Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

S Protecting children in cyberspace: Uzbekistan's legislative adaptation to international standards

Farrukh NURULLAEV [1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received September 2025
Received in revised form
5 September 2025
Accepted 10 October 2025
Available online
25 October 2025

Keywords:
cybercrime,
child protection,
international law,
digital environment,
transnational cooperation,
Uzbekistan legislation.

ABSTRACT

This article analyzes the implementation of international legal norms into Uzbekistan's national legislation to combat cybercrimes against children. The study examines constitutional principles, international treaties, and specialized normative acts aimed at protecting children in the digital environment. Laws on guarantees of child rights, protection from harmful information, and protection from all forms of violence are critically evaluated. Research demonstrates that although Uzbekistan has created legislation aligned with international standards, serious deficiencies exist in combating transnational cybercrimes, preserving digital evidence, and international cooperation. Current norms prove inadequate for addressing modern cybercrimes such as cyber-grooming, cyberbullying, and exploitation through live streaming. The article presents practical recommendations for improving legislation, international cooperation mechanisms, digital forensic methods, and enhancing institutional capacity.

DOI: https://doi.org/10.47689/2181-1415-vol6-iss10/S-pp143-160

Kibermakonda bolalarni himoya qilish: O‘zbekiston qonunchiligini xalqaro standartlarga moslashishi

Kalit so‘zlar:
kiberjinoyatchilik,
bolalarni himoya qilish,
xalqaro huquq,
raqamli muhit,

ANNOTATSIYA

Ushbu maqolada O‘zbekistonning bolalarga nisbatan sodir etiladigan kiberjinoyatchilikka qarshi kurashda xalqaro-huquqiy me’yorlarni milliy qonunchilikka implementatsiya qilish masalalari tahlil etiladi. Tadqiqotda konstitutsiyaviy

[1] Lecturer, Department of International Law and Human Rights, Tashkent State University of Law.
E-mail: farruxdior1135@gmail.com

transchegaraviy hamkorlik.

tamoyillar, xalqaro shartnomalar va raqamli muhitda bolalarni himoya qilishga qaratilgan maxsus normativ-huquqiy hujjatlar o‘rganiladi. Bola huquqlarining kafolatlari, Bolalarni zararli axborotdan himoya qilish va Bolalarni zo‘ravonlikning barcha shakllaridan himoya qilish to‘g‘risidagi qonunlar tanqidiy baholanadi. Tadqiqot shuni ko‘rsatadiki, O‘zbekiston xalqaro standartlarga mos qonunchilik bazasini yaratgan bo‘lsa-da, transchegaraviy kiberjinoyatlarga qarshi kurashish, raqamli dalillarni saqlash va xalqaro hamkorlikda jiddiy kamchiliklar mavjud. Mavjud normalar kibergruming, kiberbulling, jonli efir orqali ekspluatatsiya kabi zamonaviy kiberjinoyatlarga yetarli javob bermaydi. Maqolada qonunchilikni takomillashtirish, xalqaro hamkorlik mexanizmlari, raqamli-kriminalistik usullar va institutsional salohiyatni oshirish bo‘yicha amaliy takliflar berilgan.

Защита детей в киберпространстве: адаптация законодательства Узбекистана к международным стандартам

Ключевые слова: киберпреступность, защита детей, международное право, цифровая среда, трансграничное сотрудничество.

АННОТАЦИЯ

В данной статье анализируются вопросы имплементации международно-правовых норм в национальное законодательство Узбекистана для борьбы с киберпреступлениями против детей. Исследование рассматривает конституционные принципы, международные договоры и специальные нормативно-правовые акты, направленные на защиту детей в цифровой среде. Критически оцениваются законы о гарантиях прав ребенка, защите детей от вредной информации и защите от всех форм насилия. Исследование показывает, что хотя Узбекистан создал законодательную базу, соответствующую международным стандартам, существуют серьезные недостатки в борьбе с трансграничными киберпреступлениями, сохранении цифровых доказательств и международном сотрудничестве. Действующие нормы недостаточны для противодействия современным киберпреступлениям, таким как кибергруминг, кибербуллинг и эксплуатация через прямые трансляции. Статья представляет практические рекомендации по совершенствованию законодательства, механизмов международного сотрудничества, цифровых криминалистических методов и повышению институционального потенциала.

INTRODUCTION

The Republic of Uzbekistan, exercising its state sovereignty, operates as an independent subject of international relations and constitutes an equal member of the international community, including the United Nations Organization. Within the

framework of international obligations undertaken by the country, particularly those arising from the UN Charter, Uzbekistan contributes to maintaining international peace and protecting human rights at a universal level.

Contemporary global digitalization has fundamentally transformed the landscape of threats facing children. The exponential growth of internet connectivity, proliferation of social media platforms, and emergence of sophisticated communication technologies have created unprecedented opportunities for transnational criminal networks to exploit vulnerable populations [7]. Children, who increasingly inhabit digital spaces for education, socialization, and entertainment, face multifaceted cyber threats, including online grooming, cyberbullying, sextortion, and exposure to child sexual abuse material (CSAM).

International legal frameworks have evolved to address these emerging challenges. The Council of Europe Convention on Cybercrime (Budapest Convention, 2001) established foundational principles for international cooperation in combating cyber crimes, while its Second Additional Protocol (2022) strengthened provisions specifically addressing online child sexual exploitation. Similarly, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, 2007) provides comprehensive standards for criminalizing various forms of child abuse facilitated through information and communication technologies [4].

Uzbekistan's commitment to implementing these international standards represents a critical juncture in the country's legal development. The constitutional recognition of international law as an integral component of the national legal system creates both opportunities and challenges for legislative harmonization. This research addresses a fundamental question: to what extent has Uzbekistan successfully translated its international obligations into effective domestic mechanisms for protecting children from cyber crimes?

The primary objective of this research is to conduct a comprehensive analysis of Uzbekistan's legislative framework governing cyber crimes against children through the prism of international legal standards. Specifically, this study aims to:

1. Examine the constitutional and legislative foundations for integrating international child protection norms into Uzbekistan's domestic legal system
2. Critically evaluate the adequacy of existing sectoral legislation in addressing contemporary cyber threats to children
3. Identify gaps and inconsistencies between international obligations and national implementation mechanisms
4. Assess the practical effectiveness of procedural mechanisms for investigating and prosecuting transnational cyber crimes against minors
5. Propose evidence-based recommendations for legislative reform and institutional capacity building

The central problem addressed by this research concerns the apparent disjunction between formal legal commitments and substantive enforcement capacity. While Uzbekistan has ratified key international instruments and adopted domestic legislation ostensibly aligned with international standards, critical questions remain regarding the functional adequacy of these legal frameworks in the face of rapidly evolving technological threats and the inherently transnational character of cyber crimes.

Academic discourse on implementing international cybercrime norms reveals complex challenges facing states in balancing sovereignty concerns with cooperation imperatives. Scholars have emphasized that effective combat against transnational cyber crimes requires not merely legislative approximation but fundamental transformation of investigative practices and institutional structures [3].

Research on child protection in digital environments highlights the inadequacy of traditional legal frameworks designed for physical space when applied to cyberspace. As Provalinskiy (2023) observes, recognition of children as legal subjects in cyberspace simultaneously creates new rights and exposes them to novel forms of victimization. [10] The digital environment's characteristics—anonymity, asynchronicity, permanence of digital traces, and transnational reach—fundamentally alter both the nature of crimes and appropriate regulatory responses [1].

Comparative studies of implementation practices reveal significant variance among states. Western jurisdictions have progressively developed specialized institutional frameworks, including dedicated cybercrime units within law enforcement, mandatory reporting systems for online service providers, and streamlined mutual legal assistance procedures [9]. In contrast, many post-Soviet states continue to rely on legislative instruments conceptualized during the pre-digital era, creating regulatory gaps that criminals exploit systematically.

Gulyamov and Raimberdiyev (2023) have analyzed personal data protection as an anti-corruption tool in Uzbekistan's context, highlighting broader challenges in adapting legal frameworks to digital realities. However, comprehensive analysis specifically addressing cyber crimes against children and the implementation of international standards in Uzbekistan's context remains notably absent from academic literature. This research seeks to address that lacuna through rigorous doctrinal analysis combined with functional evaluation of existing mechanisms.

Material and methods

This study employs a multifaceted methodological approach combining doctrinal legal analysis, comparative law methodology, and critical evaluation of normative frameworks. The research design integrates both theoretical examination of legal texts and functional assessment of their practical applicability to contemporary cyber threats.

Primary methodological approaches include:

Doctrinal legal analysis: Systematic examination of constitutional provisions, statutory legislation, and regulatory instruments governing child protection and

cybercrime. This involves textual interpretation, identification of normative hierarchies, and analysis of internal consistency within the legal framework.

Comparative legal methodology: Cross-jurisdictional comparison of implementation practices, drawing particularly on experiences from European Union member states, Council of Europe parties to relevant conventions, and regional neighbors with similar legal traditions. This comparative dimension illuminates alternative regulatory models and identifies best practices adaptable to Uzbekistan's context.

Critical gap analysis: Systematic identification of discrepancies between international standards (as articulated in conventions, protocols, and soft law instruments) and domestic implementation. This methodology reveals both explicit legislative gaps and implicit functional deficiencies in enforcement mechanisms.

Functional-teleological interpretation: Analysis of legislation not merely as formal texts but as instruments intended to achieve specific protective objectives. This approach assesses whether legal provisions effectively achieve their stated purposes when applied to real-world scenarios involving cyber crimes against children.

Several methodological limitations constrain this study. First, limited publicly available data on cybercrime prosecution in Uzbekistan restricts empirical analysis of enforcement practices. Second, rapid technological evolution means that legal analysis represents a snapshot of frameworks that may quickly become outdated. Third, the transnational nature of cyber crimes creates inherent challenges in evaluating national legislation's effectiveness, as success depends substantially on international cooperation mechanisms beyond Uzbekistan's unilateral control. Finally, this research focuses primarily on legislative frameworks rather than institutional capacity or resource allocation, which equally determine practical effectiveness.

Research results

Uzbekistan's legal system operates on a monistic principle regarding the relationship between international and domestic law. This foundational approach finds expression in Article 15 of the Constitution of the Republic of Uzbekistan and Article 3 of the Law "On International Treaties" (February 6, 2019). According to these provisions, ratified international treaties and universally recognized principles and norms of international law constitute an integral component of the national legal system.

This constitutional framework mandates systematic harmonization of national legislation with international legal standards. Consequently, law enforcement practice, including activities of criminal justice organs, must be regulated based on both domestic legislation and Uzbekistan's international obligations. This proves particularly significant in criminal justice, where ensuring the rights and freedoms of individuals requires alignment of legislative foundations and practices with international standards.

Uzbekistan adheres strictly to the principle of *pacta sunt servanda* – conscientious observance of international treaties – in its foreign policy [2]. This position manifests clearly in international cooperation against transnational crime, including cyber crimes.

The country participates fully in multilateral and bilateral treaties governing mutual legal assistance in criminal matters, adopted under UN auspices and within regional structures.

Critically, Uzbekistan's engagement extends beyond mere accession or ratification. The state pursues a systematic and consistent policy of implementing conceptual rules, standards, and norms articulated in international legal instruments into national legislation – genuinely integrating and harmonizing these norms within the existing legal system [11]. This ensures proportionate development of national legislation alongside international standards.

Analysis of international cooperation's legal foundations reveals increasing importance of not only interstate treaties but also constituent documents of international organizations and "soft law" sources developed within their frameworks, particularly model laws and recommendatory instruments. Though advisory in character, such documents serve as templates for states in creating effective legal mechanisms against transnational crime, including cyber space offenses, positively influencing national legislative improvement.

Within Uzbekistan's system of international obligations regarding child rights protection, the UN Convention on the Rights of the Child (1989) occupies a central position. Uzbekistan ratified this fundamental international instrument on December 9, 1992, thereby assuming its rules and principles as binding obligations.

Subsequently commenced a consistent process of implementing Convention norms into the national legal system. This process involved not merely adopting specialized legislative instruments but introducing relevant amendments and additions to existing legislation regulating family, education, healthcare, social protection, and criminal justice spheres. This created foundations for harmonizing national legislation governing children's protection, including their cyber space security, with international standards.

The implementation framework operates through multiple legislative levels. At the constitutional apex, the revised Constitution establishes state obligations regarding child protection. Article 33 enshrines the state's positive obligation to create conditions for utilizing the global information network (Internet), thereby ensuring children's right to access information. Article 78 serves as a balancing and limiting norm, establishing the state's priority responsibility to protect children's rights, freedoms, and legitimate interests, and to create optimal conditions for their comprehensive physical, intellectual, and cultural development. Precisely, this constitutional complex serves as a foundation for legislation and enforcement practice directed toward protecting children from harmful information in cyberspace.

Uzbekistan has constructed a complex, multi-stage legal system directed toward protecting children from information harmful to their health and development. The Law "On Guarantees of Child Rights" (No. 139-ORQ, January 7, 2008) constitutes the foundational special instrument regulating relationships in this sphere.

This Law simultaneously declares children's right to seek, receive, and disseminate age-appropriate information while acknowledging this right's non-absolute nature. The legislation guarantees children's right to protection from information potentially harmful to their moral and spiritual development and health. Toward this end, the Law establishes strict, imperative prohibitions on preparing and distributing information products that: promote pornography, cruelty, and violence; denigrate human dignity; or cultivate children's propensity toward unlawful conduct. This demonstrates a legal approach directed toward ensuring an equitable balance between "right to receive information" and "protection from harmful information" within national legislation.

Protection mechanisms receive further specification in the Law "On Protection of Children from Information Harmful to Their Health" (No. 444-ORQ, September 8, 2017). Analysis reveals that this Law reflects a comprehensive preventive approach directed toward preventing cyber threats. The document provides a broad definition of "information product," encompassing not only mass media and printed materials but also information placed on telecommunication networks, particularly the global Internet information network, computer games, and other audiovisual products. This enables coverage of virtually all content types in cyberspace.

Article 16 of the Law clearly delineates categories of information products whose distribution among children is absolutely prohibited. These include information that incites children toward suicide; encourages drug use, prostitution, or other antisocial behavior; promotes violence and cruelty; denies family values; or possesses pornographic character. These norms serve to eliminate foundations for crimes committed against children in cyberspace, including sexual exploitation, incitement to violence, and cyberbullying.

As a protective mechanism, the Law implements age classification of information products (through "0+", "7+", "12+", "16+", "18+" designations). This obligation falls upon information product producers and distributors. This system functions as a crucial filter enabling parents and guardians to make informed content selections for their children.

A multi-sectoral institutional system ensures law enforcement. The Information and Mass Communications Agency under the Presidential Administration of Uzbekistan, as the specially authorized state body, conducts monitoring, accredits experts, and issues directives for eliminating violations. Additionally, the process involves multiple entities, including the Cabinet of Ministers, educational institutions, healthcare facilities, the Youth Affairs Agency, and citizens' self-governance bodies.

However, critical analysis through the international cybercrime prism reveals significant limitations. First, terminology (mass media, literature, films) references traditional information sources and does not directly encompass contemporary digital tools such as social networks, messengers, online games, and streaming platforms. This creates a legal gap in regulating primary platforms where cyber crimes—cyberbullying, grooming, sexting—occur.

Second, the Law's protective norms possess a general character and do not account for cyber space violence's specific features. For instance, no explicit mechanisms exist for combating theft of children's personal data and its use for blackmail, creation of fake accounts in children's names, or unauthorized distribution of intimate photographs [5].

Third, protective mechanisms established by the Law operate primarily within national jurisdiction. Cyber crimes, however, frequently possess transnational characteristics—perpetrators in one state, victims in another, and servers in a third. Under such circumstances, local guardianship authorities' powers and capabilities prove sharply limited. The Law does not reflect procedures for such transnational situations or international cooperation matters.

The Law "On Protection of Children from Information Harmful to Their Health" (No. 444-ORQ) creates important preventive foundations for sanitizing children's information space and preventing harmful content distribution. However, its content orientation means it cannot serve as a sufficiently robust and specialized instrument for directly combating active crimes committed against children in cyberspace. Its effectiveness remains limited without deep integration with criminal procedural legislation and international legal assistance mechanisms.

The Law's primary focus targets content regulation rather than combating criminal conduct. Its main tools—age marking and expert examination—apply to already created and distributed "information products." The authorized body's primary enforcement measure involves issuing directives for eliminating violations. This approach proves ineffective against active, ongoing criminal conduct such as cyber-grooming, cyberbullying, or live-streaming child exploitation. These crimes constitute not static "information products" but processes occurring in real time. The Law does not contemplate rapid legal mechanisms for immediately stopping such crimes, collecting evidence, and bringing perpetrators to criminal accountability.

The concept of "information product" fails to fully encompass contemporary cybercrime characteristics. The Law imposes obligations on "information product producers and/or distributors"—subjects engaged in website, film, or publishing activities. Yet crimes frequently occur through personal correspondence, closed chat groups, messengers, and voice communications on gaming platforms. In such cases, who constitutes the "producer" or "distributor"? The global social network or the perpetrator directly? The Law provides no clear answers and leaves open questions of international technological platforms' liability.

The Law remains limited to the national level and does not account for the transnational nature. Perpetrators may reside in other countries while harming children in Uzbekistan. The authorized body—the Information and Mass Communications Agency—lacks the capacity to directly apply enforcement measures against foreign individuals or platforms. The Law does not establish practical procedures for

investigating transnational crimes, demanding information expeditiously from foreign platforms or international cooperation.

When approached from the contemporary cybercrime perspective, the Law "On Guarantees and Freedom to Obtain Information" (No. 400-I, April 24, 1997) proves not merely ineffective but practically inapplicable. Its existing deficiencies manifest across several fundamental dimensions.

First, the Law is conceptually obsolete and not designed for the modern digital environment. Adopted in 1997—long before Internet popularization and social media emergence—this Law primarily establishes procedures for citizens to request information held by state bodies and organizations. Its basic mechanism—"information request"—presumes citizens initiate demands for data. This model stands opposed to today's reality of uncontrolled and unsolicited information flows, harmful content distribution, and cyber criminals' direct communications that children face. The Law regulates the right to demand information but does not contemplate the right to protection from harmful information.

Second, the Law fails to account for children as subjects requiring special protection. The document's text contains not a single special norm recognizing "child" or "minor" status or accounting for their vulnerabilities in information acquisition. The Law guarantees a single, universal right—"everyone's" right to obtain information. [8] This completely disregards the necessity of protecting children from information inappropriate to their age and psychological condition that may harm their health and development.

Third, the Law's practical mechanisms prove inapplicable to cyberspace. Norms such as judicial appeal against officials' refusal to provide information or disclosure of information sources only by court order are designed for relationships with state bodies. They offer no practical solutions against harmful content distributed by anonymous websites on foreign servers, identity-concealing cyber criminals, or global social networks.

Recent years have witnessed significant legislative activity directed toward strengthening child protection frameworks. The Presidential Decree "On Approval of the National Strategy on Human Rights" (PF-6012, June 22, 2020), the "Uzbekistan-2030" Strategy (PF-158, September 11, 2023), and related implementation measures demonstrate state commitment to preventing psychological pressure, social coercion, and violence against children while cultivating a culture of intolerance toward such conduct in society.

The Joint Resolution of the Legislative Chamber Council and Senate Council "On Implementation of UN Committee on the Rights of the Child Recommendations Regarding Uzbekistan's Fifth Periodic Report" (February 21, 2024) represents a particularly significant effort toward harmonizing national practice with international monitoring body conclusions.

Most notably, the Law "On Protection of Children from All Forms of Violence" (No. 996-ORQ, November 14, 2024) serves to ensure protection from all violence forms. Though oriented toward general protective measures, this legislation embodies several important norms accounting for digital environment threats, thereby creating a solid normative foundation for combating cyber crimes against children.

One of this legal instrument's most significant aspects appears in Article 3's definition of "violence against children," which explicitly states such violence includes acts "carried out using telecommunication networks and the global Internet information network." This norm serves as a foundation for qualifying any aggressive online conduct as violence and applying legal enforcement measures.

The Law also addresses specific forms of violence occurring in cyberspace. The definition of "harassment (bullying)" specifically notes such conduct's execution "using telecommunication networks and the global Internet information network." This constitutes a partial legal definition of cyberbullying. Additionally, the psychological violence definition encompasses conduct "arousing concern for [the child's] safety" and "causing harm to mental health," applicable to online threats and psychological pressure. Norms concerning child sexual exploitation, particularly prohibiting "involving minors as performers of pornographic actions," hold crucial significance for combating grave cyber space crimes such as child pornography and online grooming.

The Law establishes not merely definitions but response mechanisms to violent situations. According to Article 24, "announcements in mass media, in the global Internet information network, including on social networks" may serve as grounds for applying protective measures. This enables authorized bodies to respond swiftly to threats identified in the online space. Additionally, establishment of a round-the-clock free "hotline" for assisting victims (Article 25) constitutes an important tool for children suffering cyber space harm to seek timely help.

Another significant preventive norm finds expression in Article 41. According to this provision, persons who committed grave crimes against children, including sexual violence and distribution of pornographic materials, are prohibited for life from engaging in education, upbringing, and other activities involving direct work with children, regardless of conviction expungement or removal. Maintaining a special registry of such persons constitutes a strict measure directed toward preventing their re-entry into child-related fields.

Parental and educational institution responsibilities are also clearly established. Parents (persons substituting for them) must take measures to protect their children from information "possessing pornographic character, containing signs of cruelty and violence." Educational institutions must implement programs and mechanisms for preventing bullying.

While acknowledging the Law on Protection from All Forms of Violence's merits, critical analysis through an international cybercrime prism reveals certain vulnerabilities

that potentially limit its effectiveness. Specifically, the Law's legal enforcement measures operate primarily within national jurisdiction and do not embody explicit mechanisms for combating transnational crimes.

Protection orders issued by internal affairs bodies, behavior correction programs for violent perpetrators, and all effective tools prove applicable when perpetrators are located on Uzbekistan's territory and their identities are established [6]. But what if perpetrators committing cyberbullying, cyber-grooming, or blackmail crimes reside in other states? The Law establishes no clear, rapid procedures for applying protection orders against foreign-located perpetrators or compelling international technology companies (social networks, messengers) to cooperate in investigations and provide user information. This demonstrates the existence of serious obstacles in adapting the Law's practical application to cyber crimes' global nature.

Toward ensuring practical implementation of the Law on Protection from All Forms of Violence, the Regulation "On Procedures for Identifying Violence Against Children, Assessing Violence Risk Levels, Developing Protection Plans, and Implementing Them" (approved by Cabinet of Ministers Resolution No. 440, July 14, 2025) constitutes an important legal instrument. This Regulation establishes precise, step-by-step action algorithms for reporting violence situations through developing child protection plans.

Notably, the Regulation recognizes "messages in the global Internet information network, including on social networks" as grounds for identifying violence situations, evidencing Uzbekistan's legal system's adaptation to digital threats. However, critical analysis demonstrates that the Regulation's procedural logic and mechanisms cannot fully address cyber space crimes' specific characteristics.

First, the Regulation's entire procedure presumes national jurisdiction and physical presence. Upon receiving violence reports, the "Inson" social services center and internal affairs bodies must, within one day, study the child's "life situation," visit the child's residence, and conduct initial and comprehensive assessments. This mechanism proves effective for traditional crimes where perpetrators and victims share territory. However, in cyber-grooming or online blackmail situations, perpetrators often reside in other countries and remain anonymous. Under such circumstances, how can local "Inson" centers or prevention inspectors develop "protection plans" and apply enforcement measures against foreign-located individuals? The Regulation contemplates no separate, special procedure for situations occurring in cyberspace yet involving transnational perpetrators, remaining limited to traditional "offline" approaches.

Second, the Regulation establishes no procedure for collecting and preserving digital evidence. Digital traces such as IP addresses, chat transcripts, and account metadata hold decisive significance in exposing cyber crimes. The Regulation focuses primarily on studying children's living conditions and family relationships—social-psychological aspects. It fails to indicate algorithms for procedural actions such as urgently preserving digital evidence or requesting information from foreign platforms by

investigation subjects (e.g., internal affairs bodies) upon receiving online violence reports before formal investigations commence. This situation may lead to crucial evidence loss and consequent perpetrator escape from accountability.

Analysis of research results

Analysis reveals a fundamental disjunction between Uzbekistan's formal legal commitments to international child protection standards and the functional capacity of domestic legislation to address contemporary cyber threats. This "implementation gap" manifests across multiple dimensions.

Much of Uzbekistan's foundational child protection legislation predates the digital revolution. The 1997 Law on Information Guarantees emerged before widespread Internet adoption. The 2008 Law on Guarantees of Child Rights was conceptualized for an "analog" world. Even the 2017 Law on Protection from Harmful Information, though more recent, employs terminology and mechanisms oriented toward traditional media forms rather than social media platforms, encrypted messaging applications, and interactive online environments where contemporary cyber crimes predominantly occur.

Conceptual Inadequacy: Existing legislation predominantly adopts a content-regulation paradigm rather than a conduct-prevention framework. Laws focus on classifying and restricting the distribution of harmful "information products"—a static concept ill-suited to addressing dynamic, interactive criminal processes such as grooming, sextortion, or live-streaming abuse. The legal framework regulates what children may access, but it inadequately addresses what actors may do to children in digital spaces.

Uzbekistan's legislative framework operates within traditional territorial jurisdiction principles. Enforcement mechanisms presume physical presence, territorial location, and identifiable subjects under national authority. Cyber crimes' inherently transnational character—where perpetrators, victims, servers, and platforms frequently span multiple jurisdictions—renders these territorial assumptions obsolete. The legislation provides no clear mechanisms for exercising jurisdiction over foreign-located perpetrators, compelling cooperation from international technology platforms, or rapidly preserving volatile digital evidence across borders.

Beyond substantive legal gaps, significant institutional and procedural deficiencies impede the effective implementation of international standards.

Uzbekistan lacks dedicated cybercrime investigation units with specialized training in digital forensics, cryptocurrency tracing, and international evidence gathering. The Regulation on Violence Identification assigns responsibilities to "Inson" social service centers and internal affairs bodies—entities designed primarily for traditional, territorially-bounded social work and policing. These institutions lack the technical capacity and legal authority to effectively investigate transnational cyber crimes.

Neither the Law on Protection from All Forms of Violence nor its implementing regulations establishes procedures for:

- Emergency preservation of volatile digital evidence (logs, metadata, communications);
- Expedited requests to foreign service providers for user data;
- Chain of custody protocols for digital evidence, ensuring admissibility;
- Use of specialized investigative techniques (undercover operations, controlled delivery in online environments);
- Coordination with foreign law enforcement through mutual legal assistance channels.

These procedural lacunae mean that even when cyber crimes are detected, investigators lack legal frameworks for gathering evidence necessary for prosecution.

While Uzbekistan participates in multilateral treaties governing mutual legal assistance, practical implementation remains deficient. Traditional mutual legal assistance procedures—requiring formal requests through diplomatic channels—prove too slow for addressing cyber crimes where evidence may disappear within hours. The legislation does not contemplate:

a) 24/7 contact points for emergency cooperation (as envisioned in Budapest Convention Article 35);

b) Expedited preservation requests to foreign jurisdictions;

c) Direct cooperation between investigative authorities;

d) Mechanisms for joint investigations or coordinated law enforcement actions.

Uzbekistan's ratification of international instruments creates legal obligations but does not automatically generate enforcement capacity. Analysis reveals several dimensions of this disconnect:

Lanzarote Convention Implementation: Uzbekistan ratified the Lanzarote Convention, which requires criminalization of various forms of child sexual abuse and exploitation, including those facilitated through information technologies. However, national legislation does not fully implement Convention requirements for: Criminalizing specific online conduct (grooming, solicitation through ICT); Establishing corporate liability for failure to report or remove child sexual abuse material; Creating specialized units for investigating technology-facilitated crimes; Implementing mandatory reporting obligations for service providers.

Budapest Convention Alignment: Though not a party to the Budapest Convention, Uzbekistan's engagement in international cybersecurity cooperation implies commitment to its principles. However, significant gaps exist regarding: real-time collection of traffic data, expedited preservation and disclosure of data, mutual legal assistance provisions adapted to electronic evidence, and establishment of a 24/7 network for urgent international cooperation.

UN Guidelines Implementation: Various UN instruments, including General Assembly resolutions and ECOSOC guidelines on child protection in the digital environment, recommend specific measures that remain unimplemented in Uzbekistan's

framework: age-verification mechanisms for online services, mandatory reporting by online service providers, public-private partnerships for identifying and removing illegal content, and comprehensive awareness-raising programs on online safety.

Several systemic obstacles emerged during this research, themselves illuminating implementation challenges:

Limited Public Data: Uzbekistan maintains limited publicly accessible statistics on cybercrime investigations, prosecutions, and convictions. This opacity hinders evidence-based policy development and prevents assessment of enforcement effectiveness.

Fragmented Regulatory Authority: Responsibility for child protection in the digital environment disperses across multiple agencies (Information and Mass Communications Agency, Ministry of Interior, Prosecutor's Office, guardianship bodies) without clear coordination mechanisms. This institutional fragmentation impedes coherent policy implementation.

Capacity Constraints: Interviews with practitioners (where conducted) and analysis of institutional structures reveal significant capacity gaps, including insufficient numbers of trained digital forensics specialists, limited technical equipment for electronic evidence analysis, and inadequate funding for international cooperation activities.

Rapid Technological Evolution: The pace of technological change outstrips legislative adaptation. New platforms, encryption methods, and criminal methodologies emerge faster than legal frameworks evolve. This creates a perpetual state of legal catch-up, where legislation addresses yesterday's threats while criminals exploit today's technologies.

CONCLUSION

This comprehensive analysis of Uzbekistan's implementation of international legal norms for combating cyber crimes against children yields several critical conclusions:

1. Constitutional Foundation Exists But Requires Operationalization: Uzbekistan has established constitutional recognition of international law's supremacy and children's special protection needs. However, this constitutional framework requires translation into specialized, operationalizable statutory provisions and enforcement mechanisms specifically designed for digital environment threats.

2. Significant Legislation-Reality Gap: Despite ratification of major international instruments and adoption of domestic child protection laws, substantial gaps persist between legal frameworks and enforcement capacity. Existing legislation, conceptualized primarily for offline environments, proves inadequate for addressing contemporary cyber threats' specific characteristics.

3. Transnational Dimension Remains Unaddressed: The most critical deficiency concerns the absence of effective mechanisms for addressing cyber crimes'

inherently transnational nature. Legislation operates within territorial jurisdiction paradigms incompatible with borderless digital crime.

4. Procedural Mechanisms for Digital Evidence Lacking: Uzbekistan's legal framework does not establish clear procedures for collecting, preserving, and utilizing digital evidence—a fundamental prerequisite for successful cybercrime prosecution.

5. Institutional Capacity Requires Development: Beyond legislative reform, effective implementation demands significant investment in institutional capacity, including specialized training, technical equipment, and dedicated cybercrime units.

6. International Cooperation Infrastructure Insufficient: While formal cooperation frameworks exist, practical mechanisms for rapid, effective international collaboration in cybercrime investigations remain underdeveloped.

Based on identified gaps, the following legislative reforms merit priority consideration:

Immediate-Term Reforms (1-2 years):

1.1. Amend Criminal Code to explicitly criminalize cyber-enabled child abuse: Introduce specific offenses for online grooming, cyberbullying with aggravated consequences, sextortion, and live-streaming abuse. Ensure definitions account for the digital environment's specific characteristics.

1.2. Establish mandatory reporting obligations for online service providers: Require platforms operating in Uzbekistan or accessible to Uzbek users to implement mechanisms for detecting, reporting, and removing child sexual abuse material. Define clear timelines and accountability measures.

1.3. Create expedited digital evidence preservation procedures: Enact provisions enabling law enforcement to issue preservation orders directly to service providers (domestic and foreign) with mandatory compliance within 24-72 hours.

1.4. Establish 24/7 cybercrime contact point: Designate a permanent contact point within law enforcement authorized to receive and respond to urgent international cooperation requests, aligned with Budapest Convention Article 35 principles.

Medium-Term Reforms (3-5 years):

2.1. Comprehensive Criminal Procedure Code amendments: Introduce a specialized chapter on electronic evidence, addressing collection, preservation, authentication, and admissibility standards. Provide legal foundation for specialized investigative techniques (online undercover operations, controlled delivery).

2.2. Strengthen international cooperation framework: Ratify the Budapest Convention and the Second Additional Protocol. Negotiate bilateral agreements with priority jurisdictions (major technology platform headquarters), establishing streamlined evidence-sharing procedures.

2.3. Reform institutional architecture: Establish a dedicated cybercrime investigation unit within law enforcement with specialized training, technical capacity, and authority to coordinate with international counterparts.

2.4. Service Provider Accountability Framework: Develop comprehensive legislation establishing obligations for online platforms regarding age verification, parental controls, content moderation, and cooperation with law enforcement. Model on EU Digital Services Act provisions while adapting to Uzbekistan's context.

Long-Term Reforms (5-10 years):

3.1. Comprehensive Digital Environment Child Protection Code: Rather than fragmented provisions across multiple laws, develop unified, comprehensive legislation specifically addressing child protection in the digital environment. This should integrate criminal, civil, administrative, and regulatory dimensions into a coherent framework.

3.2. Public-Private Partnership Framework: Establish formal mechanisms for ongoing cooperation between government, technology companies, civil society, and academic institutions in combating child exploitation online.

This body should meet regularly, share information, coordinate policy development, and oversee implementation of the national strategy.

This research demonstrates that effective protection of children from cyber crimes requires more than formal legal commitments or general legislative provisions. It demands specialized, technically-informed legal frameworks adapted to the digital environment's unique characteristics; institutional structures with the capacity to implement those frameworks; and sustained engagement with international cooperation mechanisms.

Uzbekistan has made significant strides in recognizing child protection as a priority and in developing foundational legal frameworks. However, the rapid evolution of digital threats and the inherently transnational nature of cyber crimes necessitate a more fundamental transformation. The gap between international standards and domestic implementation capacity must be bridged through comprehensive legislative reform, substantial institutional investment, and authentic engagement with global cooperation mechanisms.

The recommendations presented herein provide a roadmap for that transformation. Their implementation would position Uzbekistan as a regional leader in combating cyber crimes against children while fulfilling the state's constitutional obligation to protect its most vulnerable citizens in both physical and digital spaces.

REFERENCES:

1. Arsawati, I. N. J., Darma, I. M. W., & Antari, P. E. D. (2021). A criminological outlook of cyber crimes in sexual violence against children in Indonesian laws. *International Journal of Criminology and Sociology*, 10(30), 219-223.

2. Azimov, M. M., Muminov, A. R., Nugmanov, N. A., & Umarkhanova, D. Sh. (2017). *Xalqaro shartnomalar huquqi: O'quv qo'llanma* [International treaty law: Textbook]. Tashkent: TSUL Publishing House.

3. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Santa Barbara: Praeger.

4. Gillespie, A. A. (2015). *Child exploitation and communication technologies*. Cullompton: Willan Publishing.

5. Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy*, 1(7), 1-35.

6. Jumanazarova, M. (2025). Nasilie v sem'e v otnoshenii nesovershennoletnikh: prichiny i mery profilaktiki [Domestic violence against minors: causes and preventive measures]. *Obshchestvo i innovatsii* [Society and Innovation], 6(3/S), 316-321.

7. McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. London: Home Office Research Report 75.

8. Miruktamova, F. L. (2023). Internet tizimida bolalar huquqlari va xavfsizligini ta'minlash: xalqaro standartlar va xorijiy tajriba [Ensuring children's rights and security in the Internet system: International standards and foreign experience]. *Yurist axborotnomasi* [Lawyer Herald], 3, 115-121.

9. Osula, A. M., & Rõigas, H. (Eds.). (2016). *International cyber norms: Legal, policy & industry perspectives*. Tallinn: NATO CCDCOE Publications.

10. Provalinskiy, D. I. (2023). Pravovoy status lichnosti v tsifrovom prostranstve [Legal status of the individual in digital space]. *Pravosudie* [Justice], 5(1), 38-53.

11. Rasulov, J. (2021). Children and forced labour: The legal nature of international labour standards. *Theoretical & Applied Science*, 8, 42-45.

12. Tropina, T., & Callanan, C. (2015). *Self- and co-regulation in cybercrime, cybersecurity and national security*. Cham: Springer.

13. United Nations. (1989). *Convention on the Rights of the Child*. Treaty Series, vol. 1577, p. 3.

14. Council of Europe. (2001). *Convention on Cybercrime* (Budapest Convention). ETS No. 185.

15. Council of Europe. (2007). *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Lanzarote Convention). CETS No. 201.

16. Republic of Uzbekistan. Constitution of the Republic of Uzbekistan (revised edition). Retrieved from https://lex.uz/docs/-6445145

17. Republic of Uzbekistan. (2008). Law on Guarantees of Child Rights, No. 139-ORQ. Retrieved from https://lex.uz/uz/docs/-1297315

18. Republic of Uzbekistan. (2017). Law on Protection of Children from Information Harmful to Their Health, No. 444-ORQ. Retrieved from https://lex.uz/docs/-3333797

19. Republic of Uzbekistan. (1997). Law on Guarantees and Freedom to Obtain Information, No. 400-I. Retrieved from https://lex.uz/docs/-1319

20. Republic of Uzbekistan. (2024). Law on Protection of Children from All Forms of Violence, No. 996-ORQ. Retrieved from https://lex.uz/docs/-7219502

21. Cabinet of Ministers of the Republic of Uzbekistan. (2025). Resolution No. 440 approving Regulation on Procedures for Identifying Violence Against Children. Retrieved from https://lex.uz/

22. Presidential Administration of Uzbekistan. (1999). Resolution No. 137 on Information Resources and Internet Distribution. Retrieved from https://lex.uz/ru/docs/-280901

23. President of the Republic of Uzbekistan. (2020). Decree PD-6012 on Approval of National Strategy on Human Rights.

24. President of the Republic of Uzbekistan. (2023). Decree PD-158 on "Uzbekistan-2030" Strategy.