

ANNOTATION

Dissertation on the topic "Problems of legal liability of juveniles for offenses in the sphere of informatization and communication" submitted for the degree of Doctor of Philosophy (PhD) in the educational programme 8D04203 — "Jurisprudence"

General characteristics of the research. The dissertation is devoted to a comprehensive scientific-legal analysis of the institution of legal responsibility of minors for offences in the field of informatisation and communication within the normative-legal system of the Republic of Kazakhstan, to the formation of conceptual foundations for improving the domestic doctrine, and to the elaboration of legislative norm-proposals. The research examines, within a single doctrinal system, the issues of ensuring the legal protection of a minor in the conditions of digital transformation and of defining the legal status of a minor in the digital environment.

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 the right of citizens, including minors, to freely seek, receive and disseminate information in paragraph 2 of Article 20 of the Constitution. However, the realisation of this right is directly linked to 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-legal relations simultaneously as victims, offenders and instruments. The digital vulnerability of minors and the special neuropsychological characteristics of their process of personal formation require a comprehensive reconsideration of the institution of their legal responsibility. This requires not only the improvement of the theoretical doctrine, but also the elaboration of legislative norm-proposals, the renewal of institutional mechanisms, and the implementation of international experience according to the principle of differentiated reception.

The objective empirical evidence of the relevance of the topic is the official statistics of the past five years. According to the data of 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 cases in 2021; the figure of 22,870 cases in 2024 increased by 5% compared with the previous year; in 2025, according to the data of the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan, the share of Internet fraud amounted to approximately 90% of registered crimes. In the financial sphere, the Anti-Fraud Centre under the National Bank of the Republic of Kazakhstan prevented more than 80,000 cases of fraud in 2024 and recovered 500 million tenge. A particularly alarming aspect among cybercrimes against property is the fact that 56% of persons involved in dropper schemes are young people aged 16 to 24.

The relevance of the research topic is also determined by international-legal parameters. The Convention against the Use of Information and Communication Technologies for Criminal Purposes, adopted by United Nations General Assembly resolution A/RES/79/243 of 24 December 2024, establishes the international framework that requires implementation at the national level in the Republic of Kazakhstan. The Lanzarote Convention of the Council of Europe (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 GDPR (2016/679) and DSA (2022/2065) Regulations of the European Union establish the international standards for the regime of enhanced protection of minors' personal data and the duty of care of platforms. The effectiveness of the existing legal mechanism and its compliance with international standards constitute the doctrinal foundation for improving the domestic doctrine.

Degree of scientific study of the research topic. The theoretical foundations of legal relations and of the institution of responsibility in the field of informatisation and communication are widely examined in domestic and foreign scientific literature. In the fundamental-theoretical direction, a special place is occupied by the comparative-legal analysis of cyberbullying by A.A. Nukusheva, B.Zh. Kuandykov and Zh. Zhailau, the study of mechanisms for protecting the interests of children in cyberspace by A.A. Zhanaliyeva and co-authors, the study in the legal sphere of the digital era by A.Zh. Tuleyuova, the analysis of criminal policy in the field of informatisation by Sh.B. Malikova and D.B. Malikov, the study of cybercrime by K. Almazkyzy, and the methodology of investigating crimes in the field of information security by K. Aratuly and E. Baigazy.

In the criminological-legal direction, the main foundations of the domestic scientific discourse are constituted by: the issue of legislative distinction between the concepts of cybersecurity and information security by Zh.O. Kulzhabayeva; the study of the principles of classification of cyberattacks by N.B. Kubanova and L.S. Serikov; the analysis of droppers as an instrument of cybercrime by K.R. Useinova and co-authors; the study of the legal definition of AI by R.S. Zhaltyrbayeva; the comparative study of the legal regulation of personal data in the conditions of AI by B.A. Umitchinova, Yu.A. Gavrilova and G.A. Menzyuk; the comprehensive study of the problems of investigating crimes in the field of ICT by A.K. Zhilkishiyev and E. Begaliyev; the dissertation on the prevention of cybercrimes against minors by L.L. Boshayeva; the criminological characteristics of crimes against the person committed with the use of ICT by D.A. Karanov; and the comparative study of the legislation of the Russian Federation and the Republic of Kazakhstan by K.O. Karabekov. In the administrative-legal direction, the studies of E.I. Lukina, T.M. Zanina and G.A. Alibayeva with co-authors comprehensively analyse the features of the administrative responsibility of minors; the work of Karipbaev Zh.B. with co-authors in Scopus publications substantiates the legal status of this category at the international level.

A review of the scientific literature shows that the topic of the responsibility of minors for offences in the field of informatisation and communication has been examined in the legal science of the Republic of Kazakhstan in individual aspects,

but a comprehensive study as an independent doctrinal category has not yet been fully conducted, which substantiates the scientific novelty of the dissertation research.

Object of the research — legal relations arising within the framework of the social relations of minors in the field of informatisation and communication, including those arising from the commission of unlawful acts using ICT or from becoming a victim of such acts.

Subject of the research — the system of normative legal acts of the Republic of Kazakhstan regulating the responsibility of minors for offences in the field of informatisation and communication, the legal gaps therein and their manifestation in law enforcement practice, as well as the comparative-legal experience of international and foreign law.

Aim of the research — a comprehensive scientific-legal analysis of the institution of responsibility of minors for offences in the field of informatisation and communication within the normative-legal system of the Republic of Kazakhstan, the formation of conceptual foundations for improving the domestic doctrine, and the elaboration of legislative norm-proposals.

Tasks of the research. To achieve the stated aim, the following tasks were set: 1) to investigate the theoretical-legal foundations and the evolutionary formation of the institution of legal responsibility in the field of informatisation and communication; 2) to determine the criminological characteristics and the independent categories of offences in the field of ICT; 3) to analyse the status of a minor as a subject of legal relations in the field of ICT; 4) to comprehensively study the features of the responsibility of minors under the Code of the Republic of Kazakhstan on Administrative Offences and the Criminal Code of the Republic of Kazakhstan; 5) to conduct a comparative-legal analysis of the experience of the CIS countries, the Baltic States and the People's Republic of China; 6) to substantiate the categories of the information-psychological security of minors and of digital maturity as independent doctrinal foundations; 7) to develop norm-proposals for the Criminal Code and the Code on Administrative Offences of the Republic of Kazakhstan; 8) to substantiate the doctrinal foundation of the tripartite model "State — Platform — Legal Representative."

The methodological basis of the research is grounded on the general scientific principles of the theory of knowledge and of the scientific comprehension of legal reality. The work comprehensively applied general scientific methods (dialectical, system-structural, historical, formal-logical) and special scientific methods (comparative-legal, normative-dogmatic, statistical, content-analysis).

The theoretical basis of the research is constituted by the works of Kazakhstani and foreign scholars in the fields of general theory of law, information law, criminal law and criminology, and administrative law (S.S. Alexeev, I.L. Bachilo, V.A. Kopylov, A.K. Zhilkishiyev, E. Begaliyev).

The normative-legal base of the research is constituted by the Constitution of the Republic of Kazakhstan, the Law "On Informatisation" of 2015 No. 418-V, the Law "On Communications" of 2004 No. 567, the Law "On Personal Data and

Their Protection" of 2013 No. 94-V, the information security package updated by the amendments of 2023 No. 44-VIII, the Law "On the Protection of Children from Information Harmful to Their Health and Development" of 2018 No. 169-VI, the Concept of Digital Transformation of the Government of the Republic of Kazakhstan of 2023 No. 269, the "Cyber Shield of Kazakhstan" Concept approved by Resolution of the Government of the Republic of Kazakhstan of 2017 No. 407, and the Concept for the Development of Artificial Intelligence of the President of the Republic of Kazakhstan of 24 September 2024.

The empirical basis of the research is constituted by the official data of the Committee on Legal Statistics and Special Records under the Prosecutor General's Office of the Republic of Kazakhstan for the period 2019–2026, the reports of the Anti-Fraud Centre 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), and the work of Kubanova and co-authors on the comparative analysis of cyberattacks in a Scopus Q1 publication.

The scientific novelty of the research is manifested in the following: firstly, for the first time in the domestic legal science the institution of responsibility of minors for offences in the field of informatisation and communication has been analysed as a comprehensive doctrinal category; secondly, for the first time the categories of "digital maturity," "digital delict," "restorative digital justice," "counterpart obligations" and "differentiated reception" have been introduced as independent doctrinal foundations; thirdly, a comprehensive institutional-normative architecture for the prevention of offences by minors in the field of ICT has been proposed — as an author's model consisting of four mutually coordinated pillars (regulatory-platform, institutional-subject, reactive-educational, systematising-codification); fourthly, the tripartite institutional-legal model "State — Platform — Legal Representative" has been substantiated as the doctrinal foundation of the digital security of children; fifthly, the introduction of neuropsychological examination as a mandatory procedural procedure in the qualification of the criminal liability of a minor in the field of ICT has been proposed.

Main provisions submitted for defense.

Provision 1. The information-psychological security of minors must be recognised as an independent object of criminal-legal protection. It is understood as the protection of a minor from the destructive informational impact disseminated in the digital environment — from cyberbullying, suicidal content, digital grooming, unlawful profiling and the misuse of personal data — as well as the state of preservation of his psychic, emotional and moral integrity. It is proposed to supplement Chapter 7 of the Criminal Code of the Republic of Kazakhstan with Section 7-1 "Criminal offences against the information-psychological security of a minor" and to introduce Article 213-1 therein.

Provision 2. In the qualification of the criminal liability of minors in the field of ICT, the category of "digital maturity" must be introduced as an independent subject of procedural assessment. Digital maturity is understood as the level of intellectual, emotional and social-legal development of a minor's capacity to

comprehend the legal nature and virtual consequences of an act committed with the use of ICT. The scientific substantiation of the provision is the data of the study by Halibiyati H., Aratuly K., Serikhan A., Yergali A.M., Beaver K.M. (Journal of Criminal Justice, 2024, Vol. 91, Article 102153, Scopus Q1, IF 4.3), published in co-authorship of the dissertation candidate, based on the Add Health longitudinal sample (n = 20,745). It is proposed to supplement Article 80 of the Criminal Code of the Republic of Kazakhstan and Article 271 of the Criminal Procedure Code of the Republic of Kazakhstan with a norm establishing neuropsychological examination as a mandatory procedural procedure.

Provision 3. The legal definitional field of violence in the digital environment and the terminological consistency in the field of protection of children's personal data must be ensured at the legislative level. The definition of "child abuse (bullying)," introduced in 2022 into the Law "On the Rights of the Child in the Republic of Kazakhstan" of 2002 No. 345-II, does not cover the semantic characteristics of the digital environment — the anonymous mode of the subject, the asymmetry of the parties' capabilities, and the capacity of a single act for uncontrolled dissemination among a mass audience. The definitions of "cyberbullying," "digital aggression" and "profiling of children" must be introduced, as well as a norm prohibiting the automated profiling of a minor under 16 years of age — in accordance with the UN CRC/C/GC/25 (2021) and recommendation CM/Rec(2018)7 of the Council of Europe.

Provision 4. The institution of digital delicts must be introduced as an independent doctrinal category, and responsibility and restorative impact in relation to minors must be formed as a unified legal model. A digital delict is understood as an unlawful act committed through the use of ICT or in the digital environment, the object of which is the information security of society and the established order of using information resources, entailing material, administrative or criminal liability. Within the category, offences involving minors are classified into three independent categories — a minor as a victim, as an offender, and as an instrument. It is proposed to supplement Article 84 of the Criminal Code of the Republic of Kazakhstan with digital educational measures, Article 79 with the procedure of "digital expungement," and Articles 65 and 57 of the Code of the Republic of Kazakhstan on Administrative Offences.

Provision 5. A methodological conception for the qualification of the act of a minor subject must be formed, integrating into a single foundation digital maturity and participation in the conditions of artificial intelligence. The conception is based on two interrelated theoretical foundations — the category of digital maturity and a model of qualification that takes into account AI and synthetic algorithms (deepfake materials, chatbots, generative models) as an instrument participating in criminal-legal relations. At the international level, Regulation 2024/1689 of the European Union (AI Act) and the Interim Measures of the PRC of 2023 for the Administration of Generative Artificial Intelligence Services establish the foundation of this conception.

Provision 6. Participation in a crime in the conditions of artificial intelligence must be enshrined in the criminal code in a three-fold legal regime — as an

independent aggravating instrument of committing a crime, as a qualifying feature of complicity, and as an algorithm of psychic compulsion of a minor subject. It is proposed to supplement Article 210 of the Criminal Code of the Republic of Kazakhstan to cover the elements of producing phishing content and creating deepfake materials with the help of generative AI, within the framework of the reception of Articles 7–11 of the Convention adopted by UN resolution A/RES/79/243.

Provision 7. Ensuring the digital security of minors must be organised on the basis of the tripartite institutional-legal model "State — Platform — Legal Representative." The model forms the legal protection of a minor in the digital space as a mutually complementary intersection of the regulatory function of the state, the duty of care of the information intermediary, and the mentoring function (digital parenting) of the legal representative; as the legal mechanism for implementing the model, the institution of "counterpart obligations" is proposed, and as specialised subjects — the institutions of the cyber-squad and the digital ombudsman. Empirical substantiation: according to the UNICEF study of 2024, only 38% of parents are regularly aware of their children's online activity, and only 12% actively use parental control tools.

Provision 8. For the first time, an author's comprehensive institutional-normative architecture for the prevention of offences by minors in the field of ICT must be introduced into the criminal-legal, administrative-legal and information-legal 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 model "State — Platform — Parent"), reactive-educational, and systematising-codification — and integrates Provisions 1–7 of this research into a single doctrinal system.

The theoretical significance of the research is determined by the introduction into the domestic doctrine of the categories "superinstitution of information relations," "digital delict," "digital maturity," "restorative digital justice" and "differentiated reception" proposed in the work. The practical significance of the research is determined by the possibility of applying the developed legislative norm-proposals in improving the Criminal Code of the Republic of Kazakhstan and the Code on Administrative Offences, the Laws "On the Rights of the Child in the Republic of Kazakhstan," "On Personal Data and Their Protection" and "On the Protection of Children from Information Harmful to Their Health and Development."

Approbation of the research results. The main provisions and scientific conclusions contained in the dissertation have been published in the works of the author, including in the Scopus journal article 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 Kubanova N., Nessipbayeva I., Dyussebaliev 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, designations and abbreviations, an introduction, four chapters (ten sections), a conclusion and a list of used literature.