Publicationes Universitatis Miskolcinensis
Sectio Juridica et Politica, Tomus XLIII/2 (2025), pp. 199–219.
https://doi.org/10.32978/sjp.2025.024

AN ANALYSIS OF IRAN'S LEGISLATIVE RESPONSE TO CHILD VICTIMIZATION IN CYBERSPACE: A CRIMINAL POLICY PERSPECTIVE

IRÁN JOGALKOTÁSI VÁLASZA A GYERMEKEK KIBERTÉRBEN VALÓ ÁLDOZATTÁ VÁLÁSÁRA: BÜNTETŐPOLITIKAI NÉZŐPONT

MARYAM DELSHAD* – ALI NAJAFI TAVAANA** – AMIRHASAN NIAZPOUR***

The entry into cyberspace has created risks, especially for children, who are among the most vulnerable. This article evaluates Iran's criminal policy response to child victimization in cyberspace by analyzing existing laws, their effectiveness, and the strengths and weaknesses of the criminal justice system. It also proposes solutions for improved child protection. Key aspects of reactive criminal policy include special criminalization, global jurisdiction over child cyber pornography, support for NGOs, specialized cybercrime departments, and formal protection measures for child victims. The findings aim to enhance Iran1s approach to cybercrimes against children.

Keywords: *child victimization, cyberspace, criminal policy, differential criminalization, supportive penalization, cyber pornography*

Az emberi tevékenység kibertérbe való belépése kockázatokat is hordoz, különösen a gyermekek számára, akik a legsebezhetőbbek közé tartoznak. Ez a tanulmány Irán büntetőpolitikai válaszát értékeli a gyermekek kibertérben való áldozattá válására, elemezve a meglévő jogszabályokat, azok hatékonyságát, valamint a büntető igazságszolgáltatási rendszer erősségeit és gyengeségeit.

* MARYAM DELSHAD
Ph.D candidate
Department of Criminal Law and Criminology
Central Tehran Branch, Islamic Azad University, Tehran, Iran. (Corresponding Author)
delshadmaryam@yahoo.com

** ALI NAJAFI TAVAANA
assistant professor
Department of Criminal Law and Criminology
Central Tehran Branch, Islamic Azad University, Tehran, Iran
ali.najafi_tavana@iauctb.ac.ir

*** AMIRHASAN NIAZPOUR
associate professor
Department of Criminal Law and Criminology
Shahid Beheshti University, Tehran, Iran
niapah@yahoo.com

Javaslatokat is megfogalmaz a gyermekvédelem javítására. A reaktív büntetőpolitika kulcselemei közé tartozik a speciális kriminalizálás, a globális joghatóság a gyermekekkel kapcsolatos kiber-pornográfia felett, a civil szervezetek támogatása, a kiberbűnözéssel foglalkozó szakosított osztályok létrehozása és a gyermekáldozatok hivatalos védelme. Az eredmények célja Irán megközelítésének javítása a gyermekek ellen elkövetett kibertéri bűncselekmények kezelésében.

Kulcsszavak: *gyermekáldozattá válás, kibertér, büntetőpolitika, differenciált kriminalizálás, támogató büntetőjogi szankciók, kiberpornográfia*

Introduction

With the expansion of cyberspace and increased access of children to the internet, the risks of child victimization in this space have significantly increased. Cyberspace, despite offering numerous educational and recreational opportunities, also provides a platform for various crimes against children, including sexual abuse, financial exploitation, and psychological harm. Therefore, the criminal policies of different countries, including Iran, require an effective and proportionate response to these threats.

Child victimization in cyberspace occurs when a child, while engaging in activities in this virtual environment, becomes a target for abusers. In other words, it refers to the physical and psychological harm caused to children through the use of electronic devices and participation in social networks, where they establish communication and interact with potential abusers. This harm is distinct from that which can occur to any individual, including children, due to the improper use of electronic devices.

Given the increasing number of children present in cyberspace, the likelihood of their victimization also rises. Therefore, criminal policy intervention to address the dangers in cyberspace has become more crucial, and the criminal justice system must provide special protection for victimized children.[1]

Through victimology and doctrinal legal research, recent Iranian domestic studies have increasingly addressed the difficulties associated with child victimization in cyberspace.[2] They have emphasized the need for specialized protection methods and helped build the conceptual framework for cybercrime.[3] They also urge for more legislative clarity, judicial specialty and support systems for child victims, and they mainly concentrate on the constraints and structure of Iran's legal system, notably its

---

1 HAJIDEHABADI, Ahmad, SALIMI, Ehsan.: Principles of Criminalization in Cyberspace (A Critical Approach to the Computer Crime Act). *Majlis and Rahbord* No. 80, 2015, 79.

2 NADERI, Hamaseh: The Cyberspace Harms for Children. *International Journal of Advanced Research in Humanities and Law* Vol. 1, No. 2, 2024, 62–63. https://doi.org/10.63053/ijrel.12

3 ROUHANI MOGHA, Mohammad, MOUSAVI, Seyed Javad, AGHAEI BAJESTANI, Mohammad: The process of child victimization in cyberspace with emphasis on economic factors. *Strategic Studies of Jurisprudence and Law* Vol. 3, No. 4, 2022, pp. 37–53. https://dor.isc.ac/dor/20.1001.1.26767163.1400.3.4.3.8

reactive criminal policy.[4] Academic literature from several jurisdictions provides a deeper understanding of how different criminal systems address child victimization in cyberspace. In the European Union, a framework developed under the EU Kids Online project emphasizes evidence-based digital policy that balances children's rights to protection and participation.[5] In the United Kingdom, studies have analyzed grooming processes in online child sexual exploitation cases, offering practical legal and psychological insights for prevention.[6] From an Islamic perspective, Malaysia has implemented a Sharia-sensitive criminal policy that addresses online sexual offenses through the Communications and Multimedia Act and Child Act 2001. Research highlights the integration of moral education with legal enforcement as a preventive strategy.[7] These examples reveal the diversity of legal responses and offer comparative perspectives relevant to Iran's evolving criminal policy framework.

Considering the issues mentioned above, a question arises: What criminal policy does Iran have regarding child victimization in cyberspace? This study aims to answer this question by examining the reactive measures (after the crime) in Iranian criminal law concerning child victims in cyberspace and evaluating Iran's criminal policy toward child victimization in cyberspace.

1. Substantive Reactive Criminal Policy

The typology of special protection for victims is based on two criteria: the victim's vulnerability and the criminal behavior that causes victimization.[8] The typology of child victimization protection is determined based on their level of vulnerability to crime through two forms of criminal support: substantive and procedural. In terms of substantive criminal support, reactive prevention through criminal protection for victimized children involves criminalizing harmful behaviors and implementing differential penalization, which has a preventive aspect based on Jeremy Bentham's

---

4 EHSSANPOUR, Seyed Reza, GHADAMI AZIZABAD, Mosayeb: The Components of the Optimal Preventive Criminal Policy Toward Sexual Victimization of Children in Cyberspace. *The Quarterly Journal of Judicial Law Views* Vol. 29, No. 105, 2024, 5–8. https://dor.isc.ac/dor/20.1001.1.22520007.1403.29.105.1.8

5 LIVINGSTONE, Sonia, ÓLAFSSON, Kjartan, POTHONG, Krittiya: Digital play on children's terms: A child rights approach to designing digital experiences. *New Media & Society* Vol. 27, No. 3, 2025, 1470. https://doi.org/10.1177/14614448231196579

6 WHITTLE, Helen, HAMILTON-GIACHRITSIS, Catherine, BEECH, Anthony: A review of online grooming: Characteristics and methods. *Aggression and Violent Behavior* Vol. 18, No. 1, 2013, 62–63, 70. https://doi.org/10.1016/j.avb.2012.09.003

7 ISLAM, Md Zahidu, ZULHUDA, Sonny, MOHD BADROL AFANDI, Nor Hafizah, SHAFY, Mohamed Affan: Ensuring safe cyberspace for children: An analysis of the legal implications of social media usage in Malaysia and Singapore. *IIUMLJ* Vol. 28, 2020, 395. http://dx.doi.org/10.31436/iiumlj.v28i(S1).591

8 RAHIMI, Hamid: Victim-centered typology of child and adolescent protection in Iranian criminal law. *Criminal Justice Newsletter, Criminal Law and Criminology Group, Faculty of Law, Shahid Beheshti University* No. 4, 2019, 32.

"criminal calculus" theory. This exemplifies the interaction between victimology, criminal policy, and criminal law.[9]

1.1. Differential Criminalization

Differentiation in criminal policy reflects the increasing complexity and diversity of human societies in terms of science, culture and economy, which, in turn, leads to a variety of crimes, offenders, pre-criminal situations, targets, and crime victims. If the primary mission of criminal policy is to produce and guarantee social and political security, this security must be defined across various domains. In addition to life and property, which are historically valued in criminal law, other areas such as the environment, human dignity, cyber values, and ethical life values also require protection and security. Thus, the differentiation of criminal legislation generally occurs within three main criteria: a) typology of crimes, b) typology of offenders, and c) typology of victims. [10]

Criminalization in cyberspace must be conducted in a way that is, first, free from bias or extreme ideology while respecting cultural norms, and second, focused on criminalizing the most harmful behaviors—not all behaviors. This is important because ideological differences between countries result in variations in the criminalization of sexual offenses, which can complicate the prosecution of crimes committed against Iranian child victims. The absence of the principle of dual criminality and the lack of extradition agreements make it difficult to apprehend perpetrators. Additionally, expanding treaties on the extradition of criminals can create a deterrent effect for nationals of the countries involved, discouraging them from committing sexual offenses against Iranian children in cyberspace. The impact of extradition on preventing sexual offenses in cyberspace is addressed in Article 20 of the Budapest Convention on Cybercrime, 2001.

What distinguishes the approach to criminalization in protecting children is the use of traditional criminal law mechanisms in a manner that differs from their application in protecting adults. Accordingly, lawmakers have adapted criminalization mechanisms to align with the unique circumstances of this vulnerable group, leading to the development of a "differentiated criminal policy" in this area.[11]

Criminalization and punishment of offenders—as the oldest approach to addressing social deviance in criminal policies—entail both general deterrence (discouraging potential offenders) and specific deterrence (preventing recidivism). This remains applicable to crimes committed in cyberspace and is a common component of global criminal policies. It is evident that criminalization in

---

[9] KERAMATI MOAZ, Hadi: Victimology of children in virtual networks. 1st ed. Tehran, Dadgostar Publications, 2020, 102–103.

[10] LAZERGES, Christian: *Introduction to criminal policy*. (A. H. Najafi Abrand Abadi, Trans.) 8th ed. Tehran, Mizan Legal Foundation, 2020, 64.

[11] ZEYNALI, Amirhamzeh: *Globalization of criminal law (In the realm of protecting children against victimization)*. 1st ed. Tehran, Mizan Legal Foundation, 2015, 404–405.

cyberspace differs significantly from conventional criminalization due to factors such as differing sexual behaviors in this environment and their divergence from traditional sexual crimes. The 1999 Vienna Conference on Combating Child Pornography on the Internet emphasized a "zero tolerance" policy and global cooperation in criminalizing child pornography.[12]

Criminalization in cyberspace must therefore be implemented in a way that, first, avoids ideological extremism while respecting national cultural norms, and second, targets only the most severe behaviors. These differences in ideology among countries impact how sexual offenses are defined, making it harder to prosecute offenders when principles like dual criminality or extradition treaties are absent. Expanding international treaties can deter foreign nationals from committing offenses against Iranian children. Article 20 of the 2001 Budapest Convention highlights the importance of extradition in curbing cyber sexual offenses.

Iran's legislative criminal policy addresses the criminalization of prohibited acts and behaviors in cyberspace through various laws, each reflecting a specific criminal policy. Notable examples include the Electronic Commerce Law (2003), the Law on Punishing Individuals Engaged in Unauthorized Audiovisual Activities (2007), and the Computer Crimes Law (2009).

1.1.1. The Computer Crimes Law

Legislation in Iran, like in many other countries, was initially shaped by a sense of necessity. Authorities, upon confronting cyberspace, realized the urgent need for specific laws. As a result, the process of legislating in this field began. However, existing mechanisms have proven insufficient to meet the evolving demands of cyberspace. Therefore, updating the law is essential, and in this regard, adopting successful global models is inevitable.[13]

The Computer Crimes Law addresses various offenses, including unauthorized access and eavesdropping, cyber forgery, computer fraud, cyber espionage, data destruction and disruption, computer theft, crimes against public morals, and more. In these cases, the intention and malicious motive of the offender receive special attention. However, for certain offenses—such as those in Article 733 (Article 5 of the Computer Crimes Law), Article 769 (Article 21), and Article 751 (Article 23) regarding government officials responsible for protecting confidential data—the law holds them liable and punishable if, due to negligence, they allow unauthorized access to data or systems. Likewise, service providers who fail to filter and monitor criminal content, thereby facilitating access to illegal material, are also considered culpable. This aspect of the law demonstrates a focus on maintaining public order and preventing

---

[12] https://ebrary.net/57625/law/international_conference_combating_child_pornography_inter net, 20th March 2025.

[13] MOHSENI, Farid: *Criminological theories*. 1st ed. Tehran, Judiciary Press and Publications Center, 2018, 251.

harm to society, while also protecting internet users from victimization—a strength of the legislation.[14]

On the other hand, "child pornography" was originally included in the draft of the Computer Crimes Law in alignment with the Cybercrime Convention. However, in the final version, the Iranian legislature, diverging from the original intent and global standards, adopted a broader and more absolute approach to cyber pornography. Article 14 of the Computer Crimes Law (Article 742 of the Islamic Penal Code), under the section "Crimes against Public Morality", states:

"Anyone who publishes, distributes, or trades obscene content via computer systems, telecommunications, or data carriers, or produces, stores, or keeps such content for the purpose of trade or corruption, shall be punished by imprisonment for a period of 91 days to 2 years, or a fine ranging from 5 million (5,000,000) rials to 40 million (40,000,000) rials, or both."

1.1.2. The Law on the Protection of Children and Adolescents

In the latest legislative developments within Iran's legal system, the legislator, in Clause 9 of Article 10 of the Law on the Protection of Children and Adolescents (passed on 20. 05. 2020), states:

"Establishing contact with a child or adolescent in cyberspace for the purpose of any sexual abuse or illicit sexual contact will be punishable by one of the punishments of degree six of the Islamic Penal Code."

Additionally, among the legislative measures aimed at addressing child victimization in cyberspace, Clause 8 of Article 10 criminalizes the import, export, and uploading of obscene or vulgar content involving children and adolescents.

Although Article 31 of the Law on the Protection of Children and Adolescents classifies all crimes under this law as public offenses, it would have been more appropriate to address separately the threats posed to children or adolescents in cyberspace due to their widespread consequences. This would enable stricter penalties and prevent such cases from being treated as "complaint-based crimes" under Article 669 of the Islamic Penal Code (Tazirat).

Negligence and carelessness by individuals mentioned in Clause A of Article 1 of the Law on the Protection of Children and Adolescents, who are responsible for monitoring or supervising children or adolescents, can be realized within cyberspace.[15] Their negligence in allowing children or adolescents to watch inappropriate images or videos online could lead to undesirable psychological and

---

[14] KERAMATI MOAZ, Hadi, ZAND RAD MAJID, P.: Iran's criminal policy regarding victimization of women and children in cyberspace. *Andisheh Vakil* 3rd Year, (6), 2024, 99. https://doi.org/10.22034/jccj.2024.462904.1581

[15] Paragraph (p) of Article 1 of the Law on the Protection of Children and Adolescents states: "Neglect and carelessness: Failure to fulfill duties such as providing the basic and essential needs of the child or adolescent or obligations related to guardianship, custody, tutelage, oversight, or care of them by parents, guardians, legal custodians, or any individual responsible for such duties."

social consequences, such as increased violent behaviors, indifference to the pain and suffering of others, and inability to distinguish between real life and virtual triggers. Parental supervision of their children in cyberspace, just as in traditional spaces, is a legal and religious duty and can be considered as part of Clause A of Article 3 of the Law on the Protection of Children and Adolescents.[16]

Sometimes, children and adolescents may be exploited in cyberspace, leading to online victimization.[17] For example, using children for advertisements or Instagram pages by others is considered a form of exploitation. Additionally, images of children or adolescents may be published on social media, where they are coerced into engaging in inappropriate behaviors, which, when shared, result in significant psychological and social harm. These harms can include isolation, feelings of shame, ridicule, dropping out of school, and more. This is also true for teachers who may take pictures of their students and publish them on cyberspace. In these cases, the legislator has proposed protective measures in Clause G of Article 3, Clause A of Article 6, and Article 32.[18] However, it would be better if the legislator provided specific guidelines in the Law on the Protection of Children and Adolescents regarding the publication of children and adolescents' images by individuals mentioned in Clause A of Article 1 of the law and teachers.

---

[16] Article 3 of the Law on the Protection of Children and Adolescents provides: "The following cases, if they place the child or adolescent at risk of victimization or cause harm to their physical, mental, social, moral, security, or educational well-being, are considered hazardous situations warranting intervention and legal protection for the child and adolescent: Paragraph (a): Lack of guardianship over the child or adolescent or neglect and carelessness in fulfilling legal and religious duties towards them by any person obligated to do so..."

[17] Paragraph (t) of Article 1 of the Law on the Protection of Children and Adolescents provides: "Abuse: Any intentional act or omission that places the physical, mental, moral, or social health of a child or adolescent at risk, including actions such as beating, imprisonment, sexual exploitation, insult, or threat against the child or adolescent, provided it constitutes an aggressive violation, or subjecting them to harsh and abnormal conditions, or withholding necessary assistance."

[18] Paragraph (zh) of Article 3 of the same law states: "Abuse of or exploitation of the child or adolescent." Paragraph (a) of Article 6 of the Law on the Protection of Children and Adolescents mandates: "The State Welfare Organization is obligated to identify, admit, support, shelter, and empower children and adolescents covered under this law by employing social workers through social service emergency measures, in cooperation with municipalities, village councils, and law enforcement, and report such cases to competent authorities." Article 32 of the aforementioned law states: "Social workers of the Welfare Organization, after becoming aware of hazardous situations as defined in Article 3 of this law, shall undertake investigations and appropriate actions as follows: (a) Summon parents, guardians, legal custodians, or other related individuals to the child or adolescent, and if necessary, summon the child or adolescent alongside them. (b) Visit the residence, workplace, school, or other relevant locations of the child or adolescent, accompanied by judicial officers if needed."

Furthermore, individuals may influence the mental and emotional well-being of children and adolescents in cyberspace, potentially causing them to run away from home or school. The legislator has addressed this issue by enacting Article 8 of the Law on Protection to safeguard children and adolescents from such harm.[19]

1.2. Supportive Criminalization

Today, in light of criminological findings—and especially the relatively new field of victimology—it is well established that children, due to their specific physical, psychological, and social conditions, are more vulnerable to criminal offenses than others. Therefore, increasing penalties for offenders who target such vulnerable victims is an important and effective tool available to criminal policymakers. In view of this criminological reality, one of the mechanisms of criminal support for protecting children from victimization is the imposition of harsher penalties. Criminal legislators, through differential criminal policy, have considered the status of the child victim as an aggravating factor, increasing the punishment for offenders whose victims are children. This policy has often been pursued in crimes against the physical and psychological integrity of children.[20]

Another significant mechanism in substantive criminal law to combat child and adolescent victimization is "supportive criminalization"—or, in other words, "predicting aggravating circumstances for penalties". The importance of this approach to protecting vulnerable individuals, as well as its connection to the "economic theory of crime" (or the "reward and punishment theory" of Gary Becker) and Bentham's "penal calculation" theory, becomes clearer in the context of supportive criminalization. This concept does not only involve increasing the type and amount of punishment; rather, its scope is much broader. In addition to enhancing punishment severity, it includes other enforcement measures alongside the primary punishment.[21]

1.2.1. The Law on Punishment of Audiovisual Offenders

One group that is particularly vulnerable to victimization in the online environment is children, especially when exploited in pornography. In this regard, the Iranian

---

[19] Article 8 of the Law on the Protection of Children and Adolescents stipulates: "Anyone who, through threats, encouragement, or persuasion, causes a child or adolescent to run away from home or school, drop out of school, deceives them for such purposes, or facilitates or provides the means for these acts, shall, if the child or adolescent runs away or drops out of school, be sentenced to one or more punishments under Grade 6 of the Islamic Penal Code. If no such runaway or dropout occurs, the individual will receive a warning from the Special Police for Children and Adolescents for the first offense and will face the aforementioned punishment in case of repetition."

[20] ZEYNALI, Amirhamzeh: *Globalization of criminal law (In the realm of protecting children against victimization)*. 1st ed. Tehran, Mizan Legal Foundation, 2015, 342.

[21] KERAMATI MOEZ, Hadi, MIRKHALILI, Seyedmahmood: Iran's Legislative Criminal Policy Approach and International Documents to Support Vulnerable Children on Social Media. *Police International Studies* 11 (41), 2020, p. 116. SID. https://sid.ir/paper/392158/en.

legislator, in the Law on Punishing Individuals Engaged in Unauthorized Audiovisual Activities (passed in 2007), stated in Note 3 of Article 3: *"The use of minors to store, display, offer, sell, or duplicate unauthorized tapes and CDs under this law shall result in the maximum penalties prescribed for the offender."*

At first glance, it may seem that the legislator intends to offer special criminal protection to children in the case of pornography. However, this is not the case, as the legislator refers to unauthorized works rather than obscene or vulgar audiovisual content. Therefore, the legislator is addressing relatively minor offenses in Articles 1 and 2 of this law, which are typically related to copyright violations.[22]

1.2.2. The Computer Crimes Law

This law introduced two major changes to Iran's legal system. First, it led to the formation of the country's first specialized judicial force, the Cyber Police, to address issues in cyberspace. Second, it established specialized cybercrime courts and prosecutor offices, which contributed to the development of the legal system. The process of investigating, identifying, and proving computer crimes is now handled through specialized procedures, with official authorities capable of addressing such matters.[23]

Chapter Four of this law, titled "Crimes against Public Morality", addresses some aspects relevant to our discussion, including Article 14 on the publication, distribution, or trafficking of obscene content.[24]

In Article 15, it is stated that anyone who engages in the following acts through computer systems, telecommunications, or data carriers will be punished as follows:

a) If they induce, encourage, threaten, or deceive individuals to access obscene content, facilitate access to such content, or teach methods for obtaining it, they will be sentenced to imprisonment for a period of 91 days to one year, or a fine ranging from five million (5,000,000) rials to twenty million (20,000,000) rials, or both. If these acts relate to vulgar content, the punishment is a fine ranging from two million (2,000,000) rials to five million (5,000,000) rials.

---

[22] KERAMATI MOEZ, Hadi, MIRKHALILI, Seyedmahmood: Iran's Legislative Criminal Policy Approach and International Documents to Support Vulnerable Children on Social Media. *Police International Studies* 11 (41), 2020, 121. SID. https://sid.ir/paper/392158/en.

[23] NOORZAD, Mojtaba: *Economic crimes in Iranian criminal law*. 1st ed. Tehran, Jangal Publications, 2010, 152–153.

[24] Article 14: Anyone who, using computer systems, telecommunications systems, or data carriers, publishes, distributes, or trades obscene content, or produces, stores, or keeps it with the intent of trading or corruption, shall be sentenced to imprisonment for a period of ninety-one days to two years or a fine ranging from five million (5,000,000) rials to forty million (40,000,000) rials, or both punishments.
Note 1: The commission of the above actions regarding obscene content shall result in a conviction to at least one of the aforementioned punishments. Obscene content and materials refer to works that include offensive and immoral scenes and depictions. Note 2: If obscene content is sent to fewer than ten people, the offender shall be sentenced to a fine ranging from one million (1,000,000) rials to five million (5,000,000) rials.

b) If they incite or encourage individuals to commit crimes against public morals, use drugs or narcotics, engage in suicide, sexual deviations, or violent behavior—or if they deceive or facilitate individuals in committing such acts—they will be sentenced to imprisonment for a period of 91 days to one year, or a fine ranging from five million (5,000,000) rials to twenty million (20,000,000) rials, or both.

Note: The provisions of this article and Article 14 do not apply to content prepared, produced, stored, provided, distributed, or traded for scientific purposes or any other rational benefit.

1.2.3. Law on the Protection of Children and Adolescents

Sometimes, children and adolescents may be exploited in cyberspace.[25] For instance, using children for advertisements on Instagram or other platforms is a form of exploitation. Additionally, there may be instances where images of a child or adolescent are published on a social network, depicting them engaging in unconventional behaviors against their will, which can cause significant psychological and social harm. Such harm can manifest as feelings of isolation, shame, mockery by others, dropping out of school, and more. This situation applies to teachers who take pictures of their students and share them on social media platforms. In such cases, the legislator has provided supportive measures in Article 3, Clause J, Article 6, and Article 32 to mitigate harm.[26] Although, it would be preferable if the legislator included guidelines for the publication of images of children and adolescents by the parties mentioned in Article 1, Clause A of the law and teachers.

Furthermore, individuals may influence the minds of children through encouragement and inducement in cyberspace, leading to a runaway child or adolescent from

---

[25] Section (T), Article 1 of the Child and Adolescent Protection Law states: "Misconduct: Any act or omission that puts the physical, psychological, moral, or social health of the child or adolescent at risk, including acts such as assault, imprisonment, sexual abuse, insult, or threats towards the child or adolescent, if the act has an element of abuse, or placing them in difficult and abnormal conditions, or failing to provide assistance to them."

[26] Section Zh, Article 3 of the Child and Adolescent Protection Law states: "Misconduct towards a child or adolescent or exploitation of them."
Paragraph A, Article 6 of the Child and Adolescent Protection Law states: "The State Welfare Organization is obligated, using social workers within the framework of emergency social services, in cooperation with municipalities or rural councils and the police, to identify, accept, support, house, and empower children and adolescents covered under this law, and to report the relevant cases to competent authorities."
Article 32 of the same law provides: "Social workers of the Welfare Organization, upon receiving information about a hazardous situation as defined in Article 3 of this law, shall conduct investigations and take appropriate measures through the following means: a. Summoning parents, guardians, legal custodians, or other individuals associated with the child or adolescent, and if necessary, summoning the child or adolescent alongside them. b. Visiting the residence, workplace, school, or other relevant places associated with the child or adolescent, accompanied by judicial officers if required."

home or school. In such instances, the legislator, through Article 8 of the protection law, aims to support the child or adolescent from such harm.[27]

According to Article 19, anyone who discloses the identity or secrets of a child victim or a child in a risky situation or explains details of a crime committed by or against a child through the mass media or by distributing, duplicating, or displaying films, photos, etc., in a way that causes others to act in defiance of the law, disseminate the crime, educate others on committing the crime, or bring harm to the child, the adolescent, or their family, shall be sentenced to imprisonment under the sixth degree of the Islamic Penal Code.

Note: If the distribution, display, or filming of photos and videos is limited and intended for scientific purposes or in the best interest of the child, or if other cases are determined by the court to be excluded from this provision, they will not be subject to the application of this article.

2. Reactive Criminal Policy

In terms of formal support for victims, a branch of criminal procedural law—often referred to as "Circuit Criminal Procedure victim"—has emerged. Through its interaction with substantive criminal law, this approach identifies the special protections and rights that vulnerable victims require during legal proceedings and obliges all participants in the criminal process to observe them.[28]

2.1. Universal Jurisdiction in Cyber Child Pornography

With the expansion of new technologies, traditional pornography, which was once manifest in physical objects, has now entered cyberspace, and its spread has accelerated dramatically. Pornographers have leveraged all advancements to produce and distribute pornography, using technologies such as lithography, photography, satellite television, various forms of video, and the internet, prompting governments to take action against the destructive impact of such content on society.[29] Cyber pornography or cyberchild pornography refers to behaviors that are definitively and

---

[27] Article 8 of the Child and Adolescent Protection Law states: "Anyone who, through threats, encouragement, or persuasion, causes a child or adolescent to run away from home or school or to drop out of school, or deceives them for such purposes, or facilitates or enables such acts, shall, in case of a resulting escape or dropout, be sentenced to one or more punishments under Grade 6 of the Islamic Penal Code. If the escape or dropout does not occur, the offender shall first receive a warning from the Special Juvenile Police, and in case of repetition, shall be subjected to the aforementioned punishments."

[28] ABADI, Abbasmansour, MOEZ, Hadi: Principles and Alternative Effects of Juvenile Criminal Proceedings. *J. Islamic L. Resch*. 22, 2021, 121.

[29] JAVAHERI, Gholamreza, ESMAEELI, Mahdi, HAJITABAR FIRUZ JAYI, H.: Cyber Pornography: from Theoretical Viewpoint to Models of Criminal Action. *Journal of Criminal Law Research* 8 (30), 2020, 191. https://doi.org/10.22054/jclr.2020.42595.1923.

conditionally blameworthy, intended for commercial purposes or to corrupt, and carried out through computer or telecommunications systems.[30]

Iran joined the 1989 Convention on the Rights of the Child in 1993 with a reservation and later acceded to its Optional Protocol. Article 2(b) of the 2007 Law on Iran's Accession to the Optional Protocol defines child pornography as any depiction of a child engaged in explicit sexual activities, or any portrayal of a child's sexual organs for primarily sexual purposes.

Additionally, Article 1(d) of the 2019 Law on the Protection of Children and Adolescents defines child pornography as works showing the sexual attractiveness of a child, including nudity and sexual acts. Articles 10 and 11 of this law impose fifth-degree imprisonment for exploiting children in pornography or coercing them to participate. If trafficking is involved, the penalty increases to fourth-degree imprisonment.

According to section (t) of Article 664 of the Code of Criminal Procedure, in cases of "cybercrimes involving the exploitation of persons under eighteen, whether the victim or perpetrator is Iranian or non-Iranian and the perpetrator is found in Iran", Iranian courts have jurisdiction. In fact, the legislator has placed cybercrimes involving the exploitation of persons under eighteen within the scope of universal jurisdiction[31], allowing the prosecution and punishment of the perpetrator even if they are not Iranian or the crime was committed outside the country, but the perpetrator is found in Iran.[32]

This provision is an example of universal jurisdiction, whereby, regardless of the specific person or country against whom the crime was committed, all countries have jurisdiction over the crime. So far, in cyberspace, only certain crimes, such as child pornography, have been categorized as international crimes subject to universal jurisdiction. Therefore, it appears that other cybercrimes, such as unauthorized access (hacking), virus spreading, and electronic money laundering, while recognized as international crimes by many countries, are not covered by this jurisdiction. The legislator has specifically mentioned crimes related to child pornography and its associated activities in this provision. It also seems that, based on international documents in this field, the term "exploitation of persons under eighteen" refers to "sexual exploitation" and its derivatives.[33] Although this

---

30 GHAFARI CHERATI, Saleh, HADI TABAR, Esmaeil, QUDSI, Seyed. Ebrahim: Computerized pornography: From causality to prevention. *Quarterly Journal of Islamic Human Rights Studies* (15), 2018, 108. https://dor.isc.ac/dor/20.1001.1.23225637.1397.7.2.5.6.

31 At the national regulatory level, Article 9 of the Islamic Penal Code (2013) states: "A perpetrator who, under a specific law or international treaties and regulations, is subject to prosecution for crimes in any country shall, if found in Iran, be prosecuted and punished in accordance with the penal laws of the Islamic Republic of Iran."

32 NOURIAN, Alireza: *Criminal procedure of cyber and telecommunication crimes*. 1st ed. Tehran, Mizan Legal Foundation, 2017, 83.

33 KHALEQI, Ali: *Notes on criminal procedure law*. 5th ed. Tehran, Shahre Danesh Legal Studies and Research Institute, 2015, 55.

provision is very broad, it can be deterrent and holds significance of international criminal policy.

In any case, defining the legal conditions for the application of universal jurisdiction will lead to the proper interpretation and application of this jurisdiction by legislators and judicial authorities, including those of the Islamic Republic of Iran, in relation to Article 9 of the Islamic Penal Code and Article 664(t) of the Code of Criminal Procedure regarding child pornography. It is suggested that the legislator include a specific provision in the bill of penal sanctions, currently under review, to address child pornography in the chapter on crimes against public morals and decency. Until then, an immediate action could be for the legislator to amend the 2019 Law on the Protection of Children and Adolescents to include provisions on universal jurisdiction, particularly in cases where the material element of child pornography occurred outside of Iran or where the victim or perpetrator is non-Iranian.

2.2. Establishment of Specialized Prosecution Units for Cybercrime Cases

Considering the unique characteristics and distinctions of crimes in virtual networks, it becomes understandable that a differentiated approach to such crimes, as compared to those committed in the real world, is needed. A brief examination of the features of cybercrimes leads to the realization that crime commission models in this space significantly differ from traditional crime models.[34]

Specializing in prosecution units and courts and training judges as experts in this field can be a turning point in supporting victims of cybercrimes by ensuring proper access to competent courts. In this regard, the Cybercrime Police or the FATA (Cyber Information Exchange Police), which operates in this specialized field, can be considered a positive development in victim support.[35]

The emergence of specialized judicial bodies will transform the judicial system and introduce new issues for the judiciary. Article 30 of the Cybercrimes Law and its note obligates the judiciary to establish specialized prosecution units, public and revolutionary courts, military courts, and appellate courts, with judges who have adequate knowledge of computer-related issues, to handle cybercrimes. Article 666 of the Armed Forces Procedural Law and Electronic Judiciary also reiterates this obligation for the judiciary.[36]

---

[34] JAVAN JAFFARI, Abdolreza: Cyber Crime and Criminal Law Approach to the Differential (Looking at the Part Computer Crime Law Islamic). *Monetary & Financial Economics* 17 (34), 2011, p. 175. https://doi.org/10.22067/pm.v17i34.27358.

[35] POURGHAHRAMANI, Babak: Comparative Study of Strategies to Protect Victims of Computer Crimes in the Criminal Law of Iran and International Documents with Emphasis on the Budapest Convention. *Criminal Law Research* 8 (1), 2017, 31. https://doi.org/10.22124/jol.2017.2286.

[36] KERAMATI MOEZ, Hadi, MIRKHALILI, Seyedmahmood: Iran's Legislative Criminal Policy Approach and International Documents to Support Vulnerable Children on Social Media. *Police International Studies* 11 (41), 2020, 115. SID. https://sid.ir/paper/392158/en.

Therefore, judges in these courts must, in addition to their legal and judicial expertise, be familiar with cyber law and virtual space regulations. It seems that judges should not only have legal qualifications but also education in computer science and virtual space, or alternatively, they should have participated in in-service training programs to acquire this knowledge.

Given the importance of judicial support for child victims in cyberspace, one of the supportive measures for children and deterrents against cybercrime targeting children could be to assign a specific judge for cybercrimes involving children. Specializing in cyber-related issues and having sufficient knowledge about children and their victimization can both bring justice closer to the decisions made and ensure better management of child victimization to minimize harm. Additionally, it can allow for actions that provide a stronger deterrent effect against the perpetrator.

2.3. Formal Protection of Child Victims in Terms of Jurisdiction

Regarding the jurisdiction of lawmakers, in some cases, the status of the victim has led Iranian courts to be deemed competent for handling cases. According to paragraph (p) of Article 664 of the Code of Criminal Procedure: "If a crime is committed by an Iranian or a foreigner outside Iran against computer systems and telecommunications systems or websites used or controlled by the three branches of government or leadership institutions or official government representations or any organization or institution providing public services, or against websites with top-level domains related to Iran, the case falls under Iranian jurisdiction."

It seems that this clause, which some interpret as supportive or "real" jurisdiction, aims to provide formal protection for victims of cybercrimes. The foundation for this right is discussed in Articles 4 and 5 of the Cybercrime Convention, though the convention makes no reference to the right of countries to apply this form of extraterritorial jurisdiction, which is worth considering.[37]

2.4. Presence of Parents in Court Sessions

According to Article 38 of the 1399 Law on the Protection of Children and Adolescents, parents, guardians, legal representatives, and the child's attorney, along with a social worker, have the right to attend court sessions and provide consultative opinions and supportive suggestions for the child and adolescent.

According to the note of this article, the court may, in addition to the provisions of Article 66 of the Criminal Procedure Code, invite representatives from NGOs authorized to work in the field of child and adolescent rights to attend the session.

Therefore, in cases where children and adolescents are victims in cyberspace and a case is filed and pursued, the child's parents have the right to attend court sessions and provide consultative opinions, as per the Criminal Procedure Code and Article 38 of the 1399 Law on the Protection of Children and Adolescents. This is in line

[37] Jalali FARAHANI, A.: *Introduction to the criminal procedure of cybercrimes*. 1st ed. Tehran, Khorsandi Publications, 2010, 285.

with the differential criminal policy for crimes against children, especially in cases where such crimes occur in cyberspace and might lead to a reputational crisis for the child, making the presence of the parents in the court session essential.

2.5. Case Studies of Practical Challenges

To better understand the practical application of Iran's legislative framework, it is helpful to examine representative case studies that reflect common patterns of child victimization in cyberspace.

- Case Study 1: Online Coercion via Messaging Platforms

In 2022, a 13-year-old girl from Shiraz began communicating with a man through a popular encrypted messaging app. Over several weeks, the man, pretending to be a teenager, manipulated her into sharing personal photos. When she attempted to end the conversation, he threatened to release the images unless she continued. The girl eventually confided in a school counselor, and her family filed a complaint.

While Iranian law criminalizes such exploitation under the 2019 Law on the Protection of Children and Adolescents, the investigation faced procedural delays due to jurisdictional ambiguities and insufficient digital forensic expertise at the provincial level. Although a specialized cybercrime unit existed, the lack of prompt coordination with the local judiciary hindered swift action. This case highlights a growing gap between the scope of legal protection and the effectiveness of its enforcement, particularly in areas outside major urban centers.

- Case Study 2: Exploitation Through Social Media Content

A widely followed Instagram page in Iran featured a six-year-old boy reviewing children's toys and food products. Behind the scenes, the child was reportedly pressured into recording hours of video content and denied privacy, rest, and educational time. The page generated substantial commercial income, managed entirely by the parents. Following growing public criticism, legal attention was drawn to the situation.

Clause 3(A) of the Law on the Protection of Children and Adolescents prohibits the exploitation of minors for personal or commercial gain, including in media. However, due to the lack of a clear legal definition for "digital exploitation", authorities were unable to pursue formal action. This case underscores the challenge of applying existing child protection laws to non-traditional but harmful digital behaviors, especially those perceived as "entertainment" or "parenting choices" in a rapidly evolving cyberspace.

2.6. Implementation Challenges and Comparative Reflections

Despite numerous legal reforms and the formation of cybercrime units with specialized functions, Iran's laws dealing with child victimization in cyberspace remain patchy and reactive in their implementation. On paper, the legislative provisions give protection. Some of these laws are the 2019 Law on the Protection of Children and Adolescents and the Computer Crimes Law. Yet in reality, enforcement is widely absent. Among other things, Article 30 of the Cybercrime Law

has required the establishment of certain courts, but the lack of specialized training among local prosecutors and judges means they generally do not work, while most of these courts continue to be inoperative or under-resourced outside of some major urban areas.

Justice is further denied to victims by procedural complexity, social stigma, and under-resourced support services. Families may be reluctant to pursue reporting due to reputational risks, issues of confidentiality, or an absence of trauma-informed procedures in police stations and courts. Also, Iranian criminal policy is very much punishment-oriented, and preventive tools are lacking-development or emphasis, including digital education, public reporting frameworks, and civil society engagement. A comparative overview of other Islamic countries highlights both shared principles and significant policy differences. Malaysian law incorporates a set of Islamic principles with modern criminal regulation. The Child Act 2001 criminalizes sexual abuse and exploitation online; the Communications and Multimedia Act 1998 holds platforms accountable for such concerns. Prevention-oriented approaches are emphasized, which include digital education in schools and human-centered hotlines for reporting abuse. In contrast to Iran, where formal complaints have to follow the judicial path, which provides little to no guarantee of anonymity or psychological support, these reporting mechanisms are considered to be child-friendly and technologically accessible.[38]

Indonesia combines Islamic cultural values with broader child rights frameworks. Its Electronic Information and Transactions Law (ITE) criminalizes child pornography and grooming, and its implementation involves awareness campaigns throughout the country. Indonesia cooperates with UNICEF and NGOs in the training of the police and school personnel, an area that still lacks in Iran with regard to coordinated, nationwide preventive infrastructures.[39]

Saudi Arabia, on the other hand, adopts a heavily punitive, Sharia-based approach. The Anti-Cybercrime Law strictly criminalizes online child exploitation with harsh penalties, but its system lacks comprehensive preventive or rehabilitative frameworks. Iran's system is similarly punitive, but unlike Saudi Arabia, Iran incorporates some statutory victim protection provisions. However, both countries face criticism for limited transparency and minimal involvement of civil society in child protection.[40]

---

[38] ISLAM, Md Zahidul, ZULHUDA, Sonny, MOHD BADROL AFANDI, Nor Hafizah, SHAFY, Mohamed Affan: Ensuring safe cyberspace for children: An analysis of the legal implications of social media usage in Malaysia and Singapore. *IIUMLJ* Vol. 28, 2020, 395. http://dx.doi.org/10.31436/iiumlj.v28i(S1).591

[39] SHOLIHAH, Hani, NURHAYATI, Sri: Child protection in the digital age through education in the Islamic educational environment. *JIE (Journal of Islamic Education*) Vol. 9, No. 1, 2024, 210, 218. https://doi.org/10.52615/jie.v9i1.353

[40] MIAN, Tariq Saeed, & ALATAWI, Eman M.: Investigating how parental perceptions of cybersecurity influence children's safety in the cyber world: A case study of Saudi Arabia. *Intelligent Information Management* Vol. 15, No. 5, 2023, p. 360. https://doi.org/10.4236/iim.2023.155017

Turkey offers a hybrid model. Though culturally rooted in Islam, it maintains a secular legal system that closely follows European models. The Turkish Penal Code and Child Protection Law are complemented by active engagement with the Budapest Convention on Cybercrime, allowing cross-border cooperation. Turkey also supports child victims through specialized cybercrime units, trained judges, and school-based education programs.[41] In contrast, Iran is not a signatory to the Budapest Convention and lacks real-time cooperation mechanisms with global tech companies or foreign law enforcement bodies.

Overall, Iran's criminal policy is still mostly reactive and punitive, with inadequate preventive instruments, poor institutional coordination, and a lack of international integration, despite legislative advancements, particularly the 2019 Child Protection Law and the Computer Crimes Law. Iran might create a more effective and balanced strategy to combat child victimization in internet by taking inspiration from Saudi Arabia's stringent deterrents, Indonesia's NGO collaborations, Malaysia's educational outreach, and Turkey's judicial expertise.

Conclusion

In the Islamic Penal Code, criminal protection of moral security is provided in several provisions, such as Article 640. The Cybercrime Law, in Article 14, criminalizes the production, transmission, distribution, or transaction of obscene and immoral data, as well as storing or retaining such data. However, Note 4 of Article 742 of this law limits "obscene content" to the display of nudity of men and women, while neglecting individuals who are intersex or gender non-conforming. The fact is that many obscene images and videos involve nudity of individuals who, based on a literal or literary interpretation of the law, are neither considered men nor women. The severity of child pornography and the taboo around exposing such individuals may actually be even more perverse, and the import of obscene data containing nudity of such individuals into the country may be considerable. The legislator has overlooked this point that humanity encompasses both men and women, which has so far been ignored in critiques by legal scholars of the Cybercrime Law, and the author of this article draws attention to this oversight.

Imposing financial penalties on cybercriminals involved in immoral activities is not very appropriate. These criminals are typically affluent and involved in the highly profitable trade of distributing and selling obscene data messages. Financial penalties lack deterrence and fail to reform or rehabilitate these criminals. They do not alter the criminal's calculation of profit and loss, especially in a crime where the only truly effective strategy for prevention and reoccurrence is the moral education of the criminal. Furthermore, the punitive approach to these dangerous criminals requires the legislator to set punishments such as exile or flogging instead of imprisonment to have a greater deterrent effect and more proportional retribution.

---

[41] KAPLAN, Yasar: Cybercrime and Child Protection in Turkey: Challenges and Progress. *Turkish Journal of Criminology and Legal Policy* Vol. 6, No. 3, 2022, 220, 221.

Regarding the substantive aspect of criminal policy in preventing child victimization, protective criminalization must first be mentioned. Criminalization in relation to children is essential due to their vulnerability, and society's acceptance of protecting the child manifests in the formulation of differential protective policies in criminal law tailored for children.

Protective sentencing is another form of legal protection. Severe criminal sanctions are an effective mechanism for addressing crimes against children. The escalation of penalties for those who commit crimes against children is the first manifestation of this protection. The differential criminal policy to combat crimes against children necessitates imposing severe punishments aimed at both general deterrence (before the crime occurs) and specific deterrence (after the crime occurs), which will dissuade the perpetrator from committing further crimes. A denial of supportive punishment through escalation is particularly applicable when a serious crime against a child result in significant physical and emotional harm.

The criminal policy of Iranian lawmakers in the case of crimes committed against children is punitive, with an emphasis on escalating punishments. For instance, the escalation of penalties is reflected in Note 2 of Article 11 of the 2019 Child and Adolescent Protection Law, and Articles 15 and 21 of the same law.

While Iran has made commendable legislative advancements—particularly through the 2019 Child and Adolescent Protection Law and the Computer Crimes Law—the implementation of these provisions remains inconsistent and reactive. Specialized cybercrime units and courts exist largely in theory, as many local prosecutors and judges lack adequate training, and support services are sparse outside major urban areas. This enforcement gap is compounded by procedural obstacles, social stigma, and the absence of trauma-informed systems. A comparative look at other Islamic countries highlights alternative approaches: Malaysia emphasizes prevention through education and user-friendly reporting systems; Indonesia engages civil society and NGOs in awareness campaigns; Saudi Arabia takes a punitive route but shares Iran's shortfalls in prevention; and Turkey integrates European models through judicial training and international cooperation under the Budapest Convention. Iran could benefit from adopting a more balanced and proactive criminal policy—blending strict deterrents with digital education, civil engagement, and institutional coordination—to more effectively protect children in cyberspace.

The imposition of financial penalties is also a form of protection. Financial penalties, especially in relation to crimes that are financially lucrative, such as economic or sexual exploitation, play an important role in dissuading perpetrators. However, in Iranian laws, the provision of criminal financial penalties is not designed to deter offenders from committing crimes against children. Additionally, continuous legal protection is seen in the form of non-criminal sanctions such as administrative, disciplinary, and civil penalties, alongside criminal penalties. Some of these continuous penalties are specifically provided in Iranian criminal law to control crimes against children.

Based on the general findings from the descriptive and analytical results, it appears that the group of child victims in cyberspace consists of those who, due to

limited parental supervision and increased free time, particularly with the growth of cyberspace and social networks, show a strong inclination to engage with this space. Since they lack the necessary literacy, experience, and knowledge to navigate this space and social relationships, they gradually trust individuals active in the space and, over time, fall victim to various forms of abuse within this environment.

References

[1] ABADI, Abbasmansour, MOEZ, Hadi: Principles and Alternative Effects of Juvenile Criminal Proceedings. *J. Islamic L. Resch*. 22, 2021, 121.

[2] EHSSANPOUR, Seyed Reza, GHADAMI AZIZABAD, Mosayeb: The Components of the Optimal Preventive Criminal Policy Toward Sexual Victimization of Children in Cyberspace. *The Quarterly Journal of Judicial Law Views* Vol. 29, No (105), 2024, 5–8. https://dor.isc.ac/dor/20.1001.1.22520007.1403.29. 105.1.8

[3] GHAFARI CHERATI, Saleh, HADI TABAR, Esmaeil, QUDSI, Seyed Ebrahim: Computerized pornography: From causality to prevention. *Quarterly Journal of Islamic Human Rights Studies* (15), 2018. https://dor.isc.ac/dor/20.1001.1.23225637.1397.7.2.5.6

[4] HAJIDEHABADI, Ahmad, & SALIMI, Ehsan: Principles of Criminalization in Cyberspace (A Critical Approach to the Computer Crime Act*)*. *Majlis and Rahbord* 21 (80), 2015, 61–88.

[5] ISLAM, Md Zahidul, ZULHUDA, Sonny, MOHD BADROL AFANDI, Nor Hafizah, SHAFY, Mohamed Affan: Ensuring safe cyberspace for children: An analysis of the legal implications of social media usage in Malaysia and Singapore. *IIUMLJ* Vol. 28, 2020, 395. http://dx.doi.org/10.31436/iiumlj.v28i(S1).591

[6] JALALI FARAHANI, A.: *Introduction to the criminal procedure of cybercrimes*. 1st ed., Tehran: Khorsandi Publications, 2010.

[7] JAVAHERI, Gholamreza, ESMAEELI, Mahdi, HAJITABAR FIRUZ JAYI, H.: Cyber Pornography: from Theoretical Viewpoint to Models of Criminal Action. *Journal of Criminal Law Research* 8 (30), 2020, pp. 173–200. https://doi.org/10.22054/jclr.2020.42595.1923

[8] JAVAN JAFFARI, Abdolreza: Cyber Crime and Criminal Law Approach to the Differential (Looking at the Part Computer Crime Law Islamic). *Monetary & Financial Economics* 17 (34), 2011. https://doi.org/10.22067/pm.v17i34.27358

[9] KAPLAN, Yasar: Cybercrime and Child Protection in Turkey: Challenges and Progress. *Turkish Journal of Criminology and Legal Policy* Vol. 6, No (3), 2022, 220–221.

[10] KERAMATI MOAZ, Hadi: *Victimology of children in virtual networks*. 1st ed., Tehran: Dadgostar Publications, 2020.

[11] KERAMATI MOAZ, Hadi, & ZAND RAD MAJID, P.: *Iran's criminal policy regarding victimization of women and children in cyberspace*. Andisheh Vakil, 3rd Year, (6), 2024. https://doi.org/10.22034/jccj.2024.462904.1581

[12] KERAMATI MOEZ, Hadi, & MIRKHALILI, Seyedmahmood: Iran's Legislative Criminal Policy Approach and International Documents to Support Vulnerable Children on Social Media. *Police International Studies* 11 (41), 2020, 102–125. https://sid.ir/paper/392158/en

[13] KHALEQI, Ali: *Notes on criminal procedure law*. 5th ed. Tehran: Shahre Danesh Legal Studies and Research Institute, 2015.

[14] LAZERGES, Christian: *Introduction to criminal policy*. (A. H. Najafi Abrand Abadi, Trans.) 8th ed. Tehran: Mizan Legal Foundation, 2020.

[15] LIVINGSTONE, Sonia, ÓLAFSSON, Kjartan, & POTHONG, Krittiya: Digital play on children's terms: A child rights approach to designing digital experiences. *New Media & Society* Vol. 27, No. (3), 2025, 1470. https://doi.org/10.1177/14614448231196579

[16] MIAN, Tariq Saeed, & ALATAWI, Eman M.: Investigating how parental perceptions of cybersecurity influence children's safety in the cyber world: A case study of Saudi Arabia. *Intelligent Information Management* Vol. 15, No. 5, 2023, p. 360. https://doi.org/10.4236/iim.2023.155017

[17] MOHSENI, Farid: *Criminological theories*. 1st ed. Tehran: Judiciary Press and Publications Center, 2018.

[18] NADERI, Hamaseh: The Cyberspace Harms for Children. *International Journal of Advanced Research in Humanities and Law* Vol. 1, No. 2, 2024, 62–63. https://doi.org/10.63053/ijrel.12

[19] NOORZAD, Mojtaba: *Economic crimes in Iranian criminal law*. 1st ed. Tehran, Jangal Publications, 2010.

[20] NOURIAN, Alireza: *Criminal procedure of cyber and telecommunication crimes*. 1st ed., Tehran: Mizan Legal Foundation, 2017.

[21] POURGHAHRAMANI, Babak: Comparative Study of Strategies to Protect Victims of Computer Crimes in the Criminal Law of Iran and International Documents with Emphasis on the Budapest Convention. *Criminal Law Research* 8 (1), 2017, pp. 1–36. https://doi.org/10.22124/jol.2017.2286

[22] RAHIMI, Hamid: *Victim-centered typology of child and adolescent protection in Iranian criminal law*. Criminal Justice Newsletter, Criminal Law and Criminology Group, Faculty of Law, Shahid Beheshti University, 2 (4), 2019.

[23] ROUHANI MOGHA, Mohammad, MOUSAVI, Seyed Javad, & AGHAEI BAJESTANI, Mohammad: The process of child victimization in cyberspace with emphasis on economic factors. *Strategic Studies of Jurisprudence and Law* Vol. 3, No. 4, 2022, 37–53. https://dor.isc.ac/dor/20.1001.1.26767163.1400.3.4.3.8

[24] SHOLIHAH, Hani, NURHAYATI, Sri: Child protection in the digital age through education in the Islamic educational environment. *JIE (Journal of Islamic Education*) Vol. 9, No. 1, 2024, 210–218. https://doi.org/10.52615/jie.v9i1.353

[25] WHITTLE, Helen, HAMILTON-GIACHRITSIS, Catherine, BEECH, Anthony: A review of online grooming: Characteristics and methods. *Aggression and Violent Behavior* Vol. 18, No. 1, 2013, 62–70. https://doi.org/10.1016/j.avb.2012.09.003

[26] ZEYNALI, Amirhamzeh: *Globalization of criminal law (In the realm of protecting children against victimization)*. 1st ed., Tehran: Mizan Legal Foundation, 2015.