Tariq Al-Sayed Abu Aqil, "Criminal Confrontation: The Use of the Dark Web to Assault Personal Data," Jerash Journal of Research and Studies 25, no. 2B (2025): 459–493, https://www.jpu.edu.jo/jpu/files/center/file_fd25d5fc8813.pdf.

Nikolopoulou, Kleopatra. 'Child-Centred Integration of Generative AI in Early Learning: Balancing Promises and Challenges'. *AI, Brain and Child* 1, no. 1 (December 2025): 21. https://doi.org/10.1007/s44436-025-00023-1.

Nurjanah, Siti, Ahmad Syarifudin, Muhammad Mujib Baidhowi, Elva Mahmudi, and Hidayat Darussalam. 'Children's Rights in Islamic Law: A Contemporary Study of Family Practices'. *MILRev: Metro Islamic Law Review* 4, no. 2 (July 2025): 933–953. https://doi.org/10.32332/milrev.v4i2.10077.

OECD, Children in the Digital Environment, 2020.

Online Safety Amendment (Social Media Minimum Age) Act 2024 (Australia), https://www.legislation.gov.au/C2024A00127/asmade/text.

Osório de Barros et al., "Artificial Intelligence and Child Development: Ethical and Privacy Implications," 2025.

Page Jeffery, Catherine. "Trust Us! We Know What We Are Doing!" Parent-Adolescent Digital Conflict in Australian Families. *Journal of Children and Media* 18, no. 4 (October 2024): 472–488. https://doi.org/10.1080/17482798.2024.2358947.

Paradise, Alex. 'Child Sexual Abuse Material, Progression to Contact Offending and the Evolution of Technology'. In *Rethinking the Police for a Better Future : Navigating Policing Challenges with Accountability and Trust*, edited by Baidya Nath Mukherjee, Ruwan Uduwerage-Perera, Meera Mathew, and Sanjeev Kumar Tripathi, 259–73. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-83173-7_17.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19 2022, on a Single Market for Digital Services (Digital Services Act).

République Française, Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (SREN), Article 15, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368.

Romil Rawat, Sanjaya Kumar Sarangi, A. Samson Arun Raj, Janet Olivia Richmond, Purvee Bhardwaj, Child Protection Laws and Crime in the Digital Era, IGI Global, July 2025, 5:8, https://www.igi-global.com/book/child-protection-laws-crime-digital/381315.

Robertson, Kirsty, and Alison McLuckie. 'Social Protection for Children: Global Landscape and Domestic Provision in the UK'. *Paediatrics and Child Health (United Kingdom)* 36, no. 2 (2026): 45–49. https://doi.org/10.1016/j.paed.2025.11.007.

S. Bhalla et al., "Child Victimisation in Cybercrime Environments," 2025.

Sameer Hinduja, Justin W. Patchin, "The Role of Hope in Bullying and Cyberbullying Prevention," Front. Sociol., Sec. Sociological Theory 10 (2025): 4, https://doi.org/10.3389/fsoc.2025.1576372.

Sonia Livingstone, Realising Children's Rights in Relation to the Digital Environment, UN Committee on the Rights of the Child (CRC/C/GC/25), 2021, para. 84, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en.

Tara A. Kristick, Online Child Sexual Exploitation: Understanding the Origins and Problems within the Criminal Justice System, 2025, 40.

Tariq Al-Sayed Mahmoud Abu Aqil, "Criminal Confrontation of Exploiting Technical Development in Assault on the Child's Right to the Picture: Comparative Study," Journal of Legal Studies, no. 9 (February 2026): 389–395, https://www.nuwab.bh/wp-content/uploads/2026/02/D8A7D984D8B9D8AFD8AF-D8A7D984D8AAD8A7D8B3D8A9.pdf.

Terry Flew, Timothy Koskie, Agata Stepnik, "Digital Policy as Problem Space: Policy Formation, Public Opinion, and Australia's Online Safety Amendment (Social Media Minimum Age) Act 2024," The University of Sydney, Australia, December 18, 2025, 4, https://journals.sagepub.com/doi/10.1177/1329878X251406315.

Topan, Aysel, Emine Uzuntarla Güney, Betül Akkoç, Sümeyye Özdemir, and Fadime Üstüner Top. 'The Relationship Between Parents' Digital Parenting Awareness,

Their Social Media Parenting Practices, and The Social Media Usage Levels of Their Children Aged 6–18'. *Child and Adolescent Social Work Journal*, ahead of print, November 16 2025. https://doi.org/10.1007/s10560-025-01059-1.

UNICEF, Feeding Profit: How Food Environments Are Failing Children – 2025 Child Nutrition Report, September 2025.

United Nations Office at Geneva, "From Deepfakes to Luring, UN Warnings of Growing AI Risks to Children," January 26, 2026, https://www.ungeneva.org/ar/news-media/news/2026/01/115236/mn-altzyyf-almyq-aly-alastdraj-thdhyrat-ammyt-mn-mkhatr-aldhka.

United Nations, Committee on the Rights of the Child, General Comment No. 25 on the Rights of the Child in the Digital Environment, 2021, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

Vo, Nhat Dinh Quang, Duy Quy Nguyen-Phuoc, Amjad Pervez, and Jaeyoung Jay Lee. 'Parents Protect Their Children When Travelling: Exploring Traffic Safety Behavioural Intentions through the Lens of Cognitive Appraisal and Protection Motivation Theories'. *Accident Analysis and Prevention* 228 (2026). https://doi.org/10.1016/j.aap.2026.108421.

Wang, Youli, Baocheng Pan, Honghuan Fang, Jingkai Sun, Bijing Ren, Ziyi Feng, Bowen Xiao, Pin Xu, and Yan Li. 'From Family to School: The Dual Protection of Father-Child Relationship and Teacher-Student Relationship on Children's Mental Health Problems'. *BMC Psychology* 14, no. 1 (2026). https://doi.org/10.1186/s40359-025-03793-8.