The journal of El-Ryssala for studies and research in humanities

Volume : 11 / N° : 03/ 2026. pp 284-299

PISSN : 2543-3938 - EISSN : 2602-7771

The Right to Digital Protection of the Child between the Provisions of Islamic Jurisprudence and Contemporary Legislation: A Comparative Study in Light of the Challenges of Generative Artificial Intelligence

Jihane Louabdia,

Echahid Cheikh Larbi Tebessi university (Algeria),
jihane.louabdia@univ-tebessa.dz

Received: 06/07/2026 **Accepted**: 10/09/2026

Abstract:

This study examines whether Islamic juristic rulings and contemporary legislation adequately protect children in the digital environment amid risks arising from generative artificial intelligence. It argues that digital protection is a fundamental right linked to preserving life, intellect, honor, dignity, and privacy. Using descriptive-analytical, comparative, and inductive methods, the study finds that Islamic jurisprudence provides strong foundations through its objectives and principles, while contemporary legislation, despite notable progress, still requires more effective mechanisms to address deepfakes, digital exploitation, children's data collection, and harmful online content.

Keywords: *Child; Digital Protection; Islamic Jurisprudence; Generative Artificial Intelligence; Digital Privacy; Children's Rights.*

I. INTRODUCTION

The digital revolution has brought about a profound transformation in the structure of rights and freedoms. The protection of individuals is no longer confined to the traditional physical sphere but has extended to the digital environment, which has become a fundamental space for learning, communication, entertainment, and personality development. Children are among the groups most affected by this transformation because of their age-related, psychological, and cognitive vulnerabilities, as well as their increasing engagement with digital platforms, smart applications, electronic games, and artificial intelligence systems.

The significance of this subject has grown with the emergence of generative artificial intelligence, which is no longer limited to producing text, images, or audio but is now capable of generating highly realistic content. While these technologies offer valuable opportunities for education and entertainment, they may also be exploited for deception, the creation of deepfakes, blackmail, or the production of harmful content that threatens children's dignity, privacy, and psychological well-being. Consequently, the digital protection of children is no longer merely a technical or family concern but has become a matter of human rights, legislation, ethics, and Islamic jurisprudence that requires a comprehensive comparative analysis.

The importance of this study lies in its examination of an emerging dimension of children's rights that has not yet received sufficient attention in Arab juristic and legal scholarship, particularly from the perspective of linking the objectives of Islamic Sharia with the challenges posed by generative artificial intelligence. Its significance also stems from its effort to develop a comparative framework that integrates Sharia principles, legal analysis, and an understanding of contemporary technological risks.

Accordingly, the study seeks to answer the following research question:

To what extent can the rulings of Islamic jurisprudence and contemporary legislation provide effective protection for children in the digital environment in light of the emerging risks posed by generative artificial intelligence?

The study seeks to answer the following research questions:

- What is meant by the right to the digital protection of the child?
- What are the most significant risks that generative artificial intelligence poses to children?
- What is the Sharīʿah basis for this right in light of the objectives of the Sharīʿah and the juristic legal maxims?
- How have contemporary legislation and international legal instruments addressed the protection of children in the digital environment?
- What are the points of convergence and the shortcomings between the juristic and legal approaches in this field?

The study is based on the hypothesis that the digital protection of children constitutes an emerging right that can be grounded in the objectives and general principles of the Sharīʿah while also being supported through international legal instruments and contemporary legislation. However, the effectiveness of this protection depends on the ability of both legal and juristic frameworks to keep pace with the evolving risks associated with generative artificial intelligence.

The study seeks to achieve the following objectives:

- To define the concept of the right to the digital protection of the child.

- To explain the emerging risks that generative artificial intelligence poses to children's rights.
- To establish the Sharīʿah foundations of the digital protection of the child in light of the objectives of the Islamic Sharīʿah.
- To analyze the position of contemporary legislation regarding the protection of children in the digital environment.
- To propose juristic and legal mechanisms to strengthen the digital protection of children.

Literature Review

Numerous studies have examined the protection of children in the digital environment from various perspectives. Some international studies, such as the work of (Livingstone & Third, 2017), have explored the evolution of children's rights in the digital age and emphasized the importance of ensuring a safe digital environment that respects children's privacy. Reports published by (UNICEF, 2025) and (UNESCO, 2023) have also highlighted the risks associated with the use of generative artificial intelligence and its impact on children while proposing preventive and legislative measures to enhance their protection. In contrast, Islamic juristic studies have primarily focused on explaining the objectives of the Sharīʿah and the general principles that protect individuals from harm, without specifically examining the child's right to digital protection as an independent right in the context of generative artificial intelligence. Accordingly, this study distinguishes itself by integrating juristic foundations, legal analysis, and contemporary technological developments within a comparative framework that seeks to develop a comprehensive approach to protecting children in the digital environment.

The study employs the descriptive-analytical method to explain the concepts and risks associated with the digital environment, the comparative method to examine Islamic juristic rulings alongside contemporary legislation, and the inductive method to derive the relevant juristic principles and objectives of the Islamic Sharīʿah. It also adopts the critical method to evaluate the adequacy of existing legal frameworks for protecting children in the digital environment.

The study is divided into three main sections:

- **Section One:** The conceptual and Sharīʿah framework of the child's right to digital protection.
- **Section Two:** The risks of generative artificial intelligence to children's rights.
- **Section Three:** Mechanisms for protecting children in the digital environment through Islamic jurisprudence and contemporary legislation.

1. The Conceptual and Sharīʿah Framework of the Child's Right to Digital Protection

The contemporary world is undergoing rapid digital transformation that has reshaped patterns of communication, learning, entertainment, and social interaction. As a result, children are becoming increasingly engaged with the digital environment from an early age. This reality has given rise to new risks that were largely absent from the traditional environment, including cyberbullying, the theft of personal data, digital exploitation, deepfakes, and the psychological and behavioral effects associated with the unsafe use of digital technologies. Consequently, there is a growing need to recognize

digital protection as a fundamental right of the child that requires conceptual, Sharīʿah, and legal grounding to define its scope, dimensions, and mechanisms of protection.

1.1 The Concept of the Child's Right to Digital Protection and Its Legal Dimensions

1.1.1 The Concept of the Child's Right to Digital Protection

There is no universally accepted definition of the child's right to digital protection in contemporary legal scholarship. However, most definitions describe it as a set of legal, technical, and educational measures designed to protect children from the risks they may encounter while using digital media, the Internet, and smart technologies (Livingstone & Third, 2017).

It has also been defined as the set of rights and safeguards that enable children to use the digital environment safely while preserving their physical, psychological, and moral well-being and protecting their personal data, privacy, and human dignity from various forms of abuse, exploitation, and digital manipulation (UNICEF, 2025).

Based on these definitions, the child's right to digital protection may be defined as follows:

The child's right to enjoy a safe digital environment that ensures protection from the harms and risks arising from the use of digital technologies and artificial intelligence while safeguarding the child's privacy, human dignity, and best interests.

1.1.2 The Legal Dimensions of the Child's Right to Digital Protection

Digital protection for children encompasses multiple, overlapping dimensions, the most prominent of which are the following:

A. The Dimension of Digital Privacy Protection

Digital privacy is considered one of the most important rights associated with the digital environment, as children leave a significant amount of personal data while using digital platforms, smart applications, and online games. The seriousness of this issue lies in the possibility that such data may be collected, analyzed, commercially exploited, or used to influence children's behavior and shape their choices (Organisation for Economic Co operation and Development (OECD), 2025).

Consequently, modern legislation has increasingly focused on strengthening the legal protection of children's personal data, recognizing children as a vulnerable group that is particularly susceptible to digital exploitation.

B. The Dimension of Protection from Harmful Content

The digital environment constitutes an open space that enables children to access content containing violence, pornography, hate speech, or misleading information, all of which may negatively affect their psychological, moral, and cognitive development (UNESCO, 2023).

The seriousness of this issue is further intensified by the rapid advancement of recommendation algorithms, which are increasingly capable of directing children toward specific types of content based on analyses of their digital behavior.

C. The Dimension of Protection from Digital Exploitation

Digital exploitation refers to the use of digital technologies or electronic means to harm or exploit children financially, sexually, or psychologically. This includes practices such as online blackmail, digital trafficking, and the unauthorized exploitation of children's images and personal data (Interpol, 2024).

The increasing prevalence of this type of crime has prompted many international organizations to call for stronger legal protection of children within the digital environment.

D. The Dimension of Protection from the Risks of Artificial Intelligence

Generative artificial intelligence has become capable of producing text, images, audio, and video that are sometimes difficult to distinguish from authentic content. This has created new risks, including deepfakes, identity impersonation, and the creation of false content that may directly or indirectly target or exploit children (UNICEF Innocenti, 2025).

Accordingly, digital protection is no longer limited to safeguarding children from traditional harmful content. It now also encompasses protection from the complex digital practices generated by modern artificial intelligence systems.

1.2 The Sharīʿah Basis of the Child's Right to Digital Protection

Although the digital environment in its modern forms was unknown in earlier eras, this does not mean that there is no Sharīʿah basis for protecting children within it. Islamic Sharīʿah is characterized by its flexibility and its ability to address unprecedented issues and emerging developments through the objectives of the Sharīʿah (*Maqāṣid al-Sharīʿah*) and the universal legal maxims (*al-qawāʿid al-fiqhiyyah*).

1.2.1 The Digital Protection of the Child in Light of the Objectives of the Islamic Sharīʿah

The objectives of the Islamic Sharīʿah constitute the highest reference framework governing Sharīʿah rulings. They aim to promote human welfare and prevent harm.

A. Protection of Life

The protection of life is not limited to safeguarding individuals from physical harm. It also includes protection from anything that threatens psychological and moral well-being. Given the serious psychological harm that digital crimes, cyberbullying, and online blackmail may inflict on children, digital protection falls within the scope of preserving life (*ḥifẓ al-nafs*) (Al-Shatibi, 1997).

B. Protection of Intellect

The intellect is one of the five essential objectives that the Sharīʿah seeks to preserve. Since the Sharīʿah prohibits everything that corrupts or impairs the intellect, harmful digital content, misleading information, and digital addiction constitute contemporary threats that may negatively affect children's intellectual and cognitive development. Consequently, digital protection represents an extension of the objective of preserving the intellect (*ḥifẓ al-ʿaql*).

C. Protection of Honor and Human Dignity

Human dignity is one of the fundamental objectives of the Islamic Sharīʿah. Allah the Almighty says:

"And We have certainly honored the children of Adam." (Qur'an 17:70)

The relationship between digital protection and this objective is reflected in safeguarding children from online defamation, violations of privacy, the publication of offensive images and videos, and deepfakes that may damage their reputation and human dignity.

1.2.2 Digital Protection of the Child in Light of the Major Jurisprudential Rules

A. The Rule of No Harm and No Reciprocal Harm

This rule is one of the most important jurisprudential principles governing various acts and transactions. It establishes the obligation to eliminate any harm affecting children within the digital environment (Al-Hanbali, 1998).

Based on this principle, individuals, institutions, and the state are obligated to adopt measures capable of preventing digital harms or minimizing their risks.

B. The Rule of Removing Harm

Where digital harm to a child has occurred, this rule requires that it be removed and that its effects be remedied, as far as possible. This may include deleting harmful content, holding those responsible accountable, and addressing the consequences of the harm suffered by the child.

C. The Rule of Blocking the Means

This rule seeks to prevent the means that lead to harm before it occurs. Accordingly, monitoring certain applications and digital platforms, or restricting particularly dangerous uses of modern technologies, is consistent with the Sharīʿah principle of prevention and the protection of children from foreseeable risks.

D. The Principle of the Best Interests of the Child

Although the concept of the "best interests of the child" is regarded as a modern principle in international law, its underlying philosophy has long been recognized in Islamic jurisprudence, which places special emphasis on protecting minors, promoting their welfare, and giving priority to their interests whenever competing interests arise.

It is evident from the foregoing discussion that the child's right to digital protection is an emerging right necessitated by contemporary technological developments. This right extends beyond technical safeguards to encompass the protection of children's privacy, dignity, and psychological and intellectual well-being. It is also evident that Islamic Sharīʿah, through its overarching objectives and universal legal maxims, provides a solid normative foundation for recognizing this emerging right and incorporating it into the broader framework of rights designed to protect children and promote their welfare. Accordingly, the child's right to digital protection may be regarded as a contemporary manifestation of the Sharīʿah objectives of preserving life, intellect, honor, and human dignity. This provides an appropriate foundation for examining the risks that generative artificial intelligence poses to children's rights within the digital environment.

2. The Risks of Generative Artificial Intelligence to Children's Rights in the Digital Environment

The rapid development of generative artificial intelligence has brought about fundamental changes in the nature of digital interaction. Intelligent systems are now capable of generating text, images, videos, and audio that closely resemble authentic content. Although these technologies offer significant opportunities in education, learning, and creativity, they also present growing challenges and risks for children, who are among the most vulnerable groups in the digital environment.

The seriousness of these technologies lies in their capacity to influence the development of children's personalities, behavior, awareness, and perception of reality. They also create opportunities for violations of children's privacy, manipulation of their personal data, and exposure to new forms of digital violence and exploitation.

Consequently, it has become essential to examine these risks and analyze their legal, human rights, and social implications.

2.1 Risks to Children's Digital Privacy and Personal Data

Digital privacy is among the rights most vulnerable to infringement in the age of artificial intelligence, as most AI systems depend on collecting and analyzing vast amounts of data to improve their performance and enhance their services. These practices, however, raise significant legal and ethical concerns, particularly when they involve children's personal data.

2.1.1 Risks Associated with the Collection of Children's Personal Data

Artificial intelligence relies on data as the primary resource for training algorithms and supporting automated decision-making. Consequently, digital platforms and smart applications routinely collect detailed information about children, including:

- Age and gender.
- Geographic location.
- Interests and behavioral patterns.
- Educational and recreational activities.
- Daily digital interactions.

Recent studies indicate that many applications designed for children collect more personal data than is necessary to provide their services, thereby increasing the risk of misuse, data breaches, or commercial exploitation (UNICEF, 2025).

The seriousness of this issue is compounded by children's limited understanding of the nature of the information they disclose while using digital platforms and applications. As a result, they are significantly more vulnerable than adults to violations of their digital privacy.

2.1.2 Risks of Digital Profiling and Behavioral Manipulation

One of the most significant risks posed by artificial intelligence technologies is their ability to create detailed digital profiles of children by analyzing their personal data and online behavior.

Digital profiling refers to the process of classifying individuals and predicting their behavior or influencing their decisions through the use of intelligent algorithms (European Union Agency for Fundamental Rights (FRA), 2024).

For children, this practice creates the potential to:

- Influence their consumer choices.
- Shape their beliefs and opinions.
- Target them with personalized advertisements.
- Influence their future preferences and behaviors.

Such practices may undermine children's freedom of choice and personal autonomy while affecting their psychological and intellectual development.

2.1.3 Violations of the Right to Digital Privacy

The right to privacy is a fundamental human right recognized under international law. However, recent technological developments have made children increasingly

vulnerable to continuous monitoring and the collection and analysis of their personal data without a full understanding of these processes.

These risks are further amplified by the use of facial recognition technologies and the analysis of images, voice recordings, and biometric data, which enable AI systems to identify and track children with a high degree of accuracy (Organisation for Economic Co operation and Development (OECD), 2025).

As a result, children's rights to privacy and to control their personal data are increasingly at risk. Both rights have become essential components of the broader framework of children's rights in the digital age.

2.2 Risks Associated with AI-Generated Content and the Digital Exploitation of Children

In addition to the risks associated with personal data, generative artificial intelligence presents significant challenges arising from the nature of AI-generated content and its potential impact on children. These challenges are intensified by the ease with which false or harmful content can be created, often making it difficult to distinguish from authentic material.

2.2.1 Risks of Deepfakes

Deepfakes are among the most concerning applications of generative artificial intelligence, as they enable the creation of highly realistic images, videos, and audio recordings that are entirely fabricated.

For children, this technology may be used for:

- Defamation.
- Cyber blackmail.
- Identity impersonation.
- The creation and dissemination of offensive or fabricated content.

Many international organizations have warned of the growing use of deepfake technologies to target children and unlawfully exploit their images and personal data (UNICEF Innocenti, 2025).

2.2.2 Risks of the Digital Sexual Exploitation of Children

The development of artificial intelligence tools has led to the emergence of new forms of digital sexual exploitation of children. Some applications are now capable of creating fake images or videos of children or modifying real images in ways that violate their dignity and fundamental rights.

Recent international reports indicate growing concern about the use of artificial intelligence to produce and distribute child sexual exploitation material on the Internet. This has prompted many countries and international organizations to call for the criminalization of these practices and the strengthening of penalties associated with them (Interpol, 2024).

The consequences of these crimes extend beyond legal issues to include severe psychological and social effects that may remain with the child for a long time.

2.2.3 Risks of Misinformation and Cognitive Influence

Generative artificial intelligence can produce information that appears accurate and reliable despite containing errors or misleading content. This phenomenon is referred to in the technical literature as "AI hallucination."

The seriousness of this phenomenon increases when it affects children because they have a limited ability to verify the accuracy of information and distinguish authentic content from fabricated content.

Repeated exposure to misleading information may lead to:

- Forming inaccurate perceptions of reality.
- Impairing critical thinking.
- Promoting extremist or false ideas.
- Weakening trust in reliable sources of knowledge.

2.2.4 Risks of Digital Addiction and Social Isolation

Many digital platforms use algorithms designed to increase the duration of use and encourage continuous interaction with content.

With the advancement of artificial intelligence, these algorithms have become more effective at understanding children's interests and targeting them with content that captures their attention for extended periods. This may lead to:

- Digital addiction.
- Sleep disorders.
- Poor academic performance.
- Social isolation.
- Anxiety and depression among some children (UNESCO, 2023).

These effects represent some of the most significant health and psychological challenges associated with the use of modern digital technologies.

2.3 The Implications of the Risks of Artificial Intelligence for Children's Rights

The effects of the previously discussed risks are not limited to the violation of a single right of the child. Rather, they extend to affect an interconnected set of fundamental rights recognized by international conventions and national legislation.

2.3.1 The Impact on the Right to Human Dignity

Practices such as digital defamation, deepfakes, and identity impersonation harm the child's dignity and social reputation. These practices are inconsistent with the fundamental principles upon which human rights are based.

2.3.2 The Impact on the Right to Healthy Development

Exposure to harmful content, misleading information, and digital addiction may adversely affect the child's psychological, cognitive, and social development. This can negatively influence the child's ability to develop a healthy and well-balanced personality.

2.3.3 The Impact on the Right to Digital Security

Digital security has become an integral component of child protection. It is not possible to ensure that children fully enjoy their digital rights while they remain continuously exposed to hacking, cyberbullying, blackmail, or online exploitation.

2.3.4 The Impact on the Best Interests of the Child

The best interests of the child constitute the guiding principle for all policies and measures concerning children. However, many artificial intelligence applications

continue to be designed primarily according to commercial or technical considerations, without giving sufficient attention to children's privacy, safety, and developmental needs. This situation threatens the effective implementation of this principle and highlights the need to reconsider the mechanisms governing the design, development, and deployment of these systems.

It is evident from the foregoing discussion that, despite the significant opportunities generative artificial intelligence offers for learning and innovation, it also presents multiple risks that affect the core of children's rights in the digital environment. These risks include violations of digital privacy, online exploitation, deepfakes, misinformation, digital addiction, and other harmful practices that may adversely affect children's physical, psychological, cognitive, and social well-being. Addressing these challenges requires the establishment of a comprehensive protection framework that integrates Islamic legal principles (Sharia), statutory legal safeguards, technical measures, and educational strategies. These protection mechanisms will be examined in the third section through an analysis of child protection in the digital environment from the perspectives of Islamic jurisprudence and contemporary legislation.

3. Mechanisms for the Digital Protection of the Child Between Islamic Jurisprudence and Contemporary Legislation

The risks associated with generative artificial intelligence have demonstrated that protecting children in the digital environment is no longer solely an individual or family responsibility. Rather, it has become a shared responsibility involving families, educational institutions, governments, legislative bodies, technology companies, and international organizations. These challenges have also highlighted the need to develop preventive and remedial approaches that balance children's access to the benefits of modern technology with effective protection from its associated risks.

From this perspective, contemporary legal systems are increasingly moving toward the development of comprehensive frameworks for protecting children in the digital environment. This approach finds a strong foundation in Islamic jurisprudence, which recognizes the preservation of life, intellect, honor, and dignity as among the higher objectives (*Maqāṣid*) of the Sharīʿah. Accordingly, examining child protection mechanisms requires an analysis of both preventive and remedial measures capable of providing effective protection for children in the digital age.

3.1 Preventive Mechanisms for Protecting the Child in the Digital Environment

Prevention constitutes the cornerstone of protecting children from digital risks because preventing harm before it occurs is more effective than addressing its consequences afterward. This principle is consistent with the Islamic legal maxim: *"Preventing harm takes precedence over securing benefits."*

3.1.1 The Role of the Family in Achieving Digital Protection for the Child

The family represents the first line of defense against digital risks because it is the primary environment responsible for the care, education, and guidance of the child.

This role includes:

- Monitoring the child's use of digital media.
- Guiding the child toward the safe and responsible use of the Internet.
- Teaching the child the principles of digital privacy.
- Raising awareness of the risks associated with sharing personal information.
- Developing the child's ability to distinguish between safe and harmful content.

This responsibility finds its legal foundation in the Qur'anic verse:

"O you who have believed, protect yourselves and your families from a Fire." (Qur'an 66:6)

This verse establishes the obligation to care for and protect children from anything that may threaten their religious or worldly well-being.

In the contemporary digital context, this obligation extends to protecting children from cyber risks that may adversely affect their personality, psychological well-being, and intellectual development.

3.1.2 The Role of Educational Institutions in Digital Education

Schools are required to fulfill a new role in digital education by equipping children with the skills and knowledge needed to use technology safely and responsibly.

Digital education includes:

- Developing awareness of digital citizenship.
- Teaching the basic principles of cybersecurity.
- Strengthening critical thinking in relation to digital content.
- Combating misinformation and disinformation in digital media.
- Training children to protect their personal data.

UNESCO has confirmed that digital education has become one of the fundamental requirements for preparing children to live in modern digital societies (UNESCO, 2023).

3.1.3 The Role of Technology Companies in Protecting Children

Responsibility for digital protection is no longer limited to users or government authorities. Technology companies have become key stakeholders in ensuring children's digital safety.

This requires:

- Designing platforms that prioritize the best interests of the child.
- Applying the principle of Safety by Design.
- Strengthening parental control tools.
- Preventing advertising that targets children.
- Reducing the collection of unnecessary personal data.

Many international organizations have adopted this approach by calling on technology companies to integrate children's rights into every stage of designing and developing digital systems (UNICEF, 2025).

3.1.4 Digital Protection of the Child as a Preventive Objective in Islamic Jurisprudence

The digital protection of children can be viewed as a contemporary extension of the principle of prevention, which occupies a central position in Islamic jurisprudence.

Islamic Sharia does not merely prohibit harm after it occurs. Rather, it seeks to prevent the causes and means that lead to harm through principles such as:

- Blocking the means.

- Averting harm.
- Taking precaution to protect the public interest.
- Preventing harm before it occurs.

Accordingly, adopting preventive measures to protect children in the digital environment is fully consistent with the preventive approach established by Islamic Sharia across various fields.

3.2 Legislative and Judicial Mechanisms for Protecting Children in the Digital Environment

Alongside preventive measures, legal and judicial mechanisms play a crucial role in regulating the digital environment and providing effective protection for children when they are exposed to digital risks or violations.

3.2.1 Protection Provided by International Conventions

International conventions have given increasing attention to children's rights in the digital environment, particularly in response to the rapid advancement of technology.

The (United Nations, 1989) is the primary international reference in this field, as it established the following principles:

- The best interests of the child.
- The right to protection from exploitation.
- The right to privacy.
- The right to healthy development.

General Comment No. 25, issued by the Committee on the Rights of the Child in 2021, explicitly affirmed that these rights extend to the digital environment and emphasized the obligation of States to take the necessary measures to protect children online (Committee on the Rights of the Child, 2021).

3.2.2 Protection in Comparative Legislation

Many legal systems have developed legislation specifically aimed at protecting children in the digital environment.

Among the most prominent examples are:

A. The General Data Protection Regulation (GDPR)

The GDPR provides special protection for children's personal data and imposes stricter conditions on its collection, processing, and use. It also places significant obligations on organizations that process the personal data of minors (European Parliament and Council, 2016).

B. The UK Age Appropriate Design Code

The UK Age Appropriate Design Code is considered one of the most advanced legal frameworks for protecting children online. It requires digital service providers to design their products and services in a manner that respects children's rights and promotes their digital safety.

C. Recent U.S. Legislation

The United States has introduced a growing number of legislative initiatives aimed at protecting children from digital addiction, online exploitation, and harmful commercial practices on digital platforms.

3.2.3 Protection in Algerian Legislation

The Algerian legislator has given increasing attention to protecting children through:

- Child Protection (Law No. 15-12 , 2015).
- The Law on the Protection of Natural Persons in the Processing of Personal Data.
- Legal provisions relating to combating cybercrime.
- Criminal provisions concerning the protection of minors from exploitation and cyberattacks.

Despite the importance of these legal frameworks, the rapid development of artificial intelligence makes it necessary to continuously update the legal system to address emerging digital risks effectively.

3.2.4 The Role of the Judiciary in Protecting Children in the Digital Environment

The judiciary serves as the primary safeguard for enforcing the legal protection of children by:

- Interpreting legal provisions in a manner that promotes the best interests of the child.
- Ordering the removal or restriction of harmful digital content.
- Protecting children's personal data.
- Awarding compensation for harm resulting from digital violations.
- Prosecuting crimes involving the misuse of artificial intelligence.

The role of the judiciary has become increasingly important with the emergence of new forms of digital harm that require judicial interpretation capable of keeping pace with technological developments.

3.3 Towards an Integrated Approach to Protecting Children in the Age of Artificial Intelligence

Practical experience has shown that relying solely on legal measures or technological solutions is insufficient to ensure the effective protection of children in the digital environment.

Addressing the risks associated with generative artificial intelligence therefore requires an integrated approach based on cooperation among all relevant stakeholders.

3.3.1 Integrating the Jurisprudential and Legal Approaches

Islamic Sharia and modern legal systems share the common objective of protecting children and safeguarding their fundamental interests.

Islamic jurisprudence provides the ethical and value-based foundation for protection, while modern legislation establishes the legal and institutional mechanisms necessary to implement it.

Accordingly, the digital protection of children can be viewed as an area in which Islamic legal principles and contemporary legal frameworks complement one another.

The protection of children should not be limited to the stage of technology use. It should begin during the design and development of digital systems.

This requires:

- Assessing potential risks to children before launching digital products.
- Preventing harmful uses of artificial intelligence.
- Strengthening transparency and accountability.
- Taking children's developmental stages and age-specific needs into account.

II. Conclusion

The study concluded that the rapid digital transformations and the unprecedented development of generative artificial intelligence technologies have created new challenges that affect the very essence of children's rights and fundamental freedoms within the digital environment. This has made the right to digital protection a legal, legislative, and ethical necessity that cannot be overlooked. The study showed that this right is not limited to protecting personal data or reducing technical risks. It also extends to preserving the child's dignity, privacy, and psychological, mental, and intellectual well-being in the face of emerging forms of digital exploitation and manipulation.

The study also demonstrated that Islamic jurisprudence, with its rich universal objectives and flexible legal principles, possesses a strong foundational capacity to accommodate this emerging right and connect it to the objectives of preserving life, intellect, honor, and human dignity. This makes it a suitable reference framework for keeping pace with digital developments. The study further found that contemporary legislation has made significant progress in the field of children's digital protection. However, the rapid advancement of artificial intelligence applications requires continuous review of the legal framework to ensure the effectiveness and sustainability of these protections. Accordingly, achieving effective digital protection for children requires adopting an integrated approach that combines Sharia-based foundations, legal regulation, educational awareness, and safe technological design. Such an approach will help build a digital environment that respects children's rights and promotes their best interests in the age of artificial intelligence.

III. Study Findings

- The study demonstrated that the digital protection of children has emerged as an independent right driven by rapid digital transformation and advances in generative artificial intelligence. It is no longer merely a technical extension of traditional rights.
- The study identified the most significant contemporary digital threats to children as deepfakes, privacy violations, digital exploitation, behavioral profiling, and the spread of misinformation.
- The study found that the objectives of Islamic Sharia and its universal principles provide a strong juristic foundation for recognizing the right to children's digital protection and safeguarding them against emerging digital harms.
- The study showed that international conventions and contemporary legislation have made significant progress in protecting children in the digital environment, particularly in the areas of personal data protection and the prevention of online exploitation.
- The study concluded that effective digital protection for children cannot be achieved through legal measures alone. It requires an integrated approach that combines Sharia principles, legal regulation, education, and technological safeguards.

IV. Study Recommendations

- Enact specialized legislation to regulate the use of generative artificial intelligence technologies in child-related contexts, while establishing specific legal safeguards to protect children's digital rights.
- Regularly update the national legal framework to address the emerging risks associated with the rapid development of artificial intelligence and other digital technologies.
- Integrate digital literacy and cybersecurity education into school curricula and family awareness programs to strengthen children's digital awareness and promote the safe use of technology.
- Require developers of digital platforms and artificial intelligence systems to adopt the principles of the best interests of the child and safety by design in all digital products and services intended for children.
- Encourage interdisciplinary research that brings together Sharia, law, and technology to advance scholarly understanding and develop legislative solutions capable of addressing future challenges in protecting children within the digital environment.

Referrals and references

Aiken, M., & McMahon, C. (2023). Artificial Intelligence, Children and Digital Safety Emerging Legal Challenges. *International Journal of Law and Information Technology, 31*(2), 145–167.

Al-Hanbali, A. a. (1998). *Al Qawaid al Kubra* (1st ed.). Cairo: Maktabat al Thaqafah al Diniyyah.

Al-Shatibi, I. i. (1997). *Al Muwafaqat fi Usul al Shariah* (4th ed.). Beirut: Dar al Marifah.

Bietti, E. (2020). From Ethics Washing to Ethics Bashing A View on Technology Ethics. *Philosophy and Technology, 33*(4), 593–606.

Binns, R. (2018). Fairness in Machine Learning Lessons from Political Philosophy. *Proceedings of Machine Learning Research. 81*, pp. 1–11. Proceedings of Machine Learning Research.

Bygrave, L. A. (2014). *Data Privacy Law An International Perspective.* Oxford: Oxford University Press.

Committee on the Rights of the Child. (2021). *General Comment No. 25 (2021) on Childrens Rights in Relation to the Digital Environment.* Geneva: United Nations.

Crawford, K. (2021). *Atlas of AI Power, Politics, and the Planetary Costs of Artificial Intelligence.* New Haven: Yale University Press.

European Parliament and Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation GDPR).* Brussels: European Union.

European Union Agency for Fundamental Rights (FRA). (2024). *Artificial Intelligence and Fundamental Rights.* Luxembourg: Publications Office of the European Union.

Fasi, A. a. (2011). *Maqasid al Shariah al Islamiyyah wa Makarimuha.* Rabat: Dar al Gharb al Islami.

Floridi, L. (2014). *The Fourth Revolution How the Infosphere Is Reshaping Human Reality.* Oxford: Oxford University Press.

Gasser, U., & Almeida, V. A. (2017). A Layered Model for AI Governance. *IEEE Internet Computing, 21*(6), 58–62.

Ghazali, A. H. (1997). *Al Mustasfa min Ilm al Usul* (1st ed.). Beirut: Dar al Kutub al Ilmiyyah.

Interpol. (2024). *Online Child Sexual Exploitation Global Threat Assessment.* Lyon: Interpol.

Jawziyyah, M. i. (1991). *Ilam al Muwaqqiin an Rabb al Alamin* (1st ed.). Beirut: Dar Al Kutub Al Ilmiyyah.

Juwayni, A. a. (1997). *Al Burhan fi Usul al Fiqh* (1st ed.). Beirut: Dar al Kutub al Ilmiyyah.

Law No. 15-12 . (2015). Relating to Child Protection. *The Peoples Democratic Republic of Algeria*. Algeria.

Law No. 18-07 . (2018). Relating to the Protection of Natural Persons in the Field of Personal Data Processing. *The Peoples Democratic Republic of Algeria*. Algeria.

Livingstone, S., & Third, A. (2017). Children and Young Peoples Rights in the Digital Age An Emerging Agenda. *New Media and Society, 19*(5), 657–670.

Mansur, M. H. (2020). *Al Himayah al Qanuniyyah lil Bayanat al Shakhsiyyah.* Alexandria: Dar al Jamiah al Jadidah.

Marino, C., Gini, G., Vieno, A., & Spada, M. M. (2018). The Associations Between Problematic Facebook Use and Cyberbullying. *Addictive Behaviors Reports, 7*, 1–10.

Mittelstadt, B. D. (2019). Principles Alone Cannot Guarantee Ethical AI. *Nature Machine Intelligence, 1*(11), 501–507.

Murqus, S. (2018). *Al Wafi fi Sharh al Qanun al Madani.* Cairo: Dar al Nahdah al Arabiyyah.

Organisation for Economic Co operation and Development (OECD). (2025). *Hows Life for Children in the Digital Age.* Paris: OECD Publishing.

Qarafi, A. i. (1998). *Al Furuq* (1st ed.). Beirut: Alam al Kutub.

Raysuni, A. a. (2012). *Nazariyyat al Maqasid inda al Imam al Shatibi.* Cairo: Dar al Kalimah.

Saadi, M. S. (2021). *Sharh Qanun Himayat al Tifl al Jazairi.* Algiers: Dar Houma.

Salamah, A. A. (2019). *Al Qanun al Dawli li Huquq al Insan.* Cairo: Dar al Nahdah al Arabiyyah.

Shawarbi, A. a. (2017). *Jaraim al Hasib al Ali wal Internet.* Alexandria: Manshaat al Maarif.

UNESCO. (2023). *Guidance for Generative AI in Education and Research.* Paris: UNESCO.

UNICEF. (2025). *Guidance on AI and Children.* Florence: UNICEF Innocenti Research Centre.

UNICEF Innocenti. (2025). *Policy Guidance on AI for Children.* Florence: UNICEF Office of Research.

United Nations. (1989). *Convention on the Rights of the Child.* New York.

World Economic Forum. (2024). *Global Risks Report 2024.* Geneva: World Economic Forum.

Zuboff, S. (2019). *The Age of Surveillance Capitalism.* New York: PublicAffairs.

Zuhayli, W. a. (2006). *Usul al Fiqh al Islami.* Damascus: Dar al Fikr.