

Ministry of Education and Science of the Republic of Kazakhstan

Al-Farabi Kazakh National University

UDC 343.85

Manuscript rights

HALIBIYATI HALIBATI

**Problems of legal liability of juveniles for offenses in the sphere of
informatization and communication**

"8D04203 Jurisprudence"

Doctor of Philosophy (PhD)
dissertation prepared for the degree

Domestic scientific adviser: Adilgazy Serikhan

Foreign scientific adviser: Michel Remi Njiki

Republic of Kazakhstan

Almaty, 2026

Chapter 1. Offenses in the Field of Informatization and Communications and Minors' Liability: Theoretical and Methodological Foundations

1.1 Formation and Current State of the Institution of Legal Liability in the Field of Informatization and Communications

1.2 Study of the Criminological Foundations of Offenses in the Field of Informatization and Communications

Chapter 2. Comprehensive Analysis of the Institution of Legal Liability of Minors in the Field of Digital Information and Telecommunications in Kazakhstan

2.1 Legal Status of Minors as Subjects of Legal Relations in the Field of Informatization and Communications

2.2 Legal Specificity of Minors' Administrative Liability for Offenses in the Field of Informatization and Communications

2.3 Specific Features of Minors' Criminal Liability for Criminal Offenses in the Field of Informatization and Communications

Chapter 3. Comparative Legal Analysis of International Experience in Regulating Minors' Liability in Informatization and Communication Relations

3.1 Liability of Minors for Offenses in the Field of Informatization and Communications in the CIS and Baltic States

3.2 Information Security in PRC Legislation and Minors' Liability for Digital Crimes

Chapter 4. Recommendations for Improving the System of Prevention and Liability Measures for Minors' Offenses in the Field of Informatization and Communications in the Republic of Kazakhstan Based on a Comparative Legal Analysis of International and Domestic Practice

NORMATIVE REFERENCES

The following normative legal acts are cited in this dissertation:

1. The Constitution of the Republic of Kazakhstan: adopted by republican referendum on 30 August 1995, with amendments and additions.
2. The Criminal Code of the Republic of Kazakhstan: Code of the Republic of Kazakhstan No. 226-V of 3 July 2014.
3. The Criminal Procedure Code of the Republic of Kazakhstan: Code of the Republic of Kazakhstan No. 231-V of 4 July 2014.
4. The Code of the Republic of Kazakhstan on Administrative Offenses: Code of the Republic of Kazakhstan No. 235-V of 5 July 2014.
5. Law of the Republic of Kazakhstan No. 345-II of 8 August 2002 "On the Rights of the Child in the Republic of Kazakhstan."
6. Law of the Republic of Kazakhstan No. 169-VI of 2 July 2018 "On the Protection of Children from Information Harmful to Their Health and Development."
7. Law of the Republic of Kazakhstan No. 591-II of 9 July 2004 "On the Prevention of Juvenile Delinquency and the Prevention of Child Neglect and Homelessness."
8. Law of the Republic of Kazakhstan No. 142-VI of 21 February 2018 "On Commissions for Juvenile Affairs and the Protection of Their Rights."
9. Law of the Republic of Kazakhstan No. 94-V of 21 May 2013 "On Personal Data and Their Protection."
10. Law of the Republic of Kazakhstan No. 418-V of 24 November 2015 "On Informatization."
11. Law of the Republic of Kazakhstan No. 567-II of 5 July 2004 "On Communications."
12. Law of the Republic of Kazakhstan No. 18-VIII of 10 July 2023 "On Online Platforms and Online Advertising."
13. United Nations Convention on the Rights of the Child, 20 November 1989.
14. United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, A/RES/79/243, 24 December 2024.
15. Convention on Cybercrime, Budapest, 23 November 2001, ETS No. 185.
16. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25 October 2007, CETS No. 201.

DEFINITIONS

The following terms are used in this dissertation with the corresponding definitions:

1. Minor - a person under eighteen years of age who has a special legal status within the limits of administrative and criminal liability, as well as in the digital environment.
2. Field of informatization and communications - the sphere of legal regulation of information systems, information resources, data processing and dissemination processes, and communications infrastructure.
3. Offense in the field of informatization and communications - an unlawful act or omission committed by using, or in relation to, information systems, communications networks or ICT.
4. Cybercrime - a criminal offense that infringes information systems, communications networks, or the confidentiality, integrity and availability of information.
5. Information security - the state in which information and information systems are protected against unauthorized access, alteration, destruction or dissemination in terms of integrity, confidentiality and availability.
6. Children's information security - the state in which a child's rights and legitimate interests are protected from information harmful to the child's health and development, from digital threats and from destructive influence.
7. Cyberbullying - insulting, harassing, threatening or discriminatory conduct committed through ICT and characterized by anonymity, asymmetry in the parties' capacities and the rapid dissemination of harmful content.
8. Digital evidence - information stored on electronic devices or obtained through information systems and used to confirm the fact of an offense or circumstances relevant to it.
9. Dropper - an intermediary person who, within a criminal scheme, uses a bank account, card, SIM card or account to receive, transfer or conceal illegal funds.
10. Deepfake - digital material that synthetically models the image, voice or behavior of a real person through artificial intelligence technologies.
11. Internet platform - a social network, messenger, video-hosting service, gaming platform or other digital service that enables information exchange among users.
12. Digital educational measure - an educational influence measure applied to a minor offender and including elements of digital hygiene, cyberethics, digital volunteering and restoration.

SYMBOLS AND ABBREVIATIONS

AI - Artificial Intelligence

ICT - Information and Communication Technologies

UN - United Nations

CAC - Cyberspace Administration of the People's Republic of China

CETS - Council of Europe Treaty Series

CM/Rec - Recommendation of the Committee of Ministers of the Council of Europe

COPPA - U.S. Children's Online Privacy Protection Act

CRC - United Nations Committee on the Rights of the Child

CSEA - Child sexual exploitation material

CoE - Council of Europe

EU - European Union

GDPR - General Data Protection Regulation, EU 2016/679

IT - Information Technology

KZ-CERT - National Computer Incident Response Service of the Republic of Kazakhstan

Malware - Malicious software

Parental Control - Parental control software

PIPL - Personal Information Protection Law of the People's Republic of China

SIM - Subscriber Identity Module

SIM-box - a device for remote management of a large number of SIM cards

CIS - Commonwealth of Independent States

UNICEF - United Nations Children's Fund

RK - Republic of Kazakhstan

Civil Code of the RK - Civil Code of the Republic of Kazakhstan

CAO RK - Code of the Republic of Kazakhstan on Administrative Offenses

CC RK - Criminal Code of the Republic of Kazakhstan

CPC RK - Criminal Procedure Code of the Republic of Kazakhstan

MIA RK - Ministry of Internal Affairs of the Republic of Kazakhstan

PRC - People's Republic of China

RF - Russian Federation

ILA - International Legal Assistance

ILC - International Legal Cooperation

MDDIAI RK - Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan

INTRODUCTION

Relevance of the research topic. The relevance of the dissertation research is determined by the fundamental digital transformation of the global information space and the deep penetration of information and communication technologies (ICT) into social relations. In the digital era, the Republic of Kazakhstan has enshrined for citizens, including minors, the right freely to seek, receive and disseminate information in paragraph 2 of Article 20 of the Constitution [1]. However, the exercise of this right is directly connected with the increasing vulnerability of children in the digital environment: new threats such as cyberbullying, digital grooming, unlawful profiling of personal data, dropper schemes and manipulation through artificial intelligence (AI) draw minors into criminal-law relations as victims, offenders and instruments. The digital vulnerability of minors and the specific neuropsychological characteristics of their personal development require a comprehensive reconsideration of the institution of their legal liability. This requires not only the improvement of theoretical doctrine, but also the development of legislative proposals, the renewal of institutional mechanisms and the implementation of international experience according to the principle of differentiated reception.

Objective empirical evidence of the relevance of the topic is provided by official statistics for the last five years. According to the Criminal Police Department of the Ministry of Internal Affairs of the Republic of Kazakhstan, internet fraud amounted to 7,700 cases in 2019, 14,000 in 2020 and 17,800 in 2021 [8]; the 22,870 cases recorded in 2024 represented a 5% increase compared with the previous year [48]. In 2025, according to the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, internet fraud accounted for approximately 90% of registered crimes, while official data of the Prosecutor General's Office of the Republic of Kazakhstan indicate that total fraud in 2024 amounted to 45,156 cases [129]. In the financial sector, the Anti-Fraud Center under the National Bank of the Republic of Kazakhstan prevented more than 80,000 fraudulent incidents in 2024 and returned 500 million tenge [7]. According to 2025 data from the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, the overall crime rate decreased by 6.6% to 123.9 thousand [141]; the indicator for the first quarter of 2026 was 86.1% higher than in the comparable period [164]. Among cybercrimes against property, a particularly alarming point is that 56% of persons involved in dropper schemes are young people aged 16-24 [59].

The relevance of the research topic is also determined by international legal parameters. The United Nations Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, adopted by UN General Assembly resolution A/RES/79/243 of 24 December 2024, establishes an international framework requiring implementation at the national level in the Republic of Kazakhstan [41]. The Council of Europe Lanzarote Convention (CETS No. 201)

and Convention 108+, General Comment No. 25 of the UN Committee on the Rights of the Child (CRC/C/GC/25, 2021), and the European Union GDPR (2016/679) and DSA (2022/2065) regulations establish international standards for an enhanced protection regime for minors' personal data and for platforms' duty of care. The study by R.V. Kymlyk [106] proposes a consistent mechanism for determining the special legal status of a minor in the digital environment. In addition, the effectiveness of the existing legal mechanism and its compliance with international standards constitute a doctrinal foundation for improving domestic doctrine.

Degree of scientific development of the research topic. The theoretical foundations of legal relations and the institution of liability in the field of informatization and communications have been widely examined in domestic and foreign scientific literature. In the fundamental-theoretical direction, a special place is occupied by A.A. Nukusheva, B.Zh. Kuandykov and Zh. Zhailau's comparative legal analysis of cyberbullying [63], A.A. Zhanaliyeva and co-authors' study of mechanisms for protecting children's interests in cyberspace [64], A.Zh. Tuleuova's research on the legal sphere in the digital era [81], Sh.B. Malikova and D.B. Malikov's analysis of criminal policy in the field of informatization [57; 69], K. Almazkyzy's study of cybercrime [56], and K. Aratuly and E. Baigazy's methodology for investigating information-security crimes [67]. These works formed the theoretical supports for developing the dissertation subject as a comprehensive doctrinal category; however, in domestic science, the legal liability of minors in the ICT field has not been comprehensively analyzed as an independent doctrinal institution, which substantiates the scientific novelty of the dissertation research.

In the criminological and legal direction, the main pillars of domestic scientific discourse include Zh.O. Kulzhabayeva's study of the legislative distinction between cybersecurity and information security [53], N.B. Kubanova and L.S. Serikov's study of the principles for classifying cyberattacks [58], K.R. Useinova and co-authors' analysis of droppers as instruments of cybercrime [59], R.S. Zhaltyrbayeva's research on the legal definition of AI [79], B.A. Umitchinova, Yu.A. Gavrilova and G.A. Menzyuk's comparative study of the legal regulation of personal data under AI conditions [73], A.K. Zhilkishiyev and E. Begaliyev's comprehensive study of problems in investigating crimes in the ICT field [42], L.L. Boshayeva's dissertation on preventing cybercrimes against minors [18], D.A. Karanov's criminological characterization of crimes against the person committed using ICT [19], and K.O. Karabekov's comparative study of the Russian Federation and the Republic of Kazakhstan [20]. In the administrative-law direction, studies by E.I. Lukina [13; 109], T.M. Zanina [22; 89], and G.A. Alibayeva and co-authors [105] comprehensively analyze the specific features of minors' administrative liability; the work of Zh.B. Karipbaev and co-authors in Scopus publications [98] substantiates the legal status of this category at the international level.

A review of the scientific literature shows that the issue of minors' liability for offenses in the field of informatization and communications has been considered in

the legal science of the Republic of Kazakhstan in certain separate aspects, but has not yet been comprehensively studied as an independent doctrinal category.

The object of the research is the legal relations that arise within public relations involving minors in the field of informatization and communications, including as a result of committing unlawful acts using ICT or becoming victims of such acts.

The subject of the research is the system of normative legal acts of the Republic of Kazakhstan regulating minors' liability for offenses in the field of informatization and communications, the legal deficiencies contained therein and their manifestation in law-enforcement practice, as well as the comparative legal experience of international and foreign law.

The purpose of the research is to provide a comprehensive scientific and legal understanding of the institution of minors' liability for offenses in the field of informatization and communications within the normative legal system of the Republic of Kazakhstan, to form conceptual foundations for improving domestic doctrine and to develop legislative proposals.

Research objectives. To achieve this purpose, the following objectives were set: 1) to study the theoretical and legal foundations and evolutionary formation of the institution of legal liability in the field of informatization and communications; 2) to determine the criminological characteristics and independent categories of offenses in the ICT field; 3) to analyze the status of a minor as a subject of legal relations in the ICT field; 4) to comprehensively study the specific features of minors' liability under the CAO RK and the CC RK; 5) to conduct a comparative legal analysis of the experience of the CIS, the Baltic states and the PRC; 6) to substantiate minors' information-psychological security and the category of digital maturity as independent doctrinal foundations; 7) to develop legislative proposals for the CC RK and the CAO RK; 8) to substantiate the doctrinal basis of the tripartite model 'State - Platform - Legal Representative.'

The methodological basis of the research relies on the theory of cognition and on general scientific principles for the scientific comprehension of legal reality. The work uses a comprehensive set of general scientific methods (dialectical, systemic-structural, historical and formal-logical) and special scientific methods (comparative legal, normative-dogmatic, statistical and content analysis).

The theoretical basis of the research consists of the works of Kazakhstani and foreign scholars in general theory of law, information law, criminal law and criminology, and administrative law (S.S. Alekseev, I.L. Bachilo, V.A. Kopylov, A.K. Zhilkishiyev, E. Begaliyev). The normative legal base consists of the Constitution of the Republic of Kazakhstan [1], Law No. 418-V of 2015 'On Informatization' [2], Law No. 567 of 2004 'On Communications' [3], Law No. 94-V of 2013 'On Personal Data and Their Protection' [28], the information security package updated by amendments No. 44-VIII of 2023 [33], Law No. 169-VI of 2018 'On the Protection of Children from Information Harmful to Their Health and Development' [85], the digital transformation concept approved by Resolution No. 269 of the Government of

the Republic of Kazakhstan in 2023 [14], the 'Cyber Shield of Kazakhstan' concept approved by Resolution No. 407 of the Government of the Republic of Kazakhstan in 2017 [30], and the concept for the development of artificial intelligence adopted by the President of the Republic of Kazakhstan on 24 September 2024 [32].

The empirical basis of the research consists of official data for 2019-2026 from the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan [5; 6; 7; 8; 48; 141; 164], reports of the Anti-Fraud Center under the National Bank of the Republic of Kazakhstan, the study by H. Halibiyati and co-authors based on the Add Health longitudinal dataset (n = 20,745 respondents) [60], and Kubanova and co-authors' comparative analysis of cyberattacks published in a Scopus Q1 journal [9].

The scientific novelty of the research is reflected in the following: first, for the first time in domestic legal science, the institution of minors' liability for offenses in the field of informatization and communications is analyzed as a comprehensive doctrinal category; second, the categories of 'digital maturity,' 'digital delict,' 'restorative digital justice,' 'counterpart obligations' and 'differentiated reception' are introduced for the first time as independent doctrinal foundations; third, a comprehensive institutional and normative architecture for preventing minors from committing offenses in the ICT field is proposed as an author's model consisting of four mutually coordinated pillars (regulatory-platform, institutional-subject, reactive-educational, and systematization-codification); fourth, the tripartite institutional and legal model 'State - Platform - Legal Representative' is substantiated as a doctrinal foundation of children's digital security; fifth, the introduction of neuropsychological examination as a mandatory procedural measure is proposed for differentiating a minor's criminal liability in the ICT field.

Main propositions submitted for defense:

Proposition 1. The information-psychological security of minors should be recognized as an independent object of criminal-law protection. The information-psychological security of minors means the protection of a minor from destructive informational influence disseminated in the digital environment - cyberbullying, suicidal content, digital grooming, unlawful profiling and misuse of personal data - as well as the preservation of the minor's mental, emotional and moral integrity. The empirical basis of the proposition is data from the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan: every fifth Kazakhstani adolescent aged 11-15 becomes a victim of cyberbullying every month; at the international level, Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe and General Comment No. 25 of the UN Committee on the Rights of the Child (CRC/C/GC/25, 2021) establish the relevant legal category at the normative level.

Identified legal deficiency: Chapter 7 of the Criminal Code of the Republic of Kazakhstan (Articles 205-213) limits the object of criminal encroachment to the categories of 'computer information,' 'information system' and 'information and

communication network'; the mental and emotional integrity of a minor is not established as an independent object, and the elements of offenses under Articles 174 and 274 of the CC RK insufficiently differentiate destructive informational acts directed at the category of children in the digital environment.

Legislative proposal: to supplement Chapter 7 of the CC RK with Section 7-1 entitled 'Criminal Offenses against the Information-Psychological Security of a Minor' and to introduce Article 213-1: 'Article 213-1. Encroachment on the information-psychological security of a minor. 1. The intentional dissemination, using ICT or telecommunications networks, of systematic insulting, threatening or humiliating information directed at causing harm to the mental and moral development of a minor, the involvement of a minor in content tending to incite an attempt on the minor's own life, or the unlawful profiling of the minor's personal data shall be punishable by a fine in the amount of four hundred to eight hundred monthly calculation indices, or by community service, or by restriction of liberty for up to three years, or by deprivation of liberty for the same term.' In addition, it is proposed to supplement Article 115-1 of the CC RK (stalking) with a qualifying element for acts committed against a minor.

Proposition 2. In differentiating minors' criminal liability in the ICT field, the category of 'digital maturity' should be introduced as an independent subject of procedural assessment. Digital maturity means the level of intellectual, emotional and socio-legal development of a minor's ability to understand the legal nature and virtual consequences of an act committed using ICT. The scientific basis of the proposition is the study co-authored by the dissertation author, Halibiyati H., Aratuly K., Serikhan A., Yergali A.M., Beaver K.M., 'Neuropsychological Functioning and Its Association with Juvenile Arrest and Adulthood Incarceration' (Journal of Criminal Justice, 2024, Vol. 91, Article 102153, Scopus Q1, IF 4.3), based on the Add Health longitudinal sample (n = 20,745). From a comparative legal perspective, part 3 of Article 20 of the Criminal Code of the Russian Federation, Article 11 of the Latvian Criminal Law, and the PRC Law of 2021 'On the Prevention of Juvenile Delinquency' establish the international doctrinal basis of this category.

Identified legal deficiency: although part 3 of Article 15 of the CC RK establishes the rule of 'mental development not corresponding to age' as a general provision, no special mechanism or criteria have been developed for applying it to crimes in the ICT field; Articles 80-84 of the CC RK do not treat the ability to assess the virtual consequences of an act in the digital environment as an independent subject of procedural differentiation.

Legislative proposal: to supplement Article 80 of the CC RK with a part reading as follows: 'When assigning criminal liability and punishment to a minor who has committed crimes in the ICT field, the court shall treat the minor's digital maturity - the level of socio-psychological development of the ability to understand the legal nature and virtual consequences of an act committed using ICT - as an independent subject of assessment on the basis of the results of a comprehensive neuropsychological examination; if the level of digital maturity does not correspond

to chronological age, the court shall decide on releasing the person from criminal liability or applying the educational influence measures provided for in Article 84 of this Code.' It is also proposed to supplement Article 271 of the Criminal Procedure Code of the Republic of Kazakhstan with a rule establishing neuropsychological examination as a mandatory procedural measure in relation to minors who have committed crimes in the ICT field.

Proposition 3. Terminological consistency in the legal definitional field of violence in the digital environment and in the protection of children's personal data should be ensured at the legislative level. The definition of 'bullying of a child' introduced in 2022 in subparagraph 4-1) of Article 1 of Law No. 345-II of 8 August 2002 'On the Rights of the Child in the Republic of Kazakhstan' does not include the semantic characteristics of the digital environment - the subject's anonymous mode, the asymmetry of the parties' legal and technical capacities, and the capacity of a single intentional act to spread uncontrollably to a mass audience - as separate definitional features. The absence in Kazakhstani legislation of statutory definitions of the categories 'digital aggression,' 'profiling of children' and 'digital personal data of a minor' creates instability in law-enforcement practice in determining the boundaries of differentiation between Articles 130 (defamation), 131 (insult) and 115-1 (stalking) of the CC RK.

Legislative proposal: (a) to update subparagraph 4-1) of Article 1 of the Law 'On the Rights of the Child in the Republic of Kazakhstan' in the following wording: '4-1) bullying of a child - systematic acts of an insulting nature, harassment and/or intimidation; cyberbullying - a form of bullying of a child committed by using telecommunications networks, mass media or online platforms in an anonymous mode of the subject'; (b) to supplement Article 1 of the same Law with the definitions 'digital aggression' and 'profiling of children'; (c) to supplement Article 1 of Law No. 169-VI of 2018 'On the Protection of Children from Information Harmful to Their Health and Development' with wording harmonized with the definition of 'digital aggression'; (d) to supplement Law No. 94-V of 2013 'On Personal Data and Their Protection' with a rule prohibiting the profiling of minors, in accordance with UN CRC/C/GC/25 (2021) and paragraph 35 of Recommendation CM/Rec(2018)7 of the Council of Europe: 'Automated profiling of a minor under 16 years of age shall be prohibited, except for data processing carried out for educational or healthcare purposes on the basis of the express written consent of the legal representative.'

Proposition 4. The institution of digital delicts should be introduced as an independent doctrinal category, and liability and restorative influence in relation to minors should be formed as a unified legal model. A digital delict means an unlawful act committed by using ICT or in the digital environment, whose object is the information security of society and the established procedure for the use of information resources, and which entails material, administrative or criminal liability. Within this category, offenses involving minors are classified into three independent groups: (a) the minor as victim (cyberbullying, digital grooming, sexual exploitation

material); (b) the minor as offender (dropper schemes, unlawful access to information systems, dissemination of deepfake materials); (c) the minor as instrument (involvement by adult criminals in providing bank accounts or registering phishing websites). Empirical justification: according to 2025 data from the Committee under the Prosecutor General's Office of the Republic of Kazakhstan, 56 percent of persons involved in dropper schemes are young people aged 16-24.

Identified legal deficiencies: (a) part 1 of Article 65 of the CAO RK provides for the recovery from legal representatives of a fine imposed on a minor if the minor has no independent source of income, which eliminates the individualized educational effect of punishment; (b) the closed list of educational influence measures in part 2 of Article 84 of the CC RK does not take into account the substantive specific features of offenses in the ICT field; (c) Article 232-1 of the CC RK does not provide a differentiated mechanism for a minor subject; (d) the list of circumstances aggravating administrative liability in Article 57 of the CAO RK does not include the use of ICT.

Legislative proposal: (a) to supplement part 2 of Article 84 of the CC RK with an expanded list of digital educational measures: '5) completion of structured educational courses on the basics of digital hygiene and cyberethics; 6) participation in state-supervised digital volunteer (cyber squad) programs; 7) digital probation'; (b) to supplement Article 79 of the CC RK with a digital expungement procedure; (c) to supplement Article 232-1 of the CC RK with a note establishing the priority of educational measures in relation to a minor subject; (d) to supplement part 1 of Article 65 of the CAO RK with a rule on the unconditional priority of educational influence measures over a fine in relation to a minor who has committed an administrative offense in the ICT field for the first time; (e) to expand the list of circumstances aggravating administrative liability in Article 57 of the CAO RK by including the use of ICT or telecommunications networks.

Proposition 5. A methodological concept should be formed for differentiating the conduct of a minor subject that unites digital maturity and participation under conditions of artificial intelligence into a single foundation. The concept is based on two interrelated theoretical pillars: first, the category of digital maturity proposed in Proposition 2 of this research; second, a differentiation model that takes account of AI and synthetic algorithms (deepfake materials, chatbots, generative models) as instruments participating in criminal-law relations. At the international level, Regulation (EU) 2024/1689 of 13 June 2024 (AI Act) differentiates AI systems by risk level and establishes a prohibition on algorithms that exploit the vulnerability of minors; the PRC Interim Measures for the Management of Generative Artificial Intelligence Services of 13 July 2023 establish a mechanism for mandatory labeling of deepfake materials.

Identified legal deficiencies: (a) Article 28 of the CC RK does not contain a special feature differentiating the use by adult participants of AI systems, deepfake materials or automated manipulation algorithms to control a minor's behavior online;

(b) the list of aggravating circumstances in Article 54 of the CC RK does not provide for the use of ICT and AI; (c) the list of mitigating circumstances in Article 53 of the CC RK does not contain a rule recognizing a juvenile's commission of a crime under the influence of automated algorithms as a form of mental coercion.

Legislative proposal: (a) to supplement Article 28 of the CC RK with part 6 in the following wording: 'The use by an adult participant of artificial intelligence systems, deepfake materials, chatbots, generative algorithms and automated manipulation tools when involving a minor in a crime or committing a crime jointly with a minor shall be a qualifying feature indicating a particularly dangerous degree of complicity in crime'; (b) to supplement Article 54 of the CC RK with the subparagraph 'commission of a crime using ICT or artificial intelligence systems' as an aggravating circumstance; (c) to supplement Article 53 of the CC RK with a subparagraph recognizing the commission of a crime by a minor under the influence of automated algorithms that imitate human interaction as a form of mental coercion; (d) to supplement Article 3 of the CC RK with definitions of 'artificial intelligence system,' 'synthetic algorithm' and 'deepfake material.'

Proposition 6. Under conditions of artificial intelligence, complicity in crime should be established in the Criminal Code as a three-dimensional legal regime: an independent aggravating instrument of committing a crime, a qualifying feature of complicity in crime and an algorithm of mental coercion of a minor subject. This proposition expands the criminal-law differentiation component of Proposition 5 and proposes supplementing Article 210 of the CC RK with part 1-1 to cover the production of phishing content and creation of deepfake materials using generative AI, in the following wording: 'The creation, use or dissemination of programs and software products intended for the mass production of phishing content using generative artificial intelligence, the creation of deepfake materials or the development or dissemination of automated manipulation algorithms targeting minors shall entail criminal liability within the framework of reception of Articles 7-11 of the Convention adopted by UN General Assembly resolution A/RES/79/243 of 24 December 2024.'

Proposition 7. Ensuring the digital security of minors should be organized on the basis of the tripartite institutional and legal model 'State - Platform - Legal Representative.' The model constructs the legal protection of a minor in digital space as an interdependent intersection of the state's regulatory function, the information intermediary's duty of care and the legal representative's digital parenting function; the institution of counterpart obligations is proposed as the legal mechanism for implementing the model, and cyber squads and the digital ombudsman are proposed as specialized subjects. Empirical justification of the proposition: according to a 2024 UNICEF study, only 38 percent of parents are regularly informed about their children's online activity, and only 12 percent actively use parental control tools. International standard: Article 28 of Regulation (EU) 2022/2065 (DSA) establishes

platforms' duty of care; Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe establishes the principle of shared responsibility.

Legislative proposal: (a) to supplement the Law 'On Online Platforms and Online Advertising' with Article 5-1, modeled on Article 28 of the DSA, establishing platforms' duty of care, a high level of privacy by default, restrictions on personalized recommendation algorithms and the obligation to review complaints no later than within 24 calendar hours; (b) to supplement the Law 'On the Rights of the Child in the Republic of Kazakhstan' with Article 16-1 on the digital parenting duties of legal representatives and to supplement Chapter 12 of the CAO RK with Article 127-4 modeled on Article 6.17 of the Code of Administrative Offenses of the Russian Federation; (c) to supplement the Law 'On Personal Data and Their Protection' with a special chapter entitled 'Chapter 5-1. Enhanced Protection Regime for Minors' Personal Data,' modeled on Convention 108+ and Article 8 of the GDPR; (d) to supplement the Law of 30 December 2025 'On the Prevention of Offenses' with a rule on the special legal status of cyber squads; to supplement the Regulation on the Commissioner for Children's Rights approved by Decree No. 192 of the President of the Republic of Kazakhstan of 2016 with a rule establishing a specialized digital ombudsman; (e) to establish a Targeted Fund for Children's Digital Security modeled on Article 28 of the Lanzarote Convention.

Proposition 8. An author's comprehensive institutional and normative architecture for preventing minors from committing offenses in the ICT field should be introduced for the first time into the criminal-law, administrative-law and information-law doctrine of the Republic of Kazakhstan. The architecture is proposed as a unified doctrinal construction consisting of four mutually coordinated pillars - regulatory-platform, institutional-subject (the tripartite State - Platform - Parent model), reactive-educational, and systematization-codification - and forms a structural mechanism for implementing, at the institutional level, the principle of priority of prevention over sanction under the Law of the Republic of Kazakhstan of 30 December 2025 'On the Prevention of Offenses.' The architecture integrates Propositions 1-7 of this research into a unified doctrinal system: in the regulatory-platform pillar, the platform duty of care of Proposition 7; in the institutional-subject pillar, the State - Platform - Parent model; in the reactive-educational pillar, the digital educational measures of Proposition 4; and in the systematization-codification pillar, the enhanced protection regime for minors' personal data.

The theoretical significance of the research is determined by the introduction into domestic doctrine of the categories proposed in the work: 'super-institution of information relations,' 'digital delict,' 'digital maturity,' 'restorative digital justice' and 'differentiated reception.'

Approbation of the research results. The main provisions and scientific conclusions contained in the dissertation have been published in the author's works, including the article by Halibiyati H., Aratuly K., Serikhan A., Yergali A.M., Beaver K.M., 'Neuropsychological Functioning and Its Association with Juvenile Arrest and

Adulthood Incarceration' (Journal of Criminal Justice, 2024, Vol. 91, Article 102153, Scopus Q1, IF 4.3), as well as in the article by Kubanova N., Nessipbayeva I., Dyussebaliyeva S., Halibati H., Adilgazy S., 'Countering cyber attacks in the Republic of Kazakhstan' (Social & Legal Studios, 2025, Vol. 8, No. 1), and in reports at republican and international scientific-practical conferences.

Structure and scope of the work. The dissertation consists of normative references, definitions, symbols and abbreviations, an introduction, four chapters (ten sections), a conclusion and a list of references.

CHAPTER 1. OFFENSES IN THE FIELD OF INFORMATIZATION AND COMMUNICATIONS AND MINORS' LIABILITY: THEORETICAL AND METHODOLOGICAL FOUNDATIONS

1.1 Formation and Current State of the Institution of Legal Liability in the Field of Informatization and Communications

The development of legal science at the present stage is directly connected with the large-scale digitalization of social relations, as well as with the extensive penetration of information and communication technologies into public administration, the economy, education, finance, security and everyday life. Under these conditions, the field of informatization and communications is regarded not merely as an area of technical services, but also as an important legal space for the exercise of the constitutional rights and freedoms of the individual and the citizen, the effective performance of state functions and the protection of national security. Article 18 of the Constitution of the Republic of Kazakhstan establishes everyone's right to inviolability of private life and to the preservation of personal and family secrets, while Article 20 recognizes everyone's right freely to receive and disseminate information by any means not prohibited by law [1]. In this regard, the legal regulation of information relations should be assessed not only as a narrow sectoral issue, but as an integral component of ensuring the constitutional and legal order, legal security and the fundamental rights of the person in the information environment.

The legal nature of public relations in the field of informatization and communications is complex. These relations arise in connection with the creation of information systems, the formation of information resources, the collection, processing, storage, dissemination and use of data, as well as the organization of communications networks and telecommunications infrastructure. In current legislation, they are fixed through two main sectoral blocks: Law No. 418-V of 24 November 2015 "On Informatization," which regulates relations in the field of informatization [2], and Law No. 567 of 5 July 2004 "On Communications," which regulates the creation and operation of communications networks and the provision of communications services [3]. Thus, the object of the research is not limited to a narrow technical sphere; it constitutes a complex object of legal regulation composed of public-law, private-law and organizational-legal elements.

According to Levicheva (2023), children and young people are the principal value of the state; therefore, their ability to analyze information flows and comply with legality forms the foundation of a future rule-of-law state [10]. This position deepens the scientific understanding of the importance of legal education and liability

in the information sphere. At the same time, the Scopus-indexed study by Halibiyati, Aratuly, Serikhan, Yergali and Beaver (2024), based on the longitudinal Add Health sample of 20 745 respondents, proved that indicators of adolescents' neuropsychological functioning are statistically significantly associated with arrest during minority and incarceration in adulthood: low behavioral control and a reduced ability to understand guilt constitute a specific indicator for identifying a person prone to destructive behavior in the digital environment [11]. This empirical conclusion provides a scientific basis for taking into account the cognitive and motivational characteristics of the minor subject when establishing liability in the information sphere.

The need for legal protection of public relations in the field of informatization and communications is also closely linked to economic development. The reliability of e-government, digital banking and e-commerce systems is a guarantee of investors' and citizens' trust in state institutions. If the legal system is unable to respond adequately to offenses in the information sphere, this negatively affects the country's reputation in the international arena and its economic growth. Therefore, improving the legislative framework does not mean only strengthening sanctions; it also means raising the ethics of security in the information environment to the level of legal regulation.

From a theoretical perspective, the institution of liability in the field of informatization is a complex structure consisting of a synthesis of administrative, criminal and civil-law norms. The objects of offenses in this field are recognized as society's information security, the established procedure for using information resources and the legitimate interests of subjects. In the works of Belavina and Shkorbatova (2023), along with strengthening the legislative framework in the field of information security, the need to create specialized mechanisms for the prevention of offenses is emphasized [12]. This scientific conclusion reinforces the practical relevance of the research topic and demonstrates the importance not only of punishment, but also of preventive measures.

The practical relevance of the topic is consistent with the implementation of the Republic of Kazakhstan's digital strategy. The Concept for the Development of Digital Transformation, the Information and Communication Technologies Sector and Cybersecurity of the Republic of Kazakhstan for 2023-2029, approved by Resolution No. 269 of the Government of the Republic of Kazakhstan of 28 March 2023, defines the legal reliability of the information space as a strategic objective [14]. Any vulnerability in information infrastructure may lead to the interruption of public services or to the leakage of citizens' important data. In this regard, by studying the historical and legal path of protecting public relations in the information sphere, it becomes possible to assess the mistakes and achievements of previous periods and to propose effective legal models oriented toward the future.

In domestic legal science, the study of legal issues in the field of informatization developed in close connection with the need to form the national

legislation of the Republic of Kazakhstan. The Scopus-indexed research of Tatarinova, Dzhanadilov and Tatarinov (2017) analyzes conceptual issues in identifying the main types of offenses in the field of informatization; according to the authors, in order to reveal the legal nature of unlawful acts committed through IT technologies, it is necessary to examine the correspondence between norms of international law and national legislation [15]. This direction increases the practical significance of the legal qualification of offenses.

In the legal regulation of digital law and telecommunications, the works of foreign scholars, in particular Lawrence Lessig and Cass Sunstein, occupy a special place. Lessig's concept of "Code is Law," proposed in his work *Code and Other Laws of Cyberspace* (1999), revealed the architectural nature of legal regulation in the digital environment. In his view, behavior in cyberspace is regulated not only by legal norms, but also by software code and technical algorithms. This theory created the need to consider the symbiosis of law and technology in ensuring information security.

Another important direction in the legal regulation of telecommunications is the study of international standards for the use of information resources. The research of Marwick, Fontaine and boyd (2017) examines minors' attitudes toward privacy and personal responsibility on social media and empirically studies the level of susceptibility to digital risks among adolescents with low socio-economic status [16]. Their concepts highlight the transboundary nature of offenses in the information sphere and the need to develop universal methods for countering them.

One of the important aspects in the study of legal protection in the field of informatization and communications is the theory of data protection. The European scientific school, particularly research surrounding the GDPR Regulation, places the informational autonomy of the individual at the center. Scholars in this field analyze the impact of information systems on human rights and have proposed new concepts concerning the right to be forgotten and the sovereignty of personal data.

A review of the literature on legal protection in the field of informatization and communications confirms the multifaceted nature of this topic and its close connection with various branches of legal science, including administrative, criminal, civil and international law. Scholarly views evolve in line with technological change: whereas earlier attention was focused mainly on protecting information infrastructure, today digital human rights, the ethics of artificial intelligence and comprehensive mechanisms for ensuring legality in cyberspace have come to the forefront. Analysis of scientific works shows that the effectiveness of legal protection in the information sphere depends not only on the quality of legal norms, but also on the level of legal culture, international cooperation and the compatibility of technological capabilities with law.

An analysis of the dynamics of the development of scholarly views shows that their evolution has been associated with three main technological factors.

The infrastructural stage, involving the formation of communications networks, was a period in which scholars, in particular E.I. Lukina, considered liability mainly

from the standpoint of protecting technical means and networks. The scientific discourse developed within the framework of "telecommunications law" [13].

The content stage, associated with the mass spread of the Internet, shifted attention to the content of information, harmful content and cybercrime. The concept of "information-psychological security," reflected in the works of Dinislamova and Zanina-Lukina, is a product of this stage [21; 22].

The algorithmic stage, involving AI and Big Data, is reflected in contemporary scientific works that study liability in the field of informatization in the context of the operation of automated systems and algorithms.

The substantive similarity among these concepts lies in their recognition of the vulnerability of the information environment and of the need to protect it. The difference, however, lies in the "cost" of such protection. In the Scopus-indexed research of Yuzikova, Komyakova, Khomyachenko and Chasova (2021), the relationship between minors' deviant behavior and the information environment is analyzed in a moral and psychological aspect [23]. This concept is distinguished by its treatment of legal liability not merely as a sanction, but as a factor regulating the process of a person's socialization. Such an approach supplements legal protection with educational and preventive functions.

Socio-economic factors have also had a significant influence on the formation of scholarly views. Scholars who study the problem of digital inequality link liability in the information sphere with economic status. In their view, users from lower socio-economic groups are more likely either to become victims of information offenses or inadvertently to become offenders. This position gives rise to a discourse on the need to take the subject's social situation into account when establishing legal liability. Statistics also confirm this conclusion: according to data from the Anti-Fraud Center, 87% of victims of internet fraud in Kazakhstan are pensioners, while the frequency with which minors are exposed to digital risks is directly connected with their level of social protection [7].

In addition, Law No. 193-VII of 6 February 2023 "On Digital Assets" was aimed at regulating new relations in the field of digital mining and crypto-asset circulation [31]; on 24 September 2024, by Decree of the President of the Republic of Kazakhstan, the Concept for the Development of Artificial Intelligence for 2024-2029 was approved, marking the beginning of legal support for new technological stages of digital transformation [32]. Law of the Republic of Kazakhstan No. 44-VIII of 11 December 2023 "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Issues of Information Security, Informatization and Digital Assets," which entered into force on 11 February 2024, introduced significant amendments to the Law on Personal Data Protection and clarified the procedure for notifying incidents, the definition of a personal data breach, and the prohibition on collecting and storing copies of identity documents [33].

The development of information exchange systems in society has also contributed to the improvement of legislative technique. Historically, legal regulation

has moved from relatively narrow infrastructural norms oriented toward organizing free technical services to a more complex model based on security, accountability, permissibility and legal guarantees. However, it would not be entirely accurate to describe this process in absolute terms as a complete transition from dispositive regulation to imperative control; in the current legal regime, the share of imperative security requirements has increased substantially, but legal guarantees such as access to information, protection of private life and freedom to use digital services have also been established alongside them. Kazakhstan's current legislation reflects this balanced model: on the one hand, requirements of national security, information security and cybersecurity are strengthened; on the other hand, the rights to personal data protection and access to information are guaranteed at the legislative level.

Kazakhstan's information policy at the present stage is developing toward large-scale digitalization and the provision of comprehensive cybersecurity. Within the legal foundations of the state program "Digital Kazakhstan," approved by Resolution No. 827 of the Government of the Republic of Kazakhstan of 12 December 2018, the institution of liability in the field of informatization has been significantly modernized. In particular, practical methods of countering offenses committed using ICT are being actively improved at both the scientific and legislative levels. As Kambarov and Sabitov (2023) note, current strategies for countering cybercrime should be based not only on punitive measures, but also on a comprehensive analysis of legal and technical tools that ensure the timely protection of national digital infrastructure [34].

The constitutional basis of the system is the Constitution of the Republic of Kazakhstan of 30 August 1995. Article 18 of the Constitution establishes everyone's right to inviolability of private life and personal and family secrets, while Article 20 guarantees the freedom to receive and disseminate information [1]. These fundamental norms are the principal legal source determining the content of all legislative acts in the information sphere. It is precisely these constitutional norms that establish the initial limits of the legal regulation of information relations: on the one hand, the state must guarantee freedom of information; on the other hand, it is obliged to protect private life, personal data, the secrecy of correspondence and other protected interests. Therefore, the content and purpose of all sectoral acts in the field of informatization and communications ultimately rest on this constitutional balance.

For the purpose of protecting the interests of the individual in the digital environment, Law No. 94-V of 21 May 2013 "On Personal Data and Their Protection" was adopted. The subject matter of this Law consists of relations arising in the collection, processing and protection of personal data. Its legal mechanism is based on the institution of the data subject's mandatory consent to the processing of his or her data and on the legal liability of operators for violating data confidentiality [28]. Following the amendments introduced by Law of the Republic of Kazakhstan No. 44-VIII, which entered into force on 11 February 2024, the Law was supplemented with norms on the official definition of a personal data breach, the obligation to notify within one working day, and the prohibition on collecting and

storing copies of identity documents; the Ministry of Digital Development, Innovations and Aerospace Industry was granted powers to inspect enterprises on the basis of a checklist consisting of 33 criteria for compliance with personal data legislation [33].

In connection with technological progress, the legislative system has been supplemented with new acts. Law of the Republic of Kazakhstan No. 193-VII of 6 February 2023 "On Digital Assets" is aimed at regulating new public relations in the field of digital mining and crypto-asset circulation [31]. The Cybersecurity Concept "Cyber Shield of Kazakhstan," approved by Resolution No. 407 of the Government of the Republic of Kazakhstan of 30 June 2017, laid the strategic foundations for protecting critical information infrastructure facilities [30]; while the Concept for the Development of Digital Transformation, the Information and Communication Technologies Sector and Cybersecurity for 2023-2029, approved by Resolution No. 269 of the Government of the Republic of Kazakhstan of 28 March 2023, defined the long-term strategic direction of the sector [14]. The Concept for the Development of Artificial Intelligence for 2024-2029, approved on 24 September 2024, determined the main guidelines of legal policy in the field of algorithmic governance and automated decision-making [32].

In the context of current digital transformation, the trend toward adapting national legislation to international standards is intensifying. The Scopus-indexed study by Satbayeva, Alimbetova and Beisenbayev (2024), published in the Bulletin of the Institute of Legislation of the Republic of Kazakhstan, substantiates the need to harmonize the legislation of the Republic of Kazakhstan with international standards and to draw on the experience of international cooperation in combating cybercrime [39]. Bolatbek, Baispayev, Musiraliyeva and Usmanova (2024) propose a technical and legal framework for detecting and reducing cybercrime through the use of university networks in the Republic of Kazakhstan in a study published in a Scopus-indexed journal [40]. The UN Convention against Cybercrime, adopted by Resolution A/RES/79/243 of 24 December 2024, provides Kazakhstan with a new international legal basis for working with transboundary digital evidence [41].

The system of normative legal acts regulating the field of informatization and communications in the Republic of Kazakhstan is an interconnected, mutually complementary structure with strict hierarchical ordering. This system forms an effective legal mechanism for protecting the state's digital sovereignty, ensuring economic progress and safeguarding citizens' rights under conditions of rapid development of information technologies. The Constitution, the Laws "On Informatization," "On Communications," "On Personal Data and Their Protection," "On Access to Information," "On National Security" and "On Digital Assets," the Criminal Code of the Republic of Kazakhstan and the Code of the Republic of Kazakhstan on Administrative Offenses, as well as the "Cyber Shield" and digital transformation concepts for 2023-2029, constitute a systematic normative architecture.

This system provides a basis for moving, at the next stage, to an assessment of its effectiveness and the quality of law-enforcement practice.

A comprehensive study of the system of normative legal acts in the field of informatization and communications makes it possible to assess the degree to which these norms are implemented in actual law-enforcement practice and the extent to which they perform preventive, protective and restorative functions. The effectiveness of legal regulation means the degree of correspondence between the objectives established in legislation and their actual socio-legal results. From this perspective, the current legal framework in the Republic of Kazakhstan is sufficiently branched and systematized: the Laws "On Informatization," "On Communications," "On Personal Data and Their Protection," "On Access to Information" and "On National Security," together with Chapter 7 of the Criminal Code of the Republic of Kazakhstan, which is devoted to criminal offenses in the field of informatization and communications, form the principal legal foundation of this sphere. At the same time, the issue of effectiveness should be assessed not only by the existence or absence of norms, but also by whether they are applied in a timely, consistent and technologically adapted manner.

In this regard, the effectiveness of legal regulation should not be measured solely by the severity of sanctions. Its real indicators are the capacity to prevent offenses, the speed with which violated rights are restored, the reliability of collecting and assessing digital evidence, and the actual level of protection of citizens' legitimate interests. Although the current legislation defines substantive legal prohibitions and obligations to a considerable extent, procedural and organizational difficulties remain at the level of law enforcement. This is especially evident in cases involving transboundary internet crimes, the prompt recording of digital traces, the classification of electronic communications, interaction with platform services and matters involving several authorized bodies. Therefore, in assessing effectiveness, the focus should not be limited to the question "does the norm exist?" but should instead prioritize the criterion "has the norm been able to reduce the actual risk?"

The study of the sufficiency of legal regulation also covers the issue of the liability of subjects in the information environment. Current legislation specifies in considerable detail the duties of communications operators, owners of information systems, personal data operators and subjects of state information infrastructure. At the same time, their risk burden is increasing, since a significant part of offenses is connected with the actions of third parties, phishing schemes, social engineering, transboundary digital services or the activities of organized cybercriminal groups. Under such conditions, legal effectiveness should not be limited to imposing duties on subjects; they also need technical standards, timely response procedures, coordinated data-exchange channels and a clear legal regime for risk management. The Concept of Digital Transformation for 2023-2029 and the "Cyber Shield of Kazakhstan" Concept provide for systematic measures precisely in this direction, aimed at strengthening information security and the resilience of digital infrastructure [14; 30]. Therefore, the

question of the sufficiency of legal regulation should be posed not only at the level of "are there requirements?" but also at the level of "have the conditions for fulfilling those requirements been created?"

Analysis of the effectiveness and problematic aspects of the existing mechanisms of legal regulation in the field of informatization and communications makes it possible to identify deeper systemic contradictions, legal gaps and weaknesses in law-enforcement practice in this sphere. In the Republic of Kazakhstan, a basic legal foundation has been formed in this area: the Constitution establishes the inviolability of private life and the right freely to receive and disseminate information; the Law "On Informatization" regulates information systems and digital infrastructure; the Law "On Communications" defines the legal regime of communications networks and services; the Law "On Personal Data and Their Protection" protects the informational interests of the individual; and the Law "On National Security" incorporates information security into the structure of national security. At the same time, the existence of legal problems does not indicate that this sphere is unregulated; rather, it shows that the sphere is developing with strong technological momentum and that existing norms require constant adaptation to the new digital reality.

First problem: the gap between the completeness of legal regulation and the quality of law enforcement. Current legislation establishes basic concepts, the rights and duties of subjects, the procedure for the functioning of information systems, the regime for processing personal data and information security requirements. However, because technological relations change rapidly, legal norms are often formulated in general terms, and their application to specific situations remains dependent on the interpretation of the law-enforcement body, the quality of technical expertise and interdepartmental coordination. The problem is not a "legislative vacuum," but the insufficient precision of norms and the absence of uniform practice in their application. Especially in information relations, the legal qualification of subjects' conduct in the virtual environment and the precise distinction between the roles of platform, operator, intermediary, user and data owner remain practically complex.

A practical manifestation of the legal problems connected with new technologies is found in deepfake technologies, synthetic media and algorithmic deception mechanisms. Official information notices of state bodies have published specific warnings that fraudsters are using deepfake technologies to steal citizens' confidential data, disseminate false investment offers, gain access to bank accounts and fabricate the image and voice of well-known persons. Although this phenomenon may be assessed under particular elements of offenses within the framework of existing criminal and civil-law norms, synthetic content such as deepfakes has its own evidentiary, expert and preventive issues.

Second problem: systemic legal issues in the field of ensuring information security. In Kazakhstan, information security and cybersecurity are established at the state strategic level: the "Cyber Shield of Kazakhstan" Concept has been adopted,

cybersecurity is included as an independent direction in the Digital Transformation Concept for 2023-2029, and the Law "On Informatization" and a number of subordinate regulatory acts establish information security requirements, monitoring, classification and incident-response procedures. Nevertheless, the main legal problem is that legal requirements and actual technical and organizational capacities for implementation do not always correspond to one another. The protection of critical information and communication infrastructure facilities, data exchange on incidents between the public and private sectors, the recording of attacks, the transformation of technical expert findings into legal evidence and the procedure for timely response require a high level of coordination in practice.

Third problem: the value balance in the field of protecting information rights. The Constitution establishes the inviolability of private life and secrecy, the Law "On Personal Data and Their Protection" regulates the collection and processing of personal data, and the Law "On Access to Information" strengthens the principle of openness [1; 28; 29]. Within this legal model itself, there is a certain natural tension: the state seeks to ensure openness, develop digital services, strengthen security and work with analytical data, while the citizen expects control over personal data, lawful limits on digital surveillance and the avoidance of excessive data collection. This dilemma becomes especially complex in the context of biometric data, platform-based data exchange, digital identification, mandatory registration for online services and the use of big data.

Legal problems connected with the situation of minors in the digital environment form a separate group. The general legal system is oriented toward protecting the rights and legitimate interests of children; Law No. 345 of the Republic of Kazakhstan of 8 August 2002 "On the Rights of the Child in the Republic of Kazakhstan" establishes the general basis for protecting children's rights and legitimate interests, while the Code of the Republic of Kazakhstan No. 518-IV of 26 December 2011 "On Marriage (Matrimony) and Family" defines the rights and duties of parents in protecting children's rights and interests. However, the digital environment makes this protection far more complex. Two legal interests collide here: on the one hand, there is a duty to protect minors from harmful information, fraud, manipulative content and digital exploitation; on the other hand, their right to education, access to information and full participation in digital society must be preserved. As noted in the work of Goryunova (2017), in studying adolescents' deviant behavior and offenses, it is important to take into account the level at which they understand the public danger of their actions and the specific features of their understanding of legal prohibitions [43]. The work of Ponomarev, Roy and Mishina (2017) analyzes issues of age-based differentiation of minors' administrative liability [44]. These conclusions substantiate the need to apply a differentiated legal approach that takes into account a person's age characteristics and psychological development when establishing liability in the information sphere. The longitudinal Scopus-indexed study by Halibiyati and others (2024) provides empirical data proving the

statistical relationship between neuropsychological functioning and a tendency toward offending in adolescence [11]. Rysaldiyeva's work (2022), devoted to the prevention of juvenile crime in the Republic of Kazakhstan, shows that institutional mechanisms of juvenile prevention exist in Kazakhstan, but that their adaptation to the digital environment remains a pressing issue [45].

The conducted systematic analysis makes it possible to identify five main problematic areas in the legal regulation of the field of informatization and communications in the Republic of Kazakhstan, despite the sufficiently developed normative framework: institutional, procedural, doctrinal, value-balance and preventive. The identified problems are not only shortcomings of the present stage, but also indicators that determine the scientific and methodological directions of future legal reforms. These conclusions provide a logical basis for moving, at the next stage, to the formulation of scientifically grounded ways to resolve these problems.

Resolving the identified systemic legal problems requires a comprehensive rethinking of the state's legal policy under conditions of technological transformation. Overcoming these issues should not be limited to isolated legislative amendments, since the current legal situation simultaneously encompasses constitutional guarantees, sectoral regulation, national security requirements, the interests of the digital economy and the duty to protect human rights. The Constitution of the Republic of Kazakhstan establishes the inviolability of private life and the right freely to receive and disseminate information, while the Laws "On Informatization," "On Personal Data and Their Protection" and "On National Security," together with the Digital Transformation Concept for 2023-2029, form the public-law and private-law foundations of this sphere. Scientifically grounded directions should be oriented toward simultaneously strengthening the systemic nature of legal regulation, technological flexibility and the specificity of legal guarantees.

1. Systematization and unification of information legislation. At present, this sphere is divided among several interconnected acts that regulate different tasks: the Law "On Informatization" regulates information systems and e-government infrastructure; the Law "On Communications" regulates telecommunications networks and services; the Law "On Personal Data and Their Protection" regulates the personal data regime; and the Law "On Access to Information" regulates access to public information. Within this structure, the legal framework is sufficiently broad, but from a scientific perspective its fragmentation brings to the fore the need for a unified conceptual apparatus and consistent law enforcement. Therefore, the proposal to adopt a single Information Code should more accurately be formulated not as a response to the absence of existing law, but as a scientifically grounded codification direction aimed at systematizing this extensive normative body. At the same time, such systematization should be carried out in accordance with the principles of legal hierarchy and sectoral coherence established in the Law "On Legal Acts."

2. Strengthening the principle of technological neutrality. In the current digital environment, if legal norms become tied to a specific technical solution, their

period of applicability shortens and legal gaps deepen as new technologies emerge. The Digital Transformation Concept for 2023-2029 and the Artificial Intelligence Development Concept for 2024-2029, approved by the Government of the Republic of Kazakhstan, indicate that the state regards digital renewal as a long-term and dynamic process. The scientific conclusion that follows from this is the need to develop legislation not through a model that reacts separately to each type of new technology, but through a flexible model that regulates according to risk, function, legal consequence and the role of the subject. Such an approach makes it possible to adapt the law to artificial intelligence, Big Data, platform services, synthetic media and other new phenomena without repeatedly making fundamental changes to legislation.

3. A comprehensive mechanism for protecting the information security of minors. In this sphere, legal regulation should not be limited to imposing duties only on the state or on owners of information systems; it is necessary to define the limits of responsibility of parents, legal representatives, educational organizations and digital platforms. The Law of the Republic of Kazakhstan "On the Rights of the Child in the Republic of Kazakhstan" establishes the general basis for protecting children's rights and legitimate interests, while the Code "On Marriage (Matrimony) and Family" defines the corresponding rights and duties of parents. Within this legal framework, it is appropriate to clarify special mechanisms for ensuring the safety of minors in the digital environment. As the Scopus-indexed study by Kubanova and others (2024) notes, the use of an interdisciplinary approach to protecting minors in the Kazakhstani context is compatible with international practice [9]. The longitudinal empirical study by Halibiyati and others (2024) substantiates the need for a differentiated legal regime that takes neuropsychological functioning into account [11]. State educational measures aimed at digital literacy and cyber hygiene should strengthen the preventive component of such a legal model.

4. Targeted use of regulatory sandboxes. In the Kazakhstani legal space, an institutional example of this approach is the AFSA FinTech Lab sandbox within the Astana International Financial Centre (AIFC); official materials of the AIFC and AFSA indicate that this platform is intended for testing innovative financial products and services in a regulated environment, while a sandbox licence grants temporary relief from certain requirements and allows a solution to be tested before full-scale regulation. From a scientific perspective, regulatory sandboxes make it possible to test new technologies, in particular services related to artificial intelligence and digital assets, in a limited and controlled environment and to identify their potential legal risks in advance. Such a mechanism enables legal policy not to restrain innovation, but rather to combine it with risk management. However, when transferring it into general national law, constitutional rights, data protection, competition and national security requirements must necessarily be observed.

Scientifically grounded ways of resolving problems in the field of informatization and communications should be oriented toward ensuring the systemic

nature of the legislative framework, technological flexibility, procedural clarity and the priority of human rights. The proposed directions include the systematization of information legislation, strengthening the principle of technological neutrality, clarifying the institution of digital evidence, adapting high standards of personal data protection to national law, forming a comprehensive model for the information security of minors, the targeted use of regulatory sandboxes and deepening international cooperation. The implementation of these directions will make it possible to strengthen the state's information sovereignty, increase the security of the digital economy and move toward a more stable level of legal order in the information society.

The scientific and practical significance of the research lies in the fact that the identified legal problems and proposed solutions form a theoretical and methodological basis for a deeper analysis in the subsequent chapters of offenses committed by minors in the ICT field and issues of their liability. The study of the formation and current state of the institution of legal liability in the field of informatization and communications serves as a fundamental basis necessary in the subsequent chapters of this work for substantiating the criminological characteristics of minors' digital offenses, the specific features of their liability, a comparative analysis of foreign legal models (the experience of the United States, Europe and the PRC), and ways to improve the legislation of the Republic of Kazakhstan.

1.2 Study of the Criminological Foundations of Offenses in the Field of Informatization and Communications

A key feature of social development at the present stage is the transfer of a substantial part of social, economic, financial, educational and administrative relations into the digital environment. The widespread dissemination of information and communication technologies has made social life easier, but it has also created new forms of criminal and other unlawful behavior. According to official data of the Bureau of National Statistics under the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan, in January-November 2024 the number of mobile communications subscribers in the Republic of Kazakhstan reached 26.1 million, the number of mobile communications subscribers with internet access reached 18.9 million, and the number of fixed internet subscribers reached 3.2 million [47]. Under conditions of such extensive digital coverage, the objective possibility of committing offenses through communications infrastructure has also increased. According to official 2024 data of the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, the total number of fraud cases amounted to 45 156, including 22 870 cases of internet fraud, which represented a 5% increase compared with the previous year [6]. This situation clearly demonstrates the need to study offenses in the field of informatization and

communications not as a merely technical or sectoral issue, but as an independent criminological phenomenon.

From a criminological perspective, offenses in the field of informatization and communications are a set of unlawful acts that infringe the functioning procedure of information systems, telecommunications networks, personal data circulation, digital services and online platforms, and that are distinguished by a high level of latency, the possibility of remote commission, a transboundary character and the rapid variability of evidentiary traces. The criminological basis for studying such offenses means comprehensively identifying their social conditionality, causes and conditions of commission, the characteristics of the offender, the victimological profile of the victim, the mechanism of commission of the offense and the prevention system. Therefore, analysis in this field should not be limited to a criminal-law characterization, but should be conducted in connection with norms regulating information-law and administrative-law relations, as well as with official statistical indicators.

The direct objects of these offenses are recognized as, first, the confidentiality, integrity and availability of information; second, the stable and lawful functioning procedure of informatization objects, communications networks and online platforms; and third, citizens' constitutional rights relating to inviolability of private life, protection of personal data and the lawful receipt and dissemination of information. Article 18 of the Constitution of the Republic of Kazakhstan establishes the inviolability of private life and personal and family secrets, while Article 20 establishes the right freely to receive and disseminate information by means not prohibited by law [1]. Therefore, offenses in the field of informatization and communications are not merely acts against technology or digital infrastructure, but socially dangerous phenomena directed against constitutional rights, the security of economic circulation, public trust and the state's information sovereignty.

The legal framework of this field consists of the Constitution of the Republic of Kazakhstan, Law No. 418-V of 24 November 2015 "On Informatization" [2], Law No. 567 of 5 July 2004 "On Communications" [3], Law No. 94-V of 21 May 2013 "On Personal Data and Their Protection" [28], Law No. 401-V of 16 November 2015 "On Access to Information" [29], Law No. 18-VIII of 10 July 2023 "On Online Platforms and Online Advertising" [48], and Law No. 94-VIII of 19 June 2024 "On Mass Media" [49]. These acts establish the legality of information circulation, the procedure for using telecommunications networks, the conditions for collecting and processing personal data, requirements for the dissemination of content in the online environment, and the principles of legality and reliability of information, objectivity and openness. In this regard, for criminological research, precise knowledge of the sectoral normative framework is especially important in determining the boundaries of an offense: unlawful behavior often arises where the boundary between permitted digital activity and acts prohibited by law becomes blurred.

The causal complex of offenses in this field is also complicated. On the one hand, the widespread dissemination of digital services, the expansion of mobile internet, and the development of online banking and remote identification have created a convenient environment for society. On the other hand, the accumulation of personal data, the digitalization of accounts and payment instruments, uneven levels of users' legal and digital literacy, insufficient cyber hygiene skills, the speed of dissemination of unlawful content and the transboundary circulation of content through foreign online platforms have complicated the criminogenic situation. In this sense, offenses in the field of informatization and communications are not a "by-product" of technological progress, but a consequence of social, legal and behavioral imbalances within digital society. The Scopus-indexed study by Kubanova and co-authors (2024) substantiates the interdisciplinary nature of combating cybercrime in the Republic of Kazakhstan and the need to consider it in connection with social security and economic stability [9]. The Scopus-indexed study by Halibiyati and co-authors (2024), based on the longitudinal Add Health sample covering 20 745 respondents, proved that indicators of adolescents' neuropsychological functioning are statistically significantly associated with arrest during minority and incarceration in adulthood [11]. This empirical conclusion provides a scientific basis for taking into account the cognitive and motivational characteristics of the subject when analyzing the determination of offenses in the information sphere.

From a victimological perspective, the victims of such offenses are extremely broad. They include ordinary citizens, consumers using digital services, business entities, state bodies, educational and healthcare organizations, as well as minors. Citizens most often suffer as a result of social engineering, false messages, fraudulent websites and applications, unlawful collection of personal data and account breaches. For legal entities, the main risks are the loss of commercial information, interruption of services, damage to business reputation and financial losses. Minors, meanwhile, should be considered a special victimological group, because they are more vulnerable to online pressure, cyberbullying, destructive content and digital manipulation. In Kazakhstan, the legal significance of this issue has been officially recognized: rules for considering applications concerning cases of cyberbullying against a child have been established through special legal norms [49].

The fourth direction is connected with victimological research. A.A. Nukusheva, B.Zh. Kuandykov and Zh. Zhailau, analyzing measures to counter cyberbullying among school-age children, show that minors are a particularly vulnerable group in relation to virtual violence, anonymous pressure and traumatic information that remains accessible for a long time [63]. A.Zh. Zhanaliyeva, B.T. Tleulesova and A.S. Koshkinbayeva, studying the mechanism for protecting the interests of the child in cyberspace, substantiate the insufficiency of children's legal protection in the information environment and the need to consider them as an independent object of protection [64]. A.B. Tursunov, E.N. Begaliyev and D.B. Malikov analyze the criminological aspects of violence and cruelty against children

and show that the victimological vulnerability of minors increases at the intersection of family, social and digital factors [65]. A.S. Moldagaliyeva, A.B. Smanova, M.T. Dosumbekova and G.K. Shulanbekova, by studying issues of protecting the rights of children who have become victims of violence, prove that a child's age characteristics, psychological vulnerability and limited access to legal protection mechanisms place the child in a special victimological category [66].

The fifth direction is devoted to the study of prevention and preventive measures. Aratuly and Baigazy, analyzing the methodology for investigating crimes in the field of information security, substantiate the special role of investigative and operational mechanisms in preventing offenses in this sphere [67]. Bazilova, through an analysis of measures for preventing computer crimes, demonstrates the importance of coordinated prevention at the state, sectoral and corporate levels [68]. Malikova and Omarova study the interaction between criminal policy in the field of information security and preventive measures, showing that their effectiveness depends directly on a preventive rather than a reactive orientation [69]. Dzhansarayeva, Malikova and Omarova, through an analysis of the concept of victimological counteraction, substantiate the special role of a victim-oriented approach in preventive work [70].

A comparative legal analysis of criminological approaches to offenses in the field of informatization and communications makes it possible to distinguish several interrelated groups of such offenses.

One group consists of offenses in the field of communications and information and communication services. This category includes the unlawful use of communications networks, fraudulent acquisition of telecommunications services, violation of the lawful operating procedure of communications operators and misuse of technical means to gain access to resources with restricted access. Article 212 of the Criminal Code of the Republic of Kazakhstan establishes liability for the unlawful modification of the state's electronic information resources [37]. Offenses in this category often have a transboundary character, because communications traffic crosses national borders and is carried out through foreign IP addresses, VPN services and anonymization tools.

Another group consists of platform-communication and media offenses. This category entered a clear legal framework after the adoption of Law No. 18-VIII of 2023 "On Online Platforms and Online Advertising" and Law No. 94-VIII of 2024 "On Mass Media" [48; 49]. It includes the dissemination of unlawful content on online platforms, placement of hidden advertising, use of fake reviews and bots, creation of intermediary accounts, digital manipulation, cyberbullying and online pressure against a child. In their study on the classification of cyberattacks, Kubanova and Serikov (2024) substantiate that such offenses rely on the specific features of platform architecture and that combating them requires the simultaneous use of technical and legal mechanisms [58].

Interim conclusion for this stage. The structural and typological analysis of offenses in the field of informatization and communications makes it possible to

divide them into six main groups according to their object, method of commission and criminogenic impact: offenses against information systems; offenses against personal data circulation; offenses in the field of communications and telecommunications; digital financial fraud; platform-media offenses; and offenses involving minors. This classification forms a methodological basis for moving, at subsequent stages, to an in-depth analysis of the determinant factors and victimological profiles of these groups. The existence of specific legal and technical features in each group indicates the need for specialized law-enforcement practice and adapted preventive measures.

The complex of determinant factors. In the modern digital environment of Kazakhstan, the emergence of offenses in the field of informatization and communications cannot be explained by a single cause. In criminological literature, such determinants are divided into several groups.

Technological determinants include the rapid development of digital infrastructure, the broad accessibility of mobile internet, the increasing complexity of online services, the spread of artificial intelligence and deepfake technologies, and the diversity and vulnerability of digital identification mechanisms. In the study by Kubanova and Serikov (2024) on the classification of cyberattacks, the role of various technical vulnerabilities in the emergence of offenses is analyzed in detail [58]. The specific feature of technological determinants is that they become more complex automatically over time: as each new technology appears, new scenarios for its misuse also emerge.

Legal and institutional determinants include the fragmentation of legislative regulation, the inconsistency of law-enforcement practice, weak interdepartmental coordination, the complexity of procedures for recording and assessing digital evidence, the limited nature of transboundary cooperation mechanisms and the lack of legal support for interaction with platforms. In the Scopus-indexed study by Satbayeva, Alimbetova and Beisenbayev (2024), which analyzes the experience of international cooperation in combating cybercrime, it is substantiated that such institutional shortcomings directly limit the effectiveness of the national legal system [39].

Criminogenic-market determinants include the formation of a cybercriminal ecosystem, the circulation of personal data and accounts on the black market, demand for dropper services, the development of hidden payment channels and the increasing complexity of the movement of illegal funds through cryptocurrency. The study by Useinova and co-authors (2025), which analyzes droppers as an instrument of cybercrime, comprehensively reveals the organized nature of such market mechanisms and the difficulties law-enforcement bodies face in disrupting them [59].

Victimological profile. The victim composition of offenses in the modern digital environment is very broad, but it has a number of specific features in its internal structure. The victimological approach regards the victim not as a passive object of the offense, but as a direct participant in the criminal event; the victim's behavior, social status, digital literacy and protective skills directly affect the

possibility of the offense being committed. Dzhanzarayeva, Malikova and Omarova (2018), analyzing the concept of victimological counteraction, substantiate the special role of a victim-oriented approach in preventive work [70].

According to the professional-functional criterion, bank employees, IT specialists, journalists and persons with access to state secrets constitute a special victimological category. They often become targets of targeted attacks, such as spear phishing and business email compromise.

Organization of the victimological chain. A significant part of modern digital offenses consists of several victimological stages. At the initial stage, a weakly protected user, often a citizen whose personal data have been leaked, receives the initial message; then psychological manipulation begins, pushing the person toward making a decision; at the final stage, actual financial or legal harm occurs. Understanding this chain from a legal perspective makes it possible to unite determinant factors and the victimological profile within a single logical framework. In the study by Moldagaliyeva, Smanova, Dosumbekova and Shulanbekova (2025), devoted to issues of protecting the rights of children who have become victims of violence, legal mechanisms for disrupting victimization chains are analyzed [66].

The determinant factors of offenses in the field of informatization and communications form a complex system manifested at technological, socio-economic, legal-institutional, psychological and criminogenic-market levels. The victimological profile is structured according to several internal criteria: age-demographic, socio-professional, digital-behavioral and professional-functional. The fact that pensioners account for 87% of the victimological composition clearly proves the need to orient preventive measures toward special groups. This analysis provides a basis, at subsequent stages, for a criminological assessment of the effectiveness of existing legal regulation and for formulating directions for improving legislation.

In the Republic of Kazakhstan, legal regulation countering offenses in the field of informatization and communications has become significantly more systematized in recent years. The current framework consists of the Constitution, the Law "On Informatization," the Law "On Personal Data and Their Protection," the Law "On Online Platforms and Online Advertising," the 2024 Law "On Mass Media," the Criminal Code of the Republic of Kazakhstan and other sectoral acts. From a formal perspective, this system covers information systems, personal data, the platform environment and digital communication, meaning that the formal scope of legal regulation is sufficiently broad. Therefore, the issue no longer lies in a legal vacuum as such, but in the extent to which these norms are capable of responding to the actual criminogenic situation.

Strengths of regulation. The first strength of legal regulation is that the main objects of encroachment in the field of informatization and communications are defined in legislation with sufficient clarity. The Law "On Informatization" establishes the logic of protecting information systems and electronic resources, while the Law "On Personal Data and Their Protection" creates a special regime for the

lawful circulation of personal information; the Laws "On Online Platforms and Online Advertising" and "On Mass Media" have brought new subjects of digital communication into the legal framework. This is significant progress compared with the previous fragmented regulation, because the platform, data and system that serve as the environment for committing offenses no longer remain outside legal assessment. Therefore, the normative structure itself has preventive potential.

Weaknesses of regulation. At the same time, a number of problematic areas that negatively affect the effectiveness of legal regulation remain.

Fragmentation of the normative structure. A number of relations remain at the intersection of several sectoral laws, blurring legal boundaries for the user. Unlawful encroachment on an information system, violation of the personal data regime, deception in online advertising, platform intermediation, damage to digital reputation and algorithmic manipulation are regulated by different acts, so neither the law-enforcement body nor the market participant always has a unified point of reference. Such normative fragmentation makes it difficult to provide precise legal qualification at an early stage of an offense.

Technological dynamics. In Kazakhstan, the scale of digital infrastructure and communications is expanding: from January to September 2024, the number of mobile communications subscribers with internet access exceeded 18.7 million, while the number of fixed internet subscribers exceeded 3.1 million [47]. Under such conditions, the forms of offenses also change rapidly: acts such as phishing, fake applications, imitation of voice or image, platform deception and influence through intermediary services do not always fit easily within the narrow wording of classical norms. Therefore, the formal existence of legal regulation does not automatically ensure its effectiveness; on the contrary, if norms operating in the digital environment are not constantly updated, they risk becoming technologically obsolete.

Effectiveness of the personal data protection regime. Current legislation establishes the subject's consent, the lawfulness of processing, protection measures and a system of restrictions. Law No. 44-VIII, which entered into force on 11 February 2024, introduced the obligation to notify of a data breach within 1 working day, a prohibition on collecting and storing copies of identity documents, except for AML/KYC purposes permitted by law, as well as inspection powers of the Committee for Personal Data Protection under the Ministry of Digital Development, Innovations and Aerospace Industry on the basis of a checklist consisting of 33 criteria [33]. However, from a criminological perspective, the weak point of this regime is that, in many offenses, the victim becomes aware of the illegal use of data only after it has already occurred. Here, the latency of the offense and the difficulty of proof are high. Thus, legal effectiveness in the field of personal data is determined not only by the text of the law, but also by the quality of organizations' actual logging, differentiation of permissions, recording of access history, immediate incident notification and compliance with state control.

Differentiation and proportionality of the institution of liability. Although the Criminal Code provides for unlawful access to information and other related elements of offenses, not all unlawful behavior reaches the criminal threshold. In the field of informatization and communications, a number of dangerous acts should also be restricted through administrative, civil-law or sectoral sanctions. In the current model, the systematic coordination of these intermediate sanctions has not been fully formed.

The legal and criminological assessment of the effectiveness of existing legal regulation is twofold. On the one hand, Kazakhstan has formed a fairly developed normative framework aimed at regulating modern digital relations and covering the main objects and subjects involved in countering offenses in the field of informatization and communications. On the other hand, its effectiveness is hindered by fragmentation, the difficulty of keeping pace with technological change, the complexity of law enforcement in the platform environment, latency in relation to personal data, the insufficiency of mechanisms for influencing intermediate dangerous behavior and uneven legal culture. These identified gaps provide a logical basis, at the next stage, for developing conceptual proposals to improve legislation.

Conceptual Proposals for Improving Legislation

The results of the analysis of the effectiveness of existing legal regulation clearly demonstrate the need to form specific conceptual proposals and practical law-enforcement guidelines. Therefore, stage 8 is not limited to general reasoning, but is presented in the form of systematic proposals aimed at improving the structure of existing legislation in accordance with the criminological nature of offenses in the field of informatization and communications.

The first proposal is to expand and clarify the legal content of platform liability. The Law "On Online Platforms and Online Advertising" introduced public relations involving online platforms into the legal field, while the Law "On Mass Media" redefined the rights and duties of subjects disseminating digital information. At the next stage, improvement of the legislation should be directed toward establishing not only general duties for platforms, but also special procedures concerning content and activity with a high risk of offenses: it is necessary to mark suspicious accounts, identify automated fake activity, require mandatory labeling of hidden advertising, establish urgent response periods for victims' complaints and introduce standards for procedural interaction with law-enforcement bodies. This will create conditions for stopping an offense at an early stage within the platform, rather than only punishing it afterward.

The second proposal is to reconsider the threshold between administrative and criminal liability and to supplement the system of sanctions affecting intermediate dangerous behavior. In the current model, a number of acts are assessed only through general rules, while behaviors such as platform-based fake activity, systematic damage to digital reputation, misleading consumers through hidden advertising and anonymous digital influence are not always distinguished with sufficient precision. In this regard, it is necessary to supplement the legislation on

administrative offenses with delicts specific to the information and communication environment, and, in cases that are repeated, organized or cause substantial harm, to clarify the mechanism for transferring such conduct to the criminal-law level. Such a differentiated model will make it possible to bring an offense within legal liability in accordance with the level of its public danger.

The third proposal is to unite legal policy against offenses in the field of informatization and communications within a single criminological concept. In the current regulatory system, although individual laws cover their own spheres, they are not all integrated into a common criminological architecture. Therefore, at the national level, it is proposed to develop a special conceptual document or comprehensive program section covering the main risks, subjects, vulnerable groups, statistical indicators and law-enforcement priorities of offenses in this field. This document would make it possible for legislative changes to acquire a systematic character based on a common strategy, rather than being incidental. The Artificial Intelligence Development Concept for 2024-2029 [38] and the Concept for the Development of Digital Transformation, the Information and Communication Technologies Sector and Cybersecurity for 2023-2029 [50] provide a strategic platform for integrating such a criminological section.

The fourth proposal is to deepen international cooperation. The transboundary nature of digital offenses means that national legal policy should not be limited to internal reforms alone. The UN Convention against Cybercrime, adopted by Resolution A/RES/79/243 of 24 December 2024, offers Kazakhstan a consistent international legal mechanism for working with transboundary digital evidence [41]. The Scopus-indexed study by Satbayeva, Alimbetova and Beisenbayev (2024) substantiates that interstate coordination directly affects the effectiveness of the national legal system [39]. The study by Sharipova, Aryn and Kuanaliyeva (2025), which analyzes international aspects of combating crime under conditions of globalization of the information society, substantiates the need for Kazakhstan's gradual adaptation to international standards [74].

After conceptual proposals have been developed, an important criterion for assessing their effectiveness is the degree of preparedness for new threats that may arise in the future. Offenses in the field of informatization and communications are not a static phenomenon; they take on new forms together with technological breakthroughs. Therefore, criminological analysis should not be limited to describing the current state of affairs, but should also consider the possibilities of forecasting future trends and preparing for them.

New forms of offenses in the era of artificial intelligence. The Concept for the Development of Artificial Intelligence for 2024-2029, approved by the Decree of the President of the Republic of Kazakhstan of 24 September 2024, defined Kazakhstan's strategic policy in this area [32]. The widespread dissemination of artificial intelligence technologies also shapes a new character of offenses. These include, in particular, voice and video modeling through deepfake technologies, the

use of chatbots for social engineering purposes, the mass production of phishing content through generative AI, the unlawful analysis of users' personal data through automated decisions, and the introduction of AI-generated forged documents into digital circulation. In the study by Zhaltyrbayeva, Dzhangabulova and Tlembayeva (2025), which analyzes the legal definition of the concept of artificial intelligence, it is noted that a consistent definition in this field has not yet been formed in Kazakhstan's legal doctrine [79]. Tlembayeva's study (2021), which examines approaches to the legal regulation of artificial intelligence, substantiates that theoretical and legislative foundations remain insufficiently developed, especially in matters of liability, legal subjectivity and risk assessment [80]. Through a comparative analysis of foreign experience in the legal regulation of personal data under conditions of AI, Umitchinova, Gavrilova and Menzyuk (2025) show that institutions such as the "right to explanation," liability for automated decisions, confidentiality guarantees when generative AI is used and algorithmic transparency are still developing in Kazakhstan [73].

Children's safety in digital space. As the experience of the EU, the United States and China shows, the digital safety of minors is becoming one of the main priorities of contemporary legal policy. In Kazakhstan, legal mechanisms in this area are developing, but it remains necessary to further clarify special regimes of platform liability toward child audiences, technical standards for content filtering and legal guarantees for parental control.

New formats of international cooperation. The UN Convention against Cybercrime of 2024 offers states unified mechanisms for working with transboundary digital evidence, the scope of mutual legal assistance and channels for operational cooperation [41]. For Kazakhstan, important directions include implementing this Convention, harmonizing it with national criminal procedure legislation and legislatively establishing mechanisms for creating international investigation teams.

The current pace of digital transformation requires forecasting the future development directions of offenses in the field of informatization and communications and developing legal mechanisms against them step by step. The misuse of artificial intelligence, the increasing complexity of digital financial services, the influence of platform algorithms on public opinion, the digital safety of minors and new formats of international cooperation constitute the main vectors of future threats. In these areas, updating the current legislative framework and deepening criminological research can move national legal policy to the forefront of technological development.

Structural and classificatory conclusions of the research. The six main groups of identified offenses, namely offenses against information systems; offenses against personal data circulation; offenses in the field of communications; digital financial fraud; platform-media offenses; and offenses involving minors, each require their own specific features and adapted legal mechanisms. This classification determines the

need for the future development of legislative policy to move from general solutions toward specialized regulation.

The study of the criminological foundations of offenses in the field of informatization and communications requires a comprehensive scientific analysis covering theoretical, historical-legal, empirical, structural-classificatory, victimological and conceptual levels. The effectiveness of legal protection in this field depends not only on the quality of legislative norms, but also on the institutional mechanisms for their implementation, digital literacy, international cooperation and victimologically oriented preventive work. The identified patterns constitute conceptual guidelines aimed at forming the strategic directions of legal policy in the digital era and strengthening the readiness of the national legal system for a new stage of technological transformation.

CHAPTER 2. COMPREHENSIVE ANALYSIS OF THE INSTITUTION OF LEGAL LIABILITY OF MINORS IN THE FIELD OF DIGITAL INFORMATION AND TELECOMMUNICATIONS IN THE REPUBLIC OF KAZAKHSTAN

2.1 Legal Status of Minors as Subjects of Legal Relations in the Field of Informatization and Communications

Under conditions of global digital transformation and the transition of the Republic of Kazakhstan to a qualitatively new stage in the development of the information society, the scientific understanding of the legal status of minors as special subjects of information legal relations is becoming one of the priority tasks of legal science. The modern information environment appears not merely as a means of communication, but also as a global living space that has become an inexhaustible source of knowledge and encompasses the political, social, economic and spiritual aspects of personal development [84]. From this perspective, minors in the Republic of Kazakhstan are turning from passive objects of state-legal protection into active and fully fledged participants in information circulation. This process requires a deep theoretical substantiation of their subject nature through the prism of their comprehensive participation in digital processes.

The place of minors as special subjects of the information society is determined by their unique socio-legal situation: according to paragraph 1 of Article 27 of the Constitution of the Republic of Kazakhstan, marriage and the family, motherhood, fatherhood and childhood are under the protection of the state, while in legal doctrine children are recognized as the highest value and future potential of the state [10]. It is precisely in the younger generation that the ethical and moral principles forming the basis for the future prosperity of the nation and the stable development of a rule-of-law state are shaped. The future of the Republic of Kazakhstan is directly connected with the formation of an intellectually developed and cultured society capable of critically analyzing and evaluating information flows. At the same time, adolescents' integration into the digital environment is accompanied by a high degree of vulnerability determined by age-specific psychology, limited life experience and an insufficient level of legal literacy.

In the system of information law, the scientific substantiation of the legal nature of minors requires a differentiated analysis of their roles as consumers and disseminators of information and as active users of modern technologies.

As consumers of information, minors exercise their fundamental right freely to receive information necessary for their comprehensive physical, intellectual, spiritual and moral development. However, the specific nature of their subject status in this role is reflected through the paradigm of the "protected subject," in which their autonomy of will is limited by the state's imperatives of ensuring information security. In the legal framework of the Republic of Kazakhstan, children's information security

is understood as the state in which children's rights and legitimate interests are protected from information harmful to their health and development.

The central instrument for regulating this role is Law of the Republic of Kazakhstan No. 169-VI of 2 July 2018 "On the Protection of Children from Information Harmful to Their Health and Development" [85]. This Law establishes strict requirements for the quality and accessibility of information products. The legal nature of the minor consumer is characterized by the existence of a normatively established "information filter" implemented through the mechanism of classifying products by age categories: "for children" (for children under six years of age), "from 6 years," "from 12 years," "from 14 years," "from 16 years" and "from 18 years." At the same time, information prohibited for dissemination among children imperatively includes information that incites suicide, antisocial actions, including the use of narcotic drugs, psychotropic substances and their precursors; justifies violence; contains obscene language; or is sexual in nature. Thus, the subject status of minors as consumers is limited in the interests of protecting their mental and moral health.

As active users of digital technologies, minors form a special legal reality and digital culture of society. The use of social networks, online games and artificial intelligence tools is becoming for them a predominant means of socialization and self-realization. In this aspect, their legal nature is manifested through intensive digital activity, which often outpaces the formation of mature legal consciousness. The vulnerability of minors as users is connected with the fact that, under the influence of peers with low legal culture or an aggressive social environment, they may commit unintentional offenses.

Systematic and comparative legal analysis, taking into account the experience of neighboring states where similar norms apply, makes it possible to conclude that the subject status of minors in information relations in the Republic of Kazakhstan has a complex and hybrid character. On the one hand, they have rights to development and access to information; on the other hand, they bear duties to comply with norms of information ethics and security. An important element of this system is the concept of children's information security, whose purpose is to protect young people from modern cyber threats while preserving opportunities for intellectual growth. State developments in this field have a significant influence on the formation of legal thinking by teaching adolescents to recognize risks and avoid unlawful behavior in internet space.

Within the structure of the subject nature of minors, a special place is occupied by the issue of the relationship between the minor's will and the actions of legal representatives, namely parents. In legal theory, it is noted that the marking of information products with age-category labels ("6+," "12+," and so on) should primarily serve as a signal for parents. This marking determines their behavioral model regarding the child's access to content. Scientific discourse points to the problem of "careless negligence" by legal representatives, in which disregard for age restrictions nullifies the effectiveness of state protection measures. In this regard,

ensuring minors' information security should be recognized as a common duty of the state, information-business entities and the family [13]. In the Republic of Kazakhstan, parents' right to control information education is supported by the possibility of public control and monitoring carried out by individuals and non-profit organizations.

Historical and legal analysis shows the evolution of the status of minors in information legislation: from the declarative proclamation of children's rights to the creation of detailed institutions for protection against destructive informational influence. In the Republic of Kazakhstan, this process has led to the formation of an institutional protection system involving authorized bodies in the fields of mass media, communications, education and internal affairs. The allocation of children's information security as an independent legal institution testifies to the recognition of the special legal nature of minors. This nature requires the combination of protective measures with the development of their individual responsibility.

Summarizing the consideration of the first stage, it should be noted that the legal status of minors in the information society of the Republic of Kazakhstan is not static. It is a dynamic legal category in which the features of a vulnerable object of protection and an active participant in information relations who is responsible for his or her actions within legally established procedures intersect.

Thus, in the information legal relations of the Republic of Kazakhstan, a minor is defined as a special subject with limited legal subjectivity. The minor's legal nature is characterized by a triad of roles: a consumer requiring imperative protection from harmful content in accordance with the norms of the Law of the Republic of Kazakhstan "On the Protection of Children from Information Harmful to Their Health and Development"; a disseminator who may bear potential administrative liability for the legality of disseminated information; and an active user who needs an increased level of legal culture. The scientific substantiation of this status is based on the need to achieve a balance between measures of state coercion and educational and upbringing initiatives. The identified special character of minors' subject status forms the necessary theoretical basis for further study of the mechanisms of their legal liability for offenses in the field of information security, which becomes the object of systematic analysis at the next stage of this work.

Within the systematic study of the legal status of minors under conditions of digital transformation in the Republic of Kazakhstan, differentiation between the categories of information legal capacity and capacity to act is becoming a key direction of scientific and theoretical analysis. Legal subjectivity in the digital environment is a complex dynamic construction in which traditional civil-law categories undergo qualitative changes under the influence of the specific features of information relations. Legal capacity, understood as the abstract possibility of possessing information rights, and capacity to act, understood as the ability to exercise these rights through one's own actions, are characterized in the context of minor participants by incompleteness and by the gradual expansion of the scope of powers as a certain age is reached.

In the Republic of Kazakhstan, minors' information legal capacity arises from birth in accordance with paragraph 2 of Article 13 of the Civil Code of the Republic of Kazakhstan and includes the potential possibility of being a subject of rights to personal data protection, access to cultural values and receipt of information contributing to the harmonious development of the person. However, unlike general civil legal capacity, children's information legal capacity has a "targeted" and "protective" character. It is determined not only by the fact of the subject's existence, but also by the state's recognition of the need to ensure the child's information security, that is, the state of protection of the child's rights and legitimate interests from destructive content. This feature confirms the thesis that a child's information legal capacity is not absolute and is corrected by imperative norms aimed at reducing risks in digital space.

The transition from abstract legal capacity in the information sphere to active capacity to act takes place in stages, which is reflected in the system for classifying information products by age. According to Article 9 of Law of the Republic of Kazakhstan No. 169-VI of 2 July 2018 "On the Protection of Children from Information Harmful to Their Health and Development," the legislator distinguishes several stages in the "maturation" of an information subject, each of which expands the limits of the subject's capacity to act [85]. This stratification is based on the psychophysiological characteristics of information perception and on the child's ability to understand the social consequences of interaction with content. The categories "for children" (for children under 6 years of age), "from 6 years," "from 12 years," "from 14 years" and "from 16 years" are not merely censorship barriers, but also markers of the gradual formation of the subject's delictual capacity in the digital environment.

Analysis of the limits of legal subjectivity in the digital environment makes it possible to distinguish the category of information capacity to act of "young children" under 12 years of age. At this stage, capacity to act is very limited: the child is recognized mainly as a consumer of "safe" content whose substance should reflect the "victory of good over evil" and should be free from depictions of violence, death or fear. The scientific basis for such a restriction is that, at this age, the child's psyche has not yet formed sufficient protective mechanisms for critically evaluating negative information. Legal subjectivity here is implemented almost entirely through the will of legal representatives, who act as a "filter" between the information environment and an as-yet-unformed consciousness.

Upon reaching the ages of 12 and 14, information capacity to act expands significantly. Kazakhstani legislation allows access to products containing depictions of accidents and disasters, and from the age of 14, episodic descriptions of the use of narcotic drugs, psychotropic substances or tobacco products in a context condemning them. At this age interval, a qualitative shift occurs: the minor moves from being a passive consumer to an active user capable of perceiving complex social phenomena, including antisocial acts, provided that they are properly interpreted. However, legal

subjectivity remains "controlled," because the state requires the mandatory presence of age-category labels on products, thereby preventing uncontrolled access to "18+" content.

In the Republic of Kazakhstan, the legislative foundations of legal capacity in access to internet resources are based on the principle that restrictions on children's rights are permissible for the purpose of protecting them. The norms of the Law of the Republic of Kazakhstan "On the Protection of Children from Information Harmful to Their Health and Development" regulating the dissemination of information through information and telecommunications networks establish special requirements for telecommunications networks, including the Internet. The child's legal capacity in the global network is limited by the obligation of providers and persons granting access to use administrative, organizational, technical and software-hardware means to block prohibited content. This creates a unique legal situation: *de jure*, the child has the right of access to information; *de facto*, the exercise of this right is possible only within the "safe perimeter" created by the state and business.

The comparative legal method makes it possible to identify similar trends in the legislation of neighboring states, where basic laws on information security also structure children's legal subjectivity through age categories and technical restrictions. The introduction of concepts of children's information security emphasizes the importance of forming legal thinking as a method of exercising information capacity to act. At the same time, the Kazakhstani model demonstrates clear centralization of control through authorized bodies in the field of information and communications, which monitor compliance with age censorship in telecommunications networks.

The role of legal representatives in the exercise of children's information capacity to act remains one of the most discussed issues. Although, under the Code of the Republic of Kazakhstan "On Marriage (Matrimony) and Family," parents are obliged to care for the moral development of the child, legislation often lacks direct mechanisms compelling parents to control children's digital activity. In legal theory, this creates a "gray zone": the state labels information, but outside public places the decision to admit the child to this information is made by parents. Thus, a minor's information capacity to act is in practice supplemented by the will of the minor's parents, which requires combining the efforts of the family and the state in order to prevent "careless negligence."

Concluding the analysis of information legal capacity and capacity to act, it should be noted that they constitute an instrument for the gradual integration of the person into digital society. The restrictions introduced by Law of the Republic of Kazakhstan No. 169-VI are not a suppression of rights, but rather a necessary condition for the formation of healthy legal consciousness. A systematic approach to determining age restrictions makes it possible to maintain a balance between freedom of information and the protection of children's life and health, which is recognized as a priority of state policy.

Thus, the analysis of minors' information legal subjectivity in the Republic of Kazakhstan has revealed its staged character, in which the scope of rights and duties is directly proportional to the subject's age category. Information legal capacity, which arises from birth, is supplemented by the gradual expansion of capacity to act, reaching its maximum by the age of 18. The legislative framework, in particular Law of the Republic of Kazakhstan No. 169-VI and the CAO RK, ensures the protection of children in the digital environment through technical filters and age-based labeling; however, the effectiveness of this system largely depends on the level of legal culture in the family and society. The identified features of legal capacity and capacity to act lay the theoretical foundation for moving to the third stage of the research: a detailed analysis of the grounds and procedure for bringing minors to legal liability for offenses in the field of information security.

The right of minors to receive information is regarded in the national legislation of the Republic of Kazakhstan as a basic guarantee of their intellectual and social development. According to Article 1 of Law of the Republic of Kazakhstan No. 169-VI of 2 July 2018 "On the Protection of Children from Information Harmful to Their Health and Development," children's access to information is defined as "children's right freely to receive and disseminate information products intended for children" [85]. This norm is consistent with the main purpose of legislation in this field, namely the regulation of public relations arising in connection with the exercise of children's rights to receive and disseminate information. In scientific and academic discourse, this right is interpreted not as absolute freedom, but as "controlled access," in which the scope of the subject's rights expands in proportion to the subject's age category and level of mental maturity.

A systematic analysis of the legal category "information product intended for children" makes it possible to conclude that the legislator connects the right to receive information with the qualitative characteristics of content. A product must correspond to a specific age group in terms of its direction, subject matter and design. Thus, in the Republic of Kazakhstan, the right of access to information is closely connected with the duty of subjects of information circulation, namely producers and distributors, to carry out age classification before dissemination begins. This creates a unique legal construction in which the child's subjective right to information is limited by the objective need to protect the child from destructive content capable of harming the child's moral and physical health.

Ensuring minors' information security is the second key element of the system of their rights in the digital environment. Kazakhstani legislation defines children's information security as "the state of ensuring the protection of children's rights and legitimate interests from information harmful to their health and development." The scientific significance of this category lies in its comprehensive nature: it includes legal, organizational and technical measures. Among the state's priority tasks is the creation of conditions preventing minors' access to information that incites suicide, provokes antisocial actions, contains obscene language or is sexual in nature.

In the era of Big Data, the right to privacy in cyberspace and the protection of minors' personal data are among the most vulnerable aspects. The global Internet stores enormous amounts of users' personal information, which often becomes the object of unlawful dissemination. Research shows that, because of the broad accessibility of networks and a low level of legal culture, minors themselves often initiate the publication of compromising information about themselves or their peers. The scientific substantiation of protecting children's online private life is based on recognition of their right to confidentiality, which should be ensured not only by technical filters, but also by the formation of a high level of digital literacy.

Analysis of the compliance of the national legislation of the Republic of Kazakhstan with international conventions makes it possible to conclude that legal norms are highly harmonized. According to Article 3 of Law of the Republic of Kazakhstan No. 169-VI, if an international treaty ratified by the Republic establishes different rules, the rules of the international treaty apply. This confirms Kazakhstan's adherence to the principles of the UN Convention on the Rights of the Child, ratified by Resolution No. 77-XIII of the Supreme Council of the Republic of Kazakhstan of 8 June 1994 [87]. While proclaiming the child's right to seek, receive and impart information (Article 13), the Convention also obliges states to develop appropriate guidelines for protecting the child from information injurious to his or her well-being (Article 17). The principle established in Kazakhstani law of taking into account children's psychological and age characteristics and their vulnerability to the negative influence of the information environment fully corresponds to international standards.

At the same time, the legislation of the Republic of Kazakhstan actively develops the principles of international cooperation in the field of protecting children from information harmful to their health. The comparative legal method shows that Kazakhstan is following the path of creating specialized legal institutions that ensure the information security of young people. The introduction of public control mechanisms that allow individuals and non-profit organizations to conduct monitoring and identify violations in cyberspace also corresponds to global practice in involving civil society in the protection of children's rights.

An important aspect of systematizing rights is the distribution of competences among state bodies that ensure the exercise of minors' rights in the field of communications and informatization. In the Republic of Kazakhstan, control functions are distributed among authorized bodies in the fields of mass media, communications, education and internal affairs. Such a polycentric model makes it possible to ensure the right to information security in all segments of digital space, from traditional mass media to telecommunications networks. A special role is assigned to the Government in developing the main directions of state policy, which determines the strategic character of this field.

In the context of scientific understanding of the issue, the role of legal representatives in the system of minors' rights cannot be ignored. Legal theory emphasizes that age-category labels on information products should serve precisely as

a signal for parents and determine their behavior regarding the child's access to content. The underdevelopment of effective mechanisms of parental responsibility for information education is recognized by the scientific community as a factor reducing the effectiveness of legislative guarantees. For the full exercise of minors' rights, a balance is needed between state regulation and the active participation of the family in teaching children safe online behavior.

Summarizing the above, it may be stated that the system of rights and freedoms of minors in the field of informatization and communications in the Republic of Kazakhstan is a dynamically developing body of law. It is based on the fundamental recognition of the child as an active subject of the information society, whose right to receive information is balanced by strict measures to ensure security and protect private life.

Within an in-depth scientific and legal analysis of the subject nature of minors, the study of legal mechanisms aimed at reducing the risks of destructive informational influence is of principled importance. Under current conditions, information security is defined as the state of protection of information and the infrastructure supporting it from accidental or intentional impacts that may result in harm to subjects of information relations. For minors, whose vulnerability is determined by age-specific psychology and insufficient life experience, the creation of such mechanisms is not only a legal but also an important social duty of the state. A systematic approach to protecting children in the digital environment requires a coherent unity of legislative prohibitions, technical filtering tools and measures to improve young people's legal literacy.

The central element of the legal protection mechanism in the Republic of Kazakhstan is the implementation of the provisions of Law of the Republic of Kazakhstan No. 169-VI of 2 July 2018 "On the Protection of Children from Information Harmful to Their Health and Development" [85]. This normative act, similar to advanced international practices and the experience of neighboring states, laid an unprecedented legal foundation for protecting minors from the destructive influence of the information environment and preserving their moral health. The scientific meaning of this mechanism is based on the definition of "information harmful to the health and development of the child," which, under the law, means information prohibited or restricted for dissemination among children. This allows the state to create a differentiated protection system that takes into account the dynamics of the person's psychophysiological maturation.

The scientific characterization of the legal foundations for classifying information products provides for dividing the entire information flow into two fundamental categories: information completely prohibited for dissemination among children and information whose dissemination is limited by certain age boundaries. The first category includes materials that encourage life-threatening acts, the use of narcotic drugs, psychotropic substances and their precursors, justify violence or contain obscene language. The second category includes information that may be

consumed only upon reaching a certain age at which adolescents' legal culture and level of intellectual development allow them adequately to analyze and critically perceive the information received.

An important component of this mechanism is the regulation of the circulation of information products, which includes their presentation and dissemination, including sale, rental, public display and placement in information and telecommunications networks, including the Internet. The legal requirement of mandatory age classification before the circulation of products begins is a preventive measure aimed at preventing the child's initial contact with harmful content. The marking of information products with special labels acts as a "social signal" that determines the behavior of legal representatives regarding the child's access to specific information. From a scientific perspective, this mechanism is designed to compensate for the minor's insufficient life experience through an authoritative expert conclusion regarding the safety of content.

Alongside classification, content filtering in the information environment appears as an important mechanism. Legislation imposes on persons organizing internet access in places accessible to children the obligation to use administrative, organizational, technical and software-hardware protection tools. This measure is aimed at creating a "safe perimeter" in educational institutions, libraries and other public spaces. In science, content filtering is regarded as a means of technical support for legal norms that makes it possible automatically to detect and block cyber threats and to analyze big data in order to identify suspicious user activity. At the same time, communications operators are often exempted from liability if access is organized on the basis of written contracts, which reflects the targeted nature of the filtering obligation for final service providers in children's institutions.

Strategic planning, reflected in the development of specialized concepts of children's information security, plays a special role in the protection system. The main purpose of such documents is the comprehensive protection of minors from information threats in the modern digital environment through the formation of legal thinking. State initiatives in this field contribute to children's ability independently to recognize cyber threats and avoid offenders in internet space. This shifts the legal mechanism from the level of external prohibitions to the level of the minor subject's internal convictions and digital hygiene.

Despite the existence of a developed normative framework, systematic analysis reveals the problem of "careless negligence" on the part of legal representatives. Ensuring information security is currently often recognized as a duty of the state and business entities, while the role of the family is not adequately assessed at the legislative level. Parents' disregard for age labels, for example when watching films with children, significantly reduces the effectiveness of the state protection mechanism. The scientific community emphasizes that even if distributors of information strictly comply with all legislative requirements, without active parental control the child's health and development remain unprotected. This creates the need

to combine the efforts of public authorities and civil society in order to form a culture of responsible parenting in the digital sphere.

In the context of administrative law, the implementation of protection mechanisms is supported by measures of legal liability. Article 456 of the Code of the Republic of Kazakhstan on Administrative Offenses ("Violation of the legislation of the Republic of Kazakhstan on the protection of children from information harmful to their health and development") provides appropriate sanctions for violation of the established requirements for the dissemination of information products or for failure to use filtering tools [86]. In addition, by establishing liability for placing advertisements involving minors in the production of content that does not correspond to their age, the legislator limits the possibility of involving children in the creation of harmful products. Such comprehensive prohibitions create a multi-level system for protecting children's rights in information space.

Thus, the study of legal protection mechanisms in the Republic of Kazakhstan confirms their systematic character, based on the imperative requirement of age-based classification of all information products and the mandatory use of filtering tools in places where children access the Internet. The scientific basis of these mechanisms rests on recognition of the priority of minors' moral and mental health over unlimited freedom of information. However, the effectiveness of legislative measures is directly connected with the level of legal culture of legal representatives, whose participation is a necessary link in the implementation of the state's protective functions. The formed theoretical basis of legal protection mechanisms makes it possible to move to the concluding stage of the research: analysis of the specific features of bringing minors to legal liability for offenses in the field of information security.

During the period of Kazakhstan's independence, the scientific evolution of legislation in the field of protecting children from information passed through several main stages. The initial stage (1991-2002) was characterized by the absence of specialized norms and relied on general guarantees of human rights. According to Article 20 of the Constitution of the Republic of Kazakhstan, adopted on 30 August 1995 and forming the foundation of the entire legal system, everyone has the right freely to receive and disseminate information by any means not prohibited by law. During this period, children's information rights were considered mainly through the prism of the general right to education and development.

The second stage (2002-2017) was marked by the adoption of Law of the Republic of Kazakhstan No. 345-II of 8 August 2002 "On the Rights of the Child in the Republic of Kazakhstan." At this stage, norms on information security began to be introduced fragmentarily into sectoral legislation, namely laws on mass media and communications. However, the absence of a unified conceptual apparatus and precise criteria for the harmfulness of information created legal gaps that did not allow effective responses to the challenges of the digital era.

The current stage, beginning in 2018 and continuing to the present, is characterized by the institutionalization of children's information security as an

independent direction of state policy. The main act of this stage is Law of the Republic of Kazakhstan No. 169-VI of 2 July 2018 "On the Protection of Children from Information Harmful to Their Health and Development" [85]. This law consolidated scattered norms and introduced a scientifically grounded system of age-based classification, which was a response to qualitative changes in the media environment.

The main purpose of the current Law is to regulate public relations arising in connection with the exercise of children's rights to receive and disseminate information, while ensuring their protection from harmful influence. The legislator placed at the foundation of the act the principles of systemacity, the comprehensive nature of state measures and mandatory consideration of minors' psychological and age characteristics. It is noteworthy that the Law recognizes the permissibility of restricting children's rights freely to receive information if such information is found to be harmful to their health and development.

Scientific analysis of the conceptual apparatus of the Law makes it possible to distinguish the category of "children's information security," which is defined as the state of ensuring protection of minors' rights and legitimate interests from destructive information. In turn, "children's access to information" is interpreted as their right freely to receive and disseminate products corresponding precisely to their age category. "Information product" means the product of mass media, as well as other audiovisual and printed products intended for an unlimited circle of persons.

The age-based classification system established in Article 9 of the Law is the central protection mechanism and includes six categories: "for children" (for children under 6 years of age), "from 6 years," "from 12 years," "from 14 years," "from 16 years" and "from 18 years." The classification process involves assessment of the subject matter, genre and probability of causing harm to the child. For example, a product "for children under 6 years of age" must contain the idea of the victory of good over evil and condemnation of violence, while the "from 14 years" category permits episodic depiction of harmful habits, such as smoking and the use of alcohol or drugs, only on condition that they are condemned.

Legislation attaches special importance to information prohibited for dissemination among children, the "18+" category. It includes information that incites suicide, antisocial actions or the use of narcotic drugs, justifies violence, contains obscene language, or is sexual in nature. The Law strictly prohibits the dissemination of such products among minors, with the exception of the Internet, to which special technical rules apply.

Mechanisms for implementing protection in the media space include the mandatory use of age-category labels. On television channels, such a label must be displayed throughout the entire period of broadcasting the product. A time restriction is established for television and radio broadcasting: products in the "from 18 years" category may not be disseminated from 6:00 to 22:00 local time. When information is disseminated through telecommunications networks, including the Internet, persons

providing access, for example in schools or internet cafes, are obliged to use hardware-software complexes for content filtering.

The system of state regulation in this field has a multi-level character. The Government of the Republic of Kazakhstan develops the main directions of state policy. The authorized body, namely the central executive body, forms policy, approves classification rules and requirements for age-category labels. Sectoral control is distributed among authorized bodies in the fields of mass media, communications, education and internal affairs. Internal affairs bodies, in particular, supervise compliance with legislation when products are directly disseminated to minors.

An important element of the current stage is the introduction of the institution of public control. Individuals and non-profit organizations have the right to monitor the dissemination of information, identify violations and inform state bodies about them. In addition, they have the right to train parents in skills for controlling children's access to information in the digital environment.

The evolution of legislation continues through a system of amendments. For example, certain editorial changes have been introduced into the Law, and a number of powers of state bodies were clarified in 2023-2025. These changes reflect the dynamic adaptation of the legal framework to new technological challenges and the need to clarify intersectoral coordination.

Thus, the formation of protection of minors' information rights in the Republic of Kazakhstan has passed from constitutional declarations to the creation of a specialized legal regime established in Law No. 169-VI of 2 July 2018. The scientific significance of this evolution lies in the transition to a risk-oriented approach, in which the child's right to receive information is balanced by a strict system of age censorship, labeling and state-public control. The legislation of the Republic of Kazakhstan in this field is based on the priority of protecting children's health while preserving access to developmental content, thereby laying a solid foundation for further improvement of mechanisms of legal liability for information delicts.

Legal liability in the field under consideration appears as "one of the main means of ensuring children's information-psychological security" [21]. At the same time, information-psychological security is interpreted in scientific literature as the state of protection of minors' individual psyche from negative psychological influence during the circulation of harmful information. The specific features of legal liability in this context are determined by "the mental and social immaturity of such offenders" and by their lack of life experience for "objectively assessing the social significance of their actions" [88].

In the Republic of Kazakhstan, minors' administrative liability in the information sphere arises upon reaching the age of sixteen, in accordance with Article 65 of the Code of the Republic of Kazakhstan on Administrative Offenses [86]. Scientific analysis of offenses in the field of information security makes it possible to identify their main features: they are culpable unlawful acts, encroach on the established

procedure for ensuring children's safety and entail appropriate sanctions. In the context of administrative-delict law, the "three-level system of harmful information" is of particular importance, including information that is:

- inconsistent with age;
- prohibited for dissemination among minors;
- prohibited for dissemination regardless of age, such as extremism and child pornography.

A comparative legal analysis of Kazakhstani legislation with similar norms of other states shows the similarity of approaches to defining the objective side of offenses. The objective side includes violation of requirements for the dissemination of information products, failure to use technical means of protection and involvement of children in the creation of harmful content. In Kazakhstan, such elements are established in Article 456 of the CAO RK [86]. Scientific discourse points to the need to eliminate "terminological redundancy" in describing information processes in the law and proposes the unified use of the categories "transmission" and "dissemination."

An important aspect of administrative liability is subject composition. If general measures apply to minors themselves from the age of 16, responsibility in relation to younger persons is often imposed on legal representatives. However, researchers note the "insufficiency of legal mechanisms" obliging parents directly to ensure the child's information security [89]. In situations of "careless negligence" by parents who ignore the product's age label, state protection measures lose their effectiveness. Science substantiates the need to introduce administrative liability of parents for allowing children to consume content that does not correspond to their age category.

Criminal liability for cybercrimes and unlawful acts in social networks is characterized by strict age limits and conditions. According to Article 15 of the Criminal Code of the Republic of Kazakhstan, the general age of criminal liability is 16 years, but for a number of serious crimes, including crimes that may be committed using information technologies, such as rape, kidnapping, incitement of social, national, clan, racial, class or religious hatred, and sabotage, liability begins at the age of 14 [90]. Criminal law regards the minor as an object of "enhanced legal protection," which determines the specific features of work with the minor.

The specific features of minors' criminal liability in cyberspace are connected with the fact that their actions are often the result of a "set of adverse life circumstances" or the influence of adult offenders. Chapter 6 of the Criminal Code of the Republic of Kazakhstan defines "Specific Features of Minors' Criminal Liability," which orients law-enforcement practice not toward repression alone, but toward methods of educational influence. Court proceedings in such cases should contribute as much as possible to the adolescent's "social adaptation."

When imposing punishment for cybercrimes such as unauthorized access to information or dissemination of malicious programs, courts are obliged to take into account "the level of physical, intellectual and psychological development of the

adolescent." The list of punishments for minors, according to Article 81 of the CC RK, is much narrower than the general list: for example, the law restricts the use of deprivation of liberty for persons under the age of 16 who have committed a minor or medium-gravity crime for the first time. The scientific trend toward "humanization of criminal policy" provides for replacing punitive influence with alternative measures of an educational nature.

The special subject nature of liability in social networks is manifested through the exercise of information rights and duties. As active users of technologies, adolescents often do not perceive the boundary between freedom of expression and unlawful behavior, such as defamation, incitement of hatred or insult. From a scientific perspective, the use of information and telecommunications technologies, including the Internet, should be considered an aggravating circumstance in view of the scale of potential harm. Bringing adolescents to liability for their actions on social networks requires proof in the case, including examination of internet pages and computer equipment.

The procedural specificity of proceedings in cases involving minors also determines their special subject status. Procedural stages should have separate tasks aimed at protecting the child's interests. A significant role is played by specialized subdivisions for juvenile affairs within internal affairs bodies, which conduct preventive work not only with children but also with their parents. Effective combating of offenses requires combining the efforts of authorities and civil society to eliminate the causes contributing to adolescent delinquency online.

Historical and legal analysis shows that the liability system has developed from general regulation toward specialization of norms. The current stage is characterized by the establishment of "administrative-prejudicial connections," under which repeated administrative offenses in the information sphere may be transformed into criminally punishable acts. This shows the preventive importance of timely administrative liability as a means of correcting a "criminal personality" at an early stage.

In conclusion, it should be noted that in the Republic of Kazakhstan minors' legal liability for information offenses is a complex legal institution combining elements of state coercion and socio-pedagogical correction. The age limits of 14 and 16 years and the conditions of liability are based on recognition of the subject's psychophysiological specificity and the priority of correction. The comparative legal method confirms the need for further development of legislation in terms of strengthening the responsibility of legal representatives and improving procedural tools for recording offenses in cyberspace.

Thus, the study of the specific features of minors' legal liability has revealed its differentiated character depending on the gravity of the information offense and the subject's age. In the administrative sphere, the main protection mechanism is Article 456 of the CAO RK, which is aimed at suppressing the circulation of harmful content. Criminal liability emphasizes educational influence and humanization while limiting

the use of strict punitive measures. Scientific analysis has proved that the effectiveness of liability in the digital environment is directly connected with the level of legal culture and the proper performance of duties by parents. The conclusions obtained complete the comprehensive study of minors' subject status in information legal relations and form a theoretical basis for practical recommendations on improving the legislation of the Republic of Kazakhstan in the field of information security.

In the modern system of administrative and information law of the Republic of Kazakhstan, law-enforcement practice in relation to minors appears as an indicator of the effectiveness of state protection mechanisms and of the correction of young people's behavior in the digital environment. Scientific analysis of the activities of law-enforcement bodies and courts makes it possible to conclude that information disputes involving minors are characterized by a high degree of complexity because of the specific subject composition and the dynamism of digital technologies. The institutionalization of minors' administrative liability is considered in dissertation research as a special legal relation, within which rights and duties established by the state are implemented in connection with the commission of delicts by subjects aged from 16 to 18.

The activities of law-enforcement bodies, namely internal affairs bodies, in resolving information disputes and suppressing offenses by minors are based on the exercise of administrative-jurisdictional powers, the scope of which is differentiated depending on the purposes of procedural actions [91]. The main problem of current practice is that all work with adolescents is entrusted only to specialized juvenile affairs subdivisions and temporary detention centers, which often reduces the overall effectiveness of rapid response to threats in information space. At the same time, internal affairs bodies have the right to draw up protocols, carry out detention and apply other measures to secure proceedings, but the absence of precise regulation of the procedure for applying them specifically to minors as special subjects creates uncertainty in law enforcement.

Judicial practice and the activities of commissions for juvenile affairs show the existence of systemic problems in the field of jurisdictional competence over information disputes. Researchers emphasize the inefficiency of "multiple jurisdiction," where cases are considered by commissions, internal affairs bodies, judges and transport authorities, which leads to the delimitation of powers and delays in case consideration. In the activities of commissions for juvenile affairs, non-compliance with the principles of promptness and inevitability of punishment in many cases results in the actual release of guilty persons from liability, thereby nullifying the importance of educational influence. In this regard, the scientific and academic community substantiates the need to grant special powers to judicial bodies for considering this category of cases or to create specialized courts for juvenile affairs, that is, juvenile justice. An important step in this direction is the establishment of

specialized interdistrict juvenile courts, as provided for in Article 27 of the Civil Procedure Code of the Republic of Kazakhstan.

Assessment of the effectiveness of legal liability in cases where adolescents commit information offenses shows a low level of achievement of the purposes of punishment. Of the spectrum of sanctions provided by legislation, in practice only warnings and administrative fines are often applied, and the latter are frequently paid not by the offender himself or herself, but by the legal representatives. Such practice eliminates achievement of the individual preventive purpose of administrative-law sanctions, because the adolescent does not experience the direct negative consequences of his or her actions. In addition, the failure to establish educational effectiveness as a purpose of liability in legislation and the unformed scale of values among modern adolescents prevent them from deeply understanding their guilt before society.

The special subject nature of minors' liability in the information sphere is determined by the imbalance between their external "adulthood" and internal psychological immaturity. Despite the expansion of the level of information awareness, modern adolescents are prone to "intellectual deceleration," which leads to the commission of offenses for the purpose of imitating immoral models of behavior disseminated through media resources or for self-assertion. In such cases, liability can arise only when the subject is aware of the actual nature and social significance of his or her actions, which requires the law enforcer to take adolescent psychology deeply into account and to apply the principle of humanization. At the same time, the status of being a minor should not itself serve as an unconditional basis for exemption from liability, because this would violate the principle of its inevitability.

The procedural features of implementing liability in the field of information relations require modernization of existing coercive measures. In cases connected with adolescents being intoxicated in the process of committing information delicts, it is proposed to expand the grounds for referral to medical examination in order to improve the reliability of the evidentiary base. Scientific literature also substantiates the need to clarify the terminology of securing measures: for example, replacing the term "personal inspection" with "administrative personal search" in order to clarify the actions of police officers when instruments of an offense are found. Notification of parents about any procedural securing measure applied to a child should be a mandatory element of practice, consistent with their duties to protect the minor's interests.

Analysis of law enforcement in the context of information security reveals not only the need to suppress offenses already committed, but also the acute need to prevent an antisocial lifestyle. Preventive activities of internal affairs bodies should be built on interaction with education, guardianship and social protection bodies, while commissions for juvenile affairs may serve as a coordinating link. Law of the Republic of Kazakhstan No. 591-II of 9 July 2004 "On the Prevention of Juvenile Delinquency and the Prevention of Child Neglect and Homelessness" lays the legal

foundation for this activity. The main vector for improving practice is recognized as the transition from combating "criminality" to correcting the person's "lifestyle," which requires the development of new legal acts taking into account international standards for the protection of children's rights. The effectiveness of jurisdictional activity directly depends on the existence of a reliable mechanism for coordinating the efforts of all subjects of the prevention system.

The comparative legal method of analyzing the practice of the Republic of Kazakhstan and neighboring states confirms the common nature of problems in the field of juvenile administrative delinquency. The legislator is moving toward strengthening guarantees of minors' rights, including by restricting the application of measures such as administrative arrest and recognizing minority as a mitigating circumstance. However, practice shows that, where an offense is of minor significance, commissions often apply measures of influence such as apology, reprimand or placement under supervision that do not always correspond to the gravity of the act and do not contribute to the offender's correction. The imperfect legislative regulation of these measures and their duplication with types of administrative punishment complicate the consistency of law enforcement.

Thus, the study of law-enforcement practice in information legal relations has revealed a critical imbalance between formally established measures for protecting minors and the actual effectiveness of their implementation. The activities of law-enforcement bodies and courts are complicated by insufficient specialization of justice in relation to adolescents and by the ineffectiveness of fine sanctions paid by parents. The scientific substantiation of reforming practice is based on the need to introduce the principle of inevitability of liability, grant the police powers to provide real social assistance to adolescents and integrate an educational component into every procedural action. The conclusions obtained emphasize that, without modernization of procedural tools and strengthening the role of specialized judicial bodies, the protection of children's rights in digital space will remain declarative, which requires a transition to systemic changes in legislation.

Scientific analysis shows that the legal status of minors in the digital environment remains fragmentary because of the insufficiency of forms of preventive activity. Existing mechanisms such as preventive registration and supervision established by Law of the Republic of Kazakhstan No. 591-II of 9 July 2004 "On the Prevention of Juvenile Delinquency and the Prevention of Child Neglect and Homelessness" are mainly oriented toward physical neglect, while "digital neglect," meaning the absence of control over a child's online activity, remains outside the area of systematic legal regulation. The problem is complicated by the insufficiency of legally established mechanisms of influence for preventing deviant behavior by family members who directly affect the child. In disadvantaged families, parents often cannot demonstrate a model of lawful behavior on the Internet, which encourages children to commit information offenses.

Analysis of the influence of internet addiction and of the gap between technology and law reveals a deep problem of inconsistency between the principles of preventive activity and current reality. It is considered that, in carrying out any preventive activity in the information sphere, priority should be given to minors' rights and legitimate interests. In practice, however, children's digital rights, including the right to privacy, data protection and access to developmental content, often become victims of the algorithmic interests of global platforms. Technological development makes it possible to create addictive interfaces that contribute to the development of internet addiction, while legal regulation in this field is limited to a general prohibition on harmful information and does not systematically address the psychological aspects of adolescents' involvement in the virtual environment.

The gap between technological development and legal regulation is manifested in the inability of state bodies promptly to identify new models of destructive behavior online. Although official statistical data show that the total number of criminal offenses committed by minors in the Republic of Kazakhstan has decreased significantly by 55% since 2013, they also indicate that identifying the informational component of delicts is becoming increasingly difficult [93]. At the same time, the significant increase in the number of administrative offenses for improper performance of duties relating to the upbringing of children in recent years, as well as the increase in cases of children being without adults at night, indirectly indicate a high level of "digital neglect." In 2025, more than 4.1 thousand meetings of commissions for juvenile affairs were held in the Republic of Kazakhstan, which is 3.7% more than in the previous year and proves an increase in the volume of preventive work [94].

The law-enforcement system often faces a situation in which the digital means of committing an offense develops faster than methodologies for proving and preventing it. This fully confirms the thesis on the need legislatively to establish the principles of supporting the family and interacting with it on issues of digital education in order to counter the negative influence of internet resources, which is recognized as a main cause of juvenile offenses, and to strengthen the responsibility of persons responsible for protecting children's information rights.

The systematic method of analyzing legal institutions makes it possible to conclude that, in order to overcome the identified problems, it is necessary to improve legal definitions and expand the subject composition of prevention. Introducing into the law provisions on volunteer organizations and their right to participate in individual preventive work will help establish a balance between the interests of the minor and the minor's family members. The use of civil society's potential enables the state to respond flexibly to cyber threats and to form in adolescents a sense of respect for society's highest values and for the law. Without a qualitative change in the approach to the normative definition of digital threats, the legal status of minors will remain vulnerable in the face of the constantly changing information environment.

Under conditions of global digital transformation and implementation of strategic documents such as the Cybersecurity Concept "Cyber Shield of Kazakhstan" and the state program "Digital Kazakhstan," the scientific substantiation of directions for improving minors' information-legal status acquires the status of an especially important state-legal task. The development of the information sphere is a key factor of state progress; however, it is accompanied by the emergence of new global threats for the most vulnerable groups of the population, namely children. Contemporary legal policy requires a transition from reactive measures to a proactive system combining technological protection, international integration and deep reform of educational and law-enforcement institutions.

A fundamental direction of reform is to strengthen children's cybersecurity through the educational paradigm and prevention. Scientific analysis shows that one of the main reasons for the effectiveness of cyber threats is the insufficient computer literacy of the population and the lack of basic information hygiene skills [95]. In this regard, within the framework of the strategic documents of the Republic of Kazakhstan, a scientifically grounded initiative has been proposed to introduce training in the basics of safe use of information and communication technologies (ICT) directly into the school curriculum. Legal consolidation of "digital literacy" as a mandatory element of the educational standard will make it possible to form mechanisms of psychological and technical self-protection among minors, thereby reducing the risk that cybercriminals will abuse their trust.

Another strategic direction is institutional reform of the system of law-enforcement bodies and improvement of their qualifications in the field of IT technologies. Legal statistics show that the effectiveness of investigating crimes committed using information technologies remains low; the main reason is the insufficient specialized knowledge of investigators and judges in the field of new technologies. As a scientifically grounded solution, it is proposed to create independent specialized twenty-four-hour units for combating cybercrime within the structure of pre-trial investigation bodies. The staffing of such units should be subject to requirements for IT knowledge combined with legal training.

Improvement of legal policy is impossible without developing methodological support for investigations and applying innovative tactics. The scientific substantiation of mechanisms for combating cyber threats against children presupposes the active use of covert investigative actions, in accordance with Article 231 of the Criminal Procedure Code of the Republic of Kazakhstan, to establish contact with persons disseminating extremist or other harmful materials. It is also appropriate to initiate the creation, at the interstate level, of a unified legal platform for exchanging experience in investigating cybercrimes and maintaining registries of blocked destructive resources. This will make it possible to move from local protection to collective cybersecurity on the scale of regional associations.

The legal substantiation of mechanisms for improving legal policy lies in recognizing children's information security as an integral element of national security.

Legal liability for offenses in the digital environment should develop from simple fines into a comprehensive system of educational and technical influence. The scientific approach requires legislation not only to prohibit content, but also to create conditions for the development of "positive content" that supports society's moral values. Coordination of the efforts of the state, the prosecutor's office and communications bodies should be aimed at creating a seamless protection mechanism in which technical blocking of threats precedes their physical impact on the child's psyche.

In conclusion, it should be noted that the proposed directions form an integral concept for modernizing minors' information-legal status. The synergy of educational reforms, international integration and specialization of law-enforcement activity will enable Kazakhstan to create an effective "Cyber Shield" system for the younger generation.

It may be concluded that improvement of minors' information-legal status in the Republic of Kazakhstan should be carried out through comprehensive modernization of legislation and law-enforcement institutions. The main ways to strengthen cybersecurity are mandatory teaching of digital hygiene in schools, introduction of new definitions of cyber threats, ratification of international conventions with necessary reservations and creation of specialized IT units in law-enforcement bodies. The scientific substantiation of such policy is based on the priority of protecting the child's health and development as the state's highest social value under conditions of an unrestricted information space. Implementation of these measures will make it possible to eliminate the gap between technological progress and legal regulation and to ensure the safe and harmonious development of the person in the digital ecosystem.

Completion of the systematic study of the legal situation of minors in the information space of the Republic of Kazakhstan makes it possible to formulate final conclusions characterizing the specific features of their legal subjectivity and delictual capacity. The analysis conducted showed that the development of the information sphere has become a key factor determining the effectiveness of state institutions and the economy, which has inevitably affected the legal status of minors as the most active users of digital systems. Under current conditions, the child's information-legal status has ceased to be merely an object of state protection and has been transformed into the status of an active, but specific, participant in legal relations. The child's activity requires detailed legislative regulation and a balanced combination of rights, freedoms and legal liability.

The distinctive features of minors' legal status in information relations lie in their staged integration into the digital environment. The research established that children's information legal capacity in Kazakhstan has a gradual character, in which the scope of accessible content and rights to use services is closely connected with age categories marked as "6+," "12+," "14+" and "16+." This stratification, established in Law of the Republic of Kazakhstan No. 169-VI, is based on scientifically grounded psychophysiological characteristics of information perception and acts as a

mechanism for ensuring the person's information security. The main purpose of such restrictions is to create a "safe perimeter" that protects the as-yet-unformed psyche from destructive influence while preserving the fundamental right to seek and receive developmental information.

Information security has special significance in the system of legal status and is considered, in the context of implementing the state program "Digital Kazakhstan," as a necessary condition for citizens' trust in technological solutions. The research confirmed that effective protection of children's rights in cyberspace is impossible without the unity and stability of information and communication infrastructure. The legal protection mechanism includes not only age-based labeling, but also mandatory content filtering in educational institutions and places of public access, which transfers legal requirements to the level of technical imperatives. However, despite the existence of the Cybersecurity Concept ("Cyber Shield of Kazakhstan"), the level of practical protection of minors is often reduced because of "digital neglect" by parents.

Analysis of minors' legal liability revealed a number of paradoxical tendencies. On the one hand, the law punishes adolescents for cybercrimes and administrative offenses online from the ages of 14 and 16 respectively; on the other hand, statistics indicate an insufficient level of effectiveness in implementing this liability. According to legal statistics, the overall effectiveness of countering crimes committed using information technologies remains low: the main reasons are the high latency of information delicts and the insufficient specialized knowledge of law-enforcement and judicial officers in the field of new computer technologies [96]. According to official data, between 2013 and 2024 the number of offenses committed by minors in the Republic of Kazakhstan decreased by approximately 55%, which is recognized as a real result of preventive measures [93].

Scientific and theoretical analysis showed that the special subject nature of minors' liability in the digital environment requires the law enforcer to take into account their "social immaturity." Offenses committed by adolescents on social networks are often caused by adverse life circumstances or by the absence of skills for critical analysis of information. In this regard, Kazakhstan's legal policy is oriented toward the priority of educational influence measures rather than repressive sanctions. However, the absence of specialized investigative and operational units working around the clock and possessing IT competencies complicates the timely detection and proper qualification of cybercrimes committed by young people.

An important aspect determining the significance of the studied features within the general system of legal regulation of the field of informatization and communications is the need for international integration. The issue of promptly obtaining data from international social networks remains acute, because the process of sending international requests for legal assistance is often slow, allowing guilty persons to hide. As a solution, the scientific need is substantiated for Kazakhstan to accede to the Council of Europe Convention on Cybercrime, the Budapest Convention,

with reservations to articles contrary to national sovereignty. This will make it possible to harmonize national law with international standards and ensure effective protection of children's rights in the transboundary information field.

Summarizing the significance of the identified features, it should be emphasized that minors' information-legal status is the "core" of the state's digital security system. The specific features of their legal subjectivity, namely age censorship, and liability, namely educational priority, constitute a specialized legal regime that should be integrated into the general architecture of the "Cyber Shield of Kazakhstan." Strengthening this status is impossible without improving the population's computer literacy and introducing instruction in the basics of safe ICT use directly in schools, which is a strategic task of the state. Scientific improvement of legal policy should proceed through the creation of specialized IT units in law-enforcement bodies and the recruitment of personnel with technical knowledge.

Scientific conclusion for the paragraph: Summarizing the results of the research, it may be concluded that minors are special subjects of information legal relations, whose legal status is characterized by a balance between expanding digital rights and imperative measures of state protection. The specificity of their liability lies in the need to combine technological control with measures of socio-pedagogical correction, which at the current stage is hindered by the lack of special knowledge among law enforcers and the underdevelopment of mechanisms of international cooperation. It has been established that children's information security is an integral element of national security and requires a systematic approach ranging from content labeling to ratification of international conventions. The problems of the latency of cybercrimes and the "digital gap" in legislation lay the theoretical foundation for further development of practical recommendations.

2.2 Legal Specificity of Minors' Administrative Liability for Offenses in the Field of Informatization and Communications

Administrative liability is a complex and multifaceted legal institution with a unique legal nature, located at the core of both the legal system and the mechanism for ensuring public administration and legal order. In modern legal science, it is considered as a special public-law relation arising between authorized subjects, such as executive authorities and officials, and individuals and legal entities in connection with the commission of administrative offenses, and aimed at implementing rights and duties established by the state [97; 98]. This institution is an integral element of state coercion and possesses all the features of general legal liability, including normative establishment, the culpable nature of the act and the occurrence of adverse consequences for the offender.

A scientific understanding of the essence of administrative liability includes analysis of various doctrinal approaches. In the domestic tradition of the Soviet and post-Soviet periods, administrative liability was interpreted as a measure of state coercion expressed through the application of administrative penalties. I.A. Galagan

defined this institution through the application of administrative sanctions, while I.S. Samoshchenko and M.Kh. Farukshin considered it as a "response" to a culpable unlawful act accompanied by state and public condemnation [102; 107]. Contemporary researchers expand this concept by describing administrative liability as a form of exercising state-authority powers aimed at applying an administrative penalty, in the manner prescribed by law, to a person who has committed an unlawful act [111].

The place of administrative liability in the legal system is determined by its close connection with public-law interests and by the need for a prompt response to offenses that do not possess the features of public danger characteristic of crimes. Unlike criminal liability, administrative delictuality covers a broad range of public relations in the field of public administration, although both types of liability pursue similar preventive purposes [101]. Official statistical data confirm the scale of this institution: according to the Committee on Legal Statistics and Special Records of the Prosecutor General's Office, 132.7 thousand criminal offenses were registered in Kazakhstan in 2024, while in 2025 this figure decreased by 6.6% to 123.9 thousand [115]; the number of administrative cases, however, remains significantly higher than the number of such crimes.

The scientific substantiation of the purposes of administrative liability makes it possible to distinguish two main categories: general prevention and individual prevention. General prevention is aimed at preventing the commission of new offenses both by the offender and by other members of society, while individual prevention, or warning, is implemented through sanctions that exert an educational influence on the guilty person. In addition, the purpose of administrative liability is to protect legal order, restore social justice and limit the harmful consequences of the committed act [100; 108].

The functions of administrative liability systematically reveal its role in the legal system. The punitive function is manifested in restricting the offender's personal, property or other rights and interests; the educational function is intended to form citizens' legal consciousness and encourage law-abiding behavior and respect for public and traditional values [99]. The regulatory function ensures the stability of public relations by establishing clear boundaries between permitted and prohibited behavior in social life. Finally, the protective function is manifested in the formation of a special legal mechanism capable of protecting the legitimate interests of legal subjects from selfish and unlawful encroachments [112].

The legal principles of administrative liability form the basis for its implementation and guarantee compliance with legality in the activities of jurisdictional bodies. Under the principle of legality, liability may be imposed only where it is directly provided for by law and in accordance with a strictly established procedural order. The principle of humanity requires consideration of a person's age and psychological characteristics when punishment is applied, and coercive measures must not have the purpose of degrading human dignity. The presumption of innocence

releases a person from the duty to prove his or her innocence and places the burden of proof on the state. The principle of inevitability of liability requires every offense to receive an appropriate legal assessment, although in practice it is combined with the possibility of exemption from liability where the act is insignificant or where the subject has a special status, such as being a minor [98; 104].

The institution of administrative liability acquires particular importance in the protection of the rights of the most vulnerable categories of the population, such as minors. Legislation establishes a special status for them, providing a number of guarantees: a higher age threshold for liability, namely 16 years; restrictions on the types of penalties that may be applied, especially the prohibition of administrative arrest; and mandatory participation of legal representatives in proceedings [106; 114]. This demonstrates that administrative liability is not only a punitive mechanism, but also a complex instrument of socio-legal correction of behavior aimed at harmonizing the interests of the individual and society [97].

A scientific analysis of the legal specificity of administrative offenses in the field of informatization and communications makes it possible to identify their special object: public relations ensuring information legal order. Under conditions of digitalization, this object comprehensively includes not only the technical reliability of communications networks, but also the information-psychological security of the individual, especially with regard to such a highly vulnerable category as minors [110]. The commission of administrative offenses in this field is determined by the use of specific means, such as computer equipment, mobile devices and software, and by the virtual nature of the environment in which they are committed, which creates the need to improve procedural measures, including examination of internet pages and computer equipment [103].

The unlawful use of information resources as a type of administrative offense is based on the need to protect the exclusive rights of the state, organizations and citizens to information. The legal essence of these acts consists in violating established rules for access to, storage and dissemination of data. Amendments introduced in 2024 to the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" introduced a new definition of personal data breach and obliged data protection officers to notify the Ministry of Digital Development within one working day [114]. For example, the circulation of information products, including sale, rental and placement on networks, in violation of legal requirements directly encroaches on the established procedure for managing resources, as is also confirmed by a systematic analysis of norms regulating the protection of children from harmful content [109]. In this regard, administrative liability serves as a means of suppressing unauthorized actions that may harm the intellectual and mental development of members of society.

Non-compliance with information security requirements is one of the rapidly developing elements of administrative offenses. International studies, including Cybersecurity Ventures 2024, show that the growth rate of cybercrime, which was 30%

in 2020-2022, reached 74% in 2023 and 83% in 2024, which requires an immediate response from the liability system [111]. The Code of the Republic of Kazakhstan on Administrative Offenses, hereinafter the CAO RK, provides for liability for failure to apply technical and organizational protection measures [114]. The legal significance of these norms is manifested in preventing serious consequences such as cybercrimes, dissemination of personal data and destructive psychological influence on citizens.

Comparative legal research shows that administrative liability in the information sphere often plays the role of "administrative prejudice" for criminal offenses [97]. Systematic violation of information security rules or repeated unlawful dissemination of information under certain circumstances may become a criminally punishable act. At the same time, scientific and technological progress forces the legislator constantly to expand the list of elements of offenses by introducing liability for violations in the operation of messengers, social networks and search engines. The adoption of the Digital Code of the Republic of Kazakhstan No. 255-VIII ZRK of 9 January 2026 opened a new stage in the regulation of this field [115].

Summarizing the above, it may be concluded that the legal nature of administrative offenses in the field of informatization and communications lies in their orientation against the established procedure for managing information processes and against the security of subjects in cyberspace. These acts are characterized by a special object, namely information legal order, by specific methods of commission and by the need for prompt state response. The scientific basis for separating them into independent elements of offenses rests on the need to protect public relations from destructive informational influence and to ensure the stability of the national segment of the Internet.

The legal status of a minor in the system of administrative law is a unique legal construction connected with the need to ensure a balance between the state's punitive function and the priority of protecting the child's interests [99; 104]. In contemporary legal doctrine, the status of a minor is considered as that of a special subject of administrative liability, determined both by an age threshold and by the actual level of psychophysiological development. In accordance with norms of international and national law, state policy in the interests of children is aimed at promoting their physical, intellectual, spiritual and moral development, as well as protecting them from factors that negatively affect such development [109]. Within administrative-delict law, this means that bringing an adolescent to liability is not an end in itself, but a means of social correction and prevention of more serious offenses in the future.

The central element of the legal status of a minor is reaching the age of administrative liability. According to Article 30 of the CAO RK, a person who has reached the age of sixteen at the time of committing an offense is subject to administrative liability, while Article 65 distinguishes minors, namely persons between sixteen and eighteen years of age, as special subjects [114]. Thus, the age from 16 to 18 is recognized by the legislator as an incomplete period of delictual capacity. Scientific literature discusses the need to lower this threshold to 14 years for

certain acts, such as petty hooliganism or damage to property [108]. Comparative legal analysis shows that the current 16-year standard remains dominant in most countries of the continental legal family, including Russia, Kazakhstan and Ukraine [97; 106].

The limits of bringing minors to legal liability are significantly narrower than those applicable to adult subjects. One of the main features is the reduced list of state coercive measures that may be applied. According to Article 66 of the CAO RK, administrative arrest is not applied to persons under eighteen years of age, and the main types of penalty are warning and administrative fine [114]. However, the effectiveness of fine sanctions in relation to adolescents is subject to scientific criticism [100; 108]. A dissertation study on the prevention of juvenile crime at the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan clearly showed that where minors have no independent income, the burden of paying fines is imposed on parents, which makes it difficult to achieve the purpose of individual prevention [104].

An important element of the protection mechanism is the subject composition of the bodies authorized to consider cases in this category. Traditionally, commissions for juvenile affairs and protection of their rights play a decisive role [105]. These commissions consider the majority of cases concerning offenses committed by adolescents, ensuring a comprehensive approach that takes into account the child's living and upbringing conditions. Under the new procedure approved on 30 March 2026, 274 such commissions operate throughout the republic, and they are the only interdepartmental bodies at the regional level that make decisions in the field of protection of children's rights. Nevertheless, contemporary science notes the insufficiency of the administrative-jurisdictional powers of such commissions and proposes transferring case-consideration functions to specialized juvenile courts [101].

A systematic analysis of minors' legal status is impossible without taking into account the principle of humanity and the presumption of innocence. The minor age of the offender is normatively established as a circumstance mitigating administrative liability. In addition, the law allows an adolescent to be released from liability where the act is insignificant and educational measures are applied instead [105; 107]. At the same time, there is also a scientific position that the "humanistic" approach should not create among adolescents a sense of impunity and that the principle of inevitability of liability must be strengthened in order to prevent criminalization of the youth environment [102].

Mechanisms for the legal protection of minors also include the activities of specialized subdivisions of internal affairs bodies, which conduct preventive work not only with adolescents themselves, but also with their parents [105]. Legal education and information are identified as the most effective forms of preventive influence contributing to the formation of law-abiding behavior. At the same time, the status of a minor implies that any interference by the state in the minor's life must be connected

with the priority of the child's interests and directed toward the child's optimal integration into public life.

It may be concluded that the legal status of a minor as a subject of administrative liability is characterized by deep specificity connected with the age and psychological characteristics of this category of persons. As a "special subject," the minor has a set of procedural guarantees that limit the application of the harshest measures of administrative coercion and give priority to educational and preventive measures [97; 99]. The scientific substantiation of such status rests on the need to provide social protection for the child and to prevent the child's involvement in criminal liability.

The scientific classification of administrative offenses in the field of informatization and communications is based on distinguishing three fundamental groups: 1) violations of rules for the use of information resources and the procedure for content circulation; 2) unlawful acts committed in internet space and the online environment, including content-related offenses and network deviations; 3) violations of the procedure for using and ensuring the security of communications and informatization infrastructure, namely technological offenses. This approach makes it possible to distinguish liability for the "content" aspect of information and the "instrumental" aspect of telecommunications processes [109]. By comparison, in the Russian Federation there is also a tendency to expand the list of elements of offenses, with more than 40 special norms, but the Kazakhstani model is distinguished by its stricter connection with the cybersecurity concept for critical facilities [116].

The legal characterization of violations of the rules for using information resources is aimed at protecting the procedure for working with data and ensuring the interests of subjects of information relations. A central role is played by Article 641 of the CAO RK, which provides for liability for violation of legislation on informatization, including failure by the owner to implement measures for the protection of personal data [114]. The legal essence of these acts lies in violating the regime established by the state for access to and storage of resources. In addition, this group includes Article 79, which protects the confidentiality of personal data and differentiates sanctions depending on whether the offender uses his or her official position. In Kazakhstan, these relations are separated into special Article 156-1, which regulates the labeling of periodicals and the time for disseminating "18+" content [109]. This reflects the prioritization of the information-psychological security of the younger generation as an independent object of legal protection.

The second group, as a logical continuation of content regulation, consists of offenses connected with committing unlawful acts in internet space. An important innovation in Kazakhstani legislation is Article 456-2, "Posting and Dissemination of False Information," introduced into the CAO RK in 2023, which covers actions both in mass media and on online platforms [114]. The sanction of this article provides for a fine of 20 MCIs for individuals and 100 MCIs for large business entities. A specific feature of the Republic of Kazakhstan is the identification of influencers, or bloggers,

as special subjects of liability, understood as users who publish information for an indefinite circle of persons for the purposes of entrepreneurial activity. This solution is aimed at countering anonymization of liability online, which is also a relevant issue for the Russian Federation, where scholars likewise identify the "illusion of anonymity" as a factor in the growth of digital delictuality [116].

The third block of offenses covers violations of the procedure for using communications infrastructure and forms the technological basis of information legal order. 3.13.the CAO RK groups together a set of norms aimed at ensuring the stability of telecommunications networks. Article 637 establishes liability for acts ranging from an unjustified refusal by a dominant operator to connect networks to the use of the radio-frequency spectrum in violation of technical parameters. The nature of infrastructural offenses also includes requirements for the use of certified equipment under Article 638 and compliance with rules for using protection tools under Article 639 [114]. In February 2026, by presidential decree, the National Security Committee was granted powers of state control over the information security of critical information and communication infrastructure facilities, as well as the power to issue prescriptions in cases of administrative offenses, which is a clear manifestation of strengthening liability in this field.

Analysis of the subject composition of offenses in the field of communications in the Republic of Kazakhstan reveals a tendency toward subsidiary liability. In addition to officials and legal entities, parents of minors are also held liable for allowing children to access harmful content under Articles 127, 134 and 435 [114]. Official regional statistics confirm the activation of this mechanism: according to the Police Department of Zhambyl Region, in 2024 protocols were drawn up and fines imposed on 143 parents under Article 127 of the CAO RK for failure to perform duties relating to parental upbringing, which represents a 155.4% increase compared with 56 cases in 2023; under Article 435, concerning hooliganism committed by a minor, the number of parents increased from 15 to 27, or by 80%. During the same period, 1,550 minors were brought to police units in the region for various administrative and criminal offenses, compared with 979 in 2023, of whom 1,525 were brought for administrative offenses [115]. This corresponds to the scientific conclusion concerning the clip thinking of the modern "digital generation" and the lowering of the threshold for critical perception of social consequences, and requires strengthening the educational function of administrative liability [103; 112].

A minor subject of administrative liability in the Republic of Kazakhstan has a distinct legal status determined by age and psychophysiological development [106]. According to Articles 30 and 65 of the CAO RK, persons who have reached the age of sixteen but have not reached the age of eighteen at the time of committing an offense are recognized as minors [114]. This age threshold of 16 years is the normative basis of delictual capacity. By comparison, the Russian Federation also establishes the age of 16 as the threshold for administrative liability, in part 1 of Article 2.3 of the Code of Administrative Offenses of the Russian Federation, which

reflects the continuity of the legal traditions of CIS countries [116]. However, Kazakhstani legislation, by placing minors in the category of "special subjects," grants them additional guarantees and limits the list of coercive measures that may be applied to them [97; 99].

The legal regulation of administrative liability in the information sphere in the Republic of Kazakhstan is aimed at protecting information legal order and the psychological security of citizens, especially children [109; 110]. The legal nature of administrative offenses in the field of informatization and communications in the Republic of Kazakhstan lies in their encroachment on the established procedure for information circulation, use of networks and ensuring cybersecurity. The scientific explanation for recognizing such acts as offenses lies in the need to protect the interests of the individual and the state from the destructive influence of the digital environment [103].

The first group of offenses is connected with violation of the procedure for the circulation of information products. Here, the central role is played by Article 156-1 of the CAO RK, which provides for liability for violation of legislation on the protection of children from harmful information [114]. The objective side of such acts is manifested in the dissemination of printed publications without an age-category label or in failure to comply with the time limits for broadcasting television and radio content classified as "18+." In the Russian Federation, similar relations are regulated by Article 6.17 of the Code of Administrative Offenses of the Russian Federation, which also regulates in detail the rules for labeling and disseminating products intended for children [116]. However, in Kazakhstan there is a clear tendency toward strict specialization of norms protecting minors' personal and biometric data in mass media [112].

The content of educational influence measures is disclosed in Article 70 of the CAO RK: explanation of the law, imposition of duties to remedy the harm caused, as well as restriction of leisure time and establishment of special requirements for behavior. Explanation of the law consists in conveying to the adolescent's consciousness information about the harmfulness of his or her act and the legal consequences in the event of repetition, which is directly connected with the formation of legal culture [97]. Restriction of leisure time may include a prohibition on visiting certain places, such as night entertainment establishments, a prohibition on using certain types of entertainment, including internet resources, or restriction of time spent outside the home. The duration of such restrictions ranges from three to six months, and failure to comply with them entails cancellation of the educational influence measure and bringing the person to liability under the general procedure [114].

The connection between administrative punishment and protection of minors' rights and interests is also reflected in the reduction of limitation periods. According to Article 71 of the CAO RK, for adolescents the limitation periods for bringing to liability and for enforcement of punishment are reduced by half compared with the

general periods. In addition, the period during which a minor is deemed to have been subjected to an administrative penalty is also shortened: it is only six months from the date of completion of enforcement of the decision, whereas for adults this period is one year under Article 72 of the CAO RK [114]. These norms are aimed at removing the "legal label" from the adolescent more quickly and facilitating the adolescent's social adaptation after committing an offense [105].

The procedural mechanism for applying punishments in the Republic of Kazakhstan is also aimed at protecting the child's interests. Exclusive jurisdiction over cases of administrative offenses committed by minors is assigned, in accordance with Article 684 of the CAO RK, to specialized interdistrict juvenile courts [114]. The mandatory participation of a legal representative and defense counsel, namely an advocate, guarantees respect for the adolescent's rights at all stages of proceedings.

Scientific analysis of the practice of applying liability measures shows that timely measures are the most effective, since impunity among adolescents aged 11-14 often leads their behavior subsequently to develop into crime [107]. Dissertation studies defended at the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan confirm this: researchers clarify that a significant proportion of crimes committed by minors arise because of insufficient timely measures to suppress earlier administrative misconduct [104]. Official statistics also confirm this trend: in 2024, the Specialized Interdistrict Juvenile Court of Aktobe Region considered 51 criminal cases involving 51 minors, compared with 38 cases in 2021, 40 in 2022 and 57 in 2023 [115].

It may be stated that in the Republic of Kazakhstan a humanized model of minors' administrative liability has been formed, characterized by strict limitation of fine sanctions, prohibition of arrest and broad application of educational measures [1; 3]. The educational and preventive purposes of punishment prevail over the punitive purpose in a manner that protects the adolescent's legitimate interests and facilitates faster socialization.

One of the central features of judicial practice in the Republic of Kazakhstan is the exclusive jurisdiction of specialized interdistrict juvenile courts over cases of administrative offenses committed by minors. According to part 2 of Article 684 of the CAO RK, it is precisely these courts that consider elements of offenses connected with petty hooliganism, knowingly false calls to special services and violations in the information sphere [114]. Scientific analysis of the activities of these courts leads to the conclusion that such specialization contributes to a deeper study of the adolescent's personality, living and upbringing conditions, and level of mental development [97; 99]. Juvenile courts are aimed at minimizing punitive influence by giving priority to measures of an educational nature, which corresponds to international standards for the protection of children's rights.

Specific judicial statistics demonstrate the operational capacity of the system: during the first 11 months of 2024, the Specialized Interdistrict Juvenile Court of Zhambyl Region received 60 administrative cases, the overwhelming majority of

which were initiated under part 3 of Article 127 of the CAO RK, failure to perform duties relating to the upbringing of a minor, and Article 442, presence of minors in entertainment establishments or outside the home at night without accompaniment by legal representatives. During the same period, the court also received 42 criminal cases involving 51 minors, most of which were initiated under Article 188 of the Criminal Code of the Republic of Kazakhstan, theft; Article 122, sexual intercourse with a person under 16 years of age; and Article 191, robbery [115]. These data show the interconnection between the institutions of administrative and criminal liability and the risk of an adolescent's transition from an administrative offense to a criminal act [104].

The activities of law-enforcement bodies, namely internal affairs bodies, in the information sphere of the Republic of Kazakhstan are characterized by a combination of jurisdictional and preventive functions. Internal affairs bodies are empowered to consider a wide range of cases, including disturbance of peace, allowing children to be present in entertainment establishments at night and dissemination of information products with prohibited content under Articles 134 and 437 of the CAO RK [114]. According to the 2024 report of the Police Department of Zhambyl Region, as a result of raid and preventive measures carried out throughout the year, 1,550 minors were brought to police units for committing various criminal and administrative offenses, compared with 979 in 2023, an increase of 58%; of these, 1,525 were brought for administrative acts and 25 for criminally punishable acts. During the same period, administrative liability was applied to 73 administrators under Article 132 of the CAO RK, allowing minors to be present in entertainment establishments at night, and fines totaling 849,160 tenge were imposed [115].

The scientific community assesses the effectiveness of applying administrative liability to minors in the Republic of Kazakhstan ambiguously [100; 108]. On the one hand, official statistics show a significant number of detected offenses, which testifies to the functioning of the system. On the other hand, the issue of enforcement of punishments remains relevant as an important factor of their effectiveness: because fines imposed on adolescents are often paid by parents, the individual preventive purpose of punishment, namely influence on the offender's consciousness, is not fully realized [101; 107]. In this regard, the need to replace fine sanctions in Kazakhstani practice with educational influence measures, such as restriction of leisure time and establishment of special requirements for behavior, is becoming increasingly substantiated.

The practice of applying Article 127 of the CAO RK, "Failure to perform duties relating to the upbringing and/or education of a minor and protection of his or her rights and interests," shows the close connection between adolescents' offenses in the information sphere and the behavior of their legal representatives. Data from Zhambyl Region confirm the active use of this mechanism: in 2024, 143 parents were brought to administrative liability under Article 127, compared with 56 in 2023, an increase of 155.4% [115]. This reflects the subsidiary nature of liability in family relations in the

Republic of Kazakhstan, where the state imposes on parents the priority duty to ensure children's information hygiene [104; 105].

The procedural aspect of legal protection in information space faces the problem of proving guilt. Under conditions of the Internet's "illusion of anonymity," identifying the offender requires the use of special scientific and technical tools [103]. Judicial practice in the Republic of Kazakhstan recognizes as evidence factual data obtained as a result of processing digital objects integrated with the unified register of administrative proceedings. At the international level, the Hack_Right program in the Netherlands, as well as studies published in the Scopus database, demonstrate the effectiveness of alternative criminal justice programs aimed at adolescents [111].

In the practice of administrative bodies of the Republic of Kazakhstan, protection of children from information-psychological influence has particular legal significance. Article 156-1 of the CAO RK, which regulates the labeling of information products, plays the role of a barrier against destructive content [114]. However, the effectiveness of this norm remains limited under conditions of free access to foreign online platforms. According to data of the United Nations Children's Fund (UNICEF) for Kazakhstan, 79% of children are exposed from early childhood to various forms of discrimination and humiliation, which makes it possible to understand the broader social context of destructive influence in information space [113].

In conclusion, it should be noted that law-enforcement practice in the field of informatization and communications in the Republic of Kazakhstan is oriented toward specialization and humanization of justice in relation to minors [97; 99]. The effectiveness of the system is ensured by the activities of juvenile courts and specialized subdivisions of internal affairs bodies, but it requires improvement of mechanisms for enforcing punishments and strengthening parental control [104; 107]. It may be concluded that the success of preventing administrative delictuality in the digital environment of the Republic of Kazakhstan depends on the integration of legal, technical and pedagogical measures of influence.

The main block of problems is the insufficiency and instability of legal norms regulating the status of a minor offender in the information sphere. The scientific community notes that the CAO RK still contains formulations that do not fully reveal the essence of the institution of administrative liability, making it difficult for both legal subjects and law enforcers to understand it adequately [111]. The situation is complicated by the "constant reforms" of legislation, where norms become outdated before stable practice for their application has time to form. A dissertation study defended at Al-Farabi Kazakh National University clearly demonstrates the dilemma of the subject of liability in relation to adolescents' digital actions: the parent, the child himself or herself, or the school? Although the current norms of the CAO RK, namely Articles 127 and 435-438, generally provide for the personal liability of adolescents over 16 years of age and the liability of parents of those aged 14-15, special articles

systematically covering the concept of "cyberspace" remain insufficiently developed [103].

Particular difficulty is created by the phenomenon of terminological duplication characteristic of the elements of offenses in the field of information security. The dispositions of the norms of the CAO RK and similar legislation of the Russian Federation often use overlapping and incompletely defined concepts such as "propaganda," "appeal," "involvement," "dissemination" and "transmission" [110]. The absence of a unified legal interpretation of these categories leads to accidental errors when qualifying minors' actions on the Internet: the boundary between expressing a personal opinion and publicly disseminating harmful content remains blurred. Scientific literature substantiates the need to simplify these constructions by introducing universal terms such as "transmission," meaning to a specific addressee, and "dissemination," meaning to an indefinite group of persons [103; 112].

The low effectiveness of the administrative fine as the main measure of influence on minors remains an important problem of law enforcement. Since the overwhelming majority of adolescents aged 16-18 have no independent income or property, the burden of paying the fine is imposed on parents [100; 101]. This mechanism contradicts the principle of personal culpable liability, because the offender does not experience the actual property deprivation provided for by the sanction. In this regard, legal science in both Kazakhstan and the Russian Federation actively discusses the need to replace fine sanctions for adolescents with warnings or educational measures that exert a corrective influence on the delinquent's consciousness [107; 108].

The issue of liability of parents, or legal representatives, for omissions in the information sphere should also not be overlooked. Despite the general establishment of upbringing duties in family legislation, administrative legislation lacks direct mechanisms obliging parents to control the content consumed by children and to comply with age labels on information products [105; 112]. Parents' disregard of these warning signals renders state protection measures ineffective, because the child may gain access to harmful information under conditions of family negligence. In this regard, doctrine substantiates the need to introduce special administrative liability of parents for allowing children to remain in an information environment that does not correspond to their age [110].

The main legal problems in applying minors' administrative liability in the information environment of the Republic of Kazakhstan are as follows: shortage of precise legal definitions and terminological duplication; instability and variability of legislation; lack of clarity in jurisdictional powers; ineffectiveness of fines where adolescents have no independent income; and imperfection of procedural tools for recording digital evidence [103; 108; 112].

Improvement of the institution of administrative liability in the information sphere of the Republic of Kazakhstan is caused by the need to adapt legal mechanisms to accelerated digitalization and to changes in threats to public security [111]. As

noted in scientific research, the level of well-being of any state may be assessed through indicators characterizing its development and the degree of spread of offenses among minors [100; 104]. Under conditions where a significant part of modern offenses has shifted into cyberspace, the current legislative system requires deep modernization aimed at eliminating systemic gaps and increasing the effectiveness of preventive influence. Promising directions for improving administrative-delict law in the Republic of Kazakhstan include conceptual renewal of the terminological apparatus, differentiation of sanctions, development of procedural tools for recording digital evidence and strengthening the role of educational influence measures.

Another important vector of reform is to separate the norms on minors' liability into an independent section of the Code. The current system, in which special rules concerning adolescents are scattered across different chapters, complicates their uniform application [97; 99]. The formation of a specialized section entitled "Administrative Liability of Minors" would make it possible to systematize the purposes, functions, types of punishment and special procedural procedures applicable to jurisdictional subjects, including the mandatory appointment of a psychological-psychiatric examination where it is presumed that an adolescent may not fully understand the danger of his or her actions [105]. This would create the necessary conditions for implementing the principle of humanity and ensure protection of the lawful rights of "digital children," who have a level of psychophysiological development requiring special treatment by the state.

Reconsideration of the effectiveness of fine sanctions is a scientifically grounded direction for improving the punishment system. Studies show that for an adolescent without independent income, an administrative fine in practice turns into parental liability, which does not contribute to achieving the purposes of individual prevention [100; 107]. To increase the effectiveness of influence, it is proposed to introduce more broadly alternative measures such as temporary correctional work of an educational nature or a warning combined with special requirements for behavior on the Internet. International practice, in particular the Netherlands' Hack_Right program, confirms the effectiveness of such an alternative approach [111]. In addition, it appears appropriate to establish in the General Part of the CAO RK the use of information and communication technologies as an aggravating circumstance, reflecting the increased social danger of "digital" offenses because of their publicity and ability instantly to reach an indefinite group of persons.

Further strengthening of preventive measures requires increasing the responsibility of parents and legal representatives for children's information security [105]. Doctrine substantiates the need to introduce into the CAO RK, as well as provisions analogous to Article 6.17 of the Code of Administrative Offenses of the Russian Federation, elements providing for parental liability for allowing children to be in an information environment that does not correspond to their age or for negligent attitudes toward adolescents' consumption of harmful content [110; 112]. The product's age label should become a legally significant signal for parents, and

disregard of it should serve as a basis for administrative influence. Consolidating the efforts of the state and the family is an important factor in protecting minors' information-psychological security from the destructive influence of cyberspace [113].

Thus, on the basis of the above, it is possible to make a substantiated conclusion that administrative liability is an important legal instrument aimed at preventing offenses by minors and forming their stable lawful behavior in the digital environment [8]. Its significance is manifested in the implementation of the purposes of general and individual prevention: it suppresses deviant behavior at early stages and prevents its development into stable criminal attitudes [98; 99]. In this regard, administrative-delict law functions not only as a mechanism of state coercion, but also as an instrument of social correction and legal education aimed at resocializing the adolescent and adapting his or her personality to the requirements of legality in the information society.

At the same time, the conducted research makes it possible to conclude that the resource of administrative-law regulation has objective limits conditioned by the material feature of the social danger of the act. In current legal reality, certain offenses committed by minors in information space possess a high degree of public danger that significantly exceeds the boundaries of an administrative offense [8]. Official data confirm this trend: in Kazakhstan, during the first 7 months of 2025, 44 criminal offenses of an extremist nature were detected, more than 4.6 thousand drug-related crimes were registered, and more than 11 tons of narcotic drugs and 23 tons of chemicals were seized [115]. Acts such as unauthorized access to important computer information, creation and dissemination of destructive malicious software, committing large-scale theft or using ICT to disseminate extremist materials encroach on the fundamental foundations of state security, property and the constitutional order.

In this regard, there arises an objective scientific and practical need for a detailed study of the legal foundations and specific features of minors' criminal liability for offenses in the field of informatization and communications. The growth of "digital delictuality" and the increasing professionalization of cybercrime among adolescents require the development of stricter and more effective mechanisms of legal protection that cannot be ensured solely within the framework of the Code on Administrative Offenses [103]. Criminal-law research makes it possible to reveal more deeply the specificity of the subjective side of cybercrimes committed by adolescents, to assess the proportionality of criminal punishments to the nature of the acts committed, and to determine criteria for distinguishing mixed elements of crimes and offenses in the virtual environment.

Formulating conclusions from the consideration of administrative-law aspects, it should be noted that the completeness of scientific inquiry requires a transition from the analysis of less dangerous offenses to the study of crimes in the field of high technologies. The logic of the research requires moving to the study of stricter forms of state response to threats in information space. Thus, the natural continuation of the work and the topic of the next section of the research will be "Specific Features of

Minors' Criminal Liability for Offenses in the Field of Informatization and Communications," which will ensure comprehensive coverage of the problem of young people's legal liability under conditions of mass digitalization.

The administrative-law analysis conducted above also shows that the failure to ensure, at the administrative level, terminological consistency in the legal definitional field of violence in the digital environment and in the protection of children's personal data appears as an objective legal deficiency. The definition of "bullying of a child" introduced in 2022 in subparagraph 4-1) of Article 1 of Law No. 345-II of 8 August 2002 "On the Rights of the Child in the Republic of Kazakhstan" does not include the semantic characteristics of the digital environment, namely the anonymous mode of the subject, the asymmetry of the parties' legal and technical capacities, and the ability of a single intentional act to spread uncontrollably to a mass audience, as separate definitional features. The absence in Kazakhstani legislation of statutory definitions of the categories "digital aggression," "profiling of children" and "digital personal data of a minor" creates instability in law-enforcement practice in determining the boundaries of differentiation between Articles 130, defamation, 131, insult, and 115-1, stalking, of the CC RK, which in turn weakens the mechanisms for distinguishing an administrative offense from a criminal offense.

To eliminate this deficiency, the following legislative proposals have been developed: (a) to update subparagraph 4-1) of Article 1 of the Law "On the Rights of the Child in the Republic of Kazakhstan" in the following wording: "bullying of a child means systematic acts of an insulting nature, harassment and/or intimidation; cyberbullying means a form of bullying of a child committed using telecommunications networks, mass media or online platforms, in the anonymous mode of the subject, under conditions of asymmetry of the parties' technical and legal capacities, and characterized by the ability of a single act to spread uncontrollably to a mass audience"; (b) to supplement Article 1 of the same Law with the definitions of "digital aggression" and "profiling of children"; (c) to supplement Article 1 of Law No. 169-VI of 2018 "On the Protection of Children from Information Harmful to Their Health and Development" with wording harmonized with the definition of "digital aggression"; (d) to supplement Article 1 of Law No. 94-V of 2013 "On Personal Data and Their Protection" with the definition of "digital personal data of a minor" and to supplement this Law with a direct prohibition on profiling minors, in accordance with General Comment No. 25 of the UN Committee on the Rights of the Child (CRC/C/GC/25, 2021) and paragraph 35 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe. This terminological consistency will ensure a legal mechanism for distinguishing an administrative offense from a criminal offense and will be further developed by supplementing Chapter 12 of the CAO RK (Articles 127-127-3), following the model of Article 6.17 of the Code of Administrative Offenses of the Russian Federation, with Article 127-4, "Failure of legal representatives to perform digital mentoring duties."

2.3 Specific Features of Minors' Criminal Liability for Criminal Offenses in the Field of Informatization and Communications

Understanding the specific features of minors' criminal liability for offenses in the field of informatization and communications begins with an initial formulation of the theoretical and legal essence of criminal liability as a legal institution. In contemporary criminal-law doctrine, criminal liability is the most acute and legally significant form of the state's response to acts with a high degree of public danger[84]. As a socio-legal phenomenon, criminal liability brings together mechanisms of state coercion aimed at restoring social justice and protecting the rights of the individual and the interests of the state amid the rapid digital transformation of public relations.

The legal nature of criminal liability is determined by the specific criminal-law relationship between the state and the person who has committed a criminal offense, while its place in the legal system is explained by the special, imperative nature of this measure of public influence. In essence, it is the strictest form of legal influence, because the objects infringed upon are of special importance. In the field of informatization and communications, such an object is the security of information and communication infrastructure, that is, the protected state of information and the infrastructure supporting it from accidental or intentional influences. The potential of cybercrimes to cause extensive harm to subjects of information relations justifies the use of criminal-law influence under the principle of ultima ratio, as the final argument of state authority[10].

The place of criminal liability in the legal system is distinguished by its greater severity compared with civil, disciplinary, and administrative liability. While other forms of legal liability are mainly aimed at compensation for harm or the regulation of managerial relations, criminal liability is designed to protect the foundations of legal order from the gravest encroachments. In the digital era, when information has become an object of purchase and sale, donation, and inheritance, as well as one of the key resources of economic circulation, unlawful interference with it requires the establishment of the strictest normative barrier[117].

The main functions of criminal liability in the information and communication sphere are classified as protective, preventive, and educational.

The protective function is implemented through the preservation of the established legal regime of information security and proprietary rights in data. It serves to ensure the legal interests of all participants in information processes.

The preventive function is aimed at preventing convicted persons from committing new offenses (special prevention), as well as deterring other persons from potential crimes (general prevention) through the threat of punishment. For minors, this function has special significance, because age-related vulnerability requires priority attention to the prevention of destructive behavior[88].

The educational function serves to form citizens' legal consciousness and behavior based on respect for law. For adolescents, this is manifested in the

development of the ability to understand the legal consequences of their actions in virtual space and in the acquisition of the foundations of legal thinking and digital culture[118].

Crime prevention, as a purpose of criminal liability, is closely connected with the category of legal culture. The Concept of Legal Policy of the Republic of Kazakhstan until 2030, approved by Decree No. 358 of the President of the Republic of Kazakhstan dated 27 October 2023, identifies the improvement of legal culture as one of the key prerequisites for the formation of a rule-of-law state. Prevention among young people is more effective than repression: the absence of legal literacy among adolescents facilitates negligent encroachments, and therefore the preventive purpose of the institution of liability must be implemented through a differentiated approach[120].

The punitive purpose is not limited to the content of sanctions; it also includes the element of restoring social justice. With respect to minors, the legislator follows the principle of humanism, limits the range of possible punishments, and gives priority to educational and rehabilitative channels of influence. This approach is institutionalized in the Criminal Code of the Republic of Kazakhstan (hereinafter, the CC RK) through the separate inclusion of Section 6 (Articles 80–89), which establishes special regulation for persons aged from 14 to 18[CC RK].

In the era of informatization, the nature of the institution of criminal liability is transformed by the specific features of the virtual environment. Online anonymity and the illusion of impunity create real risks that require the rapid renewal of criminal-law responses to new threats, including deepfake technologies, cyberterrorism, and the use of SMS blasters. At the same time, according to data from the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, the fact that the use of an SMS blaster was legally assessed for the first time in Kazakhstan in April 2026 demonstrates the ability of the law-enforcement system to adapt to new threats. In these circumstances, criminal liability becomes not merely a punitive instrument, but a mechanism for protecting the digital sovereignty of the individual and the state[9].

The theoretical and legal nature of the institution of criminal liability characterizes it as the strictest measure of state coercion, aimed at maintaining legal order, preventing criminal offenses, and ensuring the proportionate application of punishment. In the field of informatization and communications, this institution acts as a guarantee of the security of the digital environment, while its object is information and public relations concerning its use. Its systematic institutional content, combining educational and protective foundations, creates the theoretical basis for moving to the next stage of the study: an analysis of the specific features of the minor as a subject of criminal liability in digital space.

A scientific assessment of the public danger of these acts places them in a special category: unlike crimes in the physical world, the harm caused by

encroachments in the digital environment does not correspond to the offender's physical effort; an act close to minimal in effort may cause large-scale harm.

Unlawful access to information systems threatens the confidentiality of data. Its public danger is characterized by the violation of the owner's exclusive right to possess and dispose of information, as well as by the threat of harm to users' personal data. According to the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, nearly 50% of criminal offenses registered in the field of informatization and communications are classified under Article 205 of the CC RK ("Unlawful Access to Information, an Information System or a Communication Network"), which demonstrates the mass prevalence of this act and its potential to destabilize the digital environment[27].

Unlawful alteration or destruction of digital data (Article 206 of the CC RK) infringes upon the principle of information integrity. Such acts may temporarily paralyze the operation of state bodies, banking systems, and commercial organizations, causing significant economic damage. From a criminal-law perspective, this is a form of gross interference in information processes, as a result of which actual harm is caused to subjects of information relations.

A substantial violation of the rules for using information resources (Article 207 of the CC RK) threatens the accessibility and resilience of information infrastructure. The public danger of acts in this category is manifested in harm to the technological security of the state and society; in the legal doctrine of a number of states, such acts are considered comparable to the threat of terrorism[39].

The criminal-law characterization of these crimes is built on an analysis of the traditional four elements of a crime. The object of the crime is the public relations that ensure the security of computer information and information infrastructure. The objective side is characterized by active acts: unlawful intrusion, alteration, copying, or blocking of information; their concealed nature significantly complicates the process of proof. The subject, taking into account Article 15(2) and Article 80 of the CC RK, is generally a natural person who has reached the age of 16, while for certain offenses liability may begin at the age of 14. The fact that minors aged from 14 to 18 become subjects of this category of crimes is directly linked to age-related psychological development and insufficient life experience: such subjects are often incapable of adequately assessing the social significance of their actions[123]. The subjective side is usually characterized by direct intent, while the dominant motives are self-assertion among peers, game-related curiosity, or hooligan motives.

A methodologically important conclusion is that the nature of information law as a "young and rapidly developing field" requires abandoning the traditional "material" understanding of property. In the context of ICT crimes, information has the property of being "physically inseparable and reproducible"; when it is stolen or copied, vindication or restoration in the classical sense is limited. Criminal liability in this field should be oriented not toward mere punishment, but toward the formation of

legal culture and legal thinking, in order to prevent the intellectual potential of young people from being redirected into destructive channels[124].

The legal nature of criminal offenses in the field of informatization and communications lies in their orientation against information security, which combines the confidentiality, integrity, and accessibility of information within a single object. The public danger of unlawful access, data alteration, and violations of system-use rules is based on the potential to cause large-scale harm with minimal physical effort by the subject. The criminal-law characterization of these acts reveals the need to specialize investigative bodies and to study in depth the motives of minor offenders. The identified features make it possible to move logically to the next stage of the study: a detailed analysis of the specific features of the subject and subjective side of cybercrimes committed by persons under the age of 18.

An analysis of the status of a minor subject in criminal law requires a systematic approach that simultaneously takes into account formal legal criteria and the psychophysiological determinants of personal development. In criminal-law doctrine, a minor is understood as a person who has not reached the age of eighteen. This legal category serves as the main criterion for identifying a special group of subjects: persons to whom a differentiated approach is applied in matters of criminal liability and sentencing. This special status is based on recognizing the minor not only as a potential subject of crime, but also as an object of heightened state protection.

The legislator regulates age limits and the grounds of liability through the presumption of the gradual maturation of the volitional and cognitive components. Under Article 15 of the CC RK, as a general rule, criminal liability begins at the age of 16, while for a clearly defined list of serious acts, including intentional murder, kidnapping, robbery, an act of terrorism, and hostage-taking, it begins at the age of 14; Article 80 of the CC RK officially recognizes persons in this category as minors[CC RK]. With respect to the field of informatization and communications, these limits create a specific legal collision: although adolescents aged 14–17 are among the most technically competent and active users, their social and mental immaturity limits their ability to adequately understand the public danger of their actions in the virtual environment[88].

The level of minors' psychological development becomes a decisive factor in establishing guilt. Adolescence is characterized by age-related vulnerability, insufficient life experience, and the personality as a "mobile, changing systemic structure." In the context of cybercrime, this is manifested in the fact that an adolescent may perceive acts such as unlawful access to data or system blocking not as punishable conduct, but as an intellectual game or a means of self-expression, failing to fully understand the causal link between behavior and its consequences[118]. As Halibiyati and co-authors (2024) show, deficiencies in adolescents' neuropsychological indicators of verbal and behavioral control functions act as longitudinal dependent variables for juvenile arrest and adult incarceration, which

reveals the specific criminological profile of the subject of liability in the digital environment[11].

A scientific analysis of minors' legal consciousness makes it possible to distinguish defects within the structure of their legal culture. Legal consciousness is understood as the unity of knowledge about law, an internal attitude toward it, and readiness to comply with legal prescriptions. The "value contradiction" often found among minor offenders, namely the gap between declared positions and actual behavior, is a typical manifestation of a defect in legal consciousness. Legal literature distinguishes four types of adolescents' legal consciousness[120]:

- cynical, characterized by established worldview changes and the conscious commission of crimes;

- unstable, characterized by knowledge of norms, but the absence of firm legal convictions due to dependence on the situation or the adolescent's peer environment;

- nihilistic, characterized by the denial of the need to comply with the law and non-recognition of criminal-law prohibitions;

- illiterate, characterized by the absence of elementary knowledge about the legal consequences of online actions.

The principles of criminal policy with respect to minors are based on the idea of humanizing measures of criminal prosecution. The priority direction of this policy is the clear predominance of educational influence over punitive impact. Under this approach, criminal liability is understood not as mere punishment, but as an obligation to account for the committed act and to experience legal influence in a form that leads the adolescent toward rehabilitation. When making decisions in a case, investigative bodies and courts are required to take into account the adolescent's physical, intellectual, and psychological level of development, as well as the conditions of his or her life and upbringing.

In the digital era, the state's criminal policy is oriented toward the implementation of the following basic principles:

- the principle of individualization, under which punishment takes into account not only the gravity of the act, but also the adolescent's personality and his or her capacity to understand the act committed;

- the principle of limiting repression, under which deprivation of liberty is applied only in exceptional cases, when all alternative forms of sentencing have been exhausted, with priority given to compulsory measures of educational influence for minor and medium-gravity crimes;

- the principle of preventive orientation, under which priority attention is given to eliminating defects in legal consciousness and to forming legal thinking and digital culture through educational programs and social rehabilitation.

Methodologically, it is important that the status of a minor requires not merely the formal mitigation of sanctions, but also a qualitative transformation of the evidentiary process. Establishing whether the adolescent's mental development corresponds to his or her passport age and whether he or she is capable of fully

understanding the true nature and public danger of actions in digital space becomes an obligatory component of proof in criminal cases involving minors (Articles 541 and 542 of the Criminal Procedure Code of the Republic of Kazakhstan, hereinafter, the CPC RK[CPC RK]). In conditions of internet anonymity, insufficient legal literacy creates preconditions for the negligent commission of criminal offenses; this factor must not be ignored when classifying the subjective side of the act.

The legal status of a minor as a subject of criminal liability is determined by the actual combination of passport age (14–18) and the level of socio-psychological maturity. The specific feature of this status lies in its dual nature: the adolescent is simultaneously a subject of liability and an object of legal protection. The scientifically grounded priority of correction and education over punishment requires an individualized approach to minors, especially in the IT field, where defects in legal consciousness are clearly visible. The identified characteristics of subject status ensure a logical transition to the next stage of the study: a detailed analysis of the types of minors' liability for offenses in the ICT field and the mechanisms for its implementation.

The logical continuation of the theoretical analysis of the specific features of minors' liability is the systematization of types of criminal offenses committed in information space. The rapid development of the information society has fundamentally changed the structure of crime: qualitatively new methods of encroachment have emerged, and the range of objects of legal protection has expanded. Contemporary legal doctrine accepts a methodology for classifying this group of offenses according to the role of information and communication technologies (ICT) in the mechanism of criminal activity: ICT is either the direct object of encroachment or a means of committing traditional crimes[19].

Systematization of offenses by object of encroachment

A systematic analysis of legislation and scientific sources makes it possible to distinguish three main groups of criminal offenses in information space.

First, crimes against information security. In this group, ICT and the protected state of information systems, data, and communication networks constitute the direct object of criminal encroachment.

Second, crimes committed through the use of ICT and directed against the individual. This group includes acts against life, health, honor and dignity, and the inviolability of private life, where the internet functions as a means of realizing criminal intent. In particular, legislative amendments adopted in Kazakhstan in 2023 tightened sanctions for crimes committed against minors, including acts involving systematic humiliation through telecommunications networks or the internet; Article 105(2) of the CC RK was supplemented with an aggravating circumstance where incitement to suicide is committed through a telecommunications network, punishable by deprivation of liberty for five to nine years[126].

Third, other crimes in the digital environment. This category includes economic crimes, such as fraud in the field of computer information, acts against intellectual

property, and crimes against public security, including the propaganda of terrorism, knowingly false reports of acts of terrorism, and the dissemination of extremist content.

Elements of crimes against information security

Crimes against information security are characterized by encroachment upon the protected state of data and supporting infrastructure[121].

Unlawful access to digital information (Article 205 of the CC RK). The legal essence of the act lies in the violation of the legally established procedure for access to information under a confidentiality regime. According to the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, nearly half of all offenses registered in the field of informatization and communications relate to this offense. The objective side is manifested in entering an information system without the owner's permission; minors often commit such acts out of game-related motives or a desire to "test themselves"[27].

Unlawful alteration or destruction of digital data (Article 206 of the CC RK). The act infringes upon the principle of information integrity. It may cause significant harm by disrupting the operation of state and commercial systems. For legal characterization, the existence of material consequences in the form of destruction, alteration, or copying of information serves as the basis.

Creation, use, and dissemination of malicious programs (Article 210 of the CC RK). The act threatens the resilience of the entire information environment. According to Kubanova and co-authors (2024), in 2024 the number of incidents involving malware in Kazakhstan increased to 45,027, more than doubling compared with 2023; according to KZ-CERT, the total number of cyber incidents reached 68,100, which is 97% higher than in the previous year[8]. Scientific analysis confirms the extremely high latency of this group of crimes, reaching 99.7–99.8%[27].

Unlawful acts committed through the internet

The second group in the systematization consists of crimes that have "migrated" from real space into the virtual environment. Here, the use of ICT becomes a method of committing the crime, as a set of processes for searching, collecting, and transmitting information.

Crimes against the individual. The internet and social networks are common environments for violations of the inviolability of private life (Article 147 of the CC RK), dissemination of knowingly false information damaging honor and dignity (in the relevant version of Article 274 of the CC RK), and incitement to suicide (Article 105 of the CC RK). According to data summarized by Karanov (2025), violations of privacy among minors account for a significant share of network crimes, especially in the form of unlawful collection and dissemination of personal information on social networks[127].

Economic and public encroachments. These include fraud in the field of computer information (Article 190 of the CC RK, in conjunction with the special structure of Article 210 of the CC RK), as well as the use of the internet to promote

terrorism and disseminate extremist materials. Kazakh law-enforcement practice in recent years demonstrates an increase in such encroachments: according to the Committee under the Prosecutor General's Office, 201 criminal offenses were registered in the field of informatization and communications in January–October 2025, which is 86.1% higher than in the corresponding period of 2024[129].

Specific features of the subjective side and social danger

For minor subjects, the structure of criminal intent is characterized by an “illusion” of impunity, which motivates destructive acts and leads adolescents to commit actions that appear “harmless” to them. Empirical studies consistently identify self-assertion (37.5%) and game-related curiosity (21.8%) as the main motives. At the same time, insufficient legal literacy among young people leads to a lack of awareness of the criminal-law nature of online actions: hacking accounts or using another person's information without authorization is perceived as a “natural” element of network communication[19].

Thus, criminal offenses in the field of informatization and communications are divided into computer crimes directed against the principles of confidentiality, integrity, and accessibility, and traditional crimes that use the internet as a high-tech instrument. The legal characterization of these acts shows that the digital environment qualitatively changes the mechanism of crime commission, while requiring the law enforcer to take into account the degree of specialization and actual motivation of minors.

Statistical analysis shows that the most frequent offense in this field is Article 205 of the CC RK (unlawful access to information, an information system or a communication network), which accounts for nearly half of all registered offenses. The next most common is unlawful destruction or alteration of information, classified under Article 206 of the CC RK (approximately 20%), followed by acts related to the creation, use, or dissemination of malicious programs (Article 210 of the CC RK, 11%)[27]. The high latency of these acts, reaching up to 85–90%, has been repeatedly confirmed by contemporary scientific studies[18].

An analysis of the specific features of applying criminal liability to minors in the Republic of Kazakhstan makes it possible to identify several fundamental aspects.

Age limits and subject status. Under Article 80(1) of the CC RK, minors are persons who, at the time of committing a criminal offense, have reached the age of 14 but have not reached the age of 18[CC RK]. For them, criminal liability is defined as the obligation to account for the act committed in the form established by law. The factual basis of liability is an act containing all elements of a criminal offense.

Specialized justice system. Kazakhstan remains the only state in Central Asia with fully functioning specialized interdistrict courts for juvenile cases; in order to implement the Law “On the Prevention of Offenses” dated 30 December 2025, new rules regulating the activities of commissions on juvenile affairs were approved on 30 March 2026[130]. This institutional solution establishes a special procedural regime

that ensures the protection of the adolescent's rights and takes account of his or her level of psychological maturity when assessing information-related encroachments.

Restriction of punitive measures. From the general list of punishments, which includes 11 types, only six may be imposed on minors in Kazakhstan under Article 81 of the CC RK: 1) deprivation of the right to engage in certain activities; 2) a fine; 3) correctional labor; 4) community service; 5) restriction of liberty; and 6) deprivation of liberty[CC RK]. The fact that the law permits a fine to be imposed only if the convicted minor has independent income or property subject to recovery, and allows recovery from parents only with their consent, reflects the principle of individualization of liability.

imposition of the obligation to apologize to the victim, aimed at awareness of guilt and resocialization;

issuing a warning and placing the minor under the supervision of parents, persons replacing them, or a specialized state body;

probation supervision, involving requirements such as a prohibition on visiting certain places and a prohibition on changing the place of study or residence without notice.

From a criminological perspective, such measures are more effective than deprivation of liberty for young offenders in the IT field: they make it possible to work with defects in legal consciousness and to form the adolescent's legal culture in the digital environment without isolating him or her from society. Practical data confirm that the typical profile of a minor cyber offender in Kazakhstan is a 16–17-year-old adolescent whose motive is self-assertion (37.5%) or game-related curiosity (21.8%). This scientifically supports the priority of preventive and educational measures[19].

The system of criminal-law measures applied to minors has a dual character: on the one hand, it is an instrument of state coercion; on the other hand, it is a mechanism of legal protection and socialization for persons with insufficient mental and social development. In contemporary legal doctrine, criminal-law influence on adolescents is not limited to purely punitive measures. The broad use of alternative measures aimed at reducing repression and correcting the offender without breaking social ties is becoming the main direction of the humanization of criminal policy.

The list of punishments imposed on minors is characterized by significant restrictions compared with the general list of measures applicable to adults. Article 81(1) of the CC RK establishes only six types of punishment applicable to such persons: deprivation of the right to engage in certain activities, a fine, correctional labor, community service, restriction of liberty, and deprivation of liberty[CC RK]. A similar approach exists in the Russian Federation: deprivation of liberty, as the most severe measure, is not applied to minors under the age of 16 who have committed minor or medium-gravity crimes, which reflects the principle of economy of repression[131].

The purposes of punishment in relation to minors also differ significantly. While punishment for adults is justified by a combination of restoring social justice and general prevention, juvenile policy gives priority to correcting the offender and preventing new crimes. The content of punishment is the obligation to account for the act committed in a form that promotes social adaptation. Accordingly, the court must take into account not only the gravity of the act, but also the adolescent's level of mental development, living and upbringing conditions, and the influence of older persons (Article 82 of the CC RK).

Compulsory measures of educational influence occupy a special place in the system of influence measures. In the classical sense, these are not punishments, but an independent form of implementing criminal liability: the court gives a negative assessment to the act committed, while considering that the adolescent can be corrected without criminal prosecution. Articles 85–86 of the CC RK establish traditional measures such as issuing a warning, placing the minor under the supervision of parents or a specialized state body, imposing the obligation to repair the harm caused, and restricting leisure time while imposing special requirements on behavior[CC RK]. In the field of informatization, the use of these measures makes it possible to correct defects in legal consciousness in a differentiated way, while forming the adolescent's proper perception of legal requirements in the digital environment[128].

In the contemporary criminal policy of the Republic of Kazakhstan, innovative measures, including the obligation to apologize to the victim and probation supervision, have been actively introduced. Probation supervision, imposed for a period from six months to one year under Article 85(4) of the CC RK, ensures continuous monitoring of the adolescent's behavior and the fulfillment of specific obligations, such as a prohibition on visiting certain places or changing the place of study or residence without notice. These measures solve the tasks of resocialization more effectively than short-term deprivation of liberty, which often deepens criminal attitudes[132; 133].

The effectiveness of influence measures is directly connected with the level of legal culture and education. As shown in the Scopus-indexed scientific analysis by Zhakenov, Kultemirova, and Ibraeva (2024), the experience of the Republic of Kazakhstan demonstrates that the function of preventing juvenile delinquency can be effectively performed only through coordinated interaction between law-enforcement agencies and specialized institutional structures; moreover, the clear separation of the juvenile direction within legal-policy processes is recognized as a specific feature of Kazakhstan's experience among Central Asian countries[134]. Integrating legal education into the process of serving a sentence, as a fundamental principle of juvenile justice, creates the prerequisites for preventing offenses in the digital world.

Criminal-law measures applied to minors constitute a differentiated system in which punishment is regarded as *ultima ratio*, while priority is given to compulsory measures of educational influence and probation. The corrective, preventive, and

social-rehabilitative purposes of these measures can be achieved only through individualization of liability, taking into account age-specific features. Kazakh practice, including the introduction of probation supervision and the obligation to apologize, enriches the arsenal of educational tools and provides a basis for generalizing mechanisms for preventing minors' offenses in the IT field.

The practical implementation of criminal-law norms in the field of informatization and communications with respect to minors is a complex process conditioned by the specific features of the digital environment and the distinctive nature of the subject composition. A scientific study of law-enforcement practice makes it possible to identify a significant gap between the rapid development of IT and the readiness of the law-enforcement system to respond effectively to new cyber threats.

Contemporary judicial practice in the Republic of Kazakhstan and the Russian Federation shows a steady increase in the share of crimes committed using ICT. According to the Committee under the Prosecutor General's Office of the Republic of Kazakhstan, 201 criminal offenses were registered in the field of informatization and communications in January–October 2025, which is 86.1% more than in the corresponding period of 2024[22]. According to KZ-CERT, the total number of registered cyber incidents in 2024 reached 68,100, increasing by 97% compared with 2023; 66.1% of them were connected with computer viruses, network worms, and Trojan programs[135]. At the same time, in 2024 the damage from cybercrime in the country increased 41-fold compared with 2023, and in January–October 2025 reached 16.4 billion tenge, of which 99.8% constituted losses of state institutions[129].

The most pressing feature of this field is the latency of acts. Scientific literature substantiates that the registration of cybercrimes does not exceed 10–15% of their actual number; this is mainly explained by victims' failure to apply to law-enforcement bodies or their lack of confidence in the prospect of bringing the perpetrators to liability[27; 18]. For example, according to the Ministry of Internal Affairs of the Republic of Kazakhstan, the clearance rate for cybercrimes in 2024 was 28.4%, while in the first quarter of 2025 it reached 38.9%; thus, despite growth, more than half of offenses in practice remain unsolved[136].

In the structure of offenses registered in the field of informatization, Article 205 of the CC RK (unlawful access to information) predominates, accounting for nearly 50% of all cases in this category. Judicial practice shows an increase in the share of acts committed by minors through the unlawful collection and dissemination of personal information (Article 147 of the CC RK). The number of criminal cases involving the unlawful sale or dissemination of personal data has increased: in January–July 2024, 65 administrative cases were registered for violations of personal-data protection legislation, 75.7% more than in the previous year[137]. In June 2025, during a joint operation by the Ministry of Internal Affairs and the National Security Committee of the Republic of Kazakhstan, 140 persons engaged in the unlawful sale

of personal data were detained; their acts were classified under Article 205(3), Article 147(5), and Article 211(3) of the CC RK[138].

The application of criminal-law norms in information space is connected with a number of organizational, legal, and methodological difficulties.

Insufficient specialized knowledge. One of the main obstacles to high-quality investigation is the lack of in-depth knowledge of modern computer technologies among law-enforcement and judicial personnel. In practice, this leads to classification errors and the unjustified termination of cases on the ground that no elements of a crime are present[42].

Difficulties in determining the subjective side. In cases involving adolescents, law-enforcement bodies face the problem of proving intent and specific motivation. Immaturity of thinking and the illusion of anonymity complicate the correct characterization of minors' intent and the legal quality of their actions[27].

Law-enforcement practice demonstrates that systematic monitoring of social media is the most effective method for identifying destructive behavior. Scientific studies, including a study conducted in the Voronezh Region, found that approximately 19.5% of adolescents' accounts contained destructive content involving the promotion of violence or elements of humiliation[122].

As Kubanova and co-authors (2024) note, the creation of specialized cybersecurity units in Kazakhstan, including the Cybercrime Department under the Ministry of Internal Affairs of the Republic of Kazakhstan and the coordination centers KZ-CERT and KZ-FinCERT, has significantly strengthened the institutional nature of the state-level response; however, the development of a normative model for interaction between state bodies and the private sector, as well as the improvement of legal mechanisms for international cooperation, remain unresolved issues identified by these authors[9].

In Kazakhstan, judicial consideration of this category of cases falls within the exclusive jurisdiction of specialized interdistrict courts for juvenile cases. Court practice observes the principle of the priority of education over punishment; the scientific justification for this approach lies in the fact that compulsory measures of educational influence, including warning, placement under supervision, and probation supervision, are significantly more effective than deprivation of liberty in correcting an adolescent's legal consciousness. However, law-enforcement practice in the Russian Federation and the Republic of Kazakhstan clearly demonstrates the need to improve the legislative framework. In the Scopus-indexed analysis by Jilkishiyev and Begaliyev (2024), the conclusion is substantiated that it is necessary to simplify the procedure for collecting digital evidence, gradually introduce artificial intelligence technologies for analyzing suspicious actions, and create specialized units within pre-trial investigation bodies to combat cybercrimes[140].

The analysis of law-enforcement practice reveals a contradiction between the mass nature of minors' information offenses and the limited ability of the law-enforcement system to detect them under conditions of high latency. The main

difficulties are the shortage of highly specialized personnel, the technological complexity of proof, and the transboundary nature of cybercrime. Practice confirms that the most effective model of juvenile justice in the digital sphere is one that combines the prompt identification of destructive content involving minors with soft measures of educational and rehabilitative influence. The identified problems ensure the transition to the final analytical stage: a systematic examination of the set of legal problems in the implementation of criminal liability.

As a result of the scientific analysis conducted, systematic legal and organizational issues have been identified in the implementation of the institution of bringing minors to criminal liability for offenses in the field of informatization and communications. This field is characterized by a deep contradiction between the rapid digital transformation of public relations and the inertia of legal-regulation mechanisms; this contradiction creates a number of difficulties at the stages of detection, investigation, and judicial consideration of offenses.

Problems of identifying offenders and establishing identity in the digital environment are conditioned by the transboundary nature of information networks and the illusion of anonymity. According to studies, the latency of cybercrimes reaches 99.7–99.8%, while the registration rate amounts to only 10–15% of the actual number[27]. The main factors hindering identification are:

- transboundary nature, where the offender and the server may be located in different jurisdictions, requiring lengthy international cooperation procedures;

- the location of the headquarters of major ICT companies in other states, mainly in the United States, which makes it possible to obtain IP addresses and user data only through international legal-assistance requests, significantly extending the time needed to collect evidence;

- technical masking tools, where the use of anonymization and closed communities in messengers such as Viber, WhatsApp, and Telegram significantly complicates identification of the subject; in this context, the April 2026 report of the Committee under the Prosecutor General's Office of the Republic of Kazakhstan identified 18 new cyber threats, including SMS blasters, phishing mailings, and deepfake technologies[129].

The insufficiency of legal regulation under conditions of rapid technological development is manifested in the objective lag of the legislative framework behind the evolution of crime. Criminal law cannot respond quickly enough to qualitatively new methods of encroachment, such as the use of neural networks, deepfakes, and new forms of online psychological pressure. The criminal-law assessment of cyberbullying is especially relevant: despite its high social danger, it has not been separated as an independent offense in the CC RK; in the current system, its elements are covered by offenses such as insult, defamation, incitement to suicide, and violation of privacy. This approach requires the existing offenses to be supplemented with qualifying elements; otherwise, “normative lacunae” arise[126].

The main legal problems in implementing liability in the field of informatization are the technological complexity of collecting digital evidence, high latency caused by difficulties in identifying users, and the insufficiently rapid adaptation of legislation to new cyber threats. The identified deficiencies in the system of proof and normative regulation confirm the need to create a specialized legal mechanism for protecting the information security of young people, covering both the technical modernization of investigative bodies and the improvement of juvenile policy in the digital environment. These conclusions provide a direct basis for formulating the final scientific and practical recommendations of the study.

The set of systemic legal problems that arise when bringing minors to liability for cybercrimes requires the formulation of comprehensive directions for improving this institution. Scientifically grounded modernization must cover three interconnected levels: normative-legal, criminal-policy, and preventive-technological. The ultimate purpose of these changes is to create in the state a “specialized legal mechanism for protecting the information security of young people” capable of effectively combining coercive measures with educational influence.

Improvement of criminal legislation

An important aspect is the differentiation of liability depending on the gravity of the offense and the amount of harm caused. For minor offenders in the IT field, it is appropriate to introduce a flexible system for assessing public danger: this system would take into account not only formal harm, but also the nature and orientation of the subject’s intellectual potential. The list of crimes for which liability begins at the age of 14 requires expert review and ordering in relation to a number of offenses, for example Articles 177, 178, and 184 of the CC RK: the inability of adolescents to properly understand the significance of the special objects of encroachment makes the doctrinal basis for imposing liability from the age of 14 for these offenses questionable.

Improvement of criminal policy with respect to minors

Criminal policy in the digital era must shift from the paradigm of punishment to the paradigm of education and rehabilitation. The scientific basis for this shift lies in the principles of “education” and “least burdensome intervention,” which orient minors not toward stigmatization, but toward social rehabilitation. The main directions are as follows.

Development of juvenile justice. The practice of specialized interdistrict courts for juvenile cases is being consolidated as a promising model; in the new legal environment, this system requires stronger psychological and pedagogical examination in line with the requirements of the digital world, as well as deeper skills in working with digital evidence.

Introduction of elements of restorative justice. The effectiveness of the obligation to personally apologize to the victim and the obligation to repair harm is scientifically grounded; these measures form the adolescent’s awareness of the social consequences of actions committed in the virtual environment.

Development of the probation institution. The establishment of probation supervision for up to one year enables justice bodies to continuously monitor the adolescent's "digital behavior" and correct his or her legal consciousness through educational programs, while preserving social ties[25].

Development of mechanisms for preventing digital offenses

Prevention is scientifically recognized as a more effective instrument than measures of criminal prosecution. The set of proposals in this field includes the following.

Technological modernization of law-enforcement bodies. It is necessary to create specialized units, including 24/7 contact centers, staffed by employees with dual qualifications in IT and law. The use of artificial intelligence algorithms to analyze big data and automatically detect suspicious online activity by minors will make it possible to identify destructive behavior at an early stage; the Scopus study by Bolatbek and co-authors (2024), based on the example of university networks in Kazakhstan, experimentally demonstrates the effectiveness of such a system architecture[40].

Increasing legal literacy and cyber discipline. The Comprehensive Plan for the Protection of Children from Violence, the Prevention of Suicide, and the Ensuring of Their Rights and Well-Being for 2023–2025, approved by Resolution No. 748 of the Government of the Republic of Kazakhstan dated 31 August 2023, provides for 130 mandatory personal safety lessons in schools; the substantive scope of these programs must be expanded[142]. The goal is to eliminate the "contradictory core" in legal consciousness, namely the gap between technical skills and legal knowledge. As Kubanova and co-authors (2024) state, insufficient personnel qualifications and errors in system configuration have been identified as the main cause of 70% of successful cyber encroachments; this confirms the need to direct educational measures not only at children, but also at teachers and civil servants[9].

International cooperation. Given the transboundary nature of the internet, continued movement toward joining the general mechanism of the Council of Europe Convention on Cybercrime (Budapest Convention) is of strategic importance. Kazakhstan was invited to accede to this Convention in April 2023 and obtained observer status in the T-CY Committee; in November 2024, a joint roadmap seminar with the Council of Europe was held in Astana, and in October 2025 Kazakhstan signed the new UN Convention against Cybercrime[143]. These international instruments fundamentally simplify mechanisms for access to digital evidence and legal assistance in transboundary offenses committed by minors.

Social monitoring. Regular monitoring of social networks by specialized centers and the involvement of public organizations in organizing the leisure time of registered adolescents should be developed as tools for minimizing the influence of destructive internet content. In this regard, Zhumabekova and co-authors (2024) proposed a legal model for balancing protection from harm and the right of access to information within Kazakhstan's system for ensuring children's online safety[144].

Directions for improving the institution of criminal liability in the field of informatization and communications must develop along the path of a balanced combination of technological deterrence measures, the humanization of juvenile policy, and the systematic improvement of young people's legal culture. The creation of a specialized legal mechanism that integrates IT technologies into the investigation and sentence-execution process together with educational elements will enable the state to effectively counter cybercrime while preserving the social potential of the younger generation.

Summarizing the analysis conducted in Chapter Two, it is appropriate to systematize the main conclusions defining the legal specific features of minors' criminal liability in the field of informatization and communications. The study established that the penetration of digital technologies into all spheres has transformed information into an important object of property rights and a fundamental resource of economic circulation. In these circumstances, the legal nature of minors' liability acquires special features due to the properties of the virtual environment, including transboundary character, anonymity, and high speed, as well as the psychophysiological immaturity of the subjects.

Comprehensive nature of liability. One of the fundamental conclusions of the chapter is that minors' liability in the field under consideration has a comprehensive character and is implemented through the interconnection of civil-law, administrative, and criminal-liability institutions. Depending on the degree of public danger of the act and the level of its consequences, legislation provides for a differentiated approach:

civil-law liability is aimed at compensation for harm caused to intellectual property or online reputation;

criminal liability is applied as *ultima ratio* for highly dangerous acts such as unlawful access to systems, dissemination of malicious programs, or incitement to suicide.

The scientific basis of this systematic connection makes it possible to consider liability not only as a punitive instrument, but also as a mechanism for forming legal culture and legal thinking among adolescents. The analysis of law-enforcement practice in Kazakhstan confirms that the effectiveness of combating cybercrime among minors directly depends on the level of specialization of law-enforcement bodies and the degree of development of juvenile justice institutions.

Research logic of the next chapter. The accumulated theoretical arsenal and the identified legal problems, including high latency, difficulties of identification, and defects in legal consciousness, determine the logic of transition to the third chapter of the study: "Comparative Legal Analysis of International Experience in Regulating the Liability of Minors in the Field of Informatization and Communication Relations."

The criminal-law analysis conducted above also shows that the doctrinal development of the institution of minors' liability for offenses in the ICT field requires the following conceptual pillars. First, the limitation in Chapter 7 of the CC RK (Articles 205–213) of the object of criminal encroachment to the categories of

“computer information,” “information system,” and “information and communication network” does not allow the information-psychological security of a minor to be recognized without doctrinal obstacles as an independent object of criminal-law protection. The legal consequence of this doctrinal gap is that acts such as cyberbullying, digital grooming, unlawful profiling of personal data, and involvement in suicidal content do not fully fit within the existing constructions of Articles 130, 131, and 115-1 of the CC RK. To ensure continuity between these offenses, Chapter 7 should be supplemented with Section 7-1, “Criminal Offenses against the Information-Psychological Security of a Minor,” and Article 213-1 should be introduced into it; this provision would form the criminal-law support for Articles 1, 6, and 7 of the Law of 2 July 2018 No. 169-VI “On the Protection of Children from Information Harmful to Their Health and Development,” while supplementing Article 115-1 of the CC RK (stalking) with a qualifying element for acts against a minor would ensure differentiated criminal-law protection.

Second, the use of calendar age as the criterion of criminal liability under Article 15(1) and (2) of the CC RK is insufficient with respect to crimes in the ICT field. The study published with the dissertation author as co-author, Halibiyati H., Aratuly K., Serikhan A., Yergali A.M., Beaver K.M., “Neuropsychological Functioning and Its Association with Juvenile Arrest and Adulthood Incarceration” (Journal of Criminal Justice, 2024, Vol. 91, Article 102153, Scopus Q1, IF 4.3, DOI: 10.1016/j.jcrimjus.2024.102153), based on the Add Health longitudinal sample (n = 20,745), statistically proves that the level of verbal development and self-control functions as an independent predictor of the probability of arrest during minority. This empirical result constitutes a doctrinal basis for supplementing Article 80 of the CC RK with the category of “digital maturity” and for establishing neuropsychological examination, within Article 271 of the CPC RK, as a mandatory procedural measure for minors who have committed crimes in the ICT field. Digital maturity means the level of intellectual, emotional, and socio-legal development of a minor’s ability to understand the legal nature and virtual consequences of an act committed using information and communication technologies; this category is to be treated as an independent subject of procedural assessment by the court beyond formal biological age. From a comparative-law perspective, Article 20(3) of the Criminal Code of the Russian Federation, Article 11 of the Latvian Criminal Law, the 2021 Law of the PRC on the Prevention of Juvenile Delinquency, and the U.S. precedent *Roper v. Simmons* (543 U.S. 551, 2005) establish the international doctrinal basis for this category.

Third, according to 2025 data from the Committee on Legal Statistics and Special Records under the Prosecutor General’s Office of the Republic of Kazakhstan, 56% of persons involved in dropper schemes are young people aged 16–24, which justifies the need to supplement Article 232-1 of the CC RK, which entered into force on 16 September 2025, with a differentiated mechanism for minor subjects. In particular, supplementing Article 232-1 with a note stating that “where a minor

commits the act provided for in part one of this Article under the psychological influence of an adult offender or in a situation where he or she does not fully understand the legal nature of the act, the measures of educational influence provided for in Article 84 of the CC RK shall be applied with priority over criminal punishment” would ensure a genuine legal response by the state to the vulnerability arising from the minor subject’s lack of digital literacy. This doctrinal pillar substantiates the need, within the institution of digital delicts, to regulate at the legislative level the three independent roles of minors through differentiated liability mechanisms: victim (cyberbullying, digital grooming), offender (dropper schemes, unlawful access to information systems, dissemination of deepfake materials), and instrument (being induced to provide a bank account or register phishing websites).

Fourth, the participation of artificial intelligence (AI) and synthetic algorithms, including deepfake materials, chatbots, and generative models, in criminal-law relations requires doctrinal updating of the classification mechanism under Article 28 of the CC RK (complicity), the list of aggravating circumstances under Article 54 of the CC RK, and the list of mitigating circumstances under Article 53 of the CC RK. According to data from the Committee under the Prosecutor General’s Office for the first quarter of 2026, the structure of the 18 newly identified cyber threats, including SMS blasters, phishing mailings, and deepfake technologies, empirically confirms the trend of organized criminal groups systematically using AI systems, deepfake materials, and chatbots to psychologically manipulate adolescents. AI should be fixed in a threefold legal regime: as an independent aggravating means of committing a crime (Article 54), a qualifying element of complicity in a crime (Article 28), and an algorithm of mental coercion against a minor subject (Article 53); Article 3 of the CC RK should be supplemented with definitional provisions on “artificial intelligence system,” “synthetic algorithm,” and “deepfake material.” Article 210 of the CC RK should be supplemented with part 1-1 within the reception of Articles 7–11 of the Convention adopted by UN General Assembly Resolution A/RES/79/243 of 24 December 2024, so that it covers the production of phishing content and the creation of deepfake materials with the assistance of generative AI. This doctrinal pillar is the theoretical basis for the criminal-law support of the “Concept for the Development of Artificial Intelligence for 2024–2029,” approved by Resolution No. 592 of the Government of the Republic of Kazakhstan dated 24 July 2024.

Fifth, the closed list of measures of educational influence in Article 84(2) of the CC RK, including warning, placement under the supervision of legal representatives, establishment of special requirements for behavior, and socially useful work, does not take into account the substantive specific features of offenses in the ICT field. The empirical effectiveness of the Netherlands Hack_Right program (2018) substantiates the need to legislate structured educational courses on digital hygiene and cyberethics, participation in digital volunteer or cyber-squad programs, digital probation, and the digital expungement procedure. Accordingly, Article 84(2) of the CC RK should be supplemented with subparagraphs 5)–7), covering digital education courses,

participation in cyber-squad programs, and digital probation, while Article 79 should be supplemented with a digital expungement mechanism; at the administrative-law level, Article 65 of the CAO RK should be supplemented with a rule on the unconditional priority of educational measures over fines, and Article 57 should be supplemented with the use of ICT as an aggravating circumstance. This complex forms a criminal-law mechanism for the practical implementation of the principle of the priority of prevention over sanctions, enshrined in the Law “On the Prevention of Offenses” dated 30 December 2025.

Chapter 3. Comparative Legal Analysis of International Experience in Regulat-ing Minors' Liability in Informatization and Communication Relations

3.1 Liability of Minors for Offenses in the Field of Informatization and Communications in the CIS and Baltic States

The rapid digital transformation of public relations has provided the basis for the formation of new legal categories, among which the institutional system of information relations, also described by researchers as a “super-institution,” occupies a special place[145]. Within this institution, the search, storage, use, and protection of information carried out through digital technologies require legal measures aimed at reducing risks to subjects’ privacy and risks of unlawful influence. The issue becomes particularly relevant in the context of protecting the rights of minors, who, because of their age-specific characteristics and active participation in the virtual environment, become the category most frequently exposed to cyber threats[146]. In the CIS and Baltic States (the Russian Federation, Ukraine, Uzbekistan, Latvia, Lithuania, and Estonia), the formation of the protection of children’s digital rights as an independent legal institution arises from the objective need to adapt national legal systems to the challenges of the information society.

A historical and legal analysis shows that the initial basis for the formation of this institution was the development of model legislation within the CIS, in particular the Model Criminal Code adopted by the Interparliamentary Assembly of the CIS Member States (1996). On the basis of this document, the national legislation of Russia (Chapter 28 of the Criminal Code of the Russian Federation of 1996), Uzbekistan (the Criminal Code of 1994, supplemented in its latest version by Law No. ZRU-964 of 20 September 2024 concerning cyber-related provisions), and the Baltic States, which followed the path of humanizing criminal law by introducing the institution of criminal misdemeanors, was formed[145; 147]. A systematic approach makes it possible to consider the protection of children’s digital rights not merely as a set of prohibitive norms, but as a comprehensive system ensuring information security and the information sovereignty of the individual.

An important aspect of the theoretical justification is the analysis of the determinants of offenses in the field of informatization. Studies show that a low level of information culture among the population, software vulnerabilities, and the transboundary nature of cybercrime create conditions for the commission of offenses against children. In this regard, the institution of protecting children’s digital rights includes not only punitive measures, but also educational programs aimed at improving minors’ legal consciousness. For example, in the Kursk Region of the Russian Federation, legal education programs are being implemented to develop adolescents’ skills in critically assessing internet risks[146].

The legal significance of the institution under study lies in clearly defining the boundaries of permissible behavior in digital space and ensuring the inevitability of liability. As shown in the 2024 analysis by Kubanova and co-authors, the annual

growth rate of cybercrimes in CIS countries is particularly high: in 2024, the number of incidents registered by KZ-CERT reached 68,100, increasing by 97% compared with the previous year; the general pattern described by Kubanova in 2024 clearly demonstrates the tendency toward the “rejuvenation” of criminal activity in the high-technology sector, which makes it relevant to improve preventive and adaptive measures of criminal liability according to offenders’ age[9]. At the same time, a comparative analysis of Russian and Kazakh legislation reveals inconsistencies in the description of methods of committing crimes, confirming the need for further harmonization of legal norms at the interstate level.

In the CIS and Baltic States, the institution for protecting children’s digital rights has evolved from fragmentary norms to systematic legal regulation that comprehensively covers information security, criminal liability, and prevention. The purpose of this institution is to establish a protected digital environment in which legal liability prevents the unlawful use of information technologies against the interests of the younger generation. This goal requires constant monitoring of new forms of online crime and timely updating of the normative legal framework.

In conducting a comprehensive analysis of the experience of the Russian Federation, it should be noted that the development of legal regulation in this field is characterized by a transition from the fragmentary consolidation of norms to the formation of a comprehensive system for ensuring minors’ information security. In contemporary Russia, the protection of children’s digital rights is understood as an integral element of state policy aimed at reducing the risks of destructive influence under conditions of general informatization[145]. The legal basis of this process is formed by the combination of norms of international law, including the UN Convention on the Rights of the Child of 1989, and national legislation devoted to the specific features of the virtual environment.

The Concept of Information Security for Children in the Russian Federation, approved by Government Order No. 2471-r of 2 December 2015, acts as an instrument for implementing state strategy in the field under consideration and serves as a guideline for forming new prohibitions and mechanisms of protection from negative informational influence. Unlike traditional approaches, the Concept emphasizes the need to protect minors not only from technical threats, but also from “information-psychological aggression” capable of deforming the consciousness of a minor.

A systematic analysis of Russian legislation makes it possible to identify the normative acts that form the main “framework” of protection:

first, Federal Law No. 120-FZ of 24 June 1999 “On the Fundamentals of the System for the Prevention of Neglect and Juvenile Delinquency” establishes the legal basis for the activities of internal affairs bodies and other subjects in preventing offenses in the digital environment[150];

second, Federal Law No. 436-FZ of 29 December 2010 “On the Protection of Children from Information Harmful to Their Health and Development” establishes the

main mechanisms for classifying harmful information by age categories and restricting its dissemination;

third, Chapter 28 of the Criminal Code of the Russian Federation (Articles 272, 273, 274, 274.1, 274.2, and 274.3), as well as Article 272.1 (“Unlawful Use and/or Transfer, Collection and/or Storage of Computer Information”), introduced by Law No. 421-FZ of 30 November 2024 to strengthen the protection regime for personal data, contains in part 2 a qualifying element for acts involving minors’ personal data, increasing the term of deprivation of liberty to up to five years[151].

It is scientifically substantiated that repressive measures must be supplemented by methods of legal education. In the regions of the Russian Federation (Kursk and Rostov Regions and Krasnodar Krai), specialized training programs are being implemented for adolescents aged 14–18 to develop critical analysis skills regarding internet risks; these programs include interactive modules on legal liability and methods for resisting manipulation by professional criminals[146; 152].

Thus, a developed legal institution for protecting children’s digital rights has been formed in the Russian Federation. Its main characteristics are:

the priority of information security as the protected state of the individual from external digital threats;

the consolidation of the “digital” feature as a vector for strengthening criminal liability for crimes against minors, with Article 272.1 of the Criminal Code of the Russian Federation, introduced by Law No. 421-FZ of 30 November 2024, serving as a clear manifestation of this trend;

the active introduction of monitoring systems at the educational and law-enforcement levels for the early detection of destructive content;

an orientation toward legal education as a means of protecting the youth environment from victimization and improving information culture.

The experience of the Russian Federation shows that the protection of children’s digital rights is carried out through an extensive system of legislative acts in which the concept of information security and specialized norms of the Criminal Code of the Russian Federation, including Article 272.1 added in 2024, occupy a central place. The effectiveness of protection is ensured not only through strict sanctions for cybercrimes, but also through a combination of active monitoring of online space and educational initiatives. This experience is an important reference point for comparison with the legal systems of other CIS and Baltic States; its comparison with the approaches of Ukraine, Uzbekistan, and the Baltic States will be developed at the next stage of the study.

The analysis of regional approaches to protecting minors’ digital rights requires a systematic consideration of Ukraine’s experience. The Ukrainian legal system in the field of information relations developed in connection with general regional trends in the CIS, while preserving certain specific features of legislative technique. In forming the institution of information relations, Ukraine, like other countries of the region, faced the task of adapting norms of administrative and criminal law to the conditions

of rapid digital transformation. Unlike the Russian Federation, which followed the path of separating a special offense of fraud in the field of computer information (Article 159.6 of the Criminal Code of the Russian Federation), Ukrainian criminal legislation follows a different vector of criminalization[149].

Chapter XVI of the Criminal Code of Ukraine (“Crimes in the Field of the Use of Electronic Computing Machines (Computers), Systems and Computer Networks, and Telecommunication Networks,” Articles 361–363-1) contains a developed set of offenses: Article 361 of the Criminal Code of Ukraine concerns unauthorized interference with computer systems; Article 361-1 concerns the creation, dissemination, and sale of malicious software; Article 361-2 concerns unauthorized actions with restricted-access computer information; and Article 362 concerns the consequences of unauthorized actions with computer information committed by a person who has access rights[153]. This model separates systematic cybercrime offenses while also combining an approach in which, as in Ukrainian doctrine and in Uzbek and Azerbaijani legislation, the use of digital technologies is perceived as a factor that significantly increases the public danger of traditional crimes. According to open data from the Ukrainian state cyber police, the number of criminal cases initiated under Article 361 increased from 432 in 2015 to 1,795 in 2017, almost a fourfold increase, which is a clear indicator of the statistical growth of digital crimes[154].

Ensuring children’s digital security in Ukraine is based on the concepts of information sovereignty and security of information resources. The activities of law-enforcement bodies are aimed at protecting the “classical triad” of subjects, namely the individual, society, and the state, from destructive information and telecommunication influence.

The main components of the Ukrainian control system are:

- counteracting information-psychological aggression aimed at deforming the consciousness of minors;

- monitoring network resources in order to detect the promotion of destructive ideologies and attempts to recruit young people through social networks;

- repressive mechanisms that block the possibility of harming the rights of the child by unlawfully altering the form or content of digital information.

Legislative regulation in this field requires internet platforms to comply with established rules for information protection and to ensure the confidentiality of data belonging to minor users. Legal doctrine requires communications operators and owners of information systems to provide technical and organizational measures to prevent unauthorized access to children’s data and to block malicious software.

Recognizing the insufficiency of repressive measures, Ukraine, like other CIS and Baltic States, integrates methods of legal advocacy and education into the child protection system. The ultimate goal of such programs is to reduce the victimization of young people and to form minors’ skills in critically assessing online risks.

The methodological foundations of such programs include:

interactive training modules that teach adolescents to recognize the “techniques” of professional cybercriminals and psychological traps on the internet;

the formation of law-abiding behavior through explanation of measures of legal liability for offenses in the field of informatization;

victimological prevention that protects children from involvement in antisocial activities and destructive movements.

The practice of implementing these programs at the regional level confirms that carrying them out in a virtual environment familiar to young people, through educational films and social media channels, makes it possible to achieve the maximum educational effect with minimal time expenditure. Systematic legal education is a significant factor in reducing criminality among minors. Thus, Ukraine’s specific feature is a comprehensive criminal-law protection model that combines the recognition of ICT use as a qualifying element of traditional encroachments with a special chapter on crimes against computer information (Articles 361–363-1). Children’s digital security is ensured through law-enforcement control, the liability of information infrastructure subjects, and active legal education of the younger generation.

A comparison of Ukraine’s experience with the general regional standards of the CIS reveals the stability of the trend toward integrating the digital feature into the system of measures for protecting individual rights. The effectiveness of protecting minors directly depends on the balanced use of norms of administrative and criminal law, as well as on the quality of prevention programs adapted to the realities of the information society. The identified conclusions make it possible to move to the next stage of the study: consideration of the experience of the Baltic States (Latvia, Lithuania, and Estonia) within the framework of European digital security standards.

Stage 4. Study of Uzbekistan’s Experience

The substantive core of this approach is the recognition that digital transformation has changed the “scope” of information security. For Uzbekistan, this means the integration of the security of information resources and the criminal-law protection of information sovereignty into a unified system. In particular, liability for the unlawful circulation of special technical means intended for secretly obtaining information (Article 278-3 of the Criminal Code) is understood as an encroachment on the information sovereignty of the individual. At the same time, with respect to the creation and sale of software products intended for committing cybercrimes (Article 278-2 of the Criminal Code), Uzbekistan applies a “hybrid” model: the range of acts is limited to unauthorized access to computer information, which contributes to the terminological precision and clarity of legal categories[145].

In Uzbekistan, the implementation of norms on child protection and ensuring information security is carried out through strict monitoring and restriction of the dissemination of destructive content. The timely legal response to the use of digital technologies for destructive influence on the younger generation is regarded as an interest of national security.

Uzbekistan has formed a developed normative framework aimed at suppressing information-psychological aggression:

first, combating religious extremism: Article 244-1 of the Criminal Code establishes liability for preparing, storing, and disseminating materials that threaten public security, including in electronic form and through communication networks. This norm is an instrument for blocking online recruitment and propaganda channels of destructive ideologies that are most dangerous for youth audiences;

second, counteracting “false” information: legislative amendments of March 2020 supplemented the Criminal Code with Article 244-5, introducing liability for disseminating inaccurate information, including on the internet. This norm acts as an instrument of state regulation of the information space, preventing panic and destabilization of public order, which is especially important given minors’ high level of engagement with unverified content.

It is scientifically substantiated that prevention should be aimed at minors’ acquisition of skills for critically assessing and analyzing risks in the virtual environment. Legal advocacy programs implemented with state support are aimed at explaining measures of legal liability and forming intolerance toward unlawful behavior on the internet. This ensures that children do not become “victims” or “tools” of professional cybercriminals.

The conclusion arising from this analysis is that the Republic of Uzbekistan has formed a unified legal institution for protecting digital rights, characterized by the following features:

systematicity and hierarchy: the existence of a specialized chapter in the Criminal Code and the active use of presidential acts to regulate the digital economy;

priority of state security: emphasis on blocking extremist content and false information as the basis of information stability;

breadth of the protected object: protection not only of individual technical systems, but also of the interests of the individual and society in the field of informatization as a whole;

adaptability: timely criminalization of new methods of committing crimes, including digital theft and forgery.

Thus, Uzbekistan’s experience demonstrates a model of active state intervention in the digital environment in order to ensure legal order and security for minor subjects.

A scientific analysis of Uzbekistan’s experience confirms the stability of a “broad” model of legal regulation, in which information security is treated as a unified institution for protecting national sovereignty and individual rights. Strict content control combined with a system of criminal liability for ICT crimes creates an effective barrier to cyber threats. The results obtained make it possible to move to the final comparative stage of the study: comparing CIS approaches with the legal standards of the Baltic States (Latvia, Lithuania, and Estonia) in order to identify general patterns and differences in ensuring children’s digital security.

A systematic analysis shows that in the Baltic States the protection of children's personal data is integrated into the broader structure of information security, understood as the protected state of information transmitted through network technologies from unlawful influence. The data protection regime in these countries includes:

first, the information sovereignty of the individual, namely recognition of the child's right to privacy and protection from unauthorized access to computer information;

second, regulation of providers' liability, including the establishment of specific obligations for subjects that ensure the functioning of information systems, including mechanisms of liability for violating the rules for processing minors' data;

third, protection of restricted-access information, understood as a set of technical and legal measures to prevent personal data leaks, which are recognized as an element of national security.

An important feature of the legal systems of Latvia, Lithuania, and Estonia is the use of a two-tier system of criminally punishable acts, consisting of crimes and criminal misdemeanors[147]. Unlike in most CIS countries, where a "police misdemeanor" usually remains within the framework of administrative law, in the Baltic States the institution of criminal misdemeanors enables a flexible response to minors' offenses in the digital sphere.

It is scientifically substantiated that this differentiation contributes to the humanization of criminal legislation. Alternative sanctions are provided for acts that do not pose a high public danger, namely misdemeanors:

finances and correctional labor aimed at educational influence;

community service, which makes it possible to avoid state coercion and conviction in the classical sense;

deprivation of the right to engage in certain activities, which may be applied to minors in cases of offenses in the field of informatization; for example, Article 65 of the Latvian Criminal Code significantly limits the list of types of punishment that may be applied to minors, with priority given to sanctions not connected with restriction of liberty.

At the same time, strict liability is preserved for serious cybercrimes such as unlawful access to information or the creation of malicious programs, especially where the act causes grave consequences. A comparative legal analysis proves that the Baltic model of "police misdemeanor" acts as an effective tool for reducing victimization among young people and rationalizing criminal prosecution by transferring low-danger digital deviations into the category of misdemeanors.

Control of internet content in the Baltic States is carried out within the concept of information security as an additional object of any digital crime against individual rights. In accordance with European directives, states implement mechanisms to suppress recruitment into and promotion of destructive ideologies, including Directive

(EU) 2017/541 on combating terrorism and Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography.

Important aspects of control include:

blocking harmful content: Baltic legislation provides for liability for offering services to host internet resources pursuing unlawful purposes, similar to the institution of “hosting” liability in some CIS countries;

counteracting destructive influence: prohibiting the dissemination of information that harms the spiritual and moral development of minors;

protection against online solicitation: criminalizing acts involving the recruitment of children into unlawful activities through electronic communication.

As in the experience of the Russian Federation, prevention is established as a priority direction in the Baltic States. Under conditions of the high latency of cybercrimes, with studies indicating that up to 20% are detected, it is scientifically substantiated that repressive measures alone are insufficient[146]. Prevention programs in Latvia, Lithuania, and Estonia are aimed at increasing information literacy and awareness of potential threats on the internet.

The comprehensive application of prevention measures includes:

legal education: forming the foundations of legal consciousness and intolerance toward unlawful behavior in the digital environment;

victimological prevention: teaching minors methods for recognizing and avoiding cyberattacks, as well as methods for protecting personal data;

cooperation with the private sector: interaction with IT companies to ensure the availability of safe software and parental-control tools.

The comparative analysis of the experience of Russia, Ukraine, Uzbekistan, and the Baltic States confirms the formation in the CIS and Baltic region of a unified “super-institution” centered on the rights of minors. Despite differences in legislative technique, from special cyberfraud offenses in the Russian Federation to the institution of misdemeanors in the Baltic States, the general trend is recognition of the digital feature as a vector of criminalization and a priority of state policy. Effective protection of children’s digital rights requires a systematic combination of hard-law measures, active monitoring of digital space, and continuous legal education adapted to the realities of the information society.

The CIS countries (Russia, Ukraine, and Uzbekistan) are distinguished by adherence to hard-law repressive instruments that formulate criminal-law prohibitions in order to block any possibility of harm to the individual, society, and the state.

The Russian Federation emphasizes information security as the protected state of the individual from external digital threats. A specific feature of the Russian approach is the active use of administrative and preventive mechanisms, such as monitoring students’ social media accounts to detect susceptibility to destructive ideologies. Through the introduction of Article 272.1 into the Criminal Code of the Russian Federation by Law No. 421-FZ of 30 November 2024, a special sanctions system was created for liability for acts involving minors’ personal data: for acts

concerning minors' personal data, deprivation of liberty is established for a term of up to five years[8].

Ukraine, in line with the regional trends of the CIS, develops a model that preserves a separate chapter on unauthorized interference with computer systems (Articles 361–363-1), while combining it with recognition of ICT use as a qualifying element of traditional crimes; this model is aimed at ensuring the inevitability of liability for offenses in the digital environment.

Despite differences in vectors, namely state control in the CIS and protection of the rights of data subjects in the Baltic States, all the states studied follow the same fundamental principles for protecting children's rights on the internet:

first, recognition of information security as an additional protected object for all crimes against the individual committed in the digital environment;

second, a dual classification of acts distinguishing cybercrimes from traditional crimes qualified by a digital feature;

third, the need for legal education as a method of protecting the youth environment from victimization, recognized in all jurisdictions as an important factor.

In the countries studied (Russia, Ukraine, Uzbekistan, the Baltic States, and Kazakhstan, which is similar to them in terms of its regulatory model), there is a clear tendency to divide liability into criminal and administrative types, or an equivalent misdemeanor category.

Criminal liability. In the CIS countries, the dominant model divides digital offenses into two groups: genuine cybercrimes, such as unauthorized access and malicious programs, and traditional crimes qualified by a digital feature, such as theft and fraud. According to the criminological study conducted by Karabekov (2025), most cybercrimes in the Russian Federation and Kazakhstan are directed against property: 63.53% in Russia, including fraud at 50% and theft at 14%, and 94.46% in Kazakhstan, including fraud at approximately 90%[20]. According to data from the Scopus-indexed study by Kubanova and co-authors, in 2023 nearly 700,000 cybercrimes were registered in Russia, and attacks have a transboundary character[9; 39].

Administrative liability and misdemeanor. A unique feature of the legal systems of the Baltic States and Kazakhstan is the two-tier system of criminally punishable acts, consisting of crimes and criminal misdemeanors[146]. An act that does not pose great public danger and for which lighter punishments are provided, such as fines, correctional labor, or arrest, is recognized as a criminal misdemeanor. In Russia, similar acts are classified as administrative offenses or minor crimes.

Age limits and subjective characteristics

The age threshold for liability in the digital sphere has specific features due to the “rejuvenation” of criminal activity.

Russian Federation. Prevention and education programs focus primarily on the 14–18 age group. This is precisely the age group in which minors are capable of

objectively perceiving information about legal liability and the consequences of their actions.

Differentiation of punitive measures and educational influence

The specific feature of minors' liability is the priority of educational purposes over punitive purposes.

Types of punishment. Specific measures are applied to minors, including placement in educational colonies for persons under 18 and the use of alternative sanctions. In Kazakhstan, community service is actively used for misdemeanors. With respect to offenses in the field of informatization, additional punishments such as deprivation of the right to engage in certain activities are also provided (Article 81 of the CC RK). According to comparative legal data, the list of types of punishment that may be applied to minors includes three types in Bulgaria, Romania, and Turkmenistan; four types in Azerbaijan, Armenia, Hungary, Latvia, Lithuania, and Uzbekistan; five types in Tajikistan and Ukraine; and six types in Belarus, Kazakhstan, and Russia[158].

Educational measures and legal education. It is scientifically substantiated that hard-law repressive instruments must be supplemented by methods of legal education. In Russia, based on the experience of the Kursk Region, Rostov Region, and Krasnodar Krai, interactive training modules have been developed to help adolescents acquire skills for critically assessing the risks of involvement in criminal activity[152]. These programs teach minors to recognize the "psychological traps" of professional criminals and explain the consequences of applying measures of legal liability.

The comparative legal analysis confirms that, despite the commonality of the basic principles of child protection, countries use different strategies. In the CIS countries (Russia and Uzbekistan), emphasis is placed on state control and criminal-law blocking of destructive informational influence. In the Baltic States and Kazakhstan, a humanization model is being actively introduced through the institution of criminal misdemeanor, making it possible to achieve educational influence with minimal cost to the adolescent's social status. Recognition of information security as an additional object of protection is a common trend for all states; it requires law-enforcement bodies, such as Kazakhstan's Cybercrime Department or the internal affairs bodies of Russia, to adopt a strategy of "working before confrontation" through monitoring and victimological prevention.

Systematizing the specific features of minors' liability in digital space confirms that a differentiated approach to children's offenses has been formed in the CIS and Baltic States. Although criminal liability for acquisitive cybercrimes remains strict, the practice of applying educational and preventive programs based on interactive legal education is expanding. The effectiveness of protecting children's digital rights directly depends on the balance between hard-law repressive measures and the formation of information culture among the younger generation, which provides the logical completion of the study of the legal institution of liability in the field of informatization.

The contemporary criminal situation in the cyberspace of the CIS and Baltic States is characterized not only by quantitative growth, but also by qualitative transformation. This predetermines the objective need to move from hard-law repressive measures to systematically organized prevention. Under conditions of the “rejuvenation” of criminal activity, when skills in using digital technologies are formed at preschool age, traditional methods of preventing offenses require deep methodological adjustment. The scientific justification of preventive measures is based on the understanding that the information security of the child is an additional object of legal protection and that prevention of offenses must be carried out by influencing the determinants of criminal behavior before harmful influence occurs.

In the system for preventing digital offenses, legal education and awareness-raising on internet safety occupy a central place. The experience of the Kursk Region, Rostov Region, and Volgograd Region of the Russian Federation has scientifically substantiated the effectiveness of introducing specialized educational programs adapted to the realities of the information society. Programs aimed at the 14–18 age group are based on the modular principle and pursue educational objectives[152].

A systematic analysis makes it possible to distinguish four main blocks or modules of educational influence:

- first, the theoretical-criminological block: introducing minors to the nature and features of professional cybercrime;

- second, the victimological block: studying the “techniques” and manipulation schemes used by online criminals to involve children in destructive acts;

- third, the legal-liability block: detailed explanation of measures of criminal and administrative liability for offenses in the field of informatization;

- fourth, the practical-preventive block: forming skills for critically assessing risks and resisting antisocial activity.

An interactive approach using a virtual environment familiar to young people, such as educational films and case assignments, makes it possible to achieve an educational effect with limited time expenditure. The educational potential of these measures lies in developing adolescents’ ability to compare their internet behavior with the moral and legal norms established by the state.

Preventive activity is not limited to influencing the personality of the child; it must include mechanisms for regulating the activities of legal representatives and technological subjects. In the Russian Federation, the “Strategy for the Development of Education in the Russian Federation for the Period until 2030 and for the Prospective Period until 2036,” approved by Government Order No. 2040-r of 19 August 2024, is aimed at creating conditions for improving families’ information culture. The social impact of prevention programs is expanded by providing parents with tools for understanding real digital threats, such as bullying or involvement in destructive movements.

A comparative legal analysis of CIS legislation reveals a trend toward legalizing the liability of internet platforms and providers. In particular, the criminal

codes of Kazakhstan (Article 212 of the CC RK) and Turkmenistan (Article 335) introduce liability for providing hosting services to host resources pursuing unlawful purposes. This creates a legal basis for state regulation of digital infrastructure by obliging platforms to comply with information security rules and block harmful content.

State control in the field of preventing digital offenses in CIS countries is developing toward active monitoring of the information environment. In the Russian Federation, mechanisms for targeted monitoring of students' social media accounts are being introduced at the regional level, using the examples of the Kursk, Rostov, and Volgograd Regions; relevant orders of educational authorities legalize external monitoring of students' pages in order to identify destructive manifestations, extremism, and susceptibility to unlawful rallies[152]. In the state control system of CIS countries, specialized units such as Kazakhstan's Cybercrime Department, which is oriented toward the prompt detection and prevention of acquisitive cybercrimes, have special significance. Interaction between internal affairs bodies and educational organizations makes it possible to implement comprehensive plans for ensuring information security, including both technical protection and legal advocacy.

The effectiveness of preventive measures directly depends on the depth of analysis of cybercrime determinants. Researchers distinguish internal factors, such as a low level of awareness, software vulnerabilities, and youth unemployment, and external factors, such as the activities of international hacker groups and the transboundary nature of the network.

To neutralize these factors, a two-level classification of measures is proposed:

state level: improving information culture, creating databases on crime detection methodologies, and introducing educational courses;

interstate level: establishing effective cooperation within the CIS and CSTO, and adopting unified normative acts and cybersecurity standards. The UN Convention against Cybercrime, adopted by UN General Assembly Resolution A/RES/79/243 of 24 December 2024, opened a new stage in mechanisms of global cooperation[159].

Statistical data confirm that intensive legal advocacy and information-legal activities by units of the Ministry of Internal Affairs lead to a real reduction in the level of criminal activity among minors, which is especially evident in regions with high coverage by preventive measures[152]. The analysis conducted leads to the conclusion that the prevention of minors' digital offenses in the CIS and Baltic States has become a complex, interdisciplinary institution combining educational, legal, and control measures. While CIS countries are dominated by a model of state monitoring and strict content regulation, the Baltic States focus primarily on personal-data protection and legal education. The general vector of development is recognition that the most effective means of protecting children's rights on the internet is the formation of a law-abiding and information-literate person capable of independently identifying threats and resisting them.

The analysis of the nature of preventive measures revealed the important role of legal education and interactive educational programs in reducing the victimization of minors. The systematization of the experience of the CIS and Baltic States confirmed that the combination of state control, including content monitoring, and public influence, including education, creates the necessary barrier to cyber threats. These conclusions form a unified understanding of the mechanisms for ensuring children's digital security.

In this regard, the comparative legal significance of international experience is manifested in the following directions.

Terminological unification. To improve national law in the Republic of Kazakhstan, it is necessary to establish at the legislative level a uniform interpretation of the categories “cyberspace,” “cyber protection,” and “cybercrime,” which will make it possible to prevent a legal vacuum when classifying new types of encroachment.

Systematization of norms. The experience of the Republic of Belarus in developing the concept of a basic law “on ensuring information security” may serve as a guideline for Kazakhstan in integrating scattered positive and protective norms into a unified block within the institution of information relations[160]. The model of Article 272.1 of the Criminal Code of the Russian Federation (2024) also demonstrates the possibility of introducing into the relevant articles of the CC RK a qualifying element for acts involving minors' personal data.

Uniformity of judicial practice. For Kazakhstan, it is relevant to introduce the practice of adopting normative resolutions of the Supreme Court explaining issues of liability for crimes committed through the use of telecommunication networks, similar to the practice of the Supreme Courts of the Russian Federation and Belarus; this would ensure the predictability of law enforcement[161].

International experience proves that hard-law repressive instruments must be balanced with legal prevention and educational methods. The experience of the Kursk Region of the Russian Federation, involving the creation of interactive training modules for the 14–18 age group, is particularly important for Kazakhstan, where one of the main determinants of offenses is youth unemployment and insufficient information culture.

Priority directions for improving prevention in Kazakhstan based on international experience include:

- information volunteering: developing the potential of “cyber squads” to monitor and neutralize destructive content, including bullying and extremist propaganda, in the youth environment;

- victimological prevention: creating state programs to teach citizens individual strategies for protecting personal data and recognizing the “psychological traps” of cyber fraudsters;

technical advancement: expanding Kazakhstan's successful experience in blocking foreign calls from substitute numbers and creating specialized units modeled on the Cybercrime Department in all regions of the country.

From the standpoint of international cooperation, the strategically important directions for Kazakhstan are:

- accession to international conventions, including the 2024 UN Convention against Cybercrime, in order to ensure effective transboundary prosecution of offenders and real-time data exchange[159];

- use of the digital feature as a qualifying circumstance in traditional offenses such as theft and extortion, which has been partially implemented in the CC RK but requires further clarification regarding the use of artificial intelligence technologies.

The study of international experience is of fundamental importance for Kazakhstan: it makes it possible to integrate proven mechanisms for protecting the information sovereignty of the individual into the national legal field. The significance of this experience lies in the possibility of moving from a reactive model of justice, namely punishment for a committed act, to a proactive model, namely prevention through monitoring and education. The combination of strict state control typical of the CIS with European standards of personal-data protection will ensure the formation in Kazakhstan of a comprehensive system for ensuring minors' digital security.

The scientific justification of the comparative legal significance of international experience confirms the importance for Kazakhstan of developing legislation in the directions of terminological precision, strengthening preventive influence, and harmonizing national norms with international standards. Such an approach creates the basis for forming an effective strategy to combat cybercrime, oriented toward the protection of vulnerable subjects of digital relations, namely minors. This conclusion constitutes the logical result of studying the theoretical foundations and practical mechanisms of liability in the field of informatization and communications.

Summarizing the study conducted, it should be noted that the rapid transformation of public relations has led to the formation of the institution of information relations, which has turned minors' information security into an additional object of legal protection from destructive digital influence. The comparative legal analysis made it possible to identify the main determinants of cybercrime in the region: socio-economic factors in the form of youth unemployment, organizational and technical factors such as software vulnerabilities, and a low level of information culture.

The systematization of approaches to minors' liability in the field of informatization helps to identify the digital feature as a megatrend in the transformation of criminal policy; this feature serves as a vector for the criminalization of both genuine cybercrimes and traditional acts. In the CIS and Baltic States, stable preventive mechanisms have been formed that connect hard-law

repressive instruments with soft prevention mechanisms in the form of legal advocacy, interactive education, and monitoring of the information space.

The experience of the CIS and Baltic States reveals the coexistence of different models for protecting children's digital rights. In the Commonwealth countries (Russia and Uzbekistan), the dominant model is oriented toward state control and ensuring information sovereignty. In the Baltic States and partly in Kazakhstan, a humanization model is used, based on a two-tier system of criminally punishable acts, namely crimes and criminal misdemeanors, which effectively makes it possible to prevent "misconduct" among young people without excessive state coercion.

The conclusion of the paragraph emphasizes the importance of this experience in harmonizing the directions of legal prevention, personal-data protection, and state control. It is precisely the balanced combination of these elements that reduces the risks of children's victimization and ensures the inevitability of liability for offenses under the transboundary conditions of cyber threats.

3.2 Қытай Халық Республикасы заңнамасындағы ақпараттық қауіпсіздік және кәмелетке толмағандардың цифрлық қылмыстар үшін жауаптылығы

In the People's Republic of China, the formation and development of the institution of information security represents the state's systematic and gradually formed response to technological progress, the digitalization of public relations, and new threats emerging in cyberspace. The legal regulation of information security in China today is recognized not merely as a means of technical protection, but as a comprehensive legal institution aimed at protecting national security, public stability, data sovereignty, and the lawful interests of minors. In this regard, a scientific analysis of the prerequisites for the formation of the institution of information security in the Chinese legal system requires considering technological changes, social transformations, and the evolution of the legal framework in their interconnection[162].

Technological prerequisites were among the initial factors that directly influenced the formation of the institution of information security in the PRC. The rapid development of the internet and digital infrastructure, the mass spread of network services, the sharp increase in data circulation, the expansion of 5G infrastructure, and the penetration of digital platforms into all spheres of public life required the state to manage network space not only technically, but also legally. According to the 53rd Statistical Report on Internet Development in China, published by the Cyberspace Administration of China (CAC), as of December 2024 the number of internet users in the country reached 1.108 billion, while internet penetration stood at 78.6%[163]. These indicators confirm that the PRC has become one of the largest digital spaces in the world. Such large-scale digital infrastructure has generated new

legal challenges, including network attacks, unlawful circulation of data, leakage of personal information, algorithmic risks, and the involvement of minors in unlawful acts in the digital environment.

Social prerequisites also had a fundamental influence on the formation of this institution. In China, digital technologies have radically changed not only economic and administrative relations, but also everyday life, education, social interaction, and the organization of leisure. The early involvement of minors in the internet, the influence of network communications on their socialization, and the risk of exposure to harmful content have intensified public and legal attention. According to official CAC sources, as of June 2023 the number of minor internet users in China exceeded 191 million[164]. These data demonstrate that minors' participation in the digital environment is not a domestic issue, but a large-scale socio-legal problem.

The main stage in the institutional formation of information security was the Cybersecurity Law of the PRC (CSL), adopted on 7 November 2016 and in force from 1 June 2017[166]. This law defined network security as a basic element of state policy and established the duties of network operators, the real-name registration system, the protection of critical information infrastructure, and general requirements concerning data security. With amendments adopted on 28 October 2025 at the 18th session of the Standing Committee of the Fourteenth National People's Congress, the law underwent its most significant modernization since 2017: sanctions were substantially tightened, the scope of liability was expanded, the law's extraterritorial effect was strengthened, and provisions supporting the artificial intelligence sector were added. The new version entered into force on 1 January 2026[167]. Under Article 77 of the amended law, fines for serious violations were raised to 10 million yuan, approximately USD 1.4 million, and up to 1 million yuan for directly responsible senior personnel.

The theoretical analysis of the formation of the institution of information security in the PRC confirms that it arose from three interconnected prerequisites, technological, social, and legal, and that in substantive terms it developed as a comprehensive institution combining national sovereignty, data security, and the interests of minors. The analysis of these prerequisites makes it possible, at later stages, to reveal in detail the structure of the legal regulation system for information security in the PRC, the status of minors within it, and the mechanisms of liability for their digital offenses.

The system of legal regulation of information security in the PRC is a multilevel normative legal mechanism aimed at protecting state sovereignty in digital space, national security, public interest, network order, the security of data circulation, and the lawful rights of citizens, including minors. This system was formed as a result of the expansion of network infrastructure, the penetration of digital platforms into all spheres of public life, the transformation of data into an economic and strategic resource, and the increasing complexity of offenses in cyberspace. The contemporary legal model of the PRC treats information security not merely as technical security,

but as a comprehensive legal institution closely connected with national governance, data sovereignty, platform liability, and public stability[162].

Alongside the Data Security Law, the Personal Information Protection Law constitutes the third fundamental element of the PRC's information security system. The law was adopted in 2021 and established the principles of personal information processing, the procedure for obtaining consent, the rights of information subjects, and the duties of information processors. The law treats the personal information of minors under the age of 14 as sensitive personal information (敏感个人信息), requiring the consent of a parent or other legal representative for its processing (Article 31 of the PIPL). At the same time, Articles 44–47 of the law establish the data subject's rights of access, copying, correction, supplementation, and deletion, forming the Chinese structural equivalent of the “right to be forgotten” in Western doctrine. Thus, the PRC's information security system is not limited to network security and data security, but has also made the protection of the digital rights of the individual, especially the minor, an independent direction of legal regulation. This aspect is of particular importance in analyzing the legal status of minors in digital space.

The institution of protecting critical information infrastructure is also logically and legally closely connected with the PRC National Security Law adopted on 1 July 2015. Article 25 of the National Security Law establishes the general duty of the state to build a network and information security system, protect cyberspace sovereignty, and protect information infrastructure. For this reason, special laws and regulations in the field of information security in the PRC cannot be considered separately from the concept of national security. This reflects the distinctive feature of the PRC model: data security, network security, platform control, and information order are all integrated into one system within the logic of national security.

A special act that further specifies this system is the Regulation on the Online Protection of Minors, approved by State Council Decree No. 766 of 16 October 2023 and in force from 1 January 2024[165]. This Regulation is considered the first comprehensive special administrative act in the PRC dedicated to protecting minors online. It clearly provides for improving network literacy, regulating online information content, protecting personal information, preventing internet addiction, protection modes in smart terminals and applications, the duties of platforms, and the principle of social co-governance. Through this Regulation, the PRC supplemented general laws in the field of information security with a special legal regime aimed at the interests of minors.

One of the important practical directions of legal regulation concerning minors is the prevention of online gaming and digital addiction. The main official document currently in force at the central level in this field is the Notice on Strictly Limiting Minors' Addiction to Online Games, issued by the National Press and Publication Administration on 30 August 2021 (Order No. 14)[172]. Under this document, online game enterprises may provide services to minors only on Fridays, Saturdays, Sundays,

and statutory holidays from 20:00 to 21:00; all games must be connected to the real-name registration and login system; and the provision of game services to users not registered with real information is prohibited. Therefore, the PRC's system of legal regulation of information security in the field of protecting minors is implemented not through abstract declarations, but through specific temporal, technical, and organizational restrictions.

At the same time, draft acts that have not yet entered into force or have not been officially adopted must not be presented in scientific text as part of the current legal framework. For example, statements concerning a "2026 Law on the Prevention and Control of Cybercrime" may be considered only as a possible direction of legislative development, not as current law; the present official legal system is based on the laws and administrative acts mentioned above. Similarly, it would be inaccurate to describe the 2025 amendments to the Cybersecurity Law as a full-fledged special code on AI ethics: the current official framework supports such an assessment only within the narrower context of strengthening network security and legal liability, not in a broad sense[167]. Therefore, in describing the PRC's information security system, reliance only on officially adopted and effective acts is an obligatory condition of scientific accuracy.

The system of legal regulation of information security in PRC legislation is a multilevel and interconnected legal structure aimed at protecting the state's digital sovereignty, national security, data security, and citizens' lawful rights. Its foundation consists of the Cybersecurity Law (2016/2025), the Data Security Law (2021), and the Personal Information Protection Law (2021); the protection of critical information infrastructure, the processing of personal information, data classification, and cross-border control form special directions within this system; and the online protection regime concerning minors is specified through the Law on the Protection of Minors and the 2023 Regulation. In this regard, the analysis of the PRC's information security system confirms that it is not merely a technical control system, but an integrated complex of legal, institutional, and social governance mechanisms. It is precisely this legal complex that serves as the normative basis for explaining the status of minors in digital space and their liability for digital offenses.

In the legal system of the PRC, the status of minors in information legal relations appears as a comprehensive institution in which elements of state regulation, social protection, and a special legal regime intersect. PRC legislation treats minors in digital space not merely as ordinary users or vulnerable subjects requiring protection, but as an independent legal category to which special legal guarantees and specific restrictions apply. This status is primarily formed through the Law on the Protection of Minors, the Personal Information Protection Law, the Cybersecurity Law, and the Regulation on the Online Protection of Minors[165].

At the same time, PRC law recognizes minors not only as objects of restriction, but also as special subjects whose lawful interests and developmental needs must be protected in network space. Articles 1 and 2 of the Regulation on the Online

Protection of Minors establish that the purpose of online protection is to protect the lawful rights and interests of minors and to form a network environment favorable to their physical and mental health; these articles also directly provide for the principle of the best interests of minors and the principle of social co-governance. This means that the status of a minor in digital space in the PRC is defined not only through protection, but through a special legal approach adapted to the minor's age, psychological development, and the specific features of the network environment[165].

Another feature of this status is that minors' rights in information space are not granted as absolute freedom, but are combined with restrictions aimed at protecting their interests. The chapter on online protection in the PRC Law on the Protection of Minors provides that network products and services must not induce minors into addiction, and that providers of online games, online livestreaming, online audio-video, and online social networking services must introduce time-management, authority-management, and consumption-management functions with respect to minors. In this regard, the online legal status of minors in the PRC is formed through a balance between the "right to participate" and "restriction for protection."

One of the main legal guarantees defining the information-legal status of minors is the enhanced protection of personal information. The PRC Personal Information Protection Law and the Law on the Protection of Minors are aimed at preventing the unlawful collection, excessive processing, or unlawful disclosure of minors' personal information. In particular, the Law on the Protection of Minors provides that, at the request of a minor, his or her parents, or other guardians, the information processor must correct or delete the minor's personal information. Therefore, in this context, rather than directly using the Western doctrinal term "right to be forgotten," it is more accurate to describe the right in accordance with the specific norm of PRC legislation as the right to demand correction and deletion of personal information.

The status of minors in digital space is not limited to the recognition of rights; it also includes a mandatory protective architecture for the exercise of those rights. In this respect, PRC legislation establishes several key mechanisms.

First, the mechanism of real identification plays an important role. The Cybersecurity Law establishes a system of registration with real data in the fields of information publication, instant communication, and other network services, while Article 31 of the Regulation on the Online Protection of Minors provides that providers offering minors information publication and instant messaging services must request real identity data from the minor or his or her guardian. This demonstrates that minors' digital status in the PRC is based not on anonymity, but on clearly identifiable legal participation.

Second, special protection regimes for minors are introduced in the PRC. The Regulation on the Online Protection of Minors provides that network products and services intended for minors or having a significant impact on them must be equipped

with functions corresponding to their age characteristics, while smart terminals, applications, and services must apply technical measures aimed at protecting minors. In scientific text, the frequently used term “Minor Mode” or “minor mode” (未成年人模式) may be used here, but it must be explained in its legal meaning: it is not merely a market function, but part of the PRC’s special normative policy. In addition, the Guidelines for the Construction of Minor Mode on the Mobile Internet (移动互联网未成年人模式建设指南), published by the Cyberspace Administration of China on 12 November 2024, specify a coordinated protection system among mobile devices, applications, and application stores[173].

Third, in the PRC, minors’ information security is ensured through the principle of social co-governance. This principle is officially established in the Regulation on the Online Protection of Minors and in the Law on the Prevention of Juvenile Delinquency. Accordingly, responsibility for the digital security of a minor lies not only with the state or platforms, but also with schools, families, local authorities, cultural, health, telecommunications, law-enforcement, and other subjects. This approach proves that the PRC treats the minor in digital space not as a fully independent subject, but as an object of legal care jointly accompanied by various social institutions.

In analyzing the legal status of minors, the role of parents and other legal representatives is also special. PRC legislation recognizes parents or other guardians not merely as additional supervisors over minors’ actions in the digital environment, but as subjects with special duties established by law. Articles 16 and 17 of the Law on the Protection of Minors provide that parents or other guardians must educate minors in safety and law-abiding behavior, prevent their unlawful or criminal acts, and prevent their internet addiction. Articles 17 and 41 of the Regulation on the Online Protection of Minors require guardians to improve their own network literacy, educate, guide, and supervise the minor’s online behavior, and create conditions for safe and appropriate internet use. These norms form a regime of guardianship control as an integral part of the minor’s information-legal status.

In the legal system of the PRC, the information status of minors is also connected with the consequences of their independent digital behavior. If a minor’s conduct begins to acquire an unlawful character, his or her status includes not only the aspect of a “protected person,” but also the aspect of a subject requiring preventive and corrective measures. In this direction, the Law on the Prevention of Juvenile Delinquency plays an important role: it provides for early detection, prevention, intervention, and correction of minors’ bad behavior and serious bad behavior, requiring joint action by the family, school, society, and state bodies. Thus, in PRC legislation, the information-legal status of a minor is understood not merely as the status of a rights holder, but also as a status to which legal influence and resocialization mechanisms may be applied under certain circumstances.

In the PRC legal system, the information-legal status of minors is a complex legal construction formed through the combination of limited autonomy, enhanced personal data protection, a special online protection regime, parental and institutional control, and the principle of social co-governance at the state level. This status allows the minor to use the internet as a tool for development, education, and communication, while at the same time introducing special restrictions and technical-legal filters to protect his or her physical and mental health, personal information, and lawful interests. Therefore, in the PRC legal model, the status of minors in information space is closer not to a model of free digital autonomy, but to a paternalistic legal model combining protection and regulation. It is precisely this status that constitutes the main normative prerequisite for explaining minors' liability for digital offenses at later stages[165].

In the current legal policy of the PRC, the protection of minors from digital threats is viewed as an important component of the state's strategy for governing network space and of special legal policy aimed at ensuring the lawful rights and interests of minors. Legal regulation in this field is not limited to individual prohibitive norms; it is based on a comprehensive model that combines the coordinated powers of state bodies, the special duties of network product and service providers, the educational role of schools and families, and technical protection tools at the level of smart terminals and applications. This approach is primarily established in the Regulation on the Online Protection of Minors, while its legal foundations derive from the Law on the Protection of Minors, the Cybersecurity Law, and the Personal Information Protection Law[165].

The Regulation on the Online Protection of Minors is recognized as the main legal mechanism for protecting minors from digital threats in the PRC. This Regulation was published in October 2023 and entered into force on 1 January 2024; in official PRC explanations, it is assessed as the country's first comprehensive special legislative act dedicated to the online protection of minors. Articles 1–6 of the Regulation establish that the online protection of minors is aimed at forming a network environment favorable to their physical and mental health, and that the principle of the best interests of minors and the principle of social co-governance apply in this field. Thus, the PRC model for protection from digital threats is built not merely on prohibitions, but on a system in which the state, family, school, business, and society act together[165].

Protecting children from harmful and unlawful online information is one of the core elements of the PRC legal mechanism. The Regulation prohibits the dissemination through network products and services of information that harms the physical and mental health of minors; such information includes violence, pornography, terrorism and extremism, as well as content that induces minors to imitate dangerous acts, engage in risky conduct, display bad behavior, or adopt habits contrary to morality. In addition, official explanations specifically identify the impact of unlawful and harmful information on physical and mental health as one of the main

threats characteristic of minors in network space. Therefore, PRC legislation treats digital threats not only as attacks of criminal content, but also as content-based threats negatively affecting the development of minors.

In this regard, platforms are assigned specific duties to identify, process, and restrict harmful content. The Regulation requires network product and service providers to accept complaints concerning minors, verify reports, delete or block information containing signs of an offense, and establish convenient complaint channels and processing procedures that enable state supervision and public oversight. Here, the PRC model clearly shows that platforms are not neutral intermediaries, but legally responsible subjects of digital infrastructure. Therefore, the mechanism for protecting minors from digital threats is implemented not only through state filtering of content, but also through platforms' own duties of prevention, recognition, interruption, and cooperation.

Restrictions on online gaming are one of the most specific and legally clear mechanisms in the PRC system for protecting minors from digital threats. The main norm currently in force at the central level is the Notice on Strictly Limiting Minors' Addiction to Online Games of 30 August 2021. Under this document, all online game enterprises may provide services to minors only on Fridays, Saturdays, Sundays, and statutory holidays from 20:00 to 21:00; the provision of gaming services at all other times is prohibited. At the same time, all online games must be connected to the state real-name verification (实名认证) system, and users not registered with real data, including through "guest mode," may not be provided services[172].

The next direction in the PRC's protection of minors from digital threats is the introduction of special protection regimes. In this respect, the 2024 Guidelines for the Construction of Minor Mode on the Mobile Internet are of particular importance. These Guidelines were adopted on the basis of the Law on the Protection of Minors and the Regulation on the Online Protection of Minors, and are aimed at forming minor mode into a unified system at the level of smart terminal + application + application store (三方联动). The Guidelines establish requirements such as "three-party linkage," "one-click activation," optimization of time, content, and functions, and differentiation of recommended content by age[173]. Therefore, in the current PRC model, the protection of minors is implemented not only through the subsequent removal of content, but also through a pre-installed protective architecture.

The protection of minors' personal information is also a core part of the system for protection from digital threats. Under the Personal Information Protection Law, the personal information of minors under the age of 14 is considered sensitive personal information, and its processing requires the consent of a parent or other legal representative. The Law on the Protection of Minors and the Regulation on the Online Protection of Minors require information processors to observe the principles of legality, necessity, and good faith in relation to minors' personal information, and also not to collect information excessively[170]. Here, the legal protection mechanism in

the PRC recognizes digital threats not only as content-related threats, but also as threats in the form of unlawful collection, use, and dissemination of data.

Legal protection concerning minors' personal information is not limited to obtaining consent. PRC legislation also recognizes the rights of the minor or his or her legal representative to request access to, copying, correction, and deletion of information. Although this is sometimes described in scholarly literature as the "right to be forgotten," in PRC law it is more accurate to characterize it as the right to correction and deletion of personal information. The existence of such rights provides a basis for viewing the minor in digital space not merely as a passive object of protection, but as a special subject who, through a legal representative acting on his or her behalf, is given the opportunity to control his or her personal informational destiny.

The role of the school and family also occupies an important place among the legal mechanisms for protection from digital threats. Article 5 of the Regulation on the Online Protection of Minors assigns schools and families the duty to involve minors in useful activities, teach them to use the internet scientifically, civilly, safely, and appropriately, and prevent and intervene in internet addiction. Articles 17 and 41 of the Regulation provide that guardians must improve their own network literacy, supervise minors' online behavior, explain safety risks, and protect them from harmful information. Thus, in the PRC, protecting minors from digital threats is not only state control, but also a legally established family and educational duty.

The Law on the Prevention of Juvenile Delinquency also has its own place in this system. This law bases prevention on the combination of education and protection, early intervention, and tiered influence, and requires joint action by the state, school, family, and other subjects. This norm also applies to digital threats, because minors' exposure to harmful online environments, unlawful content, unlawful groups, or harmful digital behavior is assessed as one of the factors that may later lead to offenses. Therefore, the PRC model treats the protection of minors from digital threats not only as a matter of managing online content, but also as a component of offense prevention[171].

As for platform liability, PRC legislation provides legal consequences for network product and service providers that fail to perform their duties to protect minors. The Regulation establishes that network product and service providers, personal information processors, and manufacturers and sellers of smart terminals are subject to government supervision, must create complaint and reporting mechanisms, cooperate with inspections, and are liable under law if they violate established requirements. Thus, platform liability in the PRC is not limited to the declarative concept of "social responsibility"; it is implemented through specific legal duties and control procedures. In this respect, instead of mechanically transferring concepts such as VLOP (Very Large Online Platforms) from Western literature into PRC law, it is preferable to use the legal terminology of official Chinese acts: "special duties of network product and service providers"[165].

From a scientific standpoint, the PRC model for protecting minors from digital threats is based on the principle of comprehensive governance. In this model, legal prohibitions, technical restrictions, data protection, content control, platform duties, gaming time limits, real identification, parental control, and school-based educational work are integrated into one system. The distinctive feature of this model is that it is aimed not merely at eliminating the consequences of an offense, but at limiting the preconditions for the emergence of risk. In other words, protection mechanisms in the PRC are built as a preventive legal architecture preceding the criminal-law reaction.

In the legal system of the PRC, the institution of liability for minors' digital offenses is formed as part of general juvenile justice, but its content has become significantly more complex under contemporary digital conditions. This institution, on the one hand, establishes the age limits of criminal liability, specific elements of crimes, and procedural order; on the other hand, it includes mechanisms of education, correction, special influence, and resocialization. In PRC law, the main principle regarding minors is recognized as the principle of "education, persuasion, and rescue" and "education as primary, punishment as supplementary" (教育为主, 惩罚为辅); this principle is established in the Criminal Procedure Law, the Law on the Protection of Minors, and the Interpretation of the Supreme People's Court on the Application of the Criminal Procedure Law[174].

The analysis of minors' liability for digital offenses must begin, first of all, with the age-related limits of liability in the PRC Criminal Code. Under Article 17 of the Criminal Code, persons who have reached the age of 16 bear criminal liability on general grounds; persons between the ages of 14 and 16 bear liability only for serious crimes specifically listed by law; and persons between the ages of 12 and 14 may be held criminally liable only where intentional homicide or especially cruel intentional infliction of serious bodily injury has resulted in death or severe disability, and only with the approval of the Supreme People's Procuratorate. This norm was introduced by Amendment XI to the PRC Criminal Code, adopted on 26 December 2020 and in force from 1 March 2021[175]. At the same time, when sentencing persons who were under the age of 18 at the time of the crime, the principle of leniency or mitigation applies, and the death penalty is not applied to persons under 18. These rules are also the main legal criterion in the field of digital offenses, because minors who commit network or telecommunications crimes are first subject to these general age limits.

In this respect, an important feature of the institution of liability for digital offenses in the PRC is that not all digital acts apply to all age categories to the same extent. For example, although offenses such as unlawful use of an information network, unlawful intrusion into a computer system, assistance in network crime, or unlawful circulation of citizens' personal information are provided as independent offenses in the Criminal Code, most of them are not included in the list of specially enumerated serious crimes for the 14–16 age group. Therefore, in practice, full criminal liability for such offenses generally arises from the age of 16. This demonstrates that the PRC's institution concerning digital offenses combines

criminal-law influence with educational-legal influence: in some cases, special corrective measures prevail over criminal punishment.

The PRC Criminal Code does not regulate digital or information offenses committed by minors in a separate chapter; they are classified through the general criminal-law offenses concerning information and network crimes. These include, first of all, the following offenses: unlawful collection, sale, or provision of citizens' personal information (Article 253 of the Criminal Code); unlawful intrusion into a computer information system (Article 285); damage to a computer information system (Article 286); unlawful use of an information network (Article 287-1); and assistance in crime through an information network, 帮信罪 (Article 287-2)[176]. Therefore, when analyzing the institution of liability for minors' digital offenses, it is scientifically correct to consider it not through the abstract concept of "cybercrime," but through these specific general criminal-law offenses.

At the same time, in PRC law, a minor's participation in a digital offense is not always assessed in the same way. Law-enforcement practice seeks to take into account the minor's criminal intent, his or her level of understanding of the essence of the act, the influence of adults, the technical role performed, the desire to obtain material benefit, and his or her actual position. Typical cases published by the Supreme People's Procuratorate show the need not to equate a minor immediately with a professional criminal, but to assess the possibility that the minor was subject to imitation, inducement, or manipulation in the digital environment. Karanov's (2025) dissertation study on the criminological characterization and prevention of crimes against the person committed by minors using ICT also provides a theoretical and empirical basis confirming the correctness of this individualized approach[19]. This circumstance proves that the institution of liability for minors' digital offenses in the PRC has, alongside its punitive character, an individualized and rescuing element.

The special procedure of criminal proceedings also occupies an important place in understanding the institution of liability for minors' digital offenses in the PRC. The special chapter of the Criminal Procedure Law devoted to minors and the Supreme People's Court's Interpretation on its application establish special guarantees in cases involving minors: the participation of a legal representative or suitable adult, closed court hearings, special protection during the investigation and trial stages, and full explanation of the minor's rights. The Supreme Court's Interpretation clarifies that courts must be guided in such cases by the principle of "education as primary, punishment as supplementary"[177]. Therefore, even where the digital offense itself is classified under the same elements as in the case of an adult, the procedural regime applied to it has a special character corresponding to the status of a minor.

The role of parents and other guardians is also an important part of the institution of liability for minors' digital offenses in PRC legislation. Article 17 of the Criminal Code provides that, with respect to minors who are not subject to criminal liability because of age, parents or other guardians may be required to strictly

supervise and educate them. In addition, the Regulation on the Online Protection of Minors establishes the duty of guardians to supervise the minor's online behavior, improve his or her digital literacy, and prevent harmful information and addiction. The norms of the Law on the Prevention of Juvenile Delinquency allow law-enforcement bodies, where they determine in the course of a case that parents or other guardians have failed to perform their relevant duties, to warn them and require them to receive family education guidance (家庭教育指导令)[178]. Thus, in the PRC, liability for a minor's digital offense produces legal consequences not only for the minor, but also for the institution of family supervision.

One of the special humanistic mechanisms in the PRC juvenile justice system is the institution of sealing criminal records (犯罪记录封存). Under the Supreme People's Court's Interpretation on the Application of the Criminal Procedure Law, the criminal records of minors who were under the age of 18 at the time of committing a crime and who were sentenced to deprivation of liberty for up to five years or exempted from criminal punishment must be sealed. The Law on the Prevention of Juvenile Delinquency expands this protection by establishing a confidentiality regime not only for minors' criminal records, but also for records concerning special corrective education, special education, administrative punishment, compulsory measures in criminal proceedings, and exemption from criminal prosecution. Therefore, this should be described not as an abstract "erasure of the digital footprint," but more accurately as the institution of "sealing minors' records and protecting them from stigmatization."

The official practice of the PRC shows that the meaning of this institution is not to exempt the minor entirely from criminal liability, but to find a legal balance that allows him or her to return to society. Official materials of the Supreme People's Court and the procuratorial bodies note that in recent years there has been a certain growth trend in juvenile crime, including serious and network-related offenses, and therefore the model of "strict punishment where necessary, rescue and education where necessary" must be followed. This demonstrates the dual nature of the institution of liability for digital offenses in the PRC: on the one hand, socially dangerous digital behavior is not tolerated; on the other hand, legal mechanisms remain in place to preserve the minor's future and enable resocialization.

In the PRC, the institution of liability for minors' digital offenses consists of a combination of criminal-law limits, special procedural guarantees, prevention and intervention measures, special education and special corrective education, parental supervision duties, and humanistic protective mechanisms such as record sealing. The 2021 reform of the Criminal Code lowered the minimum age threshold for liability in certain circumstances to 12 years for especially serious crimes, while current practice in the field of network and telecommunication offenses continues to preserve individualized and staged influence with respect to minors. Therefore, the PRC model

is characterized as a combined model of strictness and correction in responding to minors' offenses in the digital era.

In the PRC, the system for preventing minors' digital offenses consists of interconnected multilevel mechanisms of state governance, legal regulation, platform liability, school education, and family supervision. In the current official legal model, this system is considered not merely as a means of influence after a crime has been committed, but primarily as a preventive structure aimed at early identifying and preventing the causes and risk factors of unlawful behavior. This approach is based on the principle of the best interests of minors and the principle of social co-governance established in the Regulation on the Online Protection of Minors, while its general legal basis consists of the Law on the Protection of Minors, the Law on the Prevention of Juvenile Delinquency, the Law on the Promotion of Family Education, and special regulatory acts concerning online games and digital services[165].

At the core of the prevention system in the PRC lies the concept of social co-governance (社会共治). Articles 2 and 3 of the Regulation on the Online Protection of Minors define the protection of minors online as a field jointly implemented by the state, schools, families, network product and service providers, and other social subjects. Official explanations emphasize that this Regulation is the first comprehensive special act in the PRC dedicated to the online protection of minors, and that it not only divides functions between the state and society, but also integrates them into one system. Therefore, the PRC model seeks, before responding to an individual offense, to bring under legal control the social environment that shapes the minor's digital behavior.

Another direction is real identification and managed access. In accordance with the general legal logic of network security and special regulation in the gaming field, the minor's participation in the digital environment is considered not as anonymous freedom, but as participation that is clearly identifiable and restricted according to age. This performs two functions in preventing offenses: first, it becomes more difficult for adults to use minors through false identification; second, platforms can introduce restrictions by time, content, and function according to age category. Therefore, in the PRC, the real-name registration system is not merely a security-control tool, but part of preventive legal architecture.

A further direction is early intervention in bad behavior and serious bad behavior. The Law on the Prevention of Juvenile Delinquency provides for identifying and intervening in a minor's unlawful behavior not only at the level of crime, but at earlier stages. According to the logic of the law, prevention is aimed at stopping risks observed early, preventing bad behavior from becoming serious bad behavior, and preventing serious bad behavior from becoming crime. Phenomena such as internet addiction, entry into harmful online environments, falling under the influence of unlawful groups, and assisting other persons' crimes through the network are considered precisely within this preventive approach. Therefore, the system for

preventing digital offenses in the PRC is based on the principle of “tiered intervention” before criminal reaction.

Another direction is creating conditions for minors’ safe digital development while limiting their gaming and digital participation. Official explanations state that the purpose of online protection is not only prohibition, but also providing minors with access to useful, age-appropriate content and services that do not harm health. This shows that the PRC prevention system is not one-sidedly repressive, but seeks to find a balance between “isolating the minor from danger” and “safe digital socialization.” Nevertheless, within this balance, priority is still given to state regulation and prior restriction.

The PRC legal model for information security and the protection of minors in digital space is one of the most institutionalized and multilevel systems today. The legal basis of this model consists of the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Law on the Protection of Minors, and the Regulation on the Online Protection of Minors. Official explanations state that the Regulation is the first comprehensive special act dedicated to the online protection of minors and that its content covers four main directions: improving network literacy, regulating online information content, protecting personal information, and preventing internet addiction. Therefore, the main advantage of the PRC model lies in its integration of legal regulation into a unified system rather than separate fragments[165].

In assessing the effectiveness of this legal model, it is first necessary to note its legal and institutional integrity. According to the official view, the online protection of minors is not merely the individual duty of parents or schools, but a comprehensive domestic national system based on the principle of “six protections” (六大保护): family, school, society, network, government, and judicial protection[179]. The Regulation on the Online Protection of Minors imposes specific duties on authorized state bodies, schools, families, network product and service providers, personal information processors, and smart terminal manufacturers. Official expert commentary indicates that this approach, while recognizing the minor not merely as a protected object but as an active participant of the network era, makes it possible to comprehensively establish a legal line of defense ensuring his or her safety. From this standpoint, the first strength of the PRC model is that it clearly distributes legal duties among various subjects and integrates them into one common system.

The second strength is that the model relies on specific preventive and technical-legal tools. For example, according to the official 2021 notice, all online game enterprises in the PRC may provide services to minors only on Fridays, Saturdays, Sundays, and statutory holidays from 20:00 to 21:00, and service provision at other times is prohibited; at the same time, all games must be connected to the real-name registration and login system. In addition, the Guidelines for the Construction of Minor Mode on the Mobile Internet of 12 November 2024 (CAC) provide for “three-party linkage” and “one-click activation” among smart terminals, applications, and

application stores[173]. Official publications clearly state that the purpose of these Guidelines is to move the functions for protecting minors out of a fragmented state and transform them into a unified protection system. Thus, the effectiveness of the PRC model is also reflected in the fact that it is based not only on general principles, but on applied legal and technical mechanisms.

However, the effectiveness of this PRC legal model is not assessed as absolute or flawless even in official materials. On the contrary, official assessments in recent years openly identify a number of shortcomings and unresolved issues. Official materials of the Supreme People's Procuratorate in 2026 directly state that in the field of online protection of minors, there remain problems such as insufficiently clear legal definitions of AI misuse (AI滥用), online violence (网络暴力), and other new forms of digital harm; an incompletely developed mechanism of stable and coordinated law enforcement; inconsistency of industry standards for platforms in protecting minors; and incomplete performance by enterprises of their primary responsibilities. This official recognition proves that, despite the strong legal foundation of the PRC model, the issue of rapid adaptation to new threats in the digital environment remains relevant.

Similarly, certain limitations are also recognized at the official legislative level. Official materials of the National People's Congress in 2026 noted that, despite the existence of the Law on the Protection of Minors and the Regulation on the Online Protection of Minors, issues remain due to the rapid renewal of technologies, including the unclear boundaries of regulation, insufficient convenience of rights-protection channels, and a lack of additional mechanisms[182]. In other words, the legal model has a normative basis, but questions such as which body acts within which limits, which channel a minor or his or her legal representative should choose to protect against an offense, and what standard should apply to new digital platforms have not been fully resolved. From this standpoint, the weakness of the PRC model lies not in its strict structure, but in the difficulty of flexibly adapting that structure to new digital forms.

In a scientific assessment of legal effectiveness, another limitation of the PRC model is the gap between the formal introduction of platform mechanisms and their actual effectiveness. In a 2025 official typical case of the Supreme People's Court, it was noted that although a short-video platform had a "minor mode," it failed to fully perform an actual protection function; a significant part of harmful information remained accessible through search, and the mechanisms of content review and warning were insufficient[180]. This official judicial assessment is particularly important because it demonstrates that the effectiveness of the PRC model depends not only on the existence of norms, but also on how those norms actually function within platforms. Thus, a strong legal model does not always automatically lead to equally high results; the quality of implementation is also a decisive factor.

In a scientific assessment of the PRC legal model for information security and the protection of minors in digital space, its main strengths include legal and

institutional integrity, the system of social co-governance, the presence of specific preventive mechanisms, the strict management regime for games and network services, and the active legal influence of courts and procuratorial bodies. Its main weaknesses include the insufficient legal definition of new digital threats, the inconsistency of platform standards, the incomplete stabilization of law-enforcement coordination, and the fact that the boundaries of regulation and protection channels are not always equally clear, as acknowledged in official materials themselves. Therefore, although the PRC experience is a powerful and comprehensive legal model for protecting minors in the digital era, its future effectiveness directly depends on how quickly and precisely the law adapts to new technological challenges.

The third similarity is the existence of a legal regime for personal data protection. In the PRC, this direction is systematized by the Personal Information Protection Law, and the personal information of minors under the age of 14 is placed under special protection as sensitive personal information. In Kazakhstan, personal data protection is regulated by the Law of 21 May 2013 No. 94-V “On Personal Data and Their Protection,” while official rules and current acts reflect requirements concerning the location of personal data databases and the infrastructure for their processing within the territory of the Republic of Kazakhstan, as well as the application of protection measures[184]. Thus, both states treat data as an important resource not only for the interests of the individual, but also for state legal control; however, in the PRC this regime is specified according to minors’ age category, while in Kazakhstan it operates within the general personal data protection system.

Differences. At the same time, the differences in legal regulation are much deeper. First of all, the nature of the regulatory architecture differs. In the PRC, the information security model is built as a centralized and highly specialized system through the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Regulation on the Online Protection of Minors, and the Guidelines on minor mode. In Kazakhstan, by contrast, this field is distributed across several separate laws and acts: the Law “On Informatization,” the Law “On Personal Data and Their Protection,” the Law “On the Rights of the Child in the Republic of Kazakhstan,” the Law “On the Protection of Children from Information Harmful to Their Health and Development,” the Law “On Online Platforms and Online Advertising,” and criminal and administrative legislation. Therefore, there are grounds to characterize the PRC model as unified and specialized, and the Kazakh model as sectoral and more fragmented.

The third difference concerns the depth of legal regulation of minors’ internet-use regime. In the PRC, under the official 2021 notice, the provision of online game services to minors is restricted to specific times: only on Fridays, Saturdays, Sundays, and statutory holidays from 20:00 to 21:00. At the same time, all online games must use real-name registration. In Kazakhstan’s official acts used for this comparison, including the law on protecting children from harmful information, the law on children’s rights, the law on online platforms, and basic laws in the field of

informatization, no mandatory nationwide state gaming-time limit comparable to the PRC regime was identified. This shows that the Kazakh model gives priority to content, access, and general security in protecting minors, while the PRC model additionally reaches the level of temporal management of behavior.

The fourth difference concerns the age threshold for minors' criminal liability. Under the PRC Criminal Code, general liability begins at the age of 16, a special list of serious crimes is established for persons aged 14–16, and persons aged 12–14 may be held liable only for especially serious violent crimes and only with the approval of the Supreme People's Procuratorate. Under Article 15 of the Criminal Code of Kazakhstan dated 3 July 2014 No. 226-V, general criminal liability begins at the age of 16, and for certain serious crimes at the age of 14[37]. Thus, although the general threshold in both states is 16, the PRC has an additional regime lowered to 12 years in exceptional cases, while Kazakhstan has no such exceptional 12-year threshold. Therefore, the PRC model is stricter with respect to grave crimes, while the Kazakh model preserves the traditional 16/14 structure.

The seventh difference lies in the structure of protecting minors' personal data. In the PRC, the personal information of minors under the age of 14 is legally recognized as a special category of sensitive personal information, and an enhanced consent and processing regime applies to it. In Kazakhstan's official acts used for this comparison, there is a general personal data protection regime, but no direct norm establishing the data of children under 14 as a separate sensitive category equivalent to the PRC regime was identified in those official sources[28]. This is another important difference between the two countries: in the PRC, the protection of minors' personal data is clearly differentiated by age threshold, while in Kazakhstan this field is mostly ensured through the general personal data regime and the system for protecting children from harmful information.

In a general assessment of the features of the legal systems, the PRC model may be characterized as a centralized, specialized, and highly technologically and legally managed system. In it, the status of minors in digital space, their online rights, restrictions, gaming time, personal data, platform duties, and protection regimes are regulated in detail and specifically. The Kazakh model, by contrast, may be assessed as a sectoral-normative and relatively more fragmented system: here, issues of protecting children from harmful information, regulating online platform activities, protecting personal data, and criminal liability are governed through different laws and subordinate acts. Karabekov's (2025) dissertation study on the state of cybercrime and preventive measures in the Russian Federation and the Republic of Kazakhstan empirically substantiates the sectoral and fragmented nature of combating cybercrime in post-Soviet legal systems and the need to systematize it[20]. That is, Kazakhstan's legal system also recognizes digital threats and responds to them, but it has not created a highly centralized regime concentrated in one act in the same way as the PRC.

The experience of the PRC in the field of information security and the protection of minors in the digital environment has significant legal importance for Kazakhstan. This importance lies not in the need to copy the PRC model completely, but in the possibility of adapting certain legal mechanisms of that model to Kazakhstan's current legal system. Both states treat information security as an important direction of state policy; this is also evidenced internationally by the joint participation of the PRC and Kazakhstan among the group of states that proposed the 2015 international code of conduct on international information security within the UN framework. At the same time, the PRC has formed a special and comprehensive legal regime for protecting minors online, whereas in Kazakhstan this field is regulated through several laws and subordinate acts. Therefore, the significance of the PRC experience for Kazakhstan lies primarily in the possibility of systematizing and clarifying legal regulation and strengthening a special child-oriented digital protection regime[165].

Formation of institutional and strategic foundations. The first legal significance of the PRC experience for Kazakhstan is that it demonstrates the need to distinguish the protection of minors in the digital environment not as a scattered issue within general information security policy, but as a separate legal direction. In the PRC, this task is performed by the Regulation on the Online Protection of Minors, which entered into force on 1 January 2024: it integrates issues of network literacy, harmful information, personal information protection, internet addiction, platform duties, and parental control into one system. In Kazakhstan, by contrast, similar issues are reflected at different levels in the Law "On Informatization," the Law "On Personal Data and Their Protection," the Law "On the Protection of Children from Information Harmful to Their Health and Development," the Law "On Online Platforms and Online Advertising," and the Law "On the Rights of the Child in the Republic of Kazakhstan." Therefore, the legal significance of the PRC experience for Kazakhstan is that it substantiates the need to develop a special concept, unified section, or special comprehensive legislative block dedicated to minors' digital security. This proposal remains relevant even though Kazakhstan itself, in the "Children of Kazakhstan" Concept for 2026–2030, has placed on the agenda digital mechanisms concerning children, including SIM cards for children and updating relevant norms.

Introduction of an age-differentiated protection regime. The third legal significance of the PRC experience is that it treats the minor not as a homogeneous group, but as a digital subject differentiated according to age. In the PRC, the personal information of children under the age of 14 is protected as a special sensitive category, while minor mode is constructed with differentiation by age groups. The 2024 Guidelines also provide for age-differentiated content, functions, and download procedures. In Kazakhstan, there is a law on protecting children from harmful information and rules on age classification of information products, but the official legal framework does not clearly reveal a unified system that places children's digital participation into a comprehensive regime linked to age thresholds in the way

observed in the PRC. Therefore, the significance of the PRC experience lies in showing the need for Kazakhstan to move from a single “for children” approach toward an age-differentiated legal model in protecting children’s digital rights. Such an approach would allow both legal restrictions and digital literacy measures to be adapted more precisely.

Strengthening the protection of minors’ personal data. The fourth legal significance of the PRC experience for Kazakhstan is that it treats minors’ personal data not merely within the general personal data regime, but as an additional object of enhanced protection. The PRC Personal Information Protection Law recognizes the personal information of children under the age of 14 as sensitive personal information, while the Regulation on the Online Protection of Minors strengthens parental participation, notification, complaint, and deletion mechanisms. Kazakhstan has the Law “On Personal Data and Their Protection” and related rules on protection measures, but within this official framework there is no separate, clearly enhanced category for minors’ data comparable to that of the PRC. Therefore, the PRC experience is legally significant for Kazakhstan in terms of separately identifying high-risk processing concerning minors’ data, establishing additional duties for platforms, and adapting the rights to deletion, correction, and restriction of processing to children[27]. As noted in the Scopus study by Kubanova and co-authors (2024), establishing age differentiation for minors at the legislative level in the Kazakh context would be consistent with today’s interdisciplinary approach to combating cybercrime[9].

Targeted legal control of online addiction and games. The fifth significance of the PRC experience lies in the fact that it regulates minors’ behavior in the digital environment not only through information content, but also through the time and functions of service use. Under the PRC’s official 2021 notice, all online game enterprises may provide services to minors only on Fridays, Saturdays, Sundays, and statutory holidays from 20:00 to 21:00 and must be connected to the real-name registration system. Kazakhstan’s current official acts do not contain a unified state gaming-time limit comparable to that of the PRC; the main focus is on protecting children from harmful information, age classification, and legal regulation of platforms. The Scopus study by Bolatbek and co-authors (2024) on the framework for detecting and mitigating cybercrime using university networks in Kazakhstan proves that the technical-legal mechanisms for early detection of digital risks in the Republic of Kazakhstan still require development[40]. This difference itself demonstrates the legal significance of the PRC experience for Kazakhstan: even without fully copying the Chinese model, Kazakhstan may consider targeted temporal or functional restrictions for high-risk services, such as games, livestreaming, short videos, and certain social functions. At the same time, such measures must be compatible with Kazakhstan’s own regime for personal data and child rights protection.

Elements that cannot be directly copied. Among the structural features of the PRC model, there are also elements that do not correspond to Kazakhstan’s

constitutional order and legal culture. These include, in particular, the high level of centralized control over information flows, including artificial intelligence systems, the practice of strict content censorship, complete rejection of anonymity, and the broad possibilities of law-enforcement bodies for preliminary monitoring of the digital environment. The right to inviolability of private life established in Article 18 of the Constitution of Kazakhstan, freedom of speech under Article 20, and the prohibition of censorship do not allow such elements to be mechanically copied. Therefore, learning from the PRC experience must necessarily be carried out through differentiated reception: the institutional structure concerning children's interests, mechanisms of platform liability, and the age-differentiation approach may be accepted, while centralized control and censorship elements should not be applied within Kazakhstan's constitutional order.

The legal significance of the PRC experience for Kazakhstan is manifested primarily in three directions. First, it shows the need to treat minors' digital security not as an auxiliary topic within general information policy, but as an independent field requiring special legal regulation. Second, the PRC experience proves the possibility of systematically building platform liability, an age-differentiated protection regime, enhanced protection of children's data, and specific legal restrictions concerning games and other high-risk services. Third, it offers an effective legal logic of a multilevel model for preventing minors' digital offenses, relying not only on criminal sanctions, but also on the family, school, legal education, and early prevention. In this regard, the most appropriate direction for Kazakhstan is not to copy the PRC's strict control model in full, but to adapt and introduce into national legislation its special digital protection regime for children, specified duties of platforms, and early prevention mechanisms. This approach would allow Kazakhstan to preserve its own legal structure while protecting minors' information security more systematically.

The institutional core of this legal model lies in the fact that the state acts not merely as a regulator of network space, but also as its organizer, the subject establishing security standards, and the central authority forming a special protection regime for minors. The Personal Information Protection Law identifies the personal information of minors under the age of 14 as sensitive personal information, while the Law on the Protection of Minors requires the introduction of time-management, authority-management, and consumption-management functions for online games, online livestreaming, online audio-video, and online social services. The official 2021 notice permits online game services to be provided to minors only on Fridays, Saturdays, Sundays, and statutory holidays from 20:00 to 21:00 and mandates the real-name registration system. Therefore, the main legal content of the PRC model is that the minor is treated not merely as a protected object, but as a digital subject to whom a legally special regime applies[172].

The evolution of the institution of liability for minors' digital offenses is also an important concluding feature of the PRC model. As a result of the changes introduced into Article 17 of the Criminal Code by Amendment XI in 2020, the lower threshold

of criminal liability for especially serious violent crimes was reduced in specific circumstances to 12 years; this norm has applied since 1 March 2021[175]. However, in the field of digital offenses, PRC practice does not rely solely on criminal punishment: official typical cases of the Supreme People's Procuratorate show that minors, especially in cases of assistance in crime through an information network, are often used as "instrumental persons," and therefore such cases require the combined use of punishment and rescue, education, and family guidance. This is supplemented by the Law on the Prevention of Juvenile Delinquency, which provides for special education and special corrective education, while judicial and investigative practice preserves humanistic guarantees for minors, including closed hearings, participation of a legal representative, and record sealing. Thus, in the PRC legal model, the response to digital offenses is formed as a synthesis of strictness and education.

At the same time, this model also has limitations, and they are partly acknowledged in official materials themselves. Official materials of the Supreme People's Procuratorate in 2026 indicate that, in the field of online protection of minors, the misuse of AI, online violence, insufficient clarity in legally defining new types of digital harm, inconsistent standards imposed on platforms, and interdepartmental law-enforcement mechanisms still requiring improvement remain relevant issues. Official materials of the National People's Congress also state that, despite the existing legislative framework, further improvement is needed in the boundaries of regulation, channels for rights protection, and specific mechanisms applicable to new technologies. Therefore, as a scientific conclusion, the PRC model should be assessed not as an absolute and fully completed system, but as a dynamic legal system with a strong foundation that requires continuous renewal under the conditions of new technological challenges[182].

The PRC legal model for information security and the protection of minors in digital space is a systematic, comprehensive, and multilevel structure based on a state-centered legal philosophy. Its strengths are legal and institutional integrity, the "six protections" mechanism, the specificity of platform liability, an age-differentiated legal regime, and the combination of prevention and punishment. Its weaknesses are the difficulty of rapidly adapting to technological changes, gaps in legally defining new types of digital harm, and inconsistency in platform standards. For Kazakhstan, the PRC experience is not an object for complete copying, but a starting point for differentiated reception: by adapting the special digital protection regime for children, platform duties, and early prevention mechanisms to the national legal system. Subsequent comparison of this experience with Western models will provide a basis for defining a balanced strategy for modernizing the institution of protecting minors in the field of informatization in the Republic of Kazakhstan.

CHAPTER 4. PROPOSALS FOR IMPROVING THE SYSTEM FOR PREVENTING MINORS' OFFENSES IN THE FIELD OF INFORMATIZATION AND COMMUNICATIONS AND MEASURES OF LIABILITY IN THE REPUBLIC OF KAZAKHSTAN BASED ON A COMPARATIVE LEGAL ANALYSIS OF INTERNATIONAL AND DOMESTIC EXPERIENCE

The basic foundation of international cooperation in the information sphere is the UN Charter, which establishes the principles of sovereign equality and the peaceful settlement of disputes. In the context of protecting the rights of minor users, Kazakh legislation is based on the provisions of the 1989 UN Convention on the Rights of the Child: Article 13 guarantees the child's right to seek, receive, and impart information, while Article 16 guarantees protection against unlawful interference with privacy and correspondence [3]. Article 17 of the Convention obliges states to develop mechanisms for protecting children from harmful content while ensuring their access to information from diverse sources that promotes their well-being. These international norms are directly reflected in the Law of 8 August 2002 No. 345-II "On the Rights of the Child in the Republic of Kazakhstan," which establishes the principle of priority of the child's interests and the state's obligations to ensure the child's safety in the information environment [4]. Thematic regulation is continued by the Law of 2 July 2018 No. 169-VI "On the Protection of Children from Information Harmful to Their Health and Development," which defines procedures for classifying information products by age categories, as well as the procedure for restricting access to materials that encourage suicide and other life-threatening acts [5].

In the field of protecting children's rights in the digital environment, Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe to member states, dated 4 July 2018, is of particular importance [6]. Although Kazakhstan is not a member of the Council of Europe, the principles of "safety by default" and "taking into account the best interests of the child" formulated in this document influence national lawmaking as part of international soft law. These principles are intended to develop the right of the mother, father, and child to protection by the family and the state, as established in Article 27(2) of the Constitution of the Republic of Kazakhstan.

In the field of civil-law regulation, the Civil Code of the Republic of Kazakhstan (hereinafter, the Civil Code RK) has aligned with international trends in recognizing the value of virtual property: amendments have been made to Article 115 concerning the list of non-property benefits and objects of civil rights, while Article 156(2) defines the foundations for protecting commercial secrets [7]. Article 144 of the Civil Code RK protects the right to inviolability of private life, fully corresponding to the requirements of Article 16 of the UN Convention. The protection of intellectual property and undisclosed information in the digital sphere is aligned with the acts of the World Intellectual Property Organization (WIPO) and the provisions of the 2001 Budapest Convention (ETS No. 185). However, civil legislation still lacks detailed

mechanisms of liability for moral harm caused specifically through the use of automated algorithms in the digital environment. Under Article 951 of the Civil Code RK, moral harm is subject to compensation, but in cases of the “viral” spread of destructive content on social networks, the existing criteria for assessing the amount of harm require clarification.

The administrative-law sphere has also undergone significant modernization. The Code of Administrative Offenses of the Republic of Kazakhstan (hereinafter, the CAO RK) contains norms on the use of information protection tools (Article 639) and the functioning of electronic digital signatures (Article 640) [10]. Regulation concerning violations of requirements to inform users about the results of the use of artificial intelligence (AI) systems was detailed by the Law “On Artificial Intelligence,” adopted by the Parliament of the Republic of Kazakhstan in 2024, which establishes provisions consonant with the requirements of the European Union AI Act on the ethical use of AI. In the field of personal data protection, the Law of 21 May 2013 No. 94-V “On Personal Data and Their Protection” and Article 79 of the CAO RK define liability for unlawful collection and processing of personal data [11]; these norms are aligned with the provisions of Council of Europe Convention No. 108 of 1981. However, with respect to minor offenders, the system of administrative measures is often limited to fines imposed on parents (Article 127 of the CAO RK), while mechanisms for individualized educational influence on the adolescent remain insufficient.

The logical continuation of formulating threats in the digital environment is the legislative consolidation of the term “digital aggression” [15]. At present, this term is frequently used in criminological works as a collective category of destructive informational influence, but its absence from normative legal acts prevents the precise regulation of the powers of prevention subjects. Article 23 of the Council of Europe Convention of 25 October 2007 on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, CETS No. 201) recognizes the solicitation of minors through ICT for sexual purposes as a criminally punishable act [16]. Developing this approach, it is appropriate to define digital aggression as “any hostile behavior in the digital environment carried out through destructive information (text, video, graphic images) aimed at destabilizing a person’s emotional state or involving that person in unlawful acts against life, health, or public order.” Introducing this definition into the Law of 29 April 2010 No. 271-IV “On the Prevention of Offenses” would provide specialized units with a legal basis for monitoring destructive content according to signs falling within the threshold of criminalization.

The fourth direction in improving the conceptual apparatus is the introduction of a rule prohibiting the profiling of children. Paragraph 35 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, as well as General Comment No. 25 of the UN Committee on the Rights of the Child (CRC/C/GC/25, 2021), state that profiling children for commercial or other purposes

should be prohibited by law, except where it corresponds to the best interests of the child and is ensured by legal safeguards [6]. The absence in Kazakhstan's legal system of a direct prohibition on uncontrolled digital profiling of children creates conditions for their commercial exploitation and manipulation through social network algorithms. Introducing a strict limitation on profiling into the Law "On Personal Data and Their Protection" would ensure implementation of the child's right to protection from arbitrary interference with private life, as established in Article 16 of the UN Convention [3].

Another important aspect of improving terminology is the development of the concept of "children's information security." Article 1(1) of the Law "On the Protection of Children from Information Harmful to Their Health and Development" defines this concept as "the state of protection of children's rights and lawful interests that prevents harm to their health and development from relevant information" [5]. The contemporary scientific paradigm requires expanding this definition beyond protection from external content-related threats to include the active formation of "digital literacy" skills that enable the child to act safely and meaningfully in the digital environment. This approach corresponds to paragraphs 22–24 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, which establish the state's positive obligations to educate children in the ethics of online behavior [6].

It may be concluded that improving the conceptual apparatus is an essential prerequisite for eliminating existing legal gaps and increasing the effectiveness of counteraction to digital threats. Introducing the categories "cyberbullying," "digital aggression," and "minors' digital personal data" into the legislation of the Republic of Kazakhstan would make it possible to shift preventive and law-enforcement activity from general declarations to specific algorithmic measures for protecting the individual. In line with global trends toward the humanization of digital space, this creates a reliable theoretical basis for reforming civil-law protection institutions.

The logical direction for developing the civil-law protection system is the integration into national legislation of the concept of "duty of care," widely used in international legal practice. Paragraphs 41–48 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe define the obligations of the business community, primarily IT-sector enterprises, to respect children's rights, identify, prevent, and mitigate possible negative impacts on these rights, and ensure access to effective compensation mechanisms [6]. The European regulatory model, in particular Regulation (EU) 2022/2065 of 19 October 2022 on digital services (Digital Services Act), moves platforms from passive immunity to an active role in managing risks to children's psychological well-being: Article 28 establishes a default regime of a "high level of privacy, safety and security" for minor users [19]. These approaches justify the need to treat online platforms not as technical intermediaries, but as subjects that may incur civil liability where they fail to perform systematic obligations concerning children's cybersecurity.

The second stage of the algorithm provides for determining the subsidiary liability of the online platform where the direct harm-causer is anonymous or located outside the jurisdiction of the Republic of Kazakhstan. It is proposed to treat a social network, insofar as its recommendation algorithms contribute to the viral spread of destructive content, as having a status close to that of a source of increased danger, by analogy with Article 931 of the Civil Code RK. A platform may be exempted from compensation only if it proves that it introduced “safety by default” settings and immediately restricted the content after receiving a complaint. This approach economically incentivizes technology companies to invest systematically in the early detection of digital aggression and mechanisms for protecting personal dignity.

The practical implementation of the proposed algorithm requires systematic supplementation of the Civil Code RK: Article 951 should be supplemented with a rule providing that, where obligations to ensure minors’ safety are violated, the information intermediary compensates moral harm regardless of fault. It is also necessary to consider creating a specialized state fund for compensating affected children, financed by fines imposed on technology companies for failure to comply with information security standards, based on the further development of Articles 127-3 and 645 of the CAO RK. Only by establishing strict economic and legal consequences for digital subjects is it possible to ensure genuine respect for the rights of the child in the virtual environment.

There are grounds to conclude that modernizing civil-law protection mechanisms through the introduction of an algorithm for predicting harm and strengthening platform liability is an essential condition for establishing a stable digital legal order. This model makes it possible to adapt the classical institutions of the Civil Code RK to the dynamic conditions of the information society and to effectively restore the rights of the most vulnerable subjects. The need to strengthen liability for digital violations and to purposefully correct the behavior of minor offenders creates the theoretical prerequisites for moving to the stage of reforming administrative-law instruments.

A systematic analysis of the norms of the CAO RK reveals a contradiction between the purposes of administrative punishment and the practice of implementing them with respect to minors. Under Article 64(1-1) of the CAO RK, the amount of a fine imposed on a minor must not exceed ten monthly calculation indices [10]; however, where the adolescent has no independent source of income, the actual burden of paying the fine passes to legal representatives (Article 65 of the CAO RK). This legal construction eliminates the individualized educational impact of punishment: the offender does not experience the direct consequences of his or her actions, while the punitive function of the law is manifested indirectly through a financial burden on the family. As shown in K.R. Boshayeva’s dissertation research, adolescents often perceive repressive measures as a formal barrier, and such measures are incapable of eliminating the root causes of deviant online behavior, including low digital literacy and the absence of established standards of ethical behavior in virtual space [20].

From this standpoint, developing a normative framework for “digital educational measures” as a full-fledged alternative to fines becomes particularly relevant.

The theoretical basis of the proposed reform is the concept of juvenile justice, which is actively developing in Kazakh legal scholarship. This concept postulates that administrative justice with respect to minors should be aimed not at stigmatization through punishment, but at developing their potential and preparing them for responsible life in a free society. This fully corresponds to paragraph 49 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, which requires member states to avoid excessive criminalization where children commit online offenses, including against peers, and to prioritize preventive and restorative measures [6]. In Kazakhstan, Article 3 of the Law of 29 April 2010 No. 271-IV “On the Prevention of Offenses” establishes the principle that prevention of offenses takes priority over the application of sanctions for violations [21], but the application of this principle to offenses in the information sphere requires detailed regulation.

The novelty of the proposed reform lies in the legislative consolidation of a special category of “digital educational measures” to be applied where minors commit offenses under Articles 79, 127-2, 639, 640, and 641-1 of the CAO RK. The first element of this system is mandatory completion of courses in digital hygiene, cyberethics, and information law. Unlike the current measure of “legal explanatory work,” which is one-time and usually formal, such a course should be a structured educational program. Its content should cover the protection of personal data, liability for disseminating destructive content, and the legal consequences of digital aggression, thereby implementing the child’s right to education in the field of digital literacy. This measure transforms punishment into the acquisition of socially significant competencies necessary for safe activity in the digital environment.

The second component of the reform is involving the minor offender in digital volunteering and socially useful activity on the internet. Comparative analysis of international experience in juvenile crime prevention shows the high effectiveness of involving young people in cyber teams. Within the execution of an educational influence measure, the offender may, under the supervision of specialists from relevant units, be involved in monitoring the information space to identify unlawful content. Participation in such projects under the guidance of mentors forms the adolescent’s sense of social responsibility and directs his or her technological skills into a constructive channel. This ensures achievement of the goals of social adaptation and rehabilitation established in the Law “On the Prevention of Offenses” [21].

In terms of institutional support for the reform, the main role in monitoring the execution of digital educational measures should be assigned to commissions on juvenile affairs and the protection of their rights, established by the Law of 21 February 2018 No. 142-VI “On Commissions on Juvenile Affairs and the Protection of Their Rights” [23]. Their coordinating function requires close interaction among the pedagogical community, internal affairs bodies, and psychological support centers

in order to provide continuous pedagogical support to the offender. According to the 2024 report of the Ministry of Education and Science of the Republic of Kazakhstan, the total number of school psychologists across the republic is approximately 8,000, which indicates that specialized psychological support resources are insufficient to comprehensively cover cases of digital deviation among adolescents [24]. Accordingly, only a comprehensive approach combining technical monitoring (Articles 31 and 639 of the CAO RK) with psychological correction of behavior (Article 18 of the Law on Prevention) can provide a stable long-term result in preventing adolescent cybercrime.

There are grounds to conclude that modernizing the system of administrative punishments by partially replacing fines with “digital educational measures” simultaneously humanizes legislation in accordance with the conditions of the digital era and ensures its effectiveness. The proposed model, in line with the imperatives of the UN and the Council of Europe on protecting children’s rights, creates structured mechanisms for redirecting adolescents’ destructive activity into socially useful activity. Combining material sanctions with educational and volunteering algorithms makes it possible to eliminate the imbalance of responsibility between the parent and the child and to achieve the goals of correcting the offender by developing his or her intellectual and moral potential. The need for deeper correction of the behavior of minor offenders and restoration of victims’ rights in the information sphere creates the theoretical prerequisites for moving to the next stage, devoted to the analysis of the humanization of criminal-law policy.

In the context of the structural transformation of crime under the influence of information and communication technologies (ICT), the criminal-law policy of the Republic of Kazakhstan requires a transition to diversified and humanized forms of response to minors’ deviant behavior. As substantiated in the previous stages, the dynamics of crimes in the field of informatization and communications have grown at record rates in recent years [2], while a significant proportion of offenders belong to a generation that has mastered digital technologies since preschool age. The general provisions of the Criminal Code of the Republic of Kazakhstan applicable to minors (Articles 15, 80, and 81) are characterized by their orientation toward traditional types of crime, which creates shortcomings arising from a specific normative mismatch when classifying acts in the digital sphere. The scientific justification for humanizing criminal legislation is based on the principle of the “best interests of the child” (Article 3 of the UN Convention on the Rights of the Child) [3]: it requires that measures of criminal prosecution not deepen the possible social trauma caused to the adolescent and that they promote effective reintegration into society. Developing new norms for differentiating liability that take into account the digital competence and psychological state of the adolescent “cyber offender” therefore has both theoretical and practical importance.

To implement the principle of humanization, it is proposed to supplement Chapter 6 of the Criminal Code RK with a new differentiating norm establishing a presumption

of exemption from criminal liability for minors who commit, for the first time, a minor or medium-gravity crime in the field of informatization, for example under Articles 205 and 206 of the Criminal Code RK. The condition for such exemption should be not only reconciliation with the victim (Article 68 of the Criminal Code RK), but also completion of an individually adapted “digital rehabilitation program.” The content of this program may include involving the adolescent in volunteer work to identify destructive content or participation in projects teaching media literacy to primary school students. This approach protects the adolescent from stigmatization as a criminal and from further growth of criminal activity through contact with the penitentiary environment, which is especially important in the conditions of digital society.

In the humanization process, accounting for the minor’s psychological condition when imposing punishment is of particular importance. Article 82 of the Criminal Code RK obliges the court to take into account living and upbringing conditions, the level of mental development, other personal characteristics, and the influence of older persons [8]. In the context of the digital era, scientific interest focuses on the phenomena of internet addiction and digital social isolation, which are frequent determinants of online offenses. It is proposed to supplement Article 81(7) of the Criminal Code RK with a norm allowing actual deprivation of liberty to be replaced by a special regime of restriction of liberty using remote supervision technologies (digital probation), without complete isolation from the educational process. Such a measure would allow the adolescent to continue studies at school or college while preserving probation-service monitoring of online activity. This differentiation ensures a balance between protecting society from cyber threats and the child’s right to the comprehensive development of personality.

The nature of the institution of conviction with respect to minor cyber offenders requires reconsideration. Although Article 79 of the Criminal Code RK significantly reduces the periods for expungement of conviction for minors, the long-term preservation of a criminal past in digital registers may hinder the adolescent’s future employment in the lawful ICT sector. It is theoretically justified to introduce a digital expungement procedure for adolescents who have successfully completed measures of educational influence and have committed no repeated offenses during a certain period. This would enable the child to exercise the rights to dignity and inviolability of private life guaranteed by the Constitution of the Republic of Kazakhstan and international conventions. Criminal-law policy should be aimed not at strengthening repressive pressure, but at increasing the resilience and legal culture of young citizens. Another important aspect of improving criminal legislation is accounting for the role of artificial intelligence (AI) as an aggravating or mitigating circumstance when minors are involved in cybercrimes. Contemporary studies show a trend in which organized criminal groups use AI systems to psychologically influence adolescents and involve them in fraudulent schemes. Accordingly, Article 28 of the Criminal Code RK (complicity in crime) may be differentiated by establishing that the use of

AI by adult participants to manage a minor's behavior online is a circumstance that substantially increases the public danger of the act. With respect to the adolescent, the commission of a crime under the influence of automated algorithms imitating human interaction, such as deepfakes and chatbots, should be recognized as a mitigating circumstance in the form of psychological coercion. This would ensure the principles of proportionality and fairness while protecting the most vulnerable subjects of digital space from manipulation.

There are grounds to conclude that the humanization of criminal-law policy with respect to minor cyber offenders is an objective requirement of the present era, aimed at preserving human capital and increasing the effectiveness of prevention. The transition from a punitive model to restorative and educational measures will enable the state to counter the growth of ICT crime effectively by eliminating its root causes: the deficit of legal consciousness and social responsibility among young people. The proposed differentiation norms, based on UN and Council of Europe principles, form a reliable foundation for further reforming the law-enforcement system toward digitalization and humanization.

The contemporary scientific and legal paradigm of ensuring minors' cybersecurity requires a qualitative transition from fragmented measures of state regulation to a systematic distributive model of responsibility that unites the efforts of the state, technology corporations, and legal representatives. As substantiated in the previous stages, the transboundary and anonymous nature of threats in digital space does not allow the state to effectively protect children's rights solely through the efforts of law-enforcement bodies. Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe (paragraphs 1, 8, and 30) and Articles 4 and 18 of the UN Convention on the Rights of the Child substantiate that effective protection of children's rights in the digital environment is based on the principle of shared responsibility among all stakeholders [3; 6]. Therefore, the scientific and legal justification of the tripartite "state - platform - parent" model appears as an objective necessity for harmonizing national legislation of the Republic of Kazakhstan with international standards: the powers and mutual obligations of each subject must be clearly established.

The central link of the proposed model is the state, which bears primary responsibility for respecting, protecting, and ensuring the exercise of the child's rights. Under Articles 7 and 7-1 of the Law "On the Rights of the Child in the Republic of Kazakhstan," the state, through authorized bodies, not only forms strategic policy directions, but also has the duty to coordinate the activities of all subjects participating in ensuring children's safety [4]. In present conditions, the role of the state must shift from direct administration to the function of a strategic regulator that forms a transparent and predictable normative environment, encouraging the business community and families to participate actively in ensuring digital hygiene. Important institutional mechanisms for implementing this role are the Commissioner for Children's Rights (Decree of the President of the Republic of Kazakhstan of 10

February 2016 No. 192) [26] and regional authorized bodies, which ensure monitoring of violations and the development of recommendations for improving legislation. According to the 2023–2024 report of the Commissioner for Children’s Rights, the number of complaints in the republic concerning children’s rights to privacy, information security, and rights in digital space is steadily increasing [38]. Accordingly, the state component of the model includes establishing safety standards, ensuring access to justice, and creating the institutional foundations for interdepartmental interaction.

The second imperative element of the model is the social and legal responsibility of online platforms (IT companies), which act as the main “gatekeepers” of the digital environment. Articles 8 and 14 of the 2007 Lanzarote Convention directly encourage the private sector, especially the ICT sector, to participate in developing measures to protect children from exploitation and to ensure the implementation of self-regulatory norms [16]. Under paragraph 41 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, member states should require commercial enterprises to identify, prevent, and mitigate possible adverse impacts of their activities on children’s rights [6]. Scientifically grounded modernization of Kazakhstan’s legislation should provide for the establishment of a “duty of care” for platforms: this includes the obligation to set personal data protection parameters by default and systematically assess risks to the mental health of minor users. Within the tripartite model, the platform bears responsibility for the technical architecture of safety, prompt content moderation, and providing parents with effective control tools. The conceptual consolidation of shared responsibility requires the introduction of the legal mechanism of “counterpart obligations,” under which the failure of one subject to perform functions triggers the activation of protective procedures by another. On the basis of a systematic analysis of Article 127 of the CAO RK and Article 18 of the Law “On the Prevention of Offenses,” it is appropriate to legislatively establish the following algorithm of interaction: the state provides the normative legal framework and technical infrastructure, such as specialized units; platforms guarantee the safety of the digital environment; and parents exercise direct supervision. Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe (paragraph 114) postulates the duties of internet platforms to respond promptly to complaints of violence and cooperate with national authorities [6]. Only such synergy can overcome the latency of cybercrime and ensure effective protection of a vulnerable group of users.

There are grounds to conclude that legislative consolidation of the tripartite “state - platform - parent” responsibility model is an essential condition for forming a stable system of national cybersecurity. The model, based on the UN and Council of Europe concept of shared responsibility, reduces risks to the development of the child’s personality while ensuring a balance of rights and duties for all participants in digital relations. Implementation of this model requires not only amendments to substantive and administrative law, but also the creation of new forms of public-private

partnership in the ICT sector. Further development of prevention mechanisms requires the formation of an innovative institutional direction through the creation of institutions such as cyber patrols and a digital ombudsman, which constitutes the core of the next stage.

The logical continuation of the development of Kazakhstan's system of rights-protection institutions is the conceptualization of the status of the "digital ombudsman." At present, the republic has the institution of the Commissioner for Children's Rights, which is entrusted with functions for restoring violated children's rights [26]. However, the narrow specialization of digital relations and the complexity of technological processes, including AI algorithms, big data analysis, and blockchain, determine the need to distinguish a special specialized direction of rights-protection activity. The digital ombudsman should act as an independent arbiter among the individual, the state, and transnational IT corporations, ensuring compliance with the principles of "data protection by default," the "right to be forgotten," and protection of children's digital image. The powers of such an ombudsman should include not only consideration of complaints concerning digital violence, but also independent audits of the safety of online platforms intended for children. This would ensure the implementation of the child's right to effective legal protection under paragraphs 71–73 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe and make it possible to overcome the asymmetry of opportunities between an ordinary user and a technological giant [6].

Systematic integration of these institutions into the legal space of the Republic of Kazakhstan requires amendments to a number of legislative acts. First, it is proposed to supplement the Law "On the Prevention of Offenses" with a separate chapter on cyber prevention, defining the powers of cyber patrols as subjects for monitoring and identifying determinants of digital aggression [21]. Second, it is necessary to expand the competence of the Commissioner for Children's Rights in the field of monitoring the activities of online platforms and supervising observance of children's rights to privacy, or to create within that structure a specialized office of the digital ombudsman [26]. Third, normative support for parental control tools should be strengthened through amendments to the Law of 5 July 2004 No. 567 "On Communications" and the Law of 24 November 2015 No. 418-V "On Informatization," establishing liability for service providers that fail to ensure safety settings by default for minor users [32]. A comprehensive approach would make it possible to form an integrated innovative prevention infrastructure in which technical tools are complemented by human capital and institutional oversight.

Methodologically, the effectiveness of these mechanisms directly depends on the level of digital literacy of the population. Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe (paragraph 49) establishes that digital literacy education should be included in general education programs so that children and their legal representatives can develop the ability to participate meaningfully in the digital environment [6]. Accordingly, cyber patrols and the digital

ombudsman should be viewed not only as punitive or supervisory bodies, but also as key subjects of legal education and media education. Implementing programs in Kazakhstan for training “digital mentors” from among members of parent committees and cyber patrol volunteers would create an environment of collective responsibility in which each participant in the tripartite model has the necessary protective tools. This opens the way for transition from fragmentary measures to systematic state planning in the field of children’s cybersecurity. As shown in T. Bolatbek’s study on the development of digital literacy and media education in Kazakhstan, joint work between the school and the family is a factor that significantly reduces the level of internet addiction among adolescents [33].

The technical and legal convergence of the digital ombudsman and cyber patrols should be combined with machine learning and big data analysis systems, which would allow law-enforcement bodies to detect behavioral deviations in virtual communities as early as possible. At the same time, to observe the principles of confidentiality and inviolability of private life, the target limitations of data processing and procedures for obtaining judicial authorization must be legally regulated. Accordingly, the proposed preventive institutions are aimed not at unjustifiably restricting children’s freedom of expression and rights to access information, but at creating conditions for their safe socialization in the digital environment.

There are grounds to conclude that establishing the legal status of cyber patrols and the digital ombudsman and providing normative support for technical control tools are essential conditions for creating a proactive system for protecting children’s rights in the digital environment. The proposed mechanisms create conditions for children’s safe socialization while ensuring a balance between public security interests and individual rights relating to freedom of expression and access to information. The innovative nature of these measures ensures their adaptability to future technological challenges and contributes to the fulfillment of Kazakhstan’s international obligations to protect the best interests of the child in the digital age. Since the further development of prevention mechanisms cannot achieve full effectiveness without modernizing judicial practice, the next stage is devoted to analyzing the role of the judiciary and its institutional transformation in line with the requirements of the digital era.

The final stage of the systematic modernization of mechanisms for ensuring minors’ information security in the Republic of Kazakhstan requires a scientific explanation of the role of the judiciary as a guarantor of individual rights in virtual space. As substantiated in the previous stages, the introduction of innovative prevention institutions and new models of liability cannot achieve full effectiveness without an adequate transformation of judicial activity. The analysis of law-enforcement practice shows a gap between the pace of digitalization of public relations and the readiness of the judicial system to resolve high-technology disputes. According to reviews of the Supreme Court of the Republic of Kazakhstan for 2023–2024, in cases involving

digital evidence, case consideration periods are significantly extended, and in some categories nearly 25% of cases are changed or annulled at the appellate level [34]. The record growth in the number of crimes in the field of informatization and communications in Kazakhstan over the past eight years, together with the qualitative complexity of methods of committing crimes using AI, substantiates the objective need to specialize the judiciary. The scientific justification for reforming judicial practice is based on Articles 12 and 40 of the UN Convention on the Rights of the Child, as well as paragraph 109 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, which postulate the requirement to ensure children's access to child-friendly justice [3; 6].

The main problem of the current judicial system in the context of the topic under consideration is the shortage of highly specialized knowledge among judges of general jurisdiction, which makes it difficult to competently assess specific digital evidence such as hash values, metadata concerning materials related to child sexual exploitation, or platform algorithmic parameters. Accordingly, the first scientifically grounded proposal is to introduce a system of continuous professional training and certification of judges in information disputes and cybercrimes. Under paragraph 109 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, member states are obliged to allocate sufficient resources for initial and continuous training of judicial officials, increasing their knowledge of children's online risks and methods of responding to signs of exploitation and harm [6]. Such training should not be limited to theoretical aspects, but should include practical skills in analyzing "digital traces" and understanding adolescent behavioral psychology under conditions of internet addiction. Institutionalization of this direction may be carried out through the introduction of specialized educational modules by the Academy of Justice of the Republic of Kazakhstan.

A comparative legal analysis with EU standards shows the need to strengthen control over the activities of online platforms through judicial decisions. Where facts of dissemination of harmful content or systematic failure by platforms to perform obligations to protect children are established, a juvenile court should have the authority to issue special rulings addressed to IT companies on eliminating the causes and conditions that generated the offense (Article 53 of the Criminal Procedure Code RK and Article 829-19 of the CAO RK) [10]. Developing the concept of shared responsibility among the "state - platform - parent" (see Stage 6), courts should widely apply the practice of recovering compensation for moral harm in favor of children, using the simplified algorithm for predicting harm described in Stage 3; this would create an economic incentive to improve the safety level of digital products. At the same time, courts must maintain a balance between the child's right to protection and freedom of expression and access to information.

The institutional development of juvenile justice in the digital environment requires the creation of a unified database of judicial practice concerning minors' cybercrimes, ensuring uniformity in the interpretation of norms at both the national and interstate

levels, including within the CIS. This resource would allow judicial bodies to adapt promptly to new types of cyber threats, such as the use of deepfake materials for grooming children or involvement in fraud through chatbots. Supplementing judicial statistics with details reflecting the “digital context” of the act should be considered a methodological solution that improves the quality of criminological forecasting and victimological prevention. As shown in E.A. Sabyrbayev’s dissertation study on individual rights in digital space, the quality of judicial practice is the foundation of the effectiveness of legal protection in the digital sphere [35].

There are grounds to conclude that improving judicial practice through the specialization of judges, expansion of the jurisdiction of juvenile courts, and modernization of procedures for assessing digital evidence is the final condition for forming a coherent and effective system of information security in the Republic of Kazakhstan. The proposed set of measures, based on the synergy of international standards (UN, Council of Europe) and national legal traditions, makes it possible to create an integrated mechanism for protecting the rights of vulnerable subjects in the digital age. The systematic scientific and legal study conducted has provided the basis for creating a completed strategy for modernizing the legislation and law-enforcement practice of the Republic of Kazakhstan in the field of minors’ information security; the logical continuation of the conceptual generalization of the results achieved is the justification of a draft national strategic document.

The final stage of the systematic scientific and legal study of the problems of ensuring minors’ information security in the Republic of Kazakhstan requires the conceptual generalization of the results obtained in the draft of a national strategic document. As all eight stages of the study have shown, despite the high dynamics of renewal, the current legal framework of the Republic of Kazakhstan remains fragmented. Point amendments to the criminal, administrative, and civil codes do not produce a synergistic effect without a unified ideological and organizational platform. Accordingly, it is proposed to develop and adopt a National Strategy for Children’s Digital Security (hereinafter, the Strategy), which should appear as a comprehensive legislative package and be fully harmonized with Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe and the UN Convention on the Rights of the Child [3; 6]. This document is intended to concentrate the state’s technical, legal, and pedagogical resources in order to form a safe digital ecosystem for the socialization of the younger generation.

The theoretical and methodological basis of the Strategy lies in the need to overcome the identified “regulatory gap” between the dynamics of ICT development and the pace of legislative reflection. A systematic analysis of the determinants of adolescent cybercrime identifies the main risk factors: terminological uncertainty, insufficient digital literacy, and a deficit of shared responsibility among participants in information relations. The strategic document should establish at the normative level the transition from a reactive model of “combating consequences” to a proactive model of risk management. In accordance with international standards, such an

approach provides for the introduction of the principles of “safety by default” and “taking into account the best interests of the child” in all digital products and services for children. The novelty of the proposed Strategy is reflected in its interdisciplinary nature: it concentrates norms from different branches of law around a single object, namely the child’s digital inviolability and well-being.

The second strategic priority is the modernization of institutions of legal liability through the introduction of the tripartite “state - platform - parent” model. As substantiated in Stage 6, effective cybersecurity cannot be achieved without establishing the duties of care of online platforms. The Strategy should provide for the legislative consolidation of the subsidiary liability of IT companies where data protection standards are not observed and harm is caused to children through algorithmic recommendations. At the same time, the document should include mechanisms to support parents through state programs for digital literacy education and normative support for technical control tools, ensuring implementation of the principle of shared responsibility established in Article 18 of the UN Convention [3].

The innovative core of the Strategy is the creation of institutional infrastructure for proactive prevention. The analysis conducted in Stage 7 substantiates the need to legalize the status of cyber patrols and the digital ombudsman in Kazakhstan. The strategic document should define cyber patrols as subjects of public monitoring of the information space, entitled to interact with special law-enforcement units in blocking destructive content. The digital ombudsman, in turn, should act as a key element of the data protection system by conducting independent audits of the safety of online services for children and considering complaints concerning digital violence under a simplified procedure.

The Strategy should assign a special place to judicial specialization and the digitalization of proof. As substantiated in Stage 8, the effectiveness of protecting the rights of the child in the digital era directly depends on the qualifications of the judiciary and the correctness of recording electronic traces. The document should provide for expanding the powers of juvenile courts to consider cybercrimes and introducing a system of continuous training for judges in methods of assessing digital evidence. The creation of a unified database of judicial practice on information disputes would ensure uniformity of law enforcement and predictability of the legal environment for the ICT sector, corresponding to international requirements for the quality of justice.

Financial and resource support for the Strategy may be carried out through the creation of a Target Fund for Children’s Digital Security, replenished by part of the fines imposed on technology companies for violations of cybersecurity requirements. This would create a stable mechanism for financing scientific research in cyberpsychology and implementing programs for the digital resocialization of offenders. A systematic approach requires deeper integration of Kazakhstan into international cooperation structures: this should include consideration of ratifying the 2001 Budapest Convention, as well as active participation in the development and

implementation of the Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, adopted by UN General Assembly Resolution A/RES/79/243 of 24 December 2024 [12]. This document is capable of eliminating “safe havens” for transboundary cyber offenders and making a significant contribution to the formation of global standards in the field of minors’ digital security.

There are grounds to conclude that adopting a comprehensive National Strategy for Children’s Digital Security is an essential condition for preserving the national sovereignty and human capital of the Republic of Kazakhstan under conditions of global digitalization. The proposed draft document not only summarizes legislative initiatives, but also offers an integrated architecture of digital legal order based on the balance among security, education, and human rights. Implementation of the Strategy can ensure the state’s transition from fragmentary response to systematic future-oriented design, in which every child will be equally protected by law and technology from the viral threats of the information environment.

At the institutional level, the study defines the status of new subjects such as the digital ombudsman, cyber patrols, specialized juvenile courts, and the Target Fund for Children’s Digital Security. The interaction of the elements of this system and their functions is as follows: the state provides the normative legal framework and coordination, platforms are responsible for the technical architecture of safety, and parents educate the child in the ethics of online behavior. The proposed set of measures, based on Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe (paragraphs 1, 8, 30, 41, and 109) [6], ensures the practical integration of the principle of the best interests of the child into the legal system of the Republic of Kazakhstan.

At the methodological level, the study introduces into criminological science the categories of “digital maturity,” “counterpart obligations,” and “restorative digital justice.” These categories offer new theoretical tools for analyzing the determinants of adolescent offenses. Under conditions of the globalization of digital threats, the work makes a significant contribution to criminal-law science and criminology; the research results support the hypothesis that only through the synergy of international standards (UN, Council of Europe) and innovative national mechanisms (cyber patrols, digital educational measures, and the right to be forgotten) is it possible to effectively counter the growth dynamics of ICT crime in the country.

The practical significance of the work is determined by its possible use in the activities of state bodies under the President of the Republic of Kazakhstan responsible for reforms in law enforcement, national security, and the judicial system, as well as in the process of preparing draft legislation by the Mazhilis of the Parliament of the Republic of Kazakhstan to improve legislation in the field of information security and protection of children’s rights. The conclusions of the study may be used in teaching the special courses “Criminal Law,” “Criminology,” “Information Law,” and “Protection of Minors’ Rights” at law faculties of higher

education institutions. Prospects for further development of the study are seen in research on the influence of AI on the legal consciousness of young people, development of the concept of the legal personality of the digital subject, and elaboration of global standards for the digital security of the individual.

On the basis of the results of the comparative legal and doctrinal analysis set out above, a comprehensive institutional and normative architecture is proposed for preventing offenses by minors in the field of informatization and communications. The architecture consists of four mutually coordinated pillars: regulatory-platform, institutional-subject (the tripartite State - Platform - Parent model), reactive-educational, and systematization-codification. For the purpose of normative consolidation of this architecture, the following set of interconnected normative proposals has been developed.

(1) Regulatory-platform pillar. It is proposed to supplement the Law of 10 July 2023 No. 18-VIII “On Online Platforms and Online Advertising,” following the model of Article 28 of European Union Regulation 2022/2065 (DSA), with Article 5-1: “Duty of care of online platforms in relation to minor users. Online platforms shall ensure, in relation to minor users, a high level of privacy by default, prompt content moderation, restriction of personalized recommendation algorithms, and consideration of complaints concerning violence no later than within 24 calendar hours.” At the same time, it is proposed to clarify standards for procedural interaction between platforms and law-enforcement bodies in relation to marking suspicious accounts, identifying automated false activity, and mandatory labeling of hidden advertising.

(2) Institutional-subject pillar. (a) The Law of 8 August 2002 No. 345-II “On the Rights of the Child in the Republic of Kazakhstan” should be supplemented with Article 16-1 on the digital parenting duties of legal representatives; Articles 70 and 73 of the Code of 2011 No. 518-IV “On Marriage (Matrimony) and Family” should be harmonized with the corresponding digital parenting content; (b) Chapter 12 of the CAO RK should be supplemented, following the model of Article 6.17 of the CAO of the Russian Federation, with Article 127-4 (“Failure of legal representatives to perform digital parenting duties”); (c) the Law of 30 December 2025 “On the Prevention of Offenses” should be supplemented with a norm on the special legal status of cyber patrols, while the activity of cyber patrols must be coordinated with strict legal filtering before information is transferred to law-enforcement bodies and with procedures to prevent the risk of unlawful interference with private life; (d) the Regulation on the Commissioner for Children’s Rights, approved by Decree No. 192 of the President of the Republic of Kazakhstan dated 10 February 2016, should be supplemented with a norm introducing a specialized digital ombudsman; (e) the Law of 2018 No. 142-VI “On Commissions on Juvenile Affairs and the Protection of Their Rights” should be supplemented with special powers of commissions to coordinate offenses in the digital sphere; (f) the legal mechanism of “counterpart obligations” should be established at the legislative level, through a norm providing that the failure of one subject to perform functions serves as a basis for the automatic activation of

another subject's protective procedures.

(3) Reactive-educational pillar. (a) Article 84(2) of the Criminal Code RK should be supplemented with an expanded list of digital educational measures, including courses in digital hygiene and cyberethics, participation in digital volunteer programs, and digital probation; (b) Article 79 of the Criminal Code RK should be supplemented with a digital expungement mechanism, namely a procedure for removing a criminal past from digital registers for adolescents who have successfully completed measures of educational influence; (c) Article 65(1) of the CAO RK should be supplemented with a rule on the unconditional priority of educational influence measures over fines for minors who commit an administrative offense in the ICT field for the first time; (d) the list of aggravating circumstances for administrative liability in Article 57 of the CAO RK should be expanded to include "commission of an offense using ICT or telecommunication networks"; (e) Article 232-1 of the Criminal Code RK should be supplemented with a note establishing the priority of educational measures with respect to minor subjects.

(4) Systematization-codification pillar. (a) The Law "On Personal Data and Their Protection" should be supplemented, following the model of Convention 108+ and Article 8 of the GDPR, with a special chapter titled "Chapter 5-1. Enhanced Protection Regime for Minors' Personal Data"; (b) a direct prohibition on profiling children should be established at the legislative level in accordance with General Comment No. 25 of the UN Committee on the Rights of the Child (CRC/C/GC/25, 2021) and paragraph 35 of Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe; (c) mandatory internal audit procedures for high-risk data processing and retention periods for access logs should be specified; (d) in the long term, a draft Information Code should be scientifically elaborated in accordance with the principles of legal hierarchy and sectoral coherence established in the Law of the Republic of Kazakhstan "On Legal Acts"; (e) following the model of Article 28 of the Lanzarote Convention, a "Target Fund for Children's Digital Security" should be formed from part of the fines imposed on technology companies for violations of cybersecurity requirements; (f) a specialized normative resolution of the Supreme Court of the Republic of Kazakhstan should be developed, following the model of Resolution No. 37 of the Supreme Court of the Russian Federation dated 15 December 2022, explaining criteria for assessing the authenticity of digital evidence, the methodology for analyzing deepfake materials, and the admissibility of cyber patrol monitoring.

This architecture, as a structural mechanism for overcoming at the institutional level the lag of criminal-law and administrative-law institutions behind technological development, will serve as the doctrinal basis for the national implementation of the Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, adopted by UN General Assembly Resolution A/RES/79/243 of 24 December 2024 (signed by Kazakhstan in October 2025), and will form comprehensive institutional support for the application to minor subjects of the

“Concept for the Development of Artificial Intelligence for 2024–2029,” approved by Resolution No. 592 of the Government of the Republic of Kazakhstan dated 24 July 2024, and the Law of the Republic of Kazakhstan “On Artificial Intelligence,” which entered into force in 2025.

CONCLUSION

The dissertation research devoted to a comprehensive scientific and legal understanding of the institution of liability for offenses committed by minors in the field of informatization and communications in the Republic of Kazakhstan, based on the analysis of theoretical and methodological foundations, the current state of domestic legal regulation, and comparative legal study of the experience of the CIS, Baltic States, and the PRC, makes it possible to draw the following main conclusions.

First, the historical and legal development of the institution of legal protection in the field of informatization and communications has passed through evolutionary stages from the formation of electrical communications and telegraph law to algorithmic legal regimes in the era of computer technology, the internet, content regulation, AI, and Big Data. The works of E. Ondashuly and M.B. Nurusheva[62], A.E. Zhatkanbayeva, Zh.O. Kulzhabayeva[64], and A.M. Ashim[65] substantiate the patterns of formation of this institution in domestic doctrine.

Second, the criminological nature of offenses in the field of informatization and communications made it possible to divide them into six main groups: offenses against information systems, offenses against the circulation of personal data, offenses in the field of communications and telecommunications, digital financial fraud, platform-media offenses, and network crimes directed against minors. This classification provides a comprehensive scientific basis for digital crimes, for which Kazakhstan does not yet have an independent criminological concept.

Third, official statistical data prove the need for Kazakhstan to move from a reactive legal model to a proactive preventive model. Internet fraud increased from 7,700 cases in 2019 to 17,800 in 2021[8], reached 22,870 in 2024[48], and total fraud in 2024 amounted to 45,156 cases. This requires a comprehensive renewal of mechanisms through which state criminal policy responds in a timely manner to digital threats.

Fourth, the status of minors as subjects of legal relations in the field of informatization and communications has shown that they are not only protected objects, but also special subjects with rights, duties, and limited legal autonomy. The study by H. Halibiyati and co-authors, based on the Add Health longitudinal sample (n = 20,745)[60; 151], statistically proved the character of neuropsychological functioning as an independent predictor of the probability of arrest during minority. This result forms a theoretical basis for introducing the category of “digital maturity” into domestic doctrine as an independent subject of procedural assessment.

Fifth, the analysis of administrative and criminal liability showed that the current sanctions model is not fully effective with respect to minors. Although Article 64(1-1) of the CAO RK establishes the maximum fine imposed on a minor, where an adolescent has no independent income, the fine is recovered from legal representatives, which eliminates the individualized educational effect of punishment. In addition, the closed list of educational influence measures in Article 84(2) of the

CC RK does not take into account the substantive specific features of offenses in the ICT field.

Sixth, the comparative legal analysis of the experience of the CIS, Baltic States, and the PRC made it possible to propose for Kazakhstan a hybrid legal approach based on differentiated reception. The works of A.B. Sharipova, A.A. Aryn and G.A. Kuanaliyeva[83], A.M. Satbayeva, A.R. Alimbetova and M.T. Beisenbayeva[39], and I.U. Aubakirova and A.A. Toleubek[84] substantiate the doctrinal foundations for adapting innovative mechanisms of national legal systems to Kazakhstan.

Seventh, the PRC Regulation on the Online Protection of Minors, which entered into force on 1 January 2024[165; 167], the 2021 Personal Information Protection Law, and the Cybersecurity Law amended on 28 October 2025 represent, as an example of international best practice, a comprehensive institutional model for ensuring children's digital security that is suitable for adaptation to the legal system of Kazakhstan under the principle of differentiated reception.

Eighth, the research results substantiate the need to recognize minors' information-psychological security as an independent object of criminal-law protection. It is proposed to supplement Chapter 7 of the CC RK with Section 7-1, titled "Criminal Offenses against the Information-Psychological Security of a Minor," and to introduce Article 213-1.

Ninth, it is proposed to consider the classification of digital delicts and the system of restorative influence within a single legal model. A "digital delict" is proposed as an unlawful act committed through the use of ICT or in the digital environment, whose object is information security and the established procedure for using information resources, and which entails material, administrative, or criminal liability.

Tenth, the dissertation substantiates the need to treat artificial intelligence and synthetic algorithms as an independent factor in criminal-law classification. AI systems, deepfake materials, chatbots, generative models, and automated manipulation tools may become instruments through which an adult involves a minor in crime, which requires supplementing Article 28 of the CC RK with a qualifying element, Article 54 with an aggravating circumstance, and Article 53 with a form of mental coercion.

Eleventh, a special civil-law algorithm is proposed for compensating moral harm caused to minors in the digital environment. This algorithm adapts Articles 951–952 of the Civil Code RK to the conditions of the digital era and provides for a legal presumption of moral harm in cases of network offenses.

Twelfth, the tripartite "State - Platform - Parent" model of responsibility is proposed as the institutional basis for ensuring children's cybersecurity. In this model, the state provides the normative legal framework and interdepartmental coordination, online platforms perform a "duty of care" following the model of the EU Digital Services Act, and parents perform digital mentoring duties.

Thirteenth, the research scientifically substantiates the need to adopt a “National Strategy for Children’s Digital Security” in the Republic of Kazakhstan. This Strategy would form a comprehensive institutional mechanism based on the Convention adopted by UN Resolution A/RES/79/243 of 2024[106], Recommendation CM/Rec(2018)7 of the Committee of Ministers of the Council of Europe, and the experience of the PRC.

Fourteenth, as a result of this research, the category of “digital maturity” has been introduced for the first time into Kazakh legal science as an independent doctrinal category. Normative proposals have been developed for Article 80 of the CC RK and Article 271 of the CPC RK, treating the court’s assessment of a minor’s ability to understand the legal nature and virtual consequences of an act committed using ICT as an independent subject of procedural assessment.

Fifteenth, for the first time, domestic doctrine is offered a threefold legal regime of complicity under conditions of artificial intelligence (AI): as an independent aggravating means of committing a crime (Article 54 of the CC RK), as a qualifying element of complicity in a crime (Article 28 of the CC RK), and as an algorithm of mental coercion of a minor subject (Article 53 of the CC RK).

Sixteenth, for the first time, a comprehensive institutional and normative architecture for preventing minors’ offenses in the ICT field is proposed as a unified doctrinal construction consisting of four mutually coordinated pillars: regulatory-platform, institutional-subject, reactive-educational, and systematization-codification.

In summary, the theoretical significance of the dissertation is determined by the introduction into domestic legal doctrine of the categories “super-institution of information relations,” “digital delict,” “digital maturity,” “restorative digital justice,” “counterpart obligations,” and “differentiated reception.”

The proposed measures are intended for use in the legislative activity of the committees of the Mazhilis and Senate of the Parliament of the Republic of Kazakhstan, in the methodological work of the Committee on Legal Statistics and Special Records under the Prosecutor General’s Office of the Republic of Kazakhstan, in the practical activities of the Ministry of Internal Affairs of the Republic of Kazakhstan and the Office of the Commissioner for Children’s Rights, and in the educational process of law faculties of higher education institutions.

Further development of the research results will continue in promising areas such as the legal classification of crimes committed using artificial intelligence, the criminal use of deepfake technologies against minors, the legal personality of the digital subject, legal relations in the metaverse, and digital justice for minors.

List of References:

1. Қазақстан Республикасының Конституциясы: 1995 жылғы 30 тамызда республикалық референдумда қабылданды (2022 жылғы 8 маусымдағы өзгерістер мен толықтырулармен)[Электрондық ресурс]. - URL: https://adilet.zan.kz/kaz/docs/K950001000_ (қолданылу күні: 24.04.2026).
2. Ақпараттандыру туралы: Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z1500000418> (қолданылу күні: 24.04.2026).
3. Байланыс туралы: Қазақстан Республикасының 2004 жылғы 5 шілдедегі № 567 Заңы[Электрондық ресурс]. - URL: https://adilet.zan.kz/kaz/docs/Z040000567_ (қолданылу күні: 24.04.2026).
4. Қазақстан Республикасының ұлттық қауіпсіздігі туралы: Қазақстан Республикасының 2012 жылғы 6 қаңтардағы № 527-IV Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z1200000527> (қолданылу күні: 24.04.2026).
5. Қазақстанда соңғы бес жылда қылмыс деңгейі екі есе төмендеді: ҚР Бас прокуратурасы жанындағы Құқықтық статистика және арнайы есепке алу жөніндегі комитеттің 2025 жылғы ресми деректері (қаңтар–тамыз)[Электрондық ресурс]. - URL: <https://qamqor.gov.kz> (қолданылу күні: 24.04.2026).
6. Тіркелген қылмыстық құқық бұзушылықтар туралы: ҚР Бас прокуратурасы жанындағы Құқықтық статистика және арнайы есепке алу жөніндегі комитеттің 2024 жылғы ресми статистикалық бюллетені[Электрондық ресурс]. - URL: <https://qamqor.gov.kz/crimestat> (қолданылу күні: 24.04.2026).
7. Қазақстан Республикасы Ұлттық Банкінің Ұлттық төлем корпорациясының «Антифрод» орталығының 2024 жылғы ресми есебі: 80 000-нан астам алаяқтық оқиғаның алдын алу, 500 миллион теңгенің қайтарылуы[Электрондық ресурс]. - URL: <https://nationalbank.kz> (қолданылу күні: 24.04.2026).
8. Қазақстанда интернет-алаяқтық көбейді: ҚР Ішкі істер министрлігінің Криминалдық полиция департаментінің 2021 жылғы ресми деректері (2019 ж. - 7 700, 2020 ж. - 14 000, 2021 ж. - 17 800 факті)[Электрондық ресурс]. - URL: <https://www.gov.kz/memleket/entities/mvd> (қолданылу күні: 24.04.2026).
9. Kubanova N., Nessipbayeva I., Dyussebaliev S., Halibati H., Adilgazy S. Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability // Social & Legal Studios. - 2025. - Vol. 8, No. 1. - P. 179–194. - DOI: 10.32518/sals1.2025.179.
10. Левичева А. Р. Ответственность несовершеннолетних за правонарушения в сфере информационной безопасности // Белгородский государственный

национальный исследовательский университет (Белгород, Россия). - 2023. - С. 463–465.

11. Halibiyati H., Aratuly K., Serikhan A., Yergali A. M., Beaver K. M. Neuropsychological functioning and its association with juvenile arrest and adulthood incarceration: Findings from a longitudinal sample of youth // *Journal of Criminal Justice*. - 2024. - Vol. 91. - Article No. 102153. - DOI: 10.1016/j.jcrimjus.2024.102153.

12. Белавина Е. С., Шкорбатова Н. В. Ответственность несовершеннолетних за правонарушения в сфере информационной безопасности // Калининградский филиал Санкт-Петербургского университета МВД России. - 2023. - С. 45–47.

13. Лукина Е. И. Особенности привлечения к административной ответственности за совершение правонарушений в сфере информационной безопасности несовершеннолетних // Воронежский институт МВД России. - 2015. - С. 404–406.

14. Қазақстан Республикасының цифрлық трансформациясын, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамытудың 2023–2029 жылдарға арналған тұжырымдамасы: ҚР Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысымен бекітілген[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/P2300000269> (қолданылу күні: 24.04.2026).

15. Tatarinova L., Dzhnadilov O., Tatarinov D. Conceptual problems of defining main types of offenses in the sphere of informatization // *Turan University, Almaty; Academy of Law Enforcement Agencies, Astana*. - 2017. - P. 136–139.

16. Marwick A., Fontaine C., boyd d. «Nobody Sees It, Nobody Gets Mad»: Social Media, Privacy, and Personal Responsibility Among Low-SES Youth // *Social Media + Society*. - 2017. - Vol. 3, No. 2. - P. 1–14. - DOI: 10.1177/2056305117710455.

17. Сеитов Т. Е. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: учебное пособие. - Алматы: Данекер, 2004. - 328 с.

18. Бошаева Л. Л. Предупреждение киберпреступности в отношении несовершеннолетних: дис. ... канд. юрид. наук: 5.1.4 / Бошаева Лариса Лангиевна. - М.: РосНОУ, 2024. - 230 с.

19. Каранова Д. А. Криминологическая характеристика и предупреждение преступлений против личности, совершаемых несовершеннолетними с использованием информационно-коммуникационных технологий: автореф. дис. ... канд. юрид. наук: 5.1.4 / Каранова Дарья Андреевна. - М., 2025. - 26 с.

20. Карабеков К. О. Киберпреступность в Российской Федерации и Республике Казахстан: состояние и меры предупреждения: автореф. дис. ... канд. юрид. наук: 5.1.4 / Карабеков К. О. - Омск, 2025. - 25 с.

21. Динисламова А. З. Некоторые перспективы развития системы административной ответственности за правонарушения, посягающие на информационно-психологическую безопасность несовершеннолетних // Краснодарский университет МВД России. - 2024. - № 9. - С. 1–4.

22. Занина Т. М., Лукина Е. И. Правовые проблемы привлечения к административной ответственности за правонарушения в сфере информационной безопасности несовершеннолетних // Наука и практика. Воронежский институт МВД России. - 2016. - № 2 (67). - С. 404–406.

23. Yuzikova N., Komiakova T., Khomiachenko S., Chasova T. Moral and Psychological Features of the Motivational Sphere of Juveniles who Commit Crimes: Risk Assessment of Determining Communication // European Journal of Sustainable Development. - 2021. - Vol. 10, No. 1. - P. 123–135. - DOI: 10.14207/ejsd.2021.v10n1p123.

24. International Telecommunication Union. Overview of ITU's History (1865 - present): Foundations for international cooperation and communications[Электрондық ресурс]. - URL: <https://www.itu.int/en/history/Pages/ITUsHistory.aspx> (қолданылу күні: 24.04.2026).

25. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 (revised 2013)[Электрондық ресурс]. - URL: <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm> (қолданылу күні: 24.04.2026).

26. Электрондық құжат және электрондық цифрлық қолтаңба туралы: Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370-ІІ Заңы[Электрондық ресурс]. - URL: https://adilet.zan.kz/kaz/docs/Z030000370_ (қолданылу күні: 24.04.2026).

27. Темирәлиев Т. С., Омаров Е. А. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения // Академия правоохранительных органов при Генеральной прокуратуре РК. - 2021. - С. 1–6.

28. Дербес деректер және оларды қорғау туралы: Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z1300000094> (қолданылу күні: 24.04.2026).

29. Ақпаратқа қол жеткізу туралы: Қазақстан Республикасының 2015 жылғы 16 қарашадағы № 401-V Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z1500000401> (қолданылу күні: 24.04.2026).

30. Қазақстан Республикасының киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны»): ҚР Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/P1700000407> (қолданылу күні: 24.04.2026).

31. Цифрлық активтер туралы: Қазақстан Республикасының 2023 жылғы 6 ақпандағы № 193-VІІ Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z2300000193> (қолданылу күні: 24.04.2026).

32. Қазақстан Республикасында жасанды интеллектіні дамытудың 2024–2029 жылдарға арналған тұжырымдамасы: ҚР Президентінің 2024 жылғы 24

қыркүйектегі Жарлығымен бекітілген[Электрондық ресурс]. - URL: <https://akorda.kz> (қолданылу күні: 24.04.2026).

33. Ақпараттық қауіпсіздік, ақпараттандыру және цифрлық активтер мәселелері бойынша Қазақстан Республикасының кейбір заңнамалық актілеріне өзгерістер мен толықтырулар енгізу туралы: Қазақстан Республикасының 2023 жылғы 11 желтоқсандағы № 44-VIII Заңы (2024 жылғы 11 ақпанда күшіне енді)[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z2300000044> (қолданылу күні: 24.04.2026).

34. Қамбаров А. Қ., Сабитов С. М., Абижанов С. М. Практические методы предупреждения уголовных правонарушений в сфере информатизации и связи // Alikhan Bokeikhan University, Семей; Алматинская академия МВД РК. - 2023. - С. 1–6.

35. Мельникова О. В., Сапогов В. М. Административные правонарушения и противоправное поведение несовершеннолетних: вопросы профилактики, правового просвещения и правового информирования в РФ // НОМОТНЕТІКА: Философия. Социология. Право. - 2022. - Т. 47, № 2. - С. 314–326.

36. Құқықтық актілер туралы: Қазақстан Республикасының 2016 жылғы 6 сәуірдегі № 480-V Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z1600000480> (қолданылу күні: 24.04.2026).

37. Қазақстан Республикасының Қылмыстық кодексі: 2014 жылғы 3 шілдедегі № 226-V ҚРЗ (2026 жылғы сәуірдегі жағдай бойынша өзгерістер мен толықтыруларымен)[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/K1400000226> (қолданылу күні: 24.04.2026).

38. Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі: 2014 жылғы 5 шілдедегі № 235-V ҚРЗ[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/K1400000235> (қолданылу күні: 24.04.2026).

39. Satbayeva A. M., Alimbetova A. R., Beissenbayeva M. T. Cybercrime challenges: Experience of international cooperation // Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan. - 2024. - No. 3 (78). - P. 211–221. - DOI: 10.52026/2788-5291_2024_78_3_211.

40. Bolatbek M., Baispay G., Mussiraliyeva S., Usmanova A. A framework for detection and mitigation of cyber criminal activities using university networks in Kazakhstan // Radioelectronic and Computer Systems. - 2024. - No. 2. - P. 186–202. - DOI: 10.32620/reks.2024.2.15.

41. United Nations Convention against Cybercrime: adopted by General Assembly resolution A/RES/79/243 of 24 December 2024[Электрондық ресурс]. - URL: <https://documents.un.org/doc/undoc/gen/n24/424/95/pdf/n2442495.pdf> (қолданылу күні: 24.04.2026).

42. Jilkishiyev R., Begaliyev Y. Problems of investigation of crimes in the field of information technology // Pakistan Journal of Criminology. - 2024. - Vol. 16, No. 3. - P. 97–114. - DOI: 10.62271/pjc.16.3.97.114.

43. Горюнова О. Л. Особенности расследования преступлений и правонарушений несовершеннолетних. Анализ степени осознания подростком общественной опасности своих действий // Вестник магистратуры. - 2017. - № 2 (65). - С. 76–78.

44. Пономарев О. В., Рой Н. А., Мишина Е. С. Проблемы административной ответственности несовершеннолетних // Вестник экономики, права и социологии. - 2017. - № 2. - С. 105–107.

45. Ryssaldiyeva A. Prevention of Minor Crime in Kazakhstan. - 2022. - DOI: 10.13140/RG.2.2.21813.14565.

46. Convention 108+: Convention for the protection of individuals with regard to the processing of personal data: Council of Europe, modernised by Protocol CETS No. 223 of 10 October 2018[Электрондық ресурс]. - URL: <https://www.coe.int/en/web/data-protection/convention108-and-protocol> (қолданылу күні: 24.04.2026).

47. Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan: ақпараттық-коммуникациялық технологиялар саласы бойынша ресми деректер (2024 ж. қаңтар–қараша)[Электрондық ресурс]. - URL: <https://stat.gov.kz/en/industries/business-statistics/stat-it/publications/266530/> (қолданылу күні: 24.04.2026).

48. Онлайн-платформалар және онлайн-жарнама туралы: Қазақстан Республикасының 2023 жылғы 10 шілдедегі № 18-VIII Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z2300000018> (қолданылу күні: 24.04.2026).

49. Бұқаралық ақпарат құралдары туралы: Қазақстан Республикасының 2024 жылғы 19 маусымдағы № 94-VIII Заңы[Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z2400000094> (қолданылу күні: 24.04.2026).

50. The Prosecutor General's Office of the Republic of Kazakhstan: интернет-алаяқтық пен жасанды интеллект арқылы жасалатын құқық бұзушылықтар туралы ресми ескертулер (2024–2025 жж.)[Электрондық ресурс]. - URL: <https://www.gov.kz/memleket/entities/prokuror> (қолданылу күні: 24.04.2026).

51. Оңдашұлы Е., Нурушева М. Б. Қазақстан Республикасындағы ақпарат құқықтарын конституциялық және заңдық реттеу // ҚазҰУ хабаршысы. Заң сериясы. - 2019. - № 1 (89). - Б. 39–47.

52. Жатқанбаева А. Е. Конституционно-правовые основы права на свободу получения информации // Известия Национальной академии наук Республики Казахстан. - 2012. - № 5. - С. 61–69.

53. Кулжабаева Ж. О. Законодательное разграничение понятий «кибербезопасность» и «информационная безопасность» // Вестник Института законодательства и правовой информации Республики Казахстан. - 2024. - № 4 (79). - С. 178–186.

54. Ашим А. М. Қазақстан Республикасындағы бұқаралық ақпарат құқығы // ҚазҰУ хабаршысы. Заң сериясы. - 2010. - № 3 (55). - Б. 49–51.

55. Маликова Ш. Б., Ергали А. М. Акпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қарсы тұру аясындағы мемлекеттің қылмыстық-құқықтық саясаты туралы // *Journal of Actual Problems of Jurisprudence*. - 2015. - Т. 75, № 3. - Б. 294–297.

56. Алмазқызы Қ. Киберқылмыстылық - Қазақстан Республикасының қауіпсіздігіне жаңа қылмыстық қауіп ретінде // *ҚазҰУ хабаршысы. Заң сериясы*. - 2018. - № 4 (88). - Б. 144–151.

57. Маликова Ш. Б., Омарова А. Б., Маликов Д. Б. Уголовная политика Республики Казахстан в сфере информатизации: вопросы противодействия компьютерной преступности // *Journal of Actual Problems of Jurisprudence*. - 2017. - Т. 84, № 4. - С. 90–96.

58. Кубанова Н. Б., Серикова Л. С. Принципы классификации кибератак и правовое регулирование в Республике Казахстан // *Journal of Actual Problems of Jurisprudence*. - 2024. - Т. 112, № 4. - С. 121–132. - DOI: 10.26577/JAPJ2024.112.i4.a12.

59. Усеинова К. Р., Жапарбек А. М., Токтыбаев А. А., Данияров С. Д. Дропперы как инструмент киберпреступности: история, функции, вызовы для правоохранительных органов // *Journal of Actual Problems of Jurisprudence*. - 2025. - Т. 115, № 3. - С. 109–117. - DOI: 10.26577/JAPJ2025115311.

60. Нурпеисова А. К., Қабден Н. А. Қазақстан Республикасындағы акпараттық қауіпсіздіктің жағдайы // Төртінші индустриалды революция жағдайында Қазақстан Республикасының заңнамасын жетілдірудің теориялық және құқықтық және құқық қорғау мәселелері: халықаралық ғылыми-практикалық конференция материалдары. - Қарағанды, 2018. - Б. 89–93.

61. Atakhanova G. M., Aratuly K., Abitaeva A. K. Уголовная политика Казахстана в сфере информационной безопасности // *Journal of Actual Problems of Jurisprudence*. - 2018. - Т. 85, № 1. - С. 120–129.

62. Еселева-Пионка М., Кенжегара М., Азимбекова А., Байбекова А., Исакулов Е. Правовые меры противодействия финансовому мошенничеству: анализ законодательства и практики Республики Казахстан // *Journal of Actual Problems of Jurisprudence*. - 2025. - Т. 113, № 1. - С. 139–153.

63. Нукушева А. А., Қуандықов Б. Ж., Жайлау Ж. Қазіргі юрисдикцияларда мектеп жасындағы балалар арасында кибербуллингке қарсы іс-қимыл жөніндегі заңнамасына салыстырмалы-құқықтық талдау // *Вестник Института законодательства и правовой информации Республики Казахстан*. - 2024. - № 2 (77). - Б. 248–258.

64. Жаналиева А. Ж., Тлеулесова Б. Т., Кошкинбаева А. С. Киберкеңістікте бала мүддесін қорғау механизмін жетілдіру мәселесі жайлы // *Journal of Actual Problems of Jurisprudence*. - 2022. - № 2 (106). - Б. 45–53.

65. Турсунов А. Б., Бегалиев Е. Н., Маликов Д. Б. Criminological aspects of violence and abuse of children // *Journal of Actual Problems of Jurisprudence*. - 2025. - № 4 (116). - Б. 96–104.

66. Молдағалиева А. С., Сманова А. Б., Досумбекова М. Т., Шуланбекова Г. К. Қазақстан Республикасында зорлық-зомбылық құрбаны болған балалардың құқықтарын қорғаудың кейбір мәселелері // Journal of Actual Problems of Jurisprudence. - 2025. - № 4 (116). - Б. 114–124.

67. Аратұлы Қ., Байғазы Е. Ақпараттық қауіпсіздік саласындағы қылмыстарды тергеу әдістемесі // ҚазҰУ хабаршысы. Заң сериясы. - 2016. - № 2 (78). - Б. 284–289.

68. Базилова А. А. Компьютерлік қылмыстардың алдын алу шаралары // Journal of Actual Problems of Jurisprudence. - 2016. - № 3 (79). - Б. 178–182.

69. Маликова Ш. Б., Омарова А. Б. О некоторых аспектах уголовной политики Республики Казахстан в сфере информационной безопасности // Journal of Actual Problems of Jurisprudence. - 2016. - № 2 (78). - С. 305–309.

70. Джансараева Р. Е., Маликова Ш. Б., Омарова А. Б. Виктимологическое противодействие преступности: концептуальные аспекты // Journal of Actual Problems of Jurisprudence. - 2018. - № 1 (85). - С. 238–243.

71. Жатканбаева А. Е. Об опыте правового регулирования обеспечения информационной безопасности в США и ЕС // Journal of Actual Problems of Jurisprudence. - 2018. - Т. 79, № 3. - С. 300–306.

72. Аубакирова И. У., Тoleyбек А. А. Prospects for the Implementation of the General Data Protection Regulation (GDPR) Requirements into the Legislation of Kazakhstan // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. - 2025. - Т. 80, № 1. - Б. 174–185. - DOI: 10.52026/2788-5291_2025_80_1_174.

73. Умитчинова Б. А., Гаврилова Ю. А., Мензюк Г. А. Правовое регулирование персональных данных в условиях развития искусственного интеллекта: зарубежный опыт и вызовы для Казахстана // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. - 2025. - Т. 80, № 3. - С. 37–46.

74. Шарипова А. Б., Арын А. А., Куаналиева Г. А. Международные аспекты борьбы с преступностью в условиях глобализации информационного общества // Вестник Института законодательства и правовой информации Республики Казахстан. - 2025. - Т. 80, № 1. - С. 148–155.

75. Маликова Ш. Б., Ергали А. М. Қылмыстық-құқықтық саясат: ақпараттандыру саласындағы қол сұғушылықтарға қарсы тұру жолдары // Journal of Actual Problems of Jurisprudence. - 2015. - Т. 75, № 3. - Б. 294–297.

76. Тулеуова А. Ж. Ақпараттық қауіпсіздік және қылмыстық заңнаманы жетілдіру проблемалары // Вестник КазНУ. Серия юридическая. - 2011. - № 5. - Б. 199–201.

77. Сәрпеков Р. Қ. Цифровизация правового пространства // Вестник Института законодательства и правовой информации Республики Казахстан. - 2020. - № 3 (61). - С. 12–24.

78. Шаривхан Ж., Мусипова Д. М., Осыко И. В. Цифровое общество и правовое государство: современные проблемы и решения // Вестник Института законодательства и правовой информации Республики Казахстан. - 2025. - Т. 80, № 4. - С. 54–70. - DOI: 10.52026/2788-5291_2025_80_4_54.

79. Жалтырбаева Р. С., Джангабулова А. Қ., Тілембаева Ж. О. Жасанды интеллект ұғымының құқықтық дефинициясы: теориялық негіздер мен заңнамалық тұжырымдар // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. - 2025. - Т. 80, № 4. - Б. 35–53. - DOI: 10.52026/2788-5291_2025_80_4_35.

80. Тлембаева Ж. У. О некоторых подходах к правовому регулированию искусственного интеллекта // Вестник Института законодательства и правовой информации Республики Казахстан. - 2021. - № 2 (65). - С. 61–74. - DOI: 10.52026/2788-5291_2021_65_2_61.

81. Дәулетханова Ә. А. Халыққа онлайн-платформамен тегін заң көмегін көрсету: проблемалар мен перспективасы // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. - 2025. - Т. 80, № 2. - Б. 226–234.

82. Шаривхан Ж., Мусипова Д. М., Осыко И. В. Цифрлық қоғам мен құқықтық мемлекет: қазіргі мәселелер мен шешімдер // Вестник Института законодательства и правовой информации Республики Казахстан. - 2025. - Т. 80, № 4. - Б. 54–70.

83. Калмыков Б. А. Правовое регулирование кибербезопасности в КНР: особенности и тенденции развития: автореф. дис. ... канд. юрид. наук: 5.1.4. - М., 2023. - 24 с.

84. Белавина Е. С. Ответственность несовершеннолетних за правонарушения в сфере информационной безопасности / Е. С. Белавина ; науч. рук. Н. В. Шкорбатова // Калининградский филиал Санкт-Петербургского университета МВД России. – 4 с.

85. Балаларды денсаулығы мен дамуына зардабын тигізетін ақпараттан қорғау туралы: Қазақстан Республикасының 2018 жылғы 2 шілдедегі № 169-VI Заңы // Қазақстан Республикасы Нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: <https://adilet.zan.kz/kaz/docs/Z1800000169> (жүгінген күн: 18.04.2026).

86. Әкімшілік құқық бұзушылық туралы: Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V Кодексі // Қазақстан Республикасы Нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: <https://adilet.zan.kz/kaz/docs/K1400000235> (жүгінген күн: 18.04.2026).

87. Бала құқықтары туралы конвенцияны ратификациялау туралы: Қазақстан Республикасы Жоғарғы Кеңесінің 1994 жылғы 8 маусымдағы № 77-XIII Қаулысы // Қазақстан Республикасы Нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: https://adilet.zan.kz/kaz/docs/B940001400_ (жүгінген күн: 18.04.2026).

88. Горюнова О. Л. Особенности уголовной ответственности несовершеннолетних / О. Л. Горюнова // Вестник магистратуры. – 2015. – № 11 (50). – Т. 4. – С. 63–65.

89. Занина Т. М. Правовые проблемы привлечения к административной ответственности за правонарушения в сфере информационной безопасности несовершеннолетних / Т. М. Занина, Е. И. Лукина // Наука и практика. – 2016. – № 2 (67). – С. 34–38.

90. Қазақстан Республикасының Қылмыстық кодексі: Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V Кодексі // Қазақстан Республикасы Нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: <https://adilet.zan.kz/kaz/docs/K1400000226> (жүгінген күн: 18.04.2026).

91. Стеблецова Л. А. Ответственность несовершеннолетних по административному праву и практика ее применения органами внутренних дел: автореф. дис. ... канд. юрид. наук: 12.00.14 / Стеблецова Людмила Алексеевна; [Акад. упр. МВД России]. – М., 2005. – 24 с.

92. Бриль Г. Г. Проблемы профилактики безнадзорности и правонарушений несовершеннолетних: вопросы современной юридической практики и педагогики / Г. Г. Бриль, Н. В. Ганжа // Вестник Костромского государственного университета. – 2022. – Т. 28, № 2. – С. 247–252.

93. Қазақстанда кәмелетке толмағандар арасындағы құқық бұзушылықтар саны 55%-ға азайды[Электрондық ресурс] // Қазақстан Республикасы Оқу-ағарту министрлігінің ресми интернет-ресурсы. – 2024. – 20 желтоқсан. – URL: <https://www.gov.kz/memleket/entities/edu/press/news/details/910485> (жүгінген күн: 18.04.2026).

94. Қазақстанда кәмелетке толмағандар істері жөніндегі комиссиялардың қызметі жаңартылды[Электрондық ресурс] // Қазақстан Республикасы Оқу-ағарту министрлігінің ресми интернет-ресурсы. – 2026. – URL: <https://www.gov.kz/memleket/entities/edu> (жүгінген күн: 18.04.2026).

95. Кәмелетке толмағандар арасындағы құқық бұзушылықтардың профилактикасы мен балалардың қадағалаусыз және панасыз қалуының алдын алу туралы: Қазақстан Республикасының 2004 жылғы 9 шілдедегі № 591-II Заңы // Қазақстан Республикасы Нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: https://adilet.zan.kz/kaz/docs/Z040000591_ (жүгінген күн: 18.04.2026).

96. Темиралиев Т. С. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения / Т. С. Темиралиев, Е. А. Омаров // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – С. 136–143.

97. Kozybayeva G.B., Zhanibekov A.K., Apakhayev N., Khamzina Zh.A., Buribayev Y.A. Comparative Legal Analysis of Educational Measures for Minors Who Have Committed an Administrative Offense in Kazakhstan and Ukraine //

Journal of Advanced Research in Law and Economics. – 2019. – Vol. 10, № 1. – P. 274–284. – DOI 10.14505/jarle.v10.1(39).28. (Scopus).

98. Karipbaev Zh.B., Mussin K.S. Concept of bringing minors to administrative responsibility // Вестник Карагандинского университета. Серия: Право. – 2020. – № 2 (98). – С. 32–39. – DOI 10.31489/2020L2/32-39. (Scopus).

99. Abikenova G., Kubeyev Ye.K., Bozhkarauly A., Abdikeev M., Rustembekova D. On the issue of the concept and status of minors in constitutional law and current problems of the implementation of the rights and freedoms of minors // Journal of Advanced Research in Law and Economics. – 2018. – Vol. 9, № 3 (33). – P. 805–818. (Scopus).

100. Sadykanova Zh.E., Karipova A.Ye. On the Problems and Directions for the Prevention of Juvenile Delinquency // Journal of Advanced Research in Law and Economics. – 2019. – Vol. 10, № 5 (43). – P. 1498–1504. (Scopus).

101. Mitskaya E. Non-Compliance of Kazakhstan's Criminal Law With International Anti-Corruption Standards // Access to Justice in Eastern Europe. – 2024. – Vol. 7, № 1. – P. 222–244. – DOI 10.33327/AJEE-18-7.1-r000103. (Scopus).

102. Стеблецова Л.А. Ответственность несовершеннолетних по административному праву и практика ее применения органами внутренних дел : автореф. дис. ... канд. юрид. наук : 12.00.14 / Академия управления МВД России. – Москва, 2005. – 24 с.

103. Кәмелетке толмағандардың киберкеңістіктегі құқыққа қайшы мінез-құлықтары және оларды әкімшілік-құқықтық реттеу тетіктері : PhD диссертация / әл-Фараби атындағы Қазақ ұлттық университеті. – Алматы, 2025. – URL:

https://farabi.university/storage/files/34993126346970cb02a7477934755692_Диссертация.pdf (жүгінген күні: 15.04.2026).

104. Кәмелетке толмағандар арасындағы құқық бұзушылықтардың профилактикасы : заң ғылымдарының докторы ғылыми дәрежесін алу үшін дайындалған диссертация / ҚР Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы. – Нұр-Сұлтан, 2020. – URL: <https://academy-ger.kz/uploads/6c6654f7fc0b52d508f1940ceceb342f.pdf> (жүгінген күні: 15.04.2026).

105. Алибаева Г.А., Абенова Г.А., Мусабаев М.К. Кәмелетке толмағандарды әкімшілік-құқықтық қорғау: шетелдік тәжірибе және оны Қазақстанда пайдалану қажеттілігі // ҚР Заңнама және құқықтық ақпарат институтының жаршысы. – 2020. – № 3 (61). – Б. 34–42.

106. Kymlyk R.V. Special status minor of the subject of administrative responsibility // Вестник Института законодательства и правовой информации Республики Казахстан. – 2015. – № 2 (38). – С. 112–118.

107. Мельникова О.В., Сапогов В.М. Административные правонарушения и противоправное поведение несовершеннолетних: вопросы профилактики, правового просвещения и правового информирования в РФ //

НОМОТНЕТІКА: Философия. Социология. Право. – 2022. – Т. 47, № 2. – С. 314–326.

108. Пономарев О.В., Рой Н.А., Мишина Е.С. Проблемы административной ответственности несовершеннолетних // Вестник экономики, права и социологии. – 2017. – № 2. – С. 102–105.

109. Лукина Е.И. Особенности привлечения к административной ответственности за совершение правонарушений в сфере информационной безопасности несовершеннолетних // Вестник Воронежского института МВД России. – 2016. – № 2. – С. 138–142.

110. Динисламова А.З. Некоторые перспективы развития системы административной ответственности за правонарушения, посягающие на информационно-психологическую безопасность несовершеннолетних // Гуманитарные, социально-экономические и общественные науки. – 2024. – № 9. – С. 231–237.

111. Rakhmetova G.R., Altaeva M.O., Serik G. Prospects for the Institute of Administrative Responsibility in the Republic of Kazakhstan // Journal of Actual Problems of Jurisprudence. Заң сериясы. – 2022. – № 4 (104). – Р. 37–48. – DOI 10.26577/JAPJ.2022.v104.i4.04.

112. Abylkasimov M. The main aspects of the responsibility of minors in the system of administrative law enforcement // Yessenov University Science Journal. – 2024. – URL: <https://ysj.yu.edu.kz> (жүгінген күні: 15.04.2026).

113. Исследование «Кибербуллинг среди подростков Казахстана» // Qainar Journal of Social Science. – 2024. – Vol. 3, № 4. – С. 46–58; Health Behaviour in School-aged Children Study (HBSC Kazakhstan). Ұлттық қоғамдық денсаулық орталығы. – Алматы, 2023.

114. Әкімшілік құқық бұзушылық туралы : Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V Кодексі (2026.01.09 № 257-VIII Заңымен енгізілген өзгерістер мен толықтырулармен) // Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: <https://adilet.zan.kz/kaz/docs/K1400000235> (жүгінген күні: 15.04.2026).

115. Қазақстан Республикасының Цифрлық кодексі : 2026 жылғы 9 қаңтардағы № 255-VIII ҚРЗ // Қазақстан Республикасы нормативтік құқықтық актілерінің ақпараттық-құқықтық жүйесі «Әділет». – URL: <https://adilet.zan.kz/kaz/docs/K2600000255> (жүгінген күні: 15.04.2026); Қазақстан Республикасы Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің ресми статистикасы. – URL: <https://qamqor.gov.kz> (жүгінген күні: 15.04.2026).

116. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (с изменениями и дополнениями по состоянию на 08.08.2025) // Собрание законодательства Российской Федерации. – 2002. – № 1 (ч. 1). – Ст. 1.

117. Новиков В. К., Голубчиков С. В., Уварова А. В. Юридическая ответственность молодежи за правонарушения в области информационной безопасности. -М.: Горячая линия -Телеком, 2021. -186 с.
118. Герасимова Е. В., Жидконожкина О. Н. Социально-правовые аспекты профилактики правонарушений несовершеннолетних, совершаемых под воздействием деструктивных интернет-контентов / Е. В. Герасимова, О. Н. Жидконожкина // Вестник Воронежского института МВД России. -2021. -№ 1. - С. 264–269.
119. Қазақстан Республикасы Президентінің 2023 жылғы 27 қазандағы № 358 Жарлығымен бекітілген Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасы[Электрондық ресурс]. -URL: <https://adilet.zan.kz/> (қолданылу күні: 21.04.2026).
120. Ефименко Л. А. Криминологический анализ взаимосвязи правосознания и преступности несовершеннолетних: автореф. дис. ... канд. юрид. наук: 12.00.08 / Ефименко Любовь Александровна. -Краснодар, 2004. -22 с.
121. Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V Қылмыстық кодексі (2026 жылғы 21 сәуірдегі жағдай бойынша өзгерістер мен толықтыруларымен)[Электрондық ресурс]. -URL: <https://adilet.zan.kz/kaz/docs/K1400000226> (қолданылу күні: 21.04.2026). (Мәтін бойынша:[ҚР ҚК]).
122. Наурзалиева С. М. Уголовная ответственность несовершеннолетних в Республике Казахстан: автореф. дис. ... канд. юрид. наук: 12.00.08 / Наурзалиева Сауле Мергеновна. -М., 2018. -20 с.
123. Қазақстан Республикасы Жоғарғы Сотының 2002 жылғы 11 сәуірдегі «Кәмелетке толмаған адамдардың қылмыстық құқық бұзушылықтары және оларды қылмыстық құқық бұзушылықтар мен қоғамға қарсы өзге де іс-әрекеттер жасауға тарту туралы істер жөніндегі сот практикасы туралы» № 6 нормативтік қаулысы (20.04.2018 жылғы № 8 нормативтік қаулымен өзгерістермен)[Электрондық ресурс]. -URL: https://adilet.zan.kz/kaz/docs/P02000006S_ (қолданылу күні: 21.04.2026).
124. Shukan A., Erdogan Y., Karzhasova G. B. Information technology crimes and juvenile offenders: legal and criminological analysis // Bulletin of Karaganda University. Series “Law”. -2025. -Vol. 30, No. 1 (117). -P. 80–86. -DOI: 10.31489/2025L1/80-86.
125. Кибербуллингпен күрес: балаларды қорғау, отандық және әлемдік тәжірибе[Электрондық ресурс] // ҚазАқпарат. -2022. -URL: https://kaz.inform.kz/news/kiberbullingpen-kures-balalardy-korgau-otandyk-zhane-alemdik-tazhiribe_a3904689/ (қолданылу күні: 21.04.2026).
126. Жумабеков М. Ж. Әкімшілік құқық бұзушылық туралы Қазақстан Республикасының 2014 жылғы 5 шілдедегі № 235-V кодексі (2026 жылғы 21 сәуірдегі жағдай бойынша өзгерістер мен толықтыруларымен); «Бала

- құқықтары туралы» ҚР 2002 жылғы 8 тамыздағы № 345 Заңы[Электрондық ресурс]. -URL: <https://adilet.zan.kz/> (қолданылу күні: 21.04.2026).
127. Ryssaldiyeva A. Prevention of Minor Crime in Kazakhstan / A. Ryssaldiyeva. -2022. -DOI: 10.13140/RG.2.2.21813.14565.
128. Shaisultanov S., Akimzhanov T., Abdrakhmanov B., Bazarlinova A., Bazarlinova A. Combating internet fraud through operative-search measures // Law, State & Telecommunications Review. -2024. -Vol. 16, No. 2. -P. 257–275. -DOI: 10.26512/lstr.v16i2.50740.
129. Қазақстан Республикасы Бас прокуратурасы жанындағы Құқықтық статистика және арнайы есепке алу жөніндегі комитеттің ресми деректері (2024–2025 жж.)[Электрондық ресурс]. -URL: [https://qamqor.gov.kz; http://pravstat.prokuror.gov.kz](https://qamqor.gov.kz;http://pravstat.prokuror.gov.kz) (қолданылу күні: 21.04.2026).
130. Қазақстан Республикасының 2025 жылғы 30 желтоқсандағы «Құқық бұзушылықтың алдын алу туралы» Заңы; Қазақстан Республикасы Үкіметінің 2026 жылғы 30 наурыздағы қаулысымен бекітілген кәмелетке толмағандардың істері және олардың құқықтарын қорғау жөніндегі комиссиялардың қызметі туралы ереже[Электрондық ресурс]. -URL: <https://adilet.zan.kz/> (қолданылу күні: 21.04.2026).
131. Карабанова Е. Н. Эффективность уголовной ответственности несовершеннолетних / Е. Н. Карабанова // Правопорядок: история, теория, практика. -2025. -№ 3 (46). -С. 44–48. -DOI: 10.47475/2311-696X-2025-46-3-44-48.
132. Serikbayev T. A., Baranov M. N. The crime prevention among minors and youth // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. -2013. -Vol. 3 (31). -P. 112–118 (қолданыстағы ережелер бойынша жаңартылған -2024 ж.).
133. Baimoldina S. M., Zabikh Sh. A. Improvement of Legal Measures to Prevent Crime with Regard to Minors in Kazakhstan // Journal of Advanced Research in Law and Economics. -2017. -Vol. 8, No. 3. -P. 738–748.
134. Zhakenov K., Kultemirova L., Ibraeva A. Comparative analysis of the activities of authorities to ensure the prevention of offenses in the Republic of Kazakhstan and other world countries // Security Journal. -2024. -Vol. 37. -P. 1430–1446. -DOI: 10.1057/s41284-024-00425-5.
135. Қазақстан Республикасы ұлттық компьютерлік оқиғаларға ден қою қызметінің (KZ-CERT) 2020–2024 жылдардағы ресми статистикасы мен инциденттерге шолу[Электрондық ресурс]. -URL: <https://cert.gov.kz/> (қолданылу күні: 21.04.2026).
136. Қазақстан Республикасы Ішкі істер министрлігінің 2024–2025 жылдардағы ресми баспасөз мәліметтері (киберқылмыстармен күрес бойынша)[Электрондық ресурс]. -URL: <https://www.gov.kz/memleket/entities/iim> (қолданылу күні: 21.04.2026).

137. Finprom. Жеке деректерді қорғау туралы заңнаманы бұзу бойынша 2024 жылғы статистика[Электрондық ресурс] // Finprom.kz. -2024. -URL: <https://finprom.kz/> (қолданылу күні: 21.04.2026).
138. ҚР ПМ мен ҰҚК-нің бірлескен операциясы: жеке деректерді заңсыз сатумен айналысқан 140 адамның ұсталуы (2025 ж.)[Электрондық ресурс] // ҚР ПМ ресми ақпараты. -URL: <https://www.gov.kz/memleket/entities/iim/press/news> (қолданылу күні: 21.04.2026).
139. Әубакиров А. М. Кәметке толмағандардың қылмыстылығының қазіргі сипаттамасы: статистикалық талдау (2020–2024 жж.) // Торайғыров университетінің Хабаршысы. Заң сериясы. -2022. -№ 2. -Б. 20–28.
140. Қазақстан Республикасының 2014 жылғы 4 шілдедегі № 231-V Қылмыстық-процестік кодексі (2026 жылғы 21 сәуірдегі жағдай бойынша өзгерістер мен толықтыруларымен)[Электрондық ресурс]. -URL: <https://adilet.zan.kz/kaz/docs/K1400000231> (қолданылу күні: 21.04.2026). (Мәтін бойынша:[ҚР ҚПК]).
141. Kobets M. Extraction of information from a cellular phone (mobile communication device) during investigative (search) actions // Scientific Journal of the National Academy of Internal Affairs. -2023. -Vol. 28, No. 2. -P. 52–60. -DOI: 10.56215/naia-herald/2.2023.52.
142. Қазақстан Республикасы Үкіметінің 2023 жылғы 31 тамыздағы № 748 қаулысымен бекітілген «Балаларды зорлық-зомбылықтан, суицидтің алдын алудан қорғау және олардың құқығы мен әл-ауқатын қамтамасыз ету жөніндегі 2023–2025 жылдарға арналған кешенді жоспар»[Электрондық ресурс]. -URL: <https://adilet.zan.kz/> (қолданылу күні: 21.04.2026).
143. Конвенция о киберпреступности (Будапешт, 23.11.2001) и резолюция Генеральной Ассамблеи ООН A/RES/79/243 «Конвенция Организации Объединённых Наций против киберпреступности» (24.12.2024)[Электрондық ресурс]. -URL: <https://www.coe.int/en/web/cybercrime/>; <https://documents.un.org/> (қолданылу күні: 21.04.2026).
144. Zhumabekova K., Kegembayeva Z., Otarbayeva A., Yelubayev A., Abizhanov S. Ensuring Children’s Online Safety in Kazakhstan: Balancing Protection from Harm with Rights to Information Access // Security and Human Rights Monitor. -2024. - DOI: 10.58866/fmyu6192.
145. Семькина О. И., Ключко Р. Н. «Цифровой» признак совершения преступлений как вектор криминализации (компаративный обзор подходов государств - участников СНГ) // Журнал зарубежного законодательства и сравнительного правоведения. - 2020. - № 6. - С. 34–52.
146. Байбарин А. А., Садчикова Д. Н. Методологические основы учебной программы по предупреждению вовлечения несовершеннолетних в преступную деятельность (на примере Курской области) // Вестник Удмуртского университета. Серия Экономика и право. - 2022. - Т. 32, вып. 2. - С. 390–395.

147. Уголовно-правовой режим несовершеннолетних: сравнительно-правовой обзор / сост. по данным национальных уголовных кодексов Латвии, Литвы, Эстонии, стран СНГ[Электрондық ресурс]. - URL: https://ru.wikipedia.org/wiki/Уголовно-правовой_режим_несовершеннолетних (қолданылу күні: 21.04.2026).
148. Регламент (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, и отмене Директивы 95/46/ЕС (General Data Protection Regulation)[Электрондық ресурс]. - URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (қолданылу күні: 21.04.2026).
149. Чечель Г. И., Третьяк М. И. Законодательная регламентация преступлений против собственности в сфере высоких технологий в УК Казахстана и России // Всероссийский криминологический журнал. - 2017. - Т. 11, № 1. - С. 228–236.
150. Федеральный закон Российской Федерации от 24 июня 1999 г. № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» (с изменениями и дополнениями на 2025 г.)[Электрондық ресурс]. - URL: https://www.consultant.ru/document/cons_doc_LAW_23509/ (қолданылу күні: 21.04.2026).
151. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с изменениями и дополнениями от 30.11.2024 г. № 421-ФЗ, введшим статью 272.1)[Электрондық ресурс]. - URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (қолданылу күні: 21.04.2026).
152. Рудов М. В. Реализация отдельных направлений информационно-правовой деятельности подразделений МВД России и ее влияние на результаты профилактики безнадзорности и правонарушений несовершеннолетних (по материалам Ростовской, Волгоградской областей и Краснодарского края) // Юристь-Правоведь. - 2025. - № 1 (112). - С. 196–203.
153. Уголовный кодекс Украины от 5 апреля 2001 г. № 2341-III (с изменениями на 2025 г.): Раздел XVI «Преступления в сфере использования электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей и сетей электросвязи», статьи 361, 361-1, 361-2, 362, 363, 363-1[Электрондық ресурс]. - URL: <https://urst.com.ua/ru/uku> (қолданылу күні: 21.04.2026).
154. Opendatabot: За последние пять лет количество киберпреступлений в Украине выросло вдвое[Электрондық ресурс]. - URL: <https://opendatabot.ua/ru/analytics/374-hackers> (қолданылу күні: 21.04.2026).
155. Dumchykov M., Utkina M., Bondarenko O. Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis // International Journal of Safety and Security Engineering. - 2022. - Vol. 12, Iss. 4. - P. 481–490. - DOI: 10.18280/ijss.120409.

156. Закон Республики Узбекистан от 20 сентября 2024 г. № ЗРУ-964 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с совершенствованием законодательства в сфере обеспечения кибербезопасности»[Электрондық ресурс]. - URL: <https://lex.uz/docs/7108725> (қолданылу күні: 21.04.2026).
157. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) - Article 8 «Conditions applicable to child's consent in relation to information society services»[Электрондық ресурс]. - URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (қолданылу күні: 21.04.2026).
158. Макаров О. С. Системный взгляд на нормативное обеспечение информационной безопасности в Республике Беларусь // Право и государство: теория и практика. - 2020. - № 8 (188). - С. 166–172.
159. Конвенция Организации Объединенных Наций против киберпреступности: Резолюция Генеральной Ассамблеи ООН A/RES/79/243 от 24 декабря 2024 года[Электрондық ресурс]. - URL: <https://documents.un.org/> (қолданылу күні: 21.04.2026).
160. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-3 (с изменениями на 2024 г.), Раздел XII «Преступления против компьютерной безопасности», статьи 349–355[Электрондық ресурс]. - URL: <https://etalonline.by/document/?regnum=hk9900275> (қолданылу күні: 21.04.2026).
161. Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации»[Электрондық ресурс]. - URL: <https://www.vsrfr.ru/documents/own/> (қолданылу күні: 21.04.2026).
162. 《网络安全法完成修改》[China's Cybersecurity Law amendment completed] // 全国人民代表大会网站 (ҚХР Ұлттық халық өкілдері жиналысының ресми сайты). - 2025 ж. қазан[Электрондық ресурс]. - URL: https://www.npc.gov.cn/npc/c2/c30834/202510/t20251028_449076.html (қолданылу күні: 24.04.2026).
163. 10.79亿网民如何共享美好数字生活? -- 透视第52次《中国互联网络发展状况统计报告》[1,079 млрд интернет-пайдаланушы қалай тамаша цифрлық өмірді бөліседі? - ҚХР Интернетінің дамуы туралы 52-ші статистикалық есепке шолу] // Cyberspace Administration of China (CAC). - 2023 ж. тамыз[Электрондық ресурс]. - URL: https://www.cac.gov.cn/2023-08/29/c_1694965940144802.htm (қолданылу күні: 24.04.2026); сондай-ақ 53-ші CNNIC есебі, 2024 ж. желтоқсан - 1,108 млрд пайдаланушы, 78,6% ену деңгейі.
164. 司法部、国家网信办有关负责人就《未成年人网络保护条例》答记者问[Әділет министрлігі мен САС басшыларының «Кәмелетке толмағандардың желідегі қорғалуы туралы ережеге» қатысты журналистерге жауаптары] //

Cyberspace Administration of China. - 2023 ж. 24 қазан[Электрондық ресурс]. - URL: https://www.cac.gov.cn/2023-10/24/c_1699806937449073.htm (қолданылу күні: 24.04.2026).

165. 未成年人网络保护条例 (中华人民共和国国务院令 第766号)[Кәмелетке толмағандардың желідегі қорғалуы туралы ереже, ҚХР Мемлекеттік Кеңесінің 2023 жылғы 16 қазандағы № 766 Жарлығы, 2024 ж. 1 қаңтарда күшіне енді][Электрондық ресурс]. - URL: https://www.cac.gov.cn/2023-10/24/c_1699806932316206.htm (қолданылу күні: 24.04.2026).
166. 中华人民共和国网络安全法 (2016 ж. 7 қараша, 2017 ж. 1 маусымда күшіне енді)[Желілік қауіпсіздік туралы заң] // 全国人民代表大会法律数据库[Электрондық ресурс]. - URL: <https://flk.npc.gov.cn/detail?fileId=&id=2c909fdd678bf17901678bf8276f093d> (қолданылу күні: 24.04.2026).
167. Cybersecurity Law of the People's Republic of China (2025 жылғы 28 қазанда түзетілген редакциясы, 2026 жылғы 1 қаңтардан бастап күшіне енді): translation by the Center for Security and Emerging Technology (CSET) // Georgetown University[Электрондық ресурс]. - URL: <https://cset.georgetown.edu/publication/china-cybersecurity-law-2025> (қолданылу күні: 24.04.2026). Сондай-ақ: China Briefing. China Cybersecurity Law Amendment in Effect January 1, 2026. - 2025 ж. қараша; Haynes Boone. Strictest Amendment to China's Cybersecurity Law In Effect. - 2026 ж. ақпан.
168. 中华人民共和国个人信息保护法 (2021 ж. 20 тамыз, 2021 ж. 1 қарашада күшіне енді)[Дербес ақпаратты қорғау туралы заң] // САС[Электрондық ресурс]. - URL: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (қолданылу күні: 24.04.2026).
169. 关键信息基础设施安全保护条例 (中华人民共和国国务院令 第745号)[Маңызды ақпараттық инфрақұрылымды қорғау туралы ереже, ҚХР Мемлекеттік Кеңесінің № 745 Жарлығы, 2021 ж. 1 қыркүйекте күшіне енді][Электрондық ресурс]. - URL: https://www.mee.gov.cn/zcwj/gwywj/202108/t20210817_858013.shtml (қолданылу күні: 24.04.2026).
170. 中华人民共和国未成年人保护法 (2020 ж. 17 қазандағы жаңа редакция, 2021 ж. 1 маусымда күшіне енді)[Кәмелетке толмағандарды қорғау туралы заң] // 最高人民检察院 (ҚХР Жоғарғы халық прокуратурасы)[Электрондық ресурс]. - URL: https://www.spp.gov.cn/spp/fl/202010/t20201018_482257.shtml (қолданылу күні: 24.04.2026).
171. 中华人民共和国预防未成年人犯罪法 (2020 ж. 26 желтоқсандағы жаңа редакция, 2021 ж. 1 маусымда күшіне енді)[Кәмелетке толмағандар қылмысының алдын алу туралы заң] // 最高人民检察院[Электрондық ресурс]. -

URL: https://www.spp.gov.cn/zd gz/202012/t20201227_503678.shtml (қолданылу күні: 24.04.2026).

172. 关于进一步严格管理 切实防止未成年人沉迷网络游戏的通知 (国家新闻出版署, 2021 ж. 30 тамыз)[Кәмелетке толмағандардың желілік ойындарға тәуелді болуын қатаң шектеу туралы хабарлама, Ұлттық баспасөз және басып шығару әкімшілігі][Электрондық ресурс]. - URL: https://www.nppa.gov.cn/xxfb/tzgs/202108/t20210830_666285.html (қолданылу күні: 24.04.2026).
173. 移动互联网未成年人模式建设指南[Мобильді интернетте кәмелетке толмағандар режимін құру жөніндегі нұсқаулық, САС, 2024 ж. 12 қараша][Электрондық ресурс]. - URL: <https://www.sac.gov.cn/> (қолданылу күні: 24.04.2026).
174. 中华人民共和国刑法 (1997 ж., кейінгі түзетулерімен)[ҚХР Қылмыстық кодексі] // 最高人民检察院[Электрондық ресурс]. - URL: <https://www.spp.gov.cn/> (қолданылу күні: 24.04.2026); сондай-ақ: 两高一部«关于办理帮助信息网络犯罪活动等刑事案件有关问题的意见»[Ақпараттық желі арқылы қылмысқа көмектесу істерін қарау жөніндегі ҚХР Жоғарғы соты, Жоғарғы прокуратурасы және Қоғамдық қауіпсіздік министрлігінің пікірі]. - URL: https://www.spp.gov.cn/xwfbh/wsfbt/202507/t20250728_702365.shtml#1
175. 中华人民共和国刑法修正案 (十一) (2020 ж. 26 желтоқсан, 2021 ж. 1 наурызда күшіне енді)[Қылмыстық кодексінің он бірінші түзетуі, Amendment XI]: ҚХР Төрағасының № 66 Жарлығы[Электрондық ресурс]. - URL: https://www.spp.gov.cn/zd gz/202012/t20201227_503682.shtml (қолданылу күні: 24.04.2026).
176. 为个人信息安全装上«保护锁»[Дербес ақпарат қауіпсіздігіне «қорғау құлпын» орнату] // ҚХР Ұлттық халық өкілдері жиналысы, 2021 ж. тамыз[Электрондық ресурс]. - URL: http://www.npc.gov.cn/c2/c30834/202108/t20210830_313288.html (қолданылу күні: 24.04.2026).
177. 中华人民共和国刑事诉讼法 (2018 ж. 26 қазандағы жаңа редакция)[ҚХР Қылмыстық іс жүргізу заңы][Электрондық ресурс]. - URL: https://www.spp.gov.cn/zd gz/201810/t20181027_396818.shtml (қолданылу күні: 24.04.2026).
178. 中华人民共和国家庭教育促进法 (2021 ж. 23 қазан, 2022 ж. 1 қаңтарда күшіне енді)[Отбасылық тәрбиені ілгерілету туралы заң] // 最高人民检察院[Электрондық ресурс]. - URL: https://www.spp.gov.cn/spp/fl/202110/t20211023_615333.shtml (қолданылу күні: 24.04.2026).
179. «六大保护»有你有我[«Алты қорғауда» сен де, мен де барсың] // 最高人民检察院, 2022 ж. қаңтар[Электрондық ресурс]. - URL:

https://www.spp.gov.cn/spp/zdgz/202201/t20220106_540910.shtml (қолданылу күні: 24.04.2026).

180. 最高人民法院发布涉未成年人网络保护与违法犯罪惩处典型案例[ҚХР Жоғарғы халық соты кәмелетке толмағандардың желідегі қорғалуы мен құқық бұзушылықтарына қатысты типтік істерді жариялайды, 2025 ж.][Электрондық ресурс]. - URL: <https://www.court.gov.cn/zixun/xiangqing/482021.html> (қолданылу күні: 24.04.2026).
181. 中华人民共和国最高人民检察院官方网站[ҚХР Жоғарғы халық прокуратурасының ресми сайты, кәмелетке толмағандарды қорғау жөніндегі жыл сайынғы есептер][Электрондық ресурс]. - URL: <https://www.spp.gov.cn/> (қолданылу күні: 24.04.2026).
182. 王晖：进一步完善未成年人网络保护相关立法[Ван Хуй: Кәмелетке толмағандардың желідегі қорғалуы жөніндегі заңнаманы одан әрі жетілдіру] // ҚХР Ұлттық халық өкілдері жиналысы, 2026 ж. наурыз[Электрондық ресурс]. - URL: https://www.npc.gov.cn/npc/c2/c30834/202603/t20260318_453316.html (қолданылу күні: 24.04.2026).
183. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General: International code of conduct for information security (A/69/723)[Электрондық ресурс]. - URL: <https://digitallibrary.un.org/record/786846> (қолданылу күні: 24.04.2026).
184. Бұқаралық ақпарат құралдары саласындағы уәкілетті органның нұсқамасы бойынша интернет-ресурстарға, шетелдік онлайн-платформалар мен жедел хабар алмасу сервистеріне қолжетімділікті шектеу қағидаларын бекіту туралы: ҚР Мәдениет және ақпарат министрінің 2024 жылғы 24 маусымдағы № 267-НҚ бұйрығы, ҚР Әділет министрлігінде 2024 ж. 25 маусымда № 34570 болып тіркелді[Электрондық ресурс]. - URL: <https://adilet.zan.kz/rus/docs/V2400034570> (қолданылу күні: 24.04.2026).
185. 中华人民共和国数据安全法 (2021 ж. 10 маусым, 2021 ж. 1 қыркүйекте күшіне енді)[Деректер қауіпсіздігі туралы заң] // САС[Электрондық ресурс]. - URL: https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm (қолданылу күні: 24.04.2026).
186. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation): Article 8[Электрондық ресурс]. - URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (қолданылу күні: 24.04.2026); Regulation (EU) 2022/2065 (Digital Services Act), Article 28. - URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
187. Children's Online Privacy Protection Rule (COPPA), 15 U.S.C. §§ 6501–6506; Federal Trade Commission Final Rule Amendments

(22.04.2025)[Электрондық ресурс]. - URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (қолданылу күні: 24.04.2026).

188. БҰҰ-ның киберқылмысқа қарсы Конвенциясы: БҰҰ Бас Ассамблеясының 2024 жылғы 24 желтоқсандағы A/RES/79/243 қарарымен қабылданды[Электрондық ресурс]. - URL: <https://documents.un.org/> (қолданылу күні: 24.04.2026).

189. 中华人民共和国计算机信息系统安全保护条例
(中华人民共和国国务院令 第147号, 1994 ж. 18 ақпан, 2011 ж. түзетілген редакция)[Компьютерлік ақпараттық жүйелер қауіпсіздігін қорғау туралы ереже][Электрондық ресурс]. - URL: https://www.cac.gov.cn/1994-02/19/c_126193562.htm (қолданылу күні: 24.04.2026).