How to cite this article:
Souri, R., Ahadi, F., & Pourghahramani, B. (2026). The Right to Identity of Children and Adolescents in the Digital Age: A Criminological Perspective in Light of International Instruments. *Journal of Historical Research, Law and Policy, 4*(2), 1-13. https://doi.org/10.61838/jhrlp.170

Article history:
Original Research

Dates:
Submission Date: 27 September 2025
Revision Date: 20 December 2025
Acceptance Date: 27 December 2025
First Pubication Date: 29 December 2025
Final Pubication Date: 01 June 2026

The Right to Identity of Children and Adolescents in the Digital Age: A Criminological Perspective in Light of International Instruments

1. Reza. Souri [1] : Department of Criminal Law and Criminology, Mar.C., Islamic Azad University, Maragheh, Iran
2. Fatemeh. Ahadi [2*]: Department of Criminal Law and Criminology, Mar.C., Islamic Azad University, Maragheh, Iran
3. Babak. Pourghahramani [3]: Department of Criminal Law and Criminology, Mar.C., Islamic Azad University, Maragheh, Iran

*corresponding author's email: fatemeh.ahadi2025@iau.ac.ir

ABSTRACT

This study aims to examine the emerging challenges facing the "right to identity" of children and adolescents in the digital age and to propose an effective framework for its protection. Given the vulnerability of this age group's developing identity to threats such as identity theft, cyberbullying, and online manipulation, the article seeks to answer the question of what constitutes an effective criminal and legal policy in this domain, taking into account international instruments and domestic foundations. The present research adopts a descriptive–analytical method and an interdisciplinary approach encompassing legal, criminological, and jurisprudential perspectives. Accordingly, international instruments such as the Convention on the Rights of the Child (particularly General Comment No. 25; Committee on the Rights of the Child, 2021), relevant sociological and criminological theories related to cyberspace (including "surveillance capitalism" and the "network society"), as well as the capacities of dynamic jurisprudence (the principles of la darar [no harm] and maslahah [public interest]) are analyzed and referenced. The findings indicate that the current legal system, due to its exclusive reliance on a reactive and crime-centered approach, lacks sufficient effectiveness in safeguarding the digital identity of children and adolescents. Threats in this sphere are more complex than can be addressed solely through punitive instruments. Accordingly, the study's main hypothesis—namely, the necessity of transitioning to a "hybrid preventive model"—is confirmed. This model is grounded in four pillars: legal, educational, technical, and cultural. Ultimately, the article proposes an integrated and preventive policymaking model, the key implications of which include the need for responsibility-oriented legislation for digital platforms, the promotion of critical digital literacy education rather than purely restrictive approaches, and the empowerment of the family institution as the frontline of protection. This model offers a practical pathway for moving from the current ineffective criminal policy toward a comprehensive and effective strategy.

Keywords: *right to identity; digital identity; children's rights; cybercrime; preventive criminal policy; dynamic jurisprudence; international instruments.*

Introduction

The present era is an age of transition from a purely physical world to a dual ecosystem in which the boundaries between reality and the virtual realm have become increasingly blurred. Today's children and adolescents are, in Marc Prensky's terms, "digital natives"; a generation that has been immersed in digital technologies since birth and experiences a substantial part of its socialization and identity formation within this environment (1). Identity, this

complex psychological and social construct that Erik Erikson regards as the cornerstone of a successful transition from adolescence to adulthood (2), has acquired new dimensions and challenges in this novel context. “Digital identity,” encompassing all digital footprints, social media profiles, avatars, and online interactions of an individual, develops alongside physical identity and, at times, even comes to dominate it.

The central problem of this study is the inadequacy of traditional, one-dimensional approaches in addressing this complex phenomenon. As leading scholars of criminal law in Iran have repeatedly emphasized, modern criminal policy must move away from a punitive, reactionary criminal policy toward a participatory and preventive criminal policy (3). This paradigmatic shift assumes particular importance in the field of cybercrime, especially crimes against children. Protecting the right to identity, which is guaranteed in Article 8 of the Convention on the Rights of the Child (4), requires a coherent and multidimensional theoretical and practical framework. This article seeks to answer the question of how an effective model for protecting the identity of children and adolescents in the digital ecosystem can be designed through the integration of international legal instruments, preventive criminological strategies (referred to in Iranian legal literature as “crime prevention”), and the theoretical capacities of dynamic jurisprudence. By adopting a critical perspective on the current state of the Iranian legal system—which, as noted by one prominent criminal law scholar, has in some instances suffered from “penal inflation” without adequate attention to effectiveness (5)—and by offering practical solutions, this study aims to contribute to bridging existing theoretical and practical gaps in this field.

At the dawn of the third millennium, the world witnessed a pervasive revolution that fundamentally challenged the boundaries between reality and the virtual sphere. This digital revolution has transformed the lives of “digital natives” (1)—today’s children and adolescents—more profoundly than those of any other group. Unlike previous generations, often described as “digital immigrants,” this cohort has been immersed from the outset in an ocean of information and communication technologies and experiences a substantial part of the vital process of identity formation within this environment. Identity, as a psychosocial construct that, according to Erik Erikson, forms the foundation of a successful transition from adolescence to adulthood and provides an answer to the fundamental question “Who am I?” (2), has taken on new dimensions and challenges in this context. Identity can no longer be understood solely as a physical phenomenon limited to face-to-face interactions; rather, “digital identity,” as an online self-representation, develops alongside physical identity and at times comes to overshadow it.

The digital identity of children and adolescents is exposed to a wide range of threats: from identity theft for financial and credit-related misuse to identity impersonation for the commission of other crimes; from cyberbullying, which targets the psychological well-being and self-esteem of victims (6), to online grooming, in which offenders use fabricated identities to gain children’s trust for sexual exploitation (7); and from entrapment in filter bubbles (8), which foster one-dimensional and extreme identities, to the pressure to present an idealized and unrealistic self on social media, thereby intensifying identity crises (9).

Although the Iranian legal system has addressed some of these offenses in the Computer Crimes Act (enacted in 2009), many legal scholars acknowledge that this legislation is more “crime-centered” than “victim-centered,” particularly with regard to the protection of special victims such as children (10). The law lacks a comprehensive and preventive approach and has paid insufficient attention to the identity-related dimensions of these crimes, especially in cases involving minors. This stands in contrast to international instruments, which obligate states to adopt active protective and preventive measures. This research seeks, by dissecting these challenges, to propose a conceptual model for criminal and social policymaking that draws on international standards, is inspired by

preventive criminology, and remains compatible with the jurisprudential and cultural foundations of society, thereby contributing to the realization of “digital citizenship rights” for children—a concept whose importance has been emphasized by a leading scholar in the field of information technology law in Iran (11).

As noted above, the core issue that necessitates this research is the inadequacy and lag of traditional protective paradigms in addressing this emerging phenomenon. Legal systems, including that of Iran, have traditionally adopted a “reactive” and “crime-centered” approach to social problems. As emphasized by one of the most prominent figures in Iranian criminal policy, the contemporary era requires a transition from a “reactionary criminal policy,” which intervenes only after the occurrence of crime and harm, to a “participatory and preventive criminal policy” that targets the roots and enabling conditions of criminal behavior (3). This paradigmatic shift assumes heightened significance in the context of cybercrimes against children and adolescents due to the rapid pace of technological change and the extensive scope of potential harm.

Despite efforts to enact legislation such as the Computer Crimes Act (2009), the current legal system has, in certain respects, experienced “penal inflation,” a phenomenon described by a criminal law scholar as the proliferation of criminal offenses without adequate regard for the real effectiveness of sanctions and their proportionality to the crime (5). Such laws often focus on classical forms of crime (such as fraud or theft) within a cyber context and fail to adopt a comprehensive and specialized perspective on the complex “identity-related” dimensions of these offenses, particularly when directed against children. In this process, fundamental concepts such as “digital citizenship rights,” whose realization has been emphasized (11), have been marginalized, and children are more often viewed as “victims” in need of paternalistic protection rather than as “digital citizens” endowed with rights and agency.

On the other hand, international instruments—particularly the Convention on the Rights of the Child (CRC) and its General Comment No. 25 (2021), which specifically addresses “children’s rights in the digital environment”—offer progressive and comprehensive frameworks that extend beyond mere protection and emphasize children’s “right to participation” (12). These instruments place significant responsibility on states and the private sector (digital platforms), responsibilities whose implementation requires adaptation to domestic legal and cultural structures. It is here that the capacities of dynamic jurisprudence and the theoretical foundations of Islamic law, especially principles such as “no harm” (*la darar*), “public interest” (*maslahah*), and the negation of domination (*nafy-e sabil*), can function as a bridge between global obligations and local realities, contributing to the formulation of an effective and sustainable protective model.

Methodology

In terms of its nature and objectives, the present study is classified as descriptive–analytical research. In the descriptive phase, an effort is made to systematically depict the existing situation, including the various dimensions of the challenge of children’s and adolescents’ right to digital identity, relevant national and international legal frameworks, and key criminological and sociological theories. In the subsequent analytical phase, these data and concepts are examined, critiqued, and evaluated within a coherent theoretical framework in order to identify gaps and shortcomings in the current approach and to arrive at a strategic and effective model. Data collection in this research is based on library research and documentary analysis. Accordingly, a wide range of sources—including specialized books and articles in the fields of law, criminology, and jurisprudence; international legal instruments (particularly the Convention on the Rights of the Child and General Comment No. 25); domestic laws and

regulations; and opinions and theories within legal doctrine—have been systematically reviewed and carefully analyzed.

Theoretical and Legal Foundations

Identity in the Digital Age: From Goffman to Castells

From Erving Goffman's perspective, identity can be understood as a "performance" on the stage of everyday life (13). In the digital environment, this performance acquires new and powerful tools. Users can construct multiple identities, edit themselves, and present an idealized version of who they are. Sherry Turkle describes this phenomenon as "alone together," a condition in which individuals, despite constant connectivity, experience deeper feelings of isolation and come to anchor their identity in the validation of others through likes and comments (9).

From another angle, Manuel Castells, in his analysis of the "network society," conceptualizes identity as the product of interactions within information networks (14). In this view, identity is no longer fixed or predetermined but fluid and continuously reconstructed. For children and adolescents, this fluidity represents both an opportunity for exploration and experimentation and a threat of disorientation and fragmentation. Shoshana Zuboff, through her theory of "surveillance capitalism," reveals another dimension of this threat: digital platforms are not merely spaces for interaction but data-extraction machines that predict and shape user behavior, thereby transforming users' identities into commodities for sale in data markets (15).

International Instruments: Operational Guidelines for States

The cornerstone of the protection of children's rights at the international level is the Convention on the Rights of the Child (CRC), adopted in 1989 (4). The key provisions relevant to the present discussion include:

• **Article 8 (Right to Identity):** This provision obliges States to preserve the child's identity, including nationality, name, and family relations. In the digital age, this right extends to the protection of the child's online identity.

• **Article 16 (Right to Privacy):** No child shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence. The excessive collection of children's data by digital platforms constitutes a clear violation of this article.

• **Article 17 (Access to Appropriate Information):** States must ensure children's access to information and materials from diverse sources while protecting them from harmful content.

• **Article 19 (Protection from Abuse and Neglect):** This article underscores the necessity of adopting legal, administrative, social, and educational measures to protect children from all forms of maltreatment.

The significance of this issue prompted the United Nations Committee on the Rights of the Child to dedicate General Comment No. 25 (2021) exclusively to "children's rights in the digital environment" (12). This document serves as a comprehensive guide for States and emphasizes the following key principles:

• **A rights-based approach:** The digital environment must be designed to realize children's rights, rather than merely to generate profit.

• **The best interests of the child:** In all legislation, policymaking, and commercial actions related to the digital sphere, the best interests of the child must be the primary consideration.

• **Private sector responsibility:** Businesses and digital platforms bear direct responsibility to respect children's rights and to prevent harm to them, through mechanisms such as safety and privacy by design.

• **Empowerment of children:** Children must be equipped with digital literacy so that they can participate safely, creatively, and responsibly in online spaces.

Within the Iranian legal system, which is grounded in Islamic principles, drawing upon the capacities of jurisprudence to address emerging issues is essential. Dynamic jurisprudence, by incorporating the elements of time and place into *ijtihad*, can offer effective responses to the challenges of the digital age.

• **The rule of no harm (*la darar*):** The principle "there shall be no harm and no harassment in Islam" is a well-established jurisprudential rule that negates any form of harm to oneself or others. Accordingly, any use of cyberspace that harms a child's identity, psychological well-being, or dignity is considered impermissible. This rule can serve as a foundation both for criminalizing harmful conduct and for obligating platforms to adopt preventive measures.

• **The rule of public interest (*maslahah*):** In cases of silence or ambiguity in textual sources, the public interest of the Islamic community and its members becomes the criterion for legislation. In the present context, the "best interests of the child"—which corresponds to the international legal standard—require the State to take active measures to create a safe and healthy digital environment. This interest takes precedence over the economic interests of platforms.

• **The theory of *al-manṭiqat al-farāgh* (the discretionary zone):** This theory holds that the Lawgiver has delegated certain areas of regulation to the Islamic ruler (the State) to legislate in accordance with the requirements of time and place. Digital technologies represent a clear instance of this discretionary zone, obliging the State to enact precise regulations to safeguard citizens' rights, particularly those of children.

• **The priority of prevention over treatment:** Islamic teachings prioritize the preservation of health and the prevention of harm over remedial measures. This principle also applies to social domains. Islamic criminal policy is not purely punitive; a significant portion of it is devoted to prevention through education, moral guidance, and the reform of social structures. This approach is fully aligned with contemporary models of preventive criminology.

Criminological Analysis of Risks: Dissecting Threats to Digital Identity and Reputation

Cyberspace, due to its unique characteristics, provides fertile ground for new forms of crime and deviance. From a criminological perspective, this environment possesses features that render it an ideal "crime-generating situation." The transnational nature of cybercrime, which creates complex legal and judicial challenges for prosecution and punishment, has been emphasized in the literature (16). In addition, characteristics such as anonymity, the rapid dissemination of information, and the asymmetry of power between users—particularly children—and platforms all contribute to heightened vulnerability. In this section, drawing on the conceptual distinctions introduced earlier, a criminological analysis of the most significant threats to children's digital identity and reputation is presented.

Threats to Digital Identity (The Technical–Legal Self)

This category of threats targets the technical and legal core of an individual's identity in the digital environment.

Digital Identity Theft and Impersonation

This offense, perhaps the most classical crime in this domain, involves unauthorized access to an individual's authentication information (such as usernames and passwords) and its use for fraudulent purposes. An offender

may, by assuming a child's identity, engage in unauthorized purchases, send offensive messages to others, or commit additional crimes. For the child, the harm caused by this offense extends beyond financial loss; it constitutes an "identity trauma" that fundamentally undermines the child's sense of security and control over their digital life. Although the Iranian Computer Crimes Act addresses "unauthorized access" and related offenses such as computer fraud, it does not define "digital identity impersonation" as an independent crime with a focus on its non-material harms.

Online Grooming and Internet Deception

This is among the most dangerous threats facing children in cyberspace. In this process, an adult uses a fabricated identity—often posing as a peer—and, through chat rooms, online games, or social networks, gains a child's trust. The ultimate aim is sexual, emotional, or financial exploitation. Grooming is a process-oriented crime that, through social engineering and psychological manipulation, targets the child's identity and autonomy. Many jurisdictions have recognized this conduct as a distinct criminal offense. In the Iranian legal system, while such behavior may be subsumed under broader categories such as "incitement" or "facilitating corruption," the absence of a specific criminal designation for this complex conduct represents a serious legislative gap, hindering effective prevention and response.

Identity Formation in Echo Chambers and Filter Bubbles

This constitutes an indirect yet profoundly significant threat. Personalization algorithms, by repeatedly displaying content aligned with a user's existing beliefs, confine the user within a "filter bubble" or an "echo chamber" (8). This phenomenon is particularly hazardous for adolescents who are in the process of forming their political, social, and cultural identities. Exposure to extremist viewpoints—whether political, religious, or social—without access to opposing perspectives can lead to radicalization and the development of rigid and inflexible identities. While this threat does not possess a criminal character, it represents a serious social harm that necessitates educational interventions and regulatory measures at the platform level.

Threats to Digital Reputation (The Socially Perceived Self)

This category of risks targets the child's image and social standing in both online and offline communities.

Cyberbullying

Cyberbullying refers to any hostile, intentional, and repeated behavior carried out through digital tools by an individual or group against a person who is unable to defend themselves (6). Its manifestations include sending insulting messages, spreading rumors, excluding someone from online groups, or creating fake profiles to mock the victim. Features of cyberspace—such as the persistence of content and the vast reach of audiences—render the harms of cyberbullying far more severe than those of traditional bullying. The victim is not safe from harassment even within the home. This phenomenon directly damages the child's "digital reputation" and self-esteem and may lead to tragic outcomes, including suicide. In Iranian law, such conduct may be subsumed under categories such as insult, defamation, or the dissemination of falsehoods, yet these labels do not adequately capture the "repetitive" nature of bullying and the "unequal power relationship" that constitutes one of its core elements.

Non-Consensual Sharing of Private Content and Sharenting

This threat may originate from two sources. The first is the dissemination of a child's private images or information by peers or others with the intent of damaging the child's reputation (sometimes in a retaliatory context). The second is a newer phenomenon commonly referred to as "sharenting," namely the excessive sharing of a child's information and images by the child's own parents on social media (Steinberg, 2017). Parents, often with good intentions, may share every moment of the child's life—from first steps to birthday celebrations and even embarrassing moments. Such sharing, undertaken without the child's informed consent, constructs a "digital reputation" that may later create difficulties for the child and violate the child's privacy and right to an independent identity. This phenomenon exemplifies the tension between parental rights and children's rights in the digital age.

Deepfakes and Synthetic Media

This is an emerging and highly concerning threat. With advances in generative artificial intelligence, it has become increasingly easy to produce fully realistic yet fabricated videos or audio recordings. A child's face can be placed onto inappropriate footage, or a voice resembling the child's can be generated to appear as though they are making offensive statements. This technology can destroy an individual's "digital reputation" within minutes, while proving falsification may be extremely difficult. The phenomenon challenges the very notion of "evidence" and "authenticity" in cyberspace and requires a swift and decisive legislative response. Such conduct may fall under the dissemination of falsehoods through computer systems and may also amount to insult or defamation; however, given its technical complexity and the severity of harm, it warrants special attention and potentially independent criminalization.

This analysis demonstrates that threats to children's identity in the digital environment are complex, multilayered, and dynamic. A purely punitive approach grounded in traditional criminal labels is insufficient to address these emerging phenomena. Criminal policy must therefore adopt a more comprehensive perspective and deploy preventive, educational, and regulatory strategies alongside criminal-law responses.

A Dynamic Jurisprudential Approach to the Issue

Dynamic jurisprudence, by relying on the elements of time and place, has the capacity to respond to emerging issues. Key principles in this regard include:

• **The rule of no harm (*la darar*):** This principle provides a firm basis for criminalizing any conduct that harms a child's identity, psychological well-being, and dignity in the digital environment, and for imposing obligations to prevent harm.

• **The rule of public interest (*maslahah*):** The "best interests of the child," as a definite and significant public interest, prevails over the economic interests of platforms and obliges the State to intervene actively to create a safe environment.

• **The theory of *al-manṭiqat al-farāgh* (the discretionary zone):** The sphere of digital technologies is a clear instance of the discretionary zone in which the legislature can and should enact precise rules, in light of contemporary conditions and with the aim of protecting citizens.

Presenting a Hybrid Preventive Model

The digital world is an inseparable reality in the lives of today's children and adolescents. The process of identity formation, once rooted primarily in the home, school, and neighborhood, now unfolds to a significant extent on the internet's endless stage of performance. The foregoing analyses show that a purely punitive and reactive approach is insufficient for protecting children's digital identity. An effective criminal and social policy must be comprehensive, preventive, and participatory. With the purpose of dissecting the challenges and proposing a response to this emerging reality, the present study arrives at the following conclusion: the proposed model is built on four pillars.

The Legal–Regulatory Pillar

• **Responsibility-oriented legislation:** Drawing on successful global experiences such as the GDPR in Europe, and in light of the necessity of protecting citizens' fundamental rights in cyberspace—an issue emphasized by legal scholars—there is a need to enact a "Child Online Protection Act." This law should specifically require platforms to implement safety by design, conduct child-rights impact assessments, and establish rapid and effective reporting mechanisms.

• **Reforming existing laws:** This entails revising the Iranian Computer Crimes Act and the Law on the Protection of Children and Adolescents (enacted in 2020). Although the latter represents a positive step toward protecting children, it does not address online risks in a specific and comprehensive manner. Precise definitions should be provided for crimes such as "online grooming" and "severe cyberbullying," and both criminal and non-criminal measures (including platforms' civil liability) should be incorporated. This approach is consistent with the views of a prominent Iranian criminal law scholar who emphasizes proportionality between criminalization and social realities, as well as the use of civil remedies alongside punishment (17).

• **Criminal Grooming as an Instrument of Identity Manipulation and Victimization Facilitation**

Criminal grooming is a gradual, planned, and deceptive process in which an adult—often for purposes of sexual exploitation—deliberately seeks to establish an emotional, trust-based relationship with a child or adolescent. This is not a sudden attack; rather, it is a form of "temporal and emotional investment" by the offender aimed at dismantling the child's resistance and psycho-emotional boundaries. The process typically includes the following stages:

1. **Targeting:** The offender identifies a child with specific vulnerabilities, such as loneliness, weak family relations, low self-esteem, or even the absence of formal identity and a sense of belonging.
2. **Building trust:** Through excessive affection, gifts, special attention, and the performance of a supportive friend or protector role, the offender gains the child's trust.
3. **Isolation:** The offender gradually separates the child from friends and family, instilling the idea that "only I understand you" and "our relationship is a special secret."
4. **Normalization and boundary crossing:** The offender slowly shifts emotional and physical boundaries, beginning with inappropriate jokes and gradually steering interactions toward physical contact or sexualized content.
5. **Control and abuse:** Once full dependency is secured, abuse begins, and control is maintained through threats of disclosure, the induction of guilt, or emotional blackmail.

Although grooming functions as a project of “identity stripping” and “false identity construction,” its criminological importance lies in the fact that the process directly targets the child’s right to identity. Through psychological manipulation, the offender weakens the child’s independent and authentic identity and substitutes it with a dependent and fabricated identity. This assault on identity occurs at multiple levels:

- **Erosion of social identity:** By isolating the child, the offender cuts off the child’s connection to primary identity-forming resources (family, friends, school). The child no longer perceives themselves as a member of those groups; instead, identity becomes defined within the “secret relationship” with the offender.
- **Creation of a dual, guilt-laden identity:** The child is forced to live in a dual world—an outward identity and a hidden identity saturated with secrecy, fear, and guilt. This duality destroys psychological coherence and undermines the child’s sense of worth.
- **Rewriting self-concept:** The offender reshapes the child’s self-concept by suggesting that the relationship is “special,” that the child is “more mature” than peers, and that the offender’s conduct reflects “love” rather than abuse. As a result, the child’s understanding of right and wrong, appropriate and inappropriate, and bodily boundaries is disrupted, and moral identity becomes distorted.

Finally, from a criminal policy perspective, understanding the mechanism of grooming is crucial because it shows that child protection should not focus solely on preventing the “final act of abuse.” It must also encompass the criminalization of preparatory and deceptive behaviors that target the child’s identity and psychological autonomy and that condition the child for victimization. In effect, grooming constitutes an independent offense against the child’s psychological integrity and identity.

The Educational–Cultural Pillar

• **Critical digital literacy:** Digital literacy education must go beyond technical skills and encompass “critical digital literacy.” Children and adolescents should learn how algorithms function, how to protect their privacy, how to identify fake news, and how to analyze the impact of social media on their identity and psychological well-being.

• **The role of family and school:** Parents and educators must themselves be equipped with up-to-date knowledge and, rather than adopting absolute prohibitions, pursue an approach based on dialogue and accompaniment. Organizing training workshops for parents and integrating topics related to digital citizenship into school curricula are essential.

• **The importance of empowering children as active agents rather than mere recipients of protection:**

The transition from a traditional, paternalistic view of children as passive and merely “recipients of protection” to a modern legal paradigm that recognizes them as “active agents” and “subjects of rights” constitutes one of the most fundamental transformations in childhood studies and protective policymaking. This intellectual shift, rooted in foundational instruments such as the United Nations Convention on the Rights of the Child (CRC)—particularly Article 12 concerning the child’s “right to be heard” in all matters affecting them—rests on the premise that empowering children to participate in decision-making processes is not merely a humanitarian gesture, but a key strategy for enhancing resilience and the effectiveness of protection (4). When children are given opportunities to express their experiences, fears, and solutions, protective policies move beyond abstract, top-down frameworks and become realistic, effective, and sustainable. Ultimately, this approach elevates the child from an “object of compassion” to a “partner in protection” and reinforces the belief that the most effective way to protect a child is to empower the child themselves.

The Technical–Supervisory Pillar

• **Parental control tools:** Promoting and facilitating access to effective monitoring tools that enable parents to manage both the duration and type of content consumed by their children.

• **Strengthening supervisory institutions:** Establishing or reinforcing an independent regulatory authority—similar to the Information Commissioner's Office (ICO) in the United Kingdom—to oversee platform performance in relation to data protection and children's rights, and granting this body the authority to impose fines and require corrective measures.

The Supportive–Therapeutic Pillar

• **Specialized counseling centers:** Establishing specialized counseling centers for children who have become victims of cybercrime, aimed at addressing psychological harm and the "identity trauma" resulting from such experiences.

• **Emergency helplines:** Launching telephone and online helplines for the immediate reporting of urgent cases such as severe cyberbullying or online threats.

Ultimately, safeguarding the digital identity of future generations is a collective responsibility that requires close cooperation among the State, the private sector, civil society institutions, families, and the education system. Only through an integrated and multidimensional approach can there be hope that digital natives will become creative, responsible citizens with healthy and coherent identities in both the physical and virtual worlds.

Future Work: Looking Ahead to Identity in the Metaverse

With the emergence of concepts such as the metaverse and fully immersive avatar-based identities, challenges related to the "right to identity" will acquire new and more complex dimensions. In these virtual worlds, the boundary between the real self and the avatar self may nearly disappear, raising novel questions regarding ownership of digital identity, responsibility for avatar actions, and the psychological effects of full immersion in constructed identities. Future research must boldly engage with these horizons to ensure that law and policy do not fall behind the rapid pace of technological development.

Conclusion

The digital world is an inseparable reality in the lives of today's children and adolescents. The process of identity formation, which once unfolded primarily within the home, school, and neighborhood, now largely takes place on the endless stage of the internet. With the aim of dissecting the challenges and proposing responses to this emerging reality, the present study arrives at the following conclusions:

1. **Complexity and multilayered nature of threats:** Threats to children's identity are not limited to data theft. Rather, they encompass a wide spectrum of harms, ranging from psychological manipulation in the grooming process to social destruction through cyberbullying and the covert engineering of identity by commercial algorithms. An analytical distinction among "digital identity" (the technical self), "digital reputation" (the social self), and "digital citizenship" (the responsible self) is essential for understanding this complexity and for proportionate and effective legislation.

2. **Insufficiency of the reactive–punitive approach:** Despite certain strengths, the current Iranian legal system remains largely focused on punitive and ex post responses. This approach lacks the necessary effectiveness to address the structural, preventive, and transnational harms of the digital age and therefore requires a paradigmatic reassessment.
3. **Convergence of normative sources:** Both progressive international instruments and a dynamic reinterpretation of jurisprudential sources converge on a common point: the necessity of adopting a preventive, responsibility-oriented (particularly for platforms), and participatory approach that actively involves children themselves.

On the basis of these findings, the study argues that effective protection of children's right to identity depends on the design and implementation of a "hybrid preventive and participatory model." Rather than relying on a single solution, this model proposes a coordinated set of measures across four key domains:

• **1. The legal–regulatory pillar:** Drafting a "Comprehensive Child Online Protection Law" with an emphasis on platform accountability (the principle of safety by design), the independent criminalization of emerging behaviors (such as grooming and harmful deepfakes), and the recognition of new digital rights (such as the right to be forgotten).

• **2. The educational–cultural pillar:** Integrating "critical digital literacy" into school curricula, empowering parents and educators, and—most importantly—creating genuine mechanisms for children's participation in policymaking processes that directly affect them.

• **3. The technical–supervisory pillar:** Promoting dialogue-oriented monitoring tools rather than surveillance-based mechanisms, and establishing an independent regulatory authority to oversee platform practices, address complaints, and ensure the effective enforcement of laws.

• **4. The supportive–therapeutic pillar:** Establishing specialized counseling centers to address the psychological and social harms resulting from cybercrime, with a focus on "identity trauma" and the provision of age-appropriate services for victims.

Recommendations for Policymaking and Future Research:

• **For the legislature:** Establishing a specialized interdisciplinary task force—comprising legal scholars, technology experts, psychologists, and civil society representatives—to draft a "Comprehensive Child Online Protection Law" inspired by the proposed model.

• **For the executive branch (Ministry of Education and Ministry of Communications):** Undertaking an urgent revision of school curricula and developing a national program on "critical digital literacy." Additionally, drafting executive regulations to oblige domestic and foreign platforms to comply with the principle of safety by design and to establish child-friendly reporting mechanisms.

• **For the judiciary:** Organizing specialized training programs for judges and law enforcement officers on cybercrimes against children and their psychological dimensions, and establishing specialized judicial branches to adjudicate such cases.

• **For researchers:**

– **Futures studies:** Conducting bold research on challenges to the "right to identity" in emerging technological horizons such as the metaverse, where the boundary between real identity and avatar identity may disappear entirely, as well as on the long-term effects of generative artificial intelligence on concepts of truth and identity.

– **Field studies:** Undertaking national surveys and qualitative case studies to assess the prevalence and nature of online harms among Iranian children and to understand their lived experiences and coping strategies.

– **Comparative analysis:** Conducting in-depth studies of the laws and policies of leading jurisdictions in this field (such as the European Union's Digital Services Act or the United Kingdom's Online Safety Act) and examining the feasibility of localizing their successful approaches.

Ultimately, it must be acknowledged that protecting children in the digital age is not a race to reach a finish line, but a continuous process of learning and adaptation. The ultimate goal should not be to build a "walled garden" for children, but rather to equip them with the tools, knowledge, and confidence needed to become skilled and responsible gardeners of their own digital environment.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adheried in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Prensky M. Digital Natives, Digital Immigrants. On the Horizon. 2001;9(5):1-6. doi: 10.1108/10748120110424816.
2. Erikson EH. Identity: Youth and Crisis: W. W. Norton & Company; 1968.
3. Najafi Abrandabadi AH. An Introduction to Criminal Policy. Tehran: Shahid Beheshti University; 2004.
4. United Nations. Convention on the Rights of the Child. 1989.
5. Ardabili MA. General Criminal Law (Vol. 1: The Criminal Phenomenon). Tehran: Mizan Publishing; 2016.
6. Smith PK, Mahdavi J, Carvalho M, Fisher S, Russell S, Tippett N. Cyberbullying: Its Nature and Impact in Secondary School Pupils. Journal of Child Psychology and Psychiatry. 2008;49(4):376-85. doi: 10.1111/j.1469-7610.2007.01846.x.
7. Wolak J, Mitchell KJ, Finkelhor D. Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. Pediatrics. 2007;119(2):247-57. doi: 10.1542/peds.2006-1891.
8. Pariser E. The Filter Bubble: What the Internet Is Hiding from You: Penguin UK; 2011.
9. Turkle S. Alone Together: Why We Expect More from Technology and Less from Each Other: Basic Books; 2011.

10. Walidi MS. Victimology. Tehran: Jangal Publishing; 2013.
11. Ansari B. Communication Law. Tehran: SAMT Publications; 2019.
12. Committee C. General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment. UN Committee on the Rights of the Child, 2021.
13. Goffman E. The Presentation of Self in Everyday Life: Anchor Books; 1959.
14. Castells M. The Rise of the Network Society. 2 ed: Wiley-Blackwell; 2010.
15. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: PublicAffairs; 2019.
16. Malekmohammadi H. Cyber Crimes: An Applied Approach. Tehran: Majd Publications; 2018.
17. Mirmohammad Sadeghi H. Crimes Against Persons. Tehran: Mizan Publishing; 2019.