How to cite this article:
Habibi, F. (2027). Prevention of Child Sexual Grooming in Cyberspace with Emphasis on the Capacities of the Optional Protocol to the Convention on the Rights of the Child. *Journal of Historical Research, Law and Policy, 5*(2), 1-13. https://doi.org/10.61838/jhrlp.346

Article history:
Original Research

Dates:
Submission Date: 12 February 2026
Revision Date: 23 May 2026
Acceptance Date: 30 May 2026
First Publication Date: 12 July 2026
Final Publication Date: 01 March 2027

Prevention of Child Sexual Grooming in Cyberspace with Emphasis on the Capacities of the Optional Protocol to the Convention on the Rights of the Child

1. Faranak. Habibi [1*] : Master's degree, Department of Criminal Law and Criminology, CT.C., Islamic Azad University, Tehran, Iran

*corresponding author's email: hbbfaranak@gmail.com

ABSTRACT

The expansion of modern communication technologies has transformed the phenomenon of online child grooming into a serious threat. In this process, offenders gain the trust of children in cyberspace in order to facilitate sexual exploitation. Given the vulnerability of children and the existing legal gaps, the present study aims to examine preventive strategies by evaluating the capacities of the "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography" and the Iranian legal system in addressing this phenomenon. This research was conducted using a descriptive-analytical method based on library and documentary sources. The findings indicate that, despite the absence of an explicit reference to "grooming," the Optional Protocol possesses considerable capacity to combat this crime through broad interpretation and provides a framework for the criminalization of forms of sexual exploitation as well as international cooperation. In contrast, the Iranian legal system faces a legislative gap due to the absence of an independent criminalization of grooming as an absolute offense, thereby limiting criminal intervention prior to the occurrence of the ultimate harm. Effective confrontation with this phenomenon requires the adoption of a comprehensive criminal policy based on two principal dimensions: legislative reform through the independent criminalization of grooming behavior, and the implementation of non-penal strategies. These strategies include situational prevention (technological tools and obligating platforms to monitor content and interactions) and social prevention (enhancing media literacy and providing self-protection education for children and families). Protecting children against cyber grooming requires the urgent reform of Iran's legislative system and the independent criminalization of such conduct. This measure should be accompanied by a set of complementary technological and educational strategies in order to establish an integrated protective shield and ensure a safe environment for children in cyberspace.

Keywords: *Sexual grooming, cyberspace, Optional Protocol on the Rights of the Child, child pornography, situational prevention.*

Introduction

The continuous advancement of information and communication technology has produced profound transformations in the structure of societies and has created a new platform for the transfer of criminality from the physical environment to networked space. In this transition, offenders, by benefiting from features such as anonymity and pervasive access, have found an environment conducive to committing crimes against vulnerable

groups, including children (1). Studies show that, after military crises, cyberspace has played the greatest role in violating the fundamental rights of children (2). In this context, the phenomenon of online enticement is recognized as one of the most serious emerging threats. This concept refers to a psychological and behavioral process in which the offender, by establishing continuous and friendly communication, attempts to gain the trust of the child and the child's family in order to prepare the ground for future sexual exploitation (3).

In this process, the offender, through a precise understanding of the target's emotional needs, gradually separates the child from the safe family environment and places the child in communicative isolation. The lack of deterrent legal sanctions appropriate to cyberspace, together with parents' insufficient awareness of media literacy, has significantly increased children's vulnerability to this new form of crime (4). Accordingly, accurately explaining the nature of this phenomenon and diagnosing its legal dimensions are undeniable necessities for formulating preventive policies and providing effective protection for victims.

The necessity and importance of conducting this research can be examined and explained from several fundamental dimensions. First, the unprecedented expansion of modern communication technologies has placed new generations of users, especially Generation Z and Generation Alpha, on the front line of exposure to emerging harms (1). The inherent characteristics of cyberspace, together with children's incomplete intellectual and cognitive maturity, have caused this group to be recognized as the most vulnerable segment of society against network-based abuse (2).

On the other hand, despite the increasing growth of these threats, the legal system still suffers from the serious challenge of lacking appropriate and deterrent legal sanctions for the protection of children (4). Existing legislative gaps in protecting children's privacy and the absence of independent criminalization proportionate to the requirements of the virtual environment have created a suitable ground for the continuation of criminal conduct (5).

Accordingly, a precise examination and evaluation of the domestic legal system in light of the standards and requirements set forth in international instruments gains added importance (6). Examining the extent to which existing laws conform and converge with the protective capacities of the Optional Protocol to the Convention on the Rights of the Child is an essential and necessary step toward identifying legislative deficiencies and developing effective preventive strategies to combat cybercrime (2).

A review of the research literature shows that the issue of networked criminality against children has been examined from various perspectives. Regarding the study of the Optional Protocol to the Convention on the Rights of the Child, several studies have addressed the capacities of this international instrument in confronting phenomena such as the sale of children and child pornography (2). These studies emphasize the necessity of harmonizing domestic laws with international obligations in order to eliminate legislative gaps in dealing with emerging crimes (5).

On the other hand, in the field of analyzing cybercrimes against children, researchers have pointed to the role of cyberspace in facilitating criminality and the need to adopt situational and social preventive measures (1). These scholarly texts emphasize the vulnerability of new generations in cyberspace and regard the development of public education as a fundamental solution (7). Nevertheless, studies indicate that focusing on the phenomenon of online deception and grooming of children requires more independent and in-depth research capable of offering a combination of specific penal and non-penal measures (5).

Given the complexities of the phenomenon of online grooming of children and the need to adopt comprehensive preventive measures, this research seeks to answer several fundamental questions. The first question concerns

the nature and legal capacities of international instruments and seeks to determine what solutions and obligations the Optional Protocol to the Convention on the Rights of the Child has provided for combating cyber deception of children (2).

The second question concerns the domestic legal system and examines the legislative gaps in Iran's current laws for the penal prevention of these emerging crimes and how these deficiencies can be remedied in light of international standards (8).

Finally, the third question concerns the field of non-penal prevention and seeks to answer this legal and social issue: what role do situational and social measures, such as enhancing media literacy and using access-restriction tools, play in reducing the victimization of children in the virtual environment (1)? A precise and well-reasoned answer to these questions will pave the way for developing a comprehensive protective model for legislators and policymakers in the field of communications (4).

Findings

Conceptualization and Nature of Cyber Grooming

The phenomenon of online enticement and grooming, which is recognized in research and legal texts as a precursor to the sexual exploitation of children and their deception for malicious purposes, is a complex and destructive process with profound psychological dimensions (5). In this process, the offender, by using cyberspace and exploiting children's ignorance, particular vulnerability, and intellectual immaturity, carries out a series of preparatory and planned actions. The main objective at this stage is to create a false and secret emotional relationship so that the psychological resistance of the victim is reduced and the child's trust is gained; this ultimately creates the conditions for online sexual abuse and exploitation (3).

A distinctive feature of this criminal behavior is that it is time-consuming and remains hidden from parents and supervisors. Because children are unable to properly understand and identify the deceptive nature of such communications, they cannot adequately defend their rights and unintentionally fall into the trap of offenders. This issue doubles the need for special legal protections and early legislative intervention to protect this vulnerable group (9).

From an analytical perspective, the nature and purpose of online grooming have clear boundaries and fundamental differences from other forms of computer-related criminality. While many crimes committed in cyberspace, such as internet fraud, economic deception, identity-data theft, or digital threats and intimidation, are generally committed for financial gain or reputational harm, cyber grooming directly targets the psychological and physical integrity of the child (1). In other words, in this crime, instead of attacking property or data, the offender uses time and psychological engineering to break down the child's safe boundaries and prepare the child for subsequent criminal purposes. This process-oriented feature and its focus on the fundamental destruction of the child's psyche distinguish it from other crimes and highlight the importance of giving it independent attention in penal policymaking.

The Five Stages of Grooming in Cyberspace

A) Identification and Selection of the Target

The initial step in the process of cyber grooming of children is the precise identification and selection of the victim. At this stage, offenders continuously operate in online communication environments and interactive networks, monitoring and evaluating the behavior of minor users. Cyber offenders mostly seek children who, due to the lack of necessary education and insufficient awareness of the dangers existing in cyberspace, are more vulnerable (5). These offenders, by carefully examining user profiles and children's levels of online interaction, select their targets from among those who receive less supervision from the family institution and have a more suitable background for communicating with strangers (3). Thus, the process of target selection is not a random act but is based entirely on the psychological assessment of the child, so that the starting point for implementing the scenario of deception and sexual exploitation faces the fewest possible obstacles (5).

B) Trust-Building and Normalization of Communication

After identifying the victim, cyber offenders enter the sensitive stage of gaining the child's trust. At this stage, offenders use children's natural tendency to trust others, as well as their insufficient awareness of the dangers present in the online environment, to establish initial communication (3). By concealing identity and malicious intentions, the offender attempts to present the created interactions as an ordinary emotional bond or friendship and, in this way, break the child's psychological resistance (10). This psychological process, which is based on normalizing communication, provides a suitable ground for deceiving and enticing children so that the offender can implement the ultimate objectives of sexual exploitation without arousing the suspicion of the child or the child's family (3).

C) Isolating the Child from the Family

The third step in the criminal process described above is creating distance between the victim and the child's safe environment. After the trust-building stage, offenders exploit children's insufficient awareness of online dangers and attempt to minimize the child's communication with guardians (3). At this stage, the offender uses the child's strong tendency to trust strangers to create a secret space for two-way interactions, thereby completely neutralizing family supervision (10). The formation of shared secrets between the offender and the victim causes the child gradually to distance themselves from the family circle and enter a targeted state of isolation (3). This hidden feature in cyberspace and the severing of the child's connection with their support network sharply increases the risk of cyber abuse and renders the target completely defenseless against criminal demands (10).

D) Gradual Sexual Requests

After creating isolation and gaining the victim's complete trust, the cyber offender enters the stage of abnormal requests. At this step, the offender uses the intimate and hidden space that has been formed to make gradual requests for receiving inappropriate content from the child (3). These requests often include encouraging the child to produce and send private images, which ultimately prepares the ground for a form of sexual extortion in the online environment (11). After gaining access to these images, the offender uses the tactic of digital threats and intimidation to place the child under additional pressure to continue the relationship and comply with more severe demands (5).

In this situation, the child's fear of disgrace and the publication of the inappropriate content becomes an inhibiting factor against seeking help and forces the child to submit to these psychological and sexual threats (3).

E) Final Abuse

In the final step of the process of deception and grooming of children, the offender reaches the ultimate objective, namely sexual exploitation. At this stage, the offender fully implements the plan by exploiting the victim's insufficient awareness of the dangers existing in the online environment and by taking advantage of the child's natural tendency to trust others (3). This abuse can occur in two general forms: within communication networks or in the real world. In the first case, the offender, by using digital threats and intimidation, forces the child to submit to online sexual abuse and exploitation (11). Under these conditions, by possessing the child's private content, the offender traps the child in a harmful cycle of psychological and sexual abuse.

On the other hand, this grooming and deception, which initially begins in cyberspace for sexual purposes, may lead to in-person meetings and ultimately to physical abuse in the material world (3). In fact, by eliminating the boundaries between cyberspace and reality, the offender expands the scope of the assault and directly attacks the child's physical integrity. In both cases, irreparable and profound psychological and physical harms are inflicted on the child, requiring immediate intervention by support institutions and the adoption of preventive measures.

The Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

The formation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography is rooted in the efforts of the United Nations Commission on Human Rights in the 1990s to combat the global sexual abuse of children. These efforts, which culminated in the formation of a working group in 1995, ultimately led to the drafting of this instrument. The Protocol was adopted by the United Nations General Assembly in 2000 and entered into force in 2002. The Islamic Republic of Iran also acceded to this treaty in 2007 (2). The main objective of this instrument is to provide a comprehensive legal framework for combating the root causes of crimes against children, such as poverty, discrimination, and unequal social structures, as well as strengthening international cooperation to reduce demand and combat organized networks (2).

According to Article 3 of this Protocol, States Parties are required to explicitly criminalize a set of acts in their domestic criminal laws. These offenses include any offering, delivery, or acceptance of a child for the purpose of sexual exploitation, transfer of organs for profit, or forced labor. Furthermore, the production, distribution, importation, sale, or possession of child pornographic materials in which children are used, actually or virtually, in sexual activities has been criminalized. By considering the activities of organized networks under the cover of legal persons such as travel agencies, the Protocol also provides for criminal, civil, or administrative liability for such entities (2).

In addition to criminalization, this Protocol places special emphasis on preventive approaches. Under Article 9, States are required to increase children's awareness of the risks and methods of preventing these crimes through education and information dissemination. Moreover, Article 10 emphasizes the need to strengthen international cooperation to identify and address root causes, such as poverty and underdevelopment, that increase children's vulnerability. This dual approach, both penal and preventive, reflects the comprehensive perspective of this instrument toward protecting children against sexual exploitation (2).

Examination of the Capacities of the Optional Protocol to the Convention on the Rights of the Child

Children, due to their inherent vulnerability arising from weakness in cognitive and physical abilities and their lack of the maturity required to independently defend their fundamental rights, need a special protective umbrella against various forms of abuse. The expansion of communication technologies, while creating countless opportunities, has also brought emerging threats, among which the criminal phenomenon of "online grooming" is one of the most complex and widespread. In this process, the offender uses digital tools to carry out a gradual and calculated process of gaining trust, deceiving, and ultimately preparing the child for sexual exploitation. Given the transnational and complex nature of this crime, combating it requires strong and coordinated legal frameworks at the international level. Among various global instruments, the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography is recognized as the most central and comprehensive instrument for preventing and confronting these threats (2). Although this Protocol does not explicitly use the term "grooming," its multiple capacities in criminalization, international cooperation, and broad interpretation provide effective tools for preventing this phenomenon.

A) Creating a Global Protective Structure and the Obligation to Criminalize

One of the most important capacities of this Protocol is the creation of a coherent and binding global structure for the protection of children. By transforming the protection of child victims into a transnational obligation, this instrument requires domestic legal systems to fill legal gaps and strengthen protective mechanisms (2). Articles 2 and 3 of the Protocol oblige States to precisely criminalize all dimensions of criminal conduct related to sexual exploitation, including the production, distribution, sale, and even possession of child pornographic content. Since the process of grooming is often carried out as a preliminary step toward achieving these criminal objectives, the explicit criminalization of these final offenses also provides the necessary legal ground for prosecuting preparatory acts and attempts. This approach constitutes a legal response to children's inherent inability to defend themselves and, by creating uniform judicial practices, represents a fundamental step toward ensuring their comprehensive security against emerging harms.

B) The Adaptability of the Protocol to Crimes in Cyberspace

The Optional Protocol to the Convention on the Rights of the Child was drafted at a time when the landscape of cybercrimes and the deceptive complexities of cyberspace had not yet emerged in their current form. Nevertheless, the value and effectiveness of an international instrument depend on its dynamic nature and its capacity to adapt to changing conditions over time. From this perspective, the Optional Protocol, as a "living instrument," has the capacity to apply its fundamental concepts to new forms of criminality through a broad and purposive interpretation. This interpretive approach is not only permissible but also necessary to realize the ultimate objective of the Protocol, namely the comprehensive protection of children.

Children are highly vulnerable in cyberspace due to specific psychological characteristics such as gullibility, the need for approval, and an incomplete understanding of surrounding dangers. Offenders, aware of this vulnerability, design complex processes of deception and grooming through digital tools, the ultimate purpose of which is sexual exploitation. In such a context, the traditional concepts of "prostitution" and "sexual exploitation," which may refer to physical contact or direct financial exchange, are not sufficient to confront new threats.

Therefore, these concepts must be interpreted in such a way as to include any use of modern communication tools for purposes of sexual abuse (2). Accordingly, acts such as:

Online grooming: the process of trust-building and deceiving a child in order to prepare the child for sexual exploitation.

Production of self-generated content: forcing or deceiving a child into producing and sending nude or semi-nude images or videos of themselves.

Abuse through webcam: forcing a child to perform sexual acts in front of an internet camera.

Sexual extortion: threatening a child with the disclosure of images or private information in order to compel the child to comply with sexual demands.

Preparing for an in-person meeting: using cyberspace to arrange a physical meeting for the purpose of sexual abuse.

All of these must be defined under the examples of “sexual exploitation” within the framework of the Optional Protocol. This interpretive approach eliminates the legal gaps that cyber offenders exploit to evade punishment and extends the protective umbrella of the Protocol to new technological platforms. Consequently, States’ obligations are not limited merely to combating traditional forms of exploitation but also include the prevention of and active struggle against all its modern manifestations in the digital world, thereby ensuring the effectiveness of the instrument in protecting children against contemporary dangers.

C) Strengthening International Cooperation to Combat Transnational Crimes

Effective confrontation with the phenomenon of grooming, which has a transnational nature, requires the formation of collective will and synergy at the global level (2). The Optional Protocol, as a binding instrument, has provided the necessary legal basis for this convergence. According to the obligations set forth in Articles 7, 8, and 10, States Parties are required to establish extensive judicial and police cooperation in identifying, tracking, and prosecuting offenders in cyberspace. These interactions include mechanisms such as extradition, mutual legal assistance, and the seizure and confiscation of equipment and proceeds of crime. The purpose of these provisions is to eliminate safe havens for cyber offenders and cut off the communication channels of organized networks that exploit legal gaps between geographical borders to violate the fundamental rights of children. Such cooperation is a vital tool for ensuring that offenders do not escape justice and that they are held accountable regardless of their geographical location.

Penal Prevention Strategies

Prevention of criminality, especially in complex and hidden crimes targeting children, requires the adoption of multilayered and intelligent strategies. In this regard, penal prevention through the timely and effective intervention of the criminal justice system plays a fundamental role. This approach is not limited merely to reaction after the commission of the crime; rather, by criminalizing preliminary stages and creating legal barriers, it attempts to stop the cycle of criminality before the criminal result occurs and before irreparable harms are inflicted.

A) Independent Criminalization of Online Grooming as an Absolute Offense

One of the most important and effective strategies of penal prevention in the legal system is the early intervention of the legislator in the initial stages of the formation of criminal behavior. Given the gradual, complex, and

psychological nature of the process of deceiving and grooming children for sexual purposes in computer networks, referred to as grooming (5), it is necessary for preparatory and facilitating acts of abuse to be criminalized in a fully independent manner.

In this preventive approach, the process of gaining trust, creating deceptive friendship, and psychologically preparing the child should not be regarded merely as a preliminary stage or as an attempt to commit principal offenses such as sexual assault or the production of pornography. Rather, legislative criminal policy must evolve in such a way that this behavior is recognized in itself and as an absolute legal offense, independent of result. Acceptance of this approach means that the mere commission of deceptive and purposeful behaviors aimed at grooming a child, regardless of whether the final result, such as an in-person meeting or physical harm, occurs or not, has a criminal character and warrants decisive penal response (3).

This type of independent criminalization has two strategic advantages:

Creating effective deterrence: by criminalizing the initial stages, the cost of committing the crime for potential offenders increases and their risk-taking decreases.

Facilitating proof and prosecution: proving principal offenses such as sexual assault, which often occur in secrecy and without witnesses, is highly difficult. However, proving the grooming process through documentation of digital communications is much easier and allows the judiciary to prosecute the offender before a catastrophe occurs.

Thus, by depriving offenders of opportunity in the initial stages, this penal policy creates a strong defensive barrier against the evolution of the process of child victimization.

B) Comparative Approach and the Necessity of Strengthening Domestic Laws

A comparative examination of legislative approaches shows that drafting specific regulations for protecting children in the digital environment is among the priorities of advanced legal systems. Laws such as the Children's Online Privacy Protection Act in the United States, which imposes strict requirements on website operators and online services regarding the collection of information from children under the age of 13, or similar laws in Australia and the United Kingdom, all focus on creating precise frameworks for protecting children's privacy and online security.

In Iran's legal system, although the Law on the Protection of Children and Adolescents, adopted in 2020, and the Computer Crimes Law have taken positive steps in this regard, they still require continuous strengthening and updating. The rapid developments of technology and the emergence of new methods of grooming require that protective laws specifically addressing children in cyberspace develop dynamically (8). This can be achieved by modeling successful international experiences, focusing on making online service providers accountable, and drafting transparent protocols for reporting and removing criminal content. Of course, structural and legal reforms alone are not sufficient, and the development of public education for parents, educators, and children themselves is absolutely necessary as a complementary strategy for situational and social prevention (1).

C) The Conflict between Privacy and Child Security

The process of identifying, documenting, and proving crimes committed against children in the cyber environment faces numerous legal and technical obstacles. The diversity of harms in this field, ranging from online sexual abuse and exploitation to digital threats and intimidation and economic deception, reflects the broad and complex dimensions of this crisis (7).

At the heart of these challenges lies a fundamental conflict between users' right to privacy and the undeniable necessity of ensuring children's security. Virtual platforms and messaging services, by using advanced security technologies such as end-to-end encryption, practically block the access of judicial and law-enforcement supervisory institutions to exchanged criminal content. Although this approach is designed to protect users' privacy, it creates serious disruptions and impasses in the process of collecting, documenting, and evaluating electronic evidence for detecting organized criminal networks.

On the other hand, children's natural tendency to trust, their curiosity, and their need for approval from peers or adults create a highly suitable ground for offenders to deceive and groom them (3). These vulnerable psychological characteristics allow offenders, by concealing their true identity under the protection of privacy tools, to advance the process of grooming children easily and away from the eyes of parents and supervisory institutions (5). Consequently, despite existing emphasis on the need to strengthen protective laws (8), legislative challenges related to lawful access to digital evidence and the precise boundary between legitimate privacy and its abuse for criminal purposes continue to act as a strong barrier against the timely detection and effective prosecution of this category of crimes and require innovative legal and technical solutions.

Non-Penal Prevention Strategies

Situational Prevention

Non-penal strategies in confronting cybercrime against children follow a proactive and anticipatory approach by focusing on reforming harmful environments and reducing situations conducive to victimization. In this context, situational prevention measures play a central and key role with the main objective of making crime more difficult and reducing criminal opportunities. This approach is based on the assumption that crime results from the convergence of a motivated offender, a suitable target, and the absence of a capable guardian. In cyberspace, this guardian may consist of a set of technological tools, supervisory structures, and legal requirements. Since insufficient awareness of online dangers is one of the most important factors facilitating children's victimization (1), imposing structural and supervisory restrictions in order to deprive cyber offenders of opportunity is an undeniable necessity.

Situational prevention interventions in this field can be classified into three main levels:

A) Hardening the Target through Technological Tools

One of the most practical solutions in this field is the use of technology to create defensive shields and secure the child's surrounding digital environment. These measures focus directly on "target hardening":

Content-filtering and parental-control tools: the use of filtering software and parental-control systems on smart devices is the first line of this technological defense. Given children's natural tendency to trust strangers in communication networks (3), these tools block the ground for offenders to establish hidden communication with their targets by designing a managed digital environment and restricting children's access to harmful content. In practice, these technologies frustrate the process of psychologically preparing the child by the offender, known as grooming. The development and application of these programs play a technical complementary role for support programs and public education for guardians (1).

Dedicated and secure communication infrastructures: using modern technological tools is a fundamental measure for creating a safe digital space and protecting children against various forms of online intimidation and exploitation (7). Providing dedicated communication infrastructures, such as safe SIM cards for children and adolescents, and implementing intelligent content-filtering systems at the network level constitute a structural and effective solution. These technological measures, by restricting unauthorized access and blocking pathways of deception and grooming of children (5), significantly reduce potential vulnerabilities in interactive environments and facilitate effective supervision of children's digital behavior.

B) Increasing the Risk of Committing Crime for Offenders

This category of situational measures increases the cost of committing crime for offenders by increasing the likelihood of their identification and arrest:

Obligating platforms to monitor and report immediately: one of the fundamental dimensions of situational prevention is requiring communication service providers and content-distribution platforms to actively monitor data. Realizing this preventive approach directly requires strengthening special protective laws for children in cyberspace (8). Home-screening networks and interactive media dedicated to minors must be required to establish and develop immediate reporting mechanisms so that harmful content can be identified and blocked in the shortest possible time. The imposition of such structural supervision and accountability on service providers not only blocks the pathways of deception and grooming of children (5), but also, by documenting criminal activities, greatly increases the risk of identification for offenders and significantly reduces the occurrence of online sexual abuse and exploitation, as well as virtual threats and intimidation against minors (7).

Social Prevention

One of the essential pillars of social prevention of network-based crimes against children is focusing on cognitive development and raising the level of public education. Children, due to the psychological characteristics specific to childhood, lack of sufficient knowledge and awareness of hidden threats in the virtual environment, and natural tendency to trust strangers, are highly exposed to risk (3, 9). These characteristics and intellectual immaturity significantly increase their susceptibility to various forms of online abuse (10). Therefore, designing and developing public education programs aimed at empowering guardians, teachers, and especially children themselves is an unavoidable strategy for controlling this challenge (1, 12).

A) Empowering the Family and Enhancing Media Literacy

One of the fundamental pillars of protecting children in communication networks is raising the level of media literacy among families through continuous educational programs (1, 12). The family, as the first social institution in which the child grows, plays an irreplaceable role in supervising, educating, and controlling the child's access to cyberspace (9). The necessity of implementing this educational approach arises from the fact that children, due to insufficient awareness of hidden dangers in online environments, are always exposed to serious harms (3). In addition, children's psychological tendency to trust strangers doubles the need for informed parental supervision (10). In such a context, developing and implementing scheduled training courses for parents and teachers can play a fundamental role in enhancing supervisory knowledge and empowering families in the prevention of victimization.

B) Institutionalizing Education in the Formal Education System

The school institution, alongside the family, governmental organizations, non-governmental organizations, and mass media, is one of the key pillars in implementing preventive policies (1). Therefore, teaching self-protection skills from the earliest ages and within primary educational institutions is a fundamental strategy for combating cybercrimes against children (7). Including subjects related to “digital literacy,” “user ethics,” and “awareness of cyberspace risks” in the formal curriculum of the education system is considered necessary (1, 12). Accordingly, holding awareness-raising workshops and continuous training courses at the school level plays a significant role in improving children’s and adolescents’ understanding of online threats. Furthermore, developing the above-mentioned education in the form of simultaneous counseling classes for children and parents in educational centers strengthens synergy between home and school and ultimately consolidates the defensive capabilities of society against new harms (1).

C) Training in Privacy and Data Protection Skills

One of the fundamental dimensions of children’s rights in cyberspace is the protection of their privacy, violation of which may provide the basis for numerous crimes (4). The right to security and privacy is among the fundamental rights of children and requires special protection by the legislator and society (6). Nevertheless, the lack of sufficient knowledge about online risks increases the vulnerability of this group to threats in communication networks (1). This lack of awareness may lead to the unintended disclosure of identity data, images, or personal information and subsequently facilitate the occurrence of crimes such as extortion, identity theft, and sexual exploitation of children (7, 11). Therefore, enhancing public awareness regarding data protection and providing continuous education on avoiding the sharing of personal information are undeniable necessities in preventing victimization (4). Achieving this requires holding targeted awareness-raising workshops for children and adolescents so that, by empowering them, a culture of responsibility in cyberspace becomes institutionalized (1).

D) Linking Situational and Social Prevention

Although developing public education programs for parents and educators and improving children’s behavioral skills in the virtual environment (1) are social-prevention measures by nature, they fundamentally support the effectiveness of situational measures. A child who is familiar with the dangers of cyberspace and social-engineering techniques becomes a “hard target” for offenders (3). Such a child is less likely to be deceived and share personal information or attempt to bypass technological restrictions imposed by parents. This reduces criminal opportunities and ultimately increases the cost of committing crime for the offender, leading the offender to abandon malicious objectives. Therefore, raising the child’s awareness itself functions as a control mechanism and a tool of situational prevention.

Conclusion

The emergence and increasing expansion of modern communication technologies, alongside all their undeniable advantages, have also transformed the landscape of criminality and, by facilitating anonymity and the crossing of geographical borders, have directed new threats toward the most vulnerable groups in society, especially children. In this context, the phenomenon of “online grooming,” as one of the most complex and destructive cybercrimes

aimed at preparing the ground for the sexual exploitation of children, seriously endangers their psychological security and physical integrity. In line with examining the legal dimensions of this phenomenon and providing countermeasures, this research examined the capacities of international instruments, evaluated the gaps in the domestic legal system, and explained preventive strategies.

The findings showed that at the international level, the Optional Protocol to the Convention on the Rights of the Child, despite not explicitly referring to the term “grooming,” has significant legal capacity to confront this phenomenon as a dynamic “living instrument.” By obligating States to criminalize all forms of the sale of children, child prostitution, and child pornography, this Protocol indirectly includes within its scope the preparatory and facilitating acts of these crimes, of which online grooming is a clear example. More importantly, through a broad and purposive interpretation, all modern manifestations of sexual exploitation in cyberspace, including self-generated content and sexual extortion, can be defined under the concepts contained in the Protocol. In addition, the emphasis of this instrument on strengthening international cooperation provides a key tool for combating the transnational nature of these crimes and eliminating safe havens for cyber offenders.

Despite these international capacities, their effectiveness depends on implementation within national legal systems. The findings of this research regarding Iran’s legal system indicate that, despite the existence of protective laws such as the Law on the Protection of Children and Adolescents and the Computer Crimes Law, the most important legislative deficiency is the absence of independent criminalization of online grooming. At present, this conduct can be prosecuted only as an attempt or as a preliminary act to principal crimes, proof of which is highly difficult in the initial stages and before the occurrence of final harm. Accordingly, it is recommended that the legislator, by drawing on the successful experiences of advanced legal systems, criminalize “grooming” as an absolute and independent offense, irrespective of the occurrence of a result. This measure, while creating effective deterrence, would allow the judiciary to intervene at the initial stages and before irreparable harms are inflicted, thereby stopping the cycle of criminality.

However, the penal response alone is not sufficient, and effective confrontation with this phenomenon requires the adoption of a comprehensive approach combining situational and social prevention. In the field of situational prevention, measures such as developing technological tools, including parental-control software and content filtering, providing secure communication infrastructures, such as child SIM cards, and, more importantly, obligating virtual platforms to actively monitor and immediately report criminal content can significantly reduce opportunities for crime. These measures must be complemented by social-prevention strategies centered on education and the enhancement of “media literacy” at three levels: children, parents, and the education system. Empowering families for informed supervision, incorporating digital-security concepts into textbooks, and teaching self-protection skills to children turn them into “hard targets” for offenders. These two approaches complement each other: situational prevention secures the environment, and social prevention secures the user.

Ultimately, this research showed that protecting children against emerging threats in cyberspace requires a comprehensive, intelligent, and multidimensional criminal policy in which legislative reforms, technological interventions, and public education operate in a coordinated and integrated manner. Only by creating such a strong defensive shield can one hope that future generations will benefit from technology in a safer 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 adhered 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. Ghasemi A. Analysis of Cybercrimes against Children and Preventive Strategies. Qom: University of Qom; 2015.
2. Unicef. Handbook on the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography. Florence: Innocenti Research Centre, 2009.
3. American Bar Association. Understanding Sexual Grooming in Child Abuse Cases. Child Law Practice. 2015;34.
4. Ebrahimi S, Mahmoudi V. Protection of Sexual Victims in Cyberspace. Judicial Law Perspectives Quarterly. 2016(75):9-34.
5. Ghani Zadeh Bafghi M, Hosseinzadeh Sarshaki A. A Study of the Phenomenon of Pornography and Cyber Grooming of Children in Light of Islamic Jurisprudence and Iranian Law. Legal Studies. 2022;14(1):315-41.
6. Mosaffa N. The Convention on the Rights of the Child and Its Application in Iranian Domestic Law. Tehran: Gerayesh; 2004.
7. Hosseini B. Internet Crimes against Children and Their Criminological Backgrounds. Tehran: Afraz; 2004.
8. Zeinali AH. Iran's Criminal Policy toward Sexual Exploitation of Children. Criminal Law Research. 2018;6(22):171-96.
9. Rayejian Asli M. Victimology of Children and Adolescents. Tehran: Khat-e Sevvom; 2011.
10. Gottman S. The Internet and Sexual Abuse of Children. Computer Magazine. 1998(70).
11. Flor R. Internet-Related Child Pornography. Frankfurt: Peter Lang; 2004.
12. Salimi S. Protection of Children against Pornography in Cyberspace. Criminal Law Research Quarterly. 2014;3(8):121-54.