MULTIDISCIPLINARY SCIENTIFIC RESEARCH
BJMSR VOL 11 NO 5 (2026) P-ISSN 2687-850X E-ISSN 2687-8518
Available online at https://www.cribfb.com
Journal homepage: https://www.cribfb.com/journal/index.php/BJMSR
Published by CRIBFB, USA

THE USE OF DIGITAL TECHNOLOGIES BY CRIMINAL GROUPS IN KAZAKHSTAN: CHALLENGES FOR CRIMINAL JUSTICE, THE RULE OF LAW AND STRONG INSTITUTIONS (SDG 16)

Shynar Maxutkhan [(a)1] *Nurlan Amirov* [(b)] *Talgat Akimzhanov* [(c)] *Aigul Yerubayeva* [(d)] *Serik Begimbayev* [(e)]

[(a)]*Senior Lecturer, Almaty University of Humanities and Economics, Almaty, Kazakhstan; E-mail: Lev_11@bk.ru*
[(b)]*Assistant Professor, School of Law and Public Administration, Narxoz University, Almaty, Kazakhstan; E-mail: nurlan.amirov@narxoz.kz*
[(c)]*Professor & Director, Scientific Research Institute of Law, Turan University, Almaty, Kazakhstan; E-mail: akimzhanovtk@mail.ru*
[(d)]*Assistant Professor, Sherkhan Murtaza International Taraz Innovation Institute, Taraz, Kazakhstan; E-mail: iruaitan@mail.ru*
[(e)]*Senior Lecturer, Almaty University of Humanities and Economics, Almaty, Kazakhstan; E-mail: begimbaev.serik@mail.ru*

ARTICLE INFO

Article History:

Received: 20th March 2026
Reviewed & Revised: 20th March 2026 to 14th September 2026
Accepted: 16th September 2026
Published: 19th September 2026

Keywords:

Comparative Cybercrime Law, Digital Forensics, Budapest Convention; Organized Cybercrime, Cryptocurrency Regulation, Electronic Evidence, Peace, Justice and Strong Institutions, SDG 16, Accountable Institutions, Central Asia

JEL Classification Codes:

K14, K33, K42, O33

Peer-Review Model:

External peer review was done through double-blind method.

ABSTRACT

The rapid digitalisation of the economy and public administration under the "Digital Kazakhstan" program has been accompanied by the growing use of digital technologies by organised criminal groups, which threatens peace, justice, and strong institutions (SDG 16), as well as digital infrastructure (SDG 9). Despite growing scholarly attention, no systematic comparative analysis of Kazakhstan's cybercrime legislation against international frameworks has been conducted. This study examines the compliance of Kazakhstan's legislative and institutional system for combating cybercrime with international standards, primarily the Budapest Convention on Cybercrime, in order to identify regulatory and institutional gaps. The study employs normative legal research and a structured comparative legal analysis of Articles 272–274 of the Criminal Code of Kazakhstan against the legislation of Estonia, Poland and Turkey, using national legislation, international legal acts, official statistics of the Ministry of Internal Affairs of the Republic of Kazakhstan for 2020–2023, and peer-reviewed publications indexed in Scopus and Web of Science. The results show that registered cybercrimes increased from 2,130 in 2020 to 5,120 in 2022 (a 2.4-fold increase), cryptocurrency-related offences rose from 110 to 922, only 27% of cyber incidents are officially recorded, the share of cases reaching court fell from 34% to 27.7%, and only 18% of law enforcement officers have digital forensics training. The findings suggest that Kazakhstan's cybercrime legislation is fragmented and only partially harmonised with the Budapest Convention, particularly regarding the definition of cybercrime, organised cybercrime, cryptocurrency regulation, access to electronic evidence and international cooperation, and that its capacity for accountable and effective law enforcement remains substantially weaker than that of Estonia and Poland.

INTRODUCTION

The rapid development of digital technologies has significantly transformed the criminal environment, leading to the growth of cybercrime at the global and national levels and creating new risks for peace, justice and strong institutions (SDG 16). According to international organizations, annual losses from cybercrime worldwide exceed 8 trillion USD, indicating the systemic nature of threats to economies and public administration (United Nations Office on Drugs and Crime, 2024). In Kazakhstan, the dynamics of cybercrime also show steady growth: 2,130 offences in the field of information technology were registered in 2020, 3,564 in 2021, and 5,120 in 2022 (National Cyber Security Index, 2025). At the same time, cybercrime latency remains high. According to estimates of the Ministry of Internal Affairs of the Republic of Kazakhstan, only about 27% of incidents are officially recorded, which significantly complicates the formation of an adequate criminal policy. Additionally, according to departmental audits, only 18% of law enforcement officers have adequate training in digital forensics, which limits the effectiveness of investigations into such crimes (Jilkishiyev & Begaliyev, 2024; Khamit et al., 2024).

Recent studies have documented the widespread use of cryptocurrencies, anonymization tools, phishing and artificial intelligence by criminal groups in Kazakhstan and the difficulties that law enforcement and judicial institutions face in

[1]Corresponding author: *ORCID ID: 0009-0002-8519-5750*

https://doi.org/10.46281/bjmsr.v11i4.2949

To cite this article: Maxutkhan, S., Amirov, N., Akimzhanov, T., Yerubayeva, A., & Begimbayev, S. (2026). THE USE OF DIGITAL TECHNOLOGIES BY CRIMINAL GROUPS IN KAZAKHSTAN: CHALLENGES FOR CRIMINAL JUSTICE, THE RULE OF LAW AND STRONG INSTITUTIONS (SDG 16). *Bangladesh Journal of Multidisciplinary Scientific Research, 11*(5), 26-36. https://doi.org/10.46281/bjmsr.v11i4.2949

responding to them (Bissaliyev et al., 2025; Kambarov et al., 2024; Kyzylkhojaeva, 2024; Shukan et al., 2025; Yerkenov, 2024; Zhakenov et al., 2024). Despite the growing number of studies on cybercrime in post-Soviet states, there has been no systematic comparative legal analysis of the compliance of Kazakhstan's criminal legislation on cybercrime with international standards. This primarily concerns the provisions of the Budapest Convention on Cybercrime and the standards of states that have already harmonized their legislation with it. This gap is particularly significant given that the national program "Digital Kazakhstan" continues to expand the country's digital infrastructure (SDG 9) at a pace that outpaces the corresponding development of criminal law and law-enforcement institutional mechanisms. The scientific problem addressed in this study is therefore the mismatch between the rapidly evolving digital methods used by organised crime and the fragmented, insufficiently harmonised criminal-law and institutional framework for countering them.

The choice of Poland, Estonia and Turkey as comparative jurisdictions is based on a combination of legal, institutional and technological criteria relevant to assessing the effectiveness of cybercrime countermeasures in Kazakhstan. Poland and Estonia are states parties to the Budapest Convention on Cybercrime and therefore serve as benchmarks for assessing the degree of harmonization of Kazakhstan's legislation with international requirements. In contrast, Turkey presents a mixed model of legal regulation. The novelty of the study lies in combining a doctrinal analysis of Articles 272–274 of the Criminal Code of Kazakhstan with a structured, criterion-based comparative analysis of the legislation of these jurisdictions, which represent varying degrees of compliance with the Budapest Convention. This approach makes it possible to identify specific, practically applicable regulatory gaps and to contribute both to the theoretical understanding of organized crime using digital technologies in post-Soviet legal systems and to the practical improvement of Kazakhstan's policy in countering cybercrime, consistent with the objective of building effective, accountable and inclusive institutions under SDG 16.

This study aims to identify regulatory and institutional gaps in Kazakhstan's system for combating digitally enabled organized crime through a comparative legal analysis of the Budapest Convention on Cybercrime and the legislation of Estonia, Poland, and Turkey. Methodologically, the study relies on normative legal research and a structured comparative legal analysis based on defined criteria, supported by official statistics of the Ministry of Internal Affairs of the Republic of Kazakhstan for 2020–2023 and by peer-reviewed literature indexed in Scopus and Web of Science.

The remainder of the article is structured as follows. The literature review analyses previous research on digital criminology, the institutional and legal challenges of investigating cybercrime, and the study's theoretical framework, and formulates its purpose and research questions. The materials and methods section describes the sources, the comparative criteria and the analytical procedure. The results section presents the technologies used by criminal groups, the dynamics of cybercrime in Kazakhstan, the identified enforcement problems, the comparative legal analysis and the drawbacks of the national legislative framework. The discussion compares the findings with those of previous studies, and the conclusions summarise the contribution, implications, limitations and directions for future research.

LITERATURE REVIEW

As part of the national program "Digital Kazakhstan," large-scale implementation of digital solutions is underway across various spheres of public life: e-government, digital healthcare, financial services, and education. Thus, digital technologies have introduced a new level of complexity to criminal activity. The system of law enforcement agencies and judicial institutions is not always ready to respond to digital threats (Yerkenov, 2024; Zhakenov et al., 2024).

Modern criminals are increasingly using the latest digital tools to commit crimes. The study by Stratton et al. (2017) analysed the formulation of the distinct concept of "digital criminology" as a specific scientific field that studies criminal behaviour in the context of rapid digitalisation. Nikkel (2020) also demonstrated similar dynamics, examining existing mechanisms for the abuse of the latest financial technologies (FinTech) by criminals and identifying important innovations in approaches to digital forensics. This topic is also relevant to Nosál's (2023) research, which examined the impact of artificial intelligence, blockchain technologies, and autonomous systems on the emergence of new forms of organized crime. Asli (2023) highlighted the importance of new types of digital crimes, demonstrating the evolution of criminology in the 21st century.

Institutional and legal systems do not always keep pace with technological developments, which creates significant challenges for investigating cybercrime. The study by Jilkishiyev and Begaliyev (2024) outlines key problems in investigating IT crimes in Kazakhstan, including a lack of technical training for personnel, inconsistencies in the regulatory framework, and insufficient integration of international experience. Kambarov et al. (2024) focused on preventive measures to reduce crimes in the field of informatization. The issue of legal regulation in the digital sphere is also highlighted in the study by Alzhankulova et al. (2022), which emphasizes certain legal drawbacks in the protection of copyright and related rights in the Republic of Kazakhstan. On the other hand, Ibrayeva et al. (2025), building on this issue, examined the impact of social networks on judicial practice, focusing on publicity, emotional interaction, and changes in legal processes. Grabosky et al. (2018) provided a broad overview of changes in crime and crime control strategies in the digital age (based on an analysis of existing experiences in the EU, the US, and Asia). Lasagni's (2023) study, which investigated the digitization of criminal proceedings in Italy, is also important. In particular, the author highlighted the use of electronic evidence and dedicated digital platforms for organizing judicial proceedings. Oderiy et al. (2024) highlighted the extent to which EU legal policy influences efforts to combat specific types of transnational crime, including cybercrime. When comparing the experiences of different countries, the research by Bissaliyev et al. (2025) is extremely important. They traced the use of different approaches in China, the EU, and Kazakhstan to protect personal data in the digital space, emphasizing the important role of AI in combating crime. Kyzylkhojaeva (2024) also made an important contribution by researching international organisations' positions on the role of AI in criminal justice and proposing specific areas for harmonising global approaches.

To go beyond the descriptive analysis of criminal groups' use of digital technologies in Kazakhstan, this study applies a theoretical framework grounded in cybercriminology and digital governance. These approaches make it possible to understand the role of technological transformations in the emergence of new criminal opportunities, as well as the criminal justice system's ability to respond to the challenges of the digital age. Cybercriminology is a branch of criminology that studies crimes in the digital environment (Sysoyev et al., 2020). In a digital sense, this theory helps to explain the impact of the growth of citizens' online activity, insufficient digital literacy, weak technical protection and the availability of malicious software on the spread of cybercrime in Kazakhstan (Khamit et al., 2024).

The analysis of the scientific sources has shown that, despite the growing number of publications on the use of digital technologies by criminals, the existing studies are predominantly descriptive, focus on individual technologies or individual countries, and do not offer a criterion-based comparison of Kazakhstan's cybercrime legislation with the Budapest Convention and with the legislation of states that have implemented it. Contradictions also remain in the assessment of institutional capacity: while some authors emphasize preventive and legislative measures (Kambarov et al., 2024; Yerkenov, 2024), others point to the persistent latency of cybercrime, the shortage of digital competencies and the low level of interagency cooperation (Jilkishiyev & Begaliyev, 2024; Khamit et al., 2024). These unresolved issues justify continuing research in this area and determining the specific direction of the present study.

Accordingly, the purpose of the study is to conduct a comparative legal analysis of the legislative and institutional system for combating cybercrime in the Republic of Kazakhstan against international standards to identify regulatory and institutional gaps and to justify a set of legal, institutional and technical measures aimed at strengthening the capacity of law enforcement agencies to combat organized crime using digital technologies. To achieve this purpose, the following research questions are formulated:

RQ1: How do Articles 272–274 of the Criminal Code of Kazakhstan regulate digitally-enabled organized crime, and what legal gaps can be identified in comparison with the legislative framework of Poland, Turkey and Estonia and the provisions of the Budapest Convention on Cybercrime?

RQ2: What institutional barriers (including limited digital forensic capacity, inter-agency fragmentation, and low reporting rates) hinder the effective enforcement of cybercrime legislation in Kazakhstan, and how are similar challenges addressed in Estonia?

RQ3: What specific legislative and institutional reforms are required to align the cybercrime framework of Kazakhstan with international standards, particularly the Budapest Convention on Cybercrime?

MATERIALS AND METHODS

The study is based on a normative and legal methodology, combined with comparative legal analysis, to examine the use of digital technologies by organized crime groups in Kazakhstan and the related challenges for the criminal justice system. The normative and legal methodology is based on an analysis of current legal norms, in particular Articles 272–274 of the Criminal Code, with respect to their internal consistency and compliance with international standards, primarily the Budapest Convention on Cybercrime.

The study relies on three main groups of sources. First, the national legislation of Kazakhstan was analyzed: the Criminal Code (Articles 272–274) (Republic of Kazakhstan, 2025) and the Criminal Procedure Code. Second, attention was paid to international legal acts, primarily the Budapest Convention on Cybercrime, as well as relevant European regulatory documents, particularly the EU Cybersecurity Act (European Parliament and Council of the European Union, 2019), and ENISA recommendations, which define cybersecurity standards, digital risk regulation, and international cooperation. Third, official reports and statistical materials of the Ministry of Internal Affairs of the Republic of Kazakhstan for 2020–2023 were used. The scientific basis consisted of peer-reviewed publications indexed in Scopus and Web of Science. For comparative analysis, the legislation of Estonia, Poland and Turkey was used.

The study used a structured comparative legal analysis based on eight criteria, which ensured the systematicity and comparability of the results: (1) the legal definition of cybercrime and the level of regulatory specification of acts related to the use of digital technologies; (2) the scope of provisions addressing organized cybercrime; (3) the regulation of cryptocurrencies; (4) digital forensics powers and the procedural rules on the collection and admissibility of electronic evidence; (5) cross-border cooperation mechanisms; (6) the penalty framework, including the proportionality and differentiation of sanctions; (7) the regulation of artificial intelligence and deepfake technologies; and (8) the status of implementation of the Budapest Convention. For each criterion, the level of compliance with the Budapest Convention was assessed on an ordinal scale (low/limited, partial/moderate, high/full). Applying the same criteria across jurisdictions ensured comparability of results and enabled identification of key regulatory and institutional gaps in the system for combating cybercrime. The strength of this design is that it combines doctrinal analysis of national norms with an explicit, replicable comparative matrix; its main weakness is its reliance on secondary sources and publicly available statistics, without access to closed case materials.

RESULTS

Given the rapid development of digital technologies, participants in information legal relations are increasingly encountering cybercriminals, posing a serious threat to them, as attackers can gain access to private information, personal data, and financial resources (Runciman, 2020). In view of this, countering such crimes is extremely difficult and requires a deep understanding of technologies, methods, and the specifics of the procedure for bringing perpetrators to justice. Information technology is defined as the means, methods, and technologies used to collect, process, store, transmit, and use information (UN System Chief Executives Board for Coordination, 2025) (see Table 1).

Table 1. The impact of digitalization on criminal activity

Technology	Applications	Legislative regulation	Case example
Using Cryptocurrencies (Bitcoin, Monero)	Money laundering, evasion of financial monitoring by the banking sector	Partly regulated by Articles 218, 262 of the Criminal Code of the Republic of Kazakhstan (money laundering, activities of organized criminal groups)	Trading via P2P exchanges without user verification
Darknet Possibilities	Illegal trafficking in drugs, weapons, pornographic materials, piracy of licensed content	Lack of a separate definition in the Criminal Code. There are only general norms on the circulation and the sale of drug substances.	Hosting web stores on the TOR network for the sale of drugs
Using VPN and TOR	Anonymization of digital traffic, evasion of detection of criminal activity	Partly Article 274 of the Criminal Code. VPN blocking is absent	Possibility of anonymous hacker attacks with IP hiding
Using Phishing and Social Engineering	Theft of bank data, access to social media accounts	Article 190 of the Criminal Code of the Republic of Kazakhstan (fraud); There are no specific articles on cyber fraud	Sending fake messages with phishing links, requests on behalf of the bank demanding to recall the PIN code

Sources: Shukan et al. (2025); Yerjanov et al. (2018)

The use of official reports from the Ministry of Internal Affairs of the Republic of Kazakhstan, the Financial Monitoring Agency, and analytics from the ITU and Interpol made it possible to identify dynamic changes in cybercrime (see Table 2 and Figure 1).

Table 2. Dynamics of cybercrime in the Republic of Kazakhstan

Year	Total N of cybercrimes	N with cryptocurrency	% of cases in court	N of convictions	Relapse
2020	2,130	110	34%	211	17
2021	3,564	391	28%	330	45
2022	5,120	922	27.7%	472	71

Source: UN System Chief Executives Board for Coordination (2025)

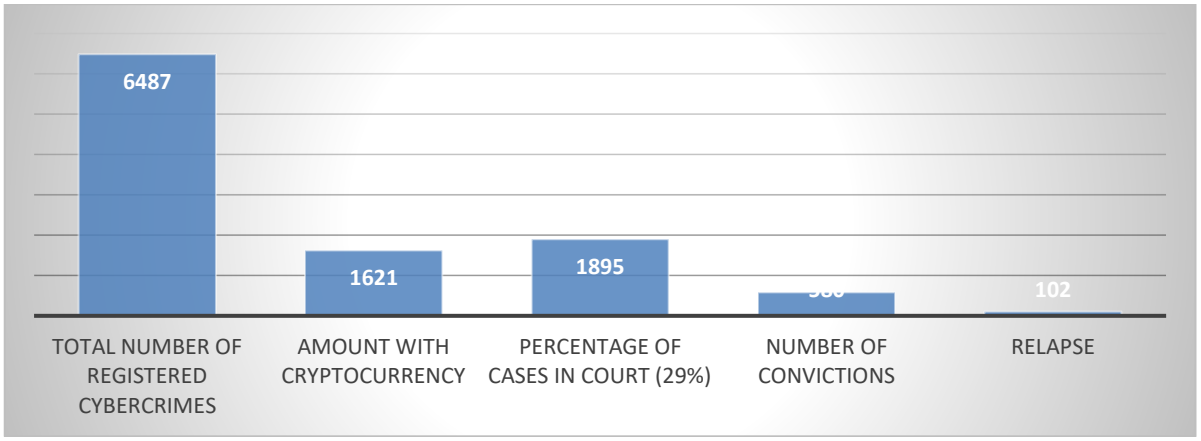

Figure 1. Dynamics of cybercrime in the Republic of Kazakhstan (2023)

In the context of investigating crimes in the field of information technology in the Republic of Kazakhstan, there are tangible problems. In particular, the problems identified from official reports and departmental audits are summarised in Table 3.

Table 3. Problems in legal counteraction to modern cybercrimes

Challenge	Description	Statistical or legal basis
Latency to cybercrime	Only 27% of incidents are officially recorded, as victims of cyber fraud rarely contact the police.	The data from the Ministry of Internal Affairs of the Republic of Kazakhstan for 2023
Lack of technical infrastructure	The lack of licensed software for decrypting or analyzing traffic, the use of outdated equipment	The budgets of the relevant structures provide funds only for the renewal of technical equipment, while funding for the purchase of the latest equipment is almost nonexistent.
Low level of acquired digital competencies	Only 18% of law enforcement officers have the appropriate level of training in digital forensics.	Internal audit of the Ministry of Internal Affairs, 2023
Difficulties of cooperation at the international level	The lack of established interaction at the level of foreign institutions during requests for legal assistance	The report of the Prosecutor General's Office of the Republic of Kazakhstan, 2022

The spread of digital assets, including cryptocurrencies and NFTs, which are not linked to any country's financial system, allows criminals to remain "in the shadows," inaccessible to state financial regulators. A comparative legal analysis of the current Criminal Code of the Republic of Kazakhstan, the Criminal Procedure Code of the Republic of Kazakhstan, and the Budapest Convention identified regulatory drawbacks. Thus, it is important to compare Kazakhstan's experience with that of other countries (See Table 4).

Table 4. Comparative legal analysis of cybercrime regulation

Comparison criterion	**Kazakhstan**	**Estonia**	**Poland**	**Turkey**	**Compliance with Budapest Convention**
Legal definition of cybercrime	Arts. 272–274 CC: general provisions on unauthorized access, malware, system interference; no unified definition	Penal Code: explicit criminalization of illegal access, data interference, system interference	Arts. 267–269b CC: detailed provisions on unlawful access, interference, and fraud	Arts. 243–245 TCC: regulates IT crimes but with limited differentiation	Partial (Kazakhstan), High (Estonia, Poland), Moderate (Turkey)
Scope of organized cybercrime provisions	No specific provisions addressing organized cyber groups in digital context	Organized crime provisions extend to cyber offences	Includes organized cyber fraud and group liability	General organized crime norms applied to cyber offences	Limited (Kazakhstan), Strong (Estonia, Poland), Moderate (Turkey)
Cryptocurrency regulation	No clear legal definition; indirect regulation via financial crime provisions	Recognized in AML frameworks; linked to cybercrime investigations	Regulated within financial and AML legislation	Limited regulation; partial recognition	Low (Kazakhstan, Turkey), High (Estonia, Poland)
Digital forensics powers	No detailed procedural rules for digital evidence (CPC gaps)	Clear procedures for collection and admissibility of digital evidence	Detailed procedural framework for digital evidence	Partial procedural regulation	Limited (Kazakhstan), High (Estonia, Poland), Moderate (Turkey)
Cross-border cooperation mechanisms	Weak institutional coordination; limited practice	Active participation in EU and international cooperation mechanisms	Strong cooperation within EU legal framework	Formal mechanisms exist but limited effectiveness	Low (Kazakhstan), High (Estonia, Poland), Moderate (Turkey)
Penalty framework	General sanctions; limited differentiation by severity or technology used	Differentiated penalties based on type of cyber offence	Proportional sanctions including aggravated forms	Moderate sanctions with limited differentiation	Partial (Kazakhstan), High (Estonia, Poland), Moderate (Turkey)
AI / Deepfake regulation	No legal definition or criminalization	Emerging regulation within digital governance framework	Limited but developing regulation	No specific regulation	Low (Kazakhstan, Turkey), Moderate (Estonia, Poland)
Status of the Budapest Convention	Not fully aligned; partial harmonization	Full implementation	Full implementation	Party with partial implementation	Partial (Kazakhstan, Turkey), Full (Estonia, Poland)

The comparative analysis showed that the regulation of cybercrime in Kazakhstan was less developed than in Estonia and Poland, particularly in terms of regulatory detail and consistency with the Budapest Convention on Cybercrime. First, Articles 272–274 of the Criminal Code of Kazakhstan established liability for basic cybercrimes but did not provide a comprehensive definition of cybercrime or differentiate offences by technological complexity. In contrast, the legislation of Estonia and Poland provided for detailed criminalization – such an approach was in line with international standards. Second, Kazakhstan's legislation did not account for the specifics of organized groups' activities in the digital environment. In contrast, in Poland and Estonia, the relevant norms had long been integrated into cybercrime regulation. These results answer RQ1, while the enforcement problems in Table 3 answer RQ2. A further gap concerns digital identity, which involves collecting digital data that identifies a person or organization in a digital environment. From a legal point of view, digital identity includes data that can be used to authenticate and confirm a person in legal relations. According to the Law of the Republic of Kazakhstan "On Electronic Document Management", digital identity is recognized as a means of electronic identification. This forms the basis for the legitimate conclusion of electronic contracts and the execution of legally significant actions.

Table 5. The drawbacks in the legislative framework of the Republic of Kazakhstan

Norm/concept	Problem	Comment
Cryptocurrency	The lack of a specific legal definition of such a concept in the Law "On Payment Systems and Transfers"	There is a need to use a separate provision of the Criminal Code to criminalize the financing of crime through cryptocurrencies.
Collection of digital evidence	The lack of a definition of a separate form, conditions of storage and acceptance for consideration.	The Criminal Procedure Code of the Republic of Kazakhstan contains only some general rules for collecting material evidence (Article 113)
Phishing	The lack of a separate element of the crime, limitation of the definition to general fraud	In some European countries (France, Germany) a separate criminalization has been introduced.
Digital identity (the collection of digital data that identifies a person or organization in a digital environment) **Deepfake (video or audio material created using artificial intelligence)**	The legislation does not define the signs of the use of AI, digital identity or deepfake (material created using artificial intelligence that faithfully imitates the voice or appearance of a specific person for	deception) The legislative framework does not control the risks of using AI systems for criminal purposes

All the above-mentioned drawbacks (Table 5) potentially contribute to the growth of the shadow economy, increased corruption and economic destabilization in Kazakhstan, and they define the areas in which legislative and institutional reform is required (RQ3).

DISCUSSIONS

The results of the study provide direct answers to the three research questions. Regarding RQ1, Articles 272–274 of the Criminal Code of Kazakhstan establish liability for basic cybercrimes but lack a unified definition of cybercrime, specific provisions on organized cyber groups and differentiated sanctions, which places Kazakhstan below Estonia and Poland and close to Turkey in terms of compliance with the Budapest Convention. Regarding RQ2, the main institutional barriers are the high latency in recording cybercrime incidents (only 27% of incidents recorded), the shortage of digital forensic capacity (18% of officers trained), fragmented interagency interaction, and weak international cooperation. About RQ3, the required reforms concern the conceptual framework of criminal legislation, the procedural regime for electronic evidence, the regulation of cryptocurrencies and AI-enabled offences, and the institutional capacity of law enforcement agencies. In particular, the results pointed to the widespread use of digital technologies by criminal groups, ranging from cryptocurrencies to artificial intelligence. This is consistent with findings from reports by Europol, the UN, and other organizations, which point to the active use of the darknet, VPNs, phishing, and cryptocurrencies (UN System Chief Executives Board for Coordination, 2025). Some documents also indicate that more than half of organized groups use digital technologies to coordinate their criminal activities (United Nations Office on Drugs and Crime, 2024). The problems identified in the reports of the Ministry of Internal Affairs of the Republic of Kazakhstan can also be confirmed in scientific literature (Ministry of Internal Affairs of the Republic of Kazakhstan, 2019). According to some studies, one of the weakest points in the fight against cybercrime in post-Soviet countries is the low level of interagency cooperation (Artemchuk et al., 2024; Kalguzhinova et al., 2023). These data coincide with the results of the study.

The results of the study confirmed that cryptocurrencies, the darknet, VPNs, phishing, and social engineering methods are actively used in Kazakhstan. This is fully consistent with literary sources and works that emphasise the decentralised nature of digital platforms as environments conducive to criminal activity. According to the Financial Monitoring Agency of the Republic of Kazakhstan, more than 400 suspicious virtual-asset transactions were recorded in 2022. Only a small number of suspicious cryptocurrency transactions are followed up with investigations or criminal proceedings. This means that most cybercrimes go unpunished (Kakeshov & Beishembek, 2022). A similar trend was found in studies by authors who emphasize that the detection rate of digital crimes in post-Soviet countries is low (Riepina et al., 2019; Smailov et al., 2021).

Despite the existence of the Information Security Incident Response Centre, most police and prosecution departments lack access to specialized digital tools. As the study showed, relying solely on basic analysis tools (MS Excel, Google Docs) to structure the evidence base indicates a lack of infrastructure for full-fledged digital forensics. Other researchers have also noted a lack of tools for applying OSINT/AI to automatically analyze digital traces (Alzhankulova et al., 2022). Comparative analysis with other countries, including the USA and Italy, indicates that effective counteraction to cybercrime is possible only with the availability of software complexes of Palantir, Maltego, GraphSense, and others, which are not available to Kazakhstani law enforcement agencies (Ramirez, 2022). This situation highlights the importance of aligning Kazakhstan's cybercrime policies with international frameworks such as the Budapest Convention on Cybercrime, which emphasises international cooperation, procedural law instruments, and harmonised definitions of cyber offences (Amanbayeva et al., 2022). Additionally, the EU Cybersecurity Act sets standards for cybersecurity capabilities and certification mechanisms that could serve as models for improving Kazakhstan's institutional and technical infrastructure in combating digital crimes. The lack of cryptanalysis experts or specialists in the collection of electronic evidence makes it impossible to effectively document criminal activity in the digital environment (Di Nicola, 2022; Kryvoshein, 2023). Against this backdrop, the fragmentation of institutional interaction also stands out. The lack of a single register of cyber incidents, fragmented databases, and limited interagency information sharing create a situation where one agency may be unaware of a crime that another is already investigating (Gaile et al., 2020). Criminal cases may lose their evidentiary basis due to untimely interagency communication. In EU countries, the EC3 network has been established under the auspices of Europol to address this issue and coordinate cyber investigations among member states. The lack of a definition of phishing and digital identity

contradicts the OECD recommendations, which highlight the need for adaptive criminal law (Fehr, 2019). Taken together, the comparison shows that the gaps identified in Kazakhstan are not unique to it but are characteristic of post-Soviet legal systems in which digital infrastructure has developed faster than criminal-law regulation; at the same time, the experience of Estonia and Poland demonstrates that full implementation of the Budapest Convention, combined with investment in forensic capacity and interagency coordination, produces measurably stronger institutions in line with SDG 16.

CONCLUSIONS

This study aimed to identify regulatory and institutional gaps in Kazakhstan's system for combating the use of digital technologies by organized criminal groups through a comparative legal analysis against the Budapest Convention on Cybercrime and the legislation of Estonia, Poland, and Turkey. It was found that the use of digital technologies by organised criminal groups poses a significant threat to Kazakhstan, and stable trends in the use of such tools were identified (cryptocurrencies, darknet capabilities, anonymisation technologies (VPN, TOR), phishing, social engineering, artificial intelligence technologies and deepfakes). Registered cybercrimes increased 2.4-fold between 2020 and 2022, while the share of cases reaching court declined.

The main problems in combating modern cybercrime were associated with high latency, insufficient technical support, low levels of digital competencies among law enforcement agencies, fragmentation of the institutional system, and limited international cooperation. The study's unique contribution is a criterion-based comparative matrix that positions Kazakhstan's legislation against the Budapest Convention and against jurisdictions with varying degrees of implementation, thereby extending the cybercriminology and digital governance literature to a post-Soviet context. The practical significance of the study lies in a comprehensive analysis of current cybercrime challenges in Kazakhstan and the justification of strategies for overcoming them.

On this basis, the following recommendations are proposed. Legal recommendations: a universal, detailed conceptual framework should be established in criminal legislation to classify crimes related to the use of digital technologies clearly, and a separate law on the regulation of cryptocurrencies and the combating of cybercrime should be enacted to meet the modern challenges of the digital economy. Institutional recommendations: specialized units should be established within law enforcement agencies to investigate information technology crimes, and law enforcement officers' skills should be enhanced through systematic training and retraining that address the latest digital threats. Technical recommendations: investments in cybersecurity should be increased to strengthen technical support for law enforcement agencies. These measures are directly aimed at strengthening institutional capacity and therefore contribute to Sustainable Development Goal 16 – ensuring peace and justice and building effective, accountable and resilient institutions – and to the secure development of digital infrastructure under SDG 9.

The study has certain limitations. Only secondary sources were used, and there was no access to closed statistical materials or case files; the ability to verify the effectiveness of specific measures taken by law enforcement agencies was therefore limited. The study also focuses mainly on Kazakhstan, so no broader regional analysis has been conducted. Future research should assess the effectiveness of legislative changes in combating cybercrime, extend the comparative analysis to other Central Asian and post-Soviet jurisdictions, and empirically examine, using primary data, how digital forensic capacity and interagency coordination affect the detection and prosecution of digitally enabled organized crime.

Author Contributions: Conceptualisation, T.A. and S.M.; Methodology, S.M. and N.A.; Software, N/A; Validation, N.A., A.Y. and S.B.; Formal Analysis, A.Y.; Investigation, Sh.M. and S.B.; Resources, S.B.; Data Curation, N.A.; Writing – Original Draft Preparation, S.M.; Writing – Review & Editing, T.A. and A.Y.; Visualization, N.A.; Supervision, T.A.; Project Administration, T.A.; Funding Acquisition, N/A. Authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study because the research does not involve vulnerable groups or sensitive issues.

Funding: The authors received no direct funding for this research.

Acknowledgements: The authors have no acknowledgements to declare.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to restrictions.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process: During the preparation of this work, the author(s) used Grammarly for proofreading and spell checking since the Authors are not native speakers. All intellectual content, analysis, and interpretations were produced solely by the authors. After using this AI tool/service, the author(s) reviewed and edited the content as needed, taking full responsibility for the publication's content.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

Alzhankulova, S., Abdualipova, K., & Myrzakhanova, S. (2022). Some problematic issues of legal regulation of copyright and related rights in the Republic of Kazakhstan. *The Scientific Heritage*, (90), 36–40. https://doi.org/10.5281/zenodo.6616140

Amanbayeva, A. G., Khan, V. V., Yensebayeva, A. R., Karatayev, T. Z., & Kussainova, L. K. (2022). Investigative Activity in the Investigation of Crimes against the Sexual Integrity of Minors. *Medicine and Law*, 41(3), 333–350.

Artemchuk, M., Marukhlenko, O., Sokrovolska, N., Mazur, H., & Riznyk, D. (2024). The impact of an economic recession on the financial support of state functions during crises. *Theoretical and Practical Research in Economic Fields*, 15(2), 350. https://doi.org/10.14505/tpref.v15.2(30).15

Asli, M. R. (2023). Digital trends of criminology and criminal justice of the 21st century. *Journal of Digital Technologies and Law*, 1(1), 235–250. https://doi.org/10.21202/jdtl.2023.9

Bissaliyev, M. S., Susi, M., & Shakirov, K. (2025). Convergence between and among the Chinese, the EU and Kazakhstan approaches towards personal data protection against the AI in the digital sphere. *Chinese Journal of International Law*, 24(2), jmaf011. https://doi.org/10.1093/chinesejil/jmaf011

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

European Parliament and Council of the European Union (2019). Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

Fehr, C. (2019). Criminal law and digital technologies: An institutional approach to rule creation in a rapidly advancing and complex setting. *McGill Law Journal*, 65(1), 67. https://doi.org/10.7202/1074418ar

Gaile, D., Tumalavičius, V., Skrastiņa, U., & Načiščionis, J. (2020). Modern economics in the context of security: Efficient use of funds and reduction of risks as one of the aims of public procurement. *Entrepreneurship and Sustainability Issues*, 8(1), 49–59. https://doi.org/10.9770/jesi.2020.8.1(4)

Grabosky, P. N., Smith, R. G., & Wright, P. (2018). Introduction. *Crime in the Digital Age* (pp. 1–18). Routledge. https://doi.org/10.4324/9780203794401-1

Ibrayeva, G., Tleugazina, D., & Ramazan, A. (2025). Social networks as a driving force for legal change: Emotional interaction and the impact of court broadcasts in Kazakhstan. *Lecture Notes in Computer Science* (pp. 257–271). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-93536-7_18

Jilkishiyev, R., & Begaliyev, Y. (2024). Problems of investigation of crimes in the field of information technology. *Pakistan Journal of Criminology*, 16(3), 97–114. https://doi.org/10.62271/pjc.16.3.97.114

Kakeshov, B. D., & Beishembek, A. K. (2022). Criminal policy, law enforcement practice and digitalization as tools for corruption prevention in judicial authorities. *European and Asian Law Review*, 5(3), 22–27. https://doi.org/10.34076/27821668_2022_5_3_22

Kalguzhinova, A., Mashabaev, A., & Ozbekov, D. (2023). Some issues in countering criminal offences in the field of informatization and communications in the Republic of Kazakhstan. *Bulletin of Science and Practice*, (8), 154–161. https://doi.org/10.33619/2414-2948/93/16

Kambarov, A., Karazhanov, M., Sabitov, S., Baigundinov, Y., & Temirgazin, R. (2024). Measures to prevent criminal offences in the field of informatization and communications in the Republic of Kazakhstan. *Law, State and Telecommunications Review*, 16(2), 276–294. https://doi.org/10.26512/lstr.v16i2.50807

Khamit, E., Mukhamadieva, G., Togaibaeva, S., Mashabayev, A., Salykova, A., & Karakushev, S. (2024). Criminological characterization of internet fraud: Experience of the Republic of Kazakhstan. *Pakistan Journal of Criminology*, 16(4), 809–822. https://doi.org/10.62271/pjc.16.4.809.822

Kryvoshein, V. (2023). Transformation of political perceptions in the age of information technologies: Analyzing the impact on political beliefs. *Futurity of Social Sciences*, 1(3), 20–32. https://doi.org/10.57125/fs.2023.09.20.02

Kyzylkhojaeva, A. (2024). Analysis of criminal justice and cyber crime in the context of artificial intelligence through the lenses of international organizations. *Alatoo Academic Studies*, 24(2), 349–361. https://doi.org/10.17015/aas.2024.242.28

Lasagni, G. (2023). The impact of digital technology on Italian criminal proceedings. *Zeitschrift für die gesamte Strafrechtswissenschaft*, 135(3), 598–619. https://hdl.handle.net/11585/964022

Ministry of Internal Affairs of the Republic of Kazakhstan (2019). Order No. 431 of 16 May 2019 on introducing amendments and additions to Order No. 995 of the Minister of Internal Affairs of the Republic of Kazakhstan dated 5 December 2015 'On approval of the model regulation on advisory consultative bodies under territorial internal affairs bodies'. *Official Legal Portal of Kazakhstan*. https://adilet.zan.kz/rus/docs/V1900018695

National Cyber Security Index (2025). Kazakhstan: Index. https://ncsi.ega.ee/country/kz/

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

Nosál, J. (2023). Crime in the digital age: A new frontier. *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 177–193). Springer International Publishing. https://doi.org/10.1007/978-3-031-24673-9_11

Oderiy, O., Orobets, K., Brynzanska, O., Veklych, V., & Shpiliarevych, V. (2024). The impact of EU criminal law policy on the prevention of transnational environmental crime. *Pakistan Journal of Criminology*, 16(3), 1155–1172. https://doi.org/10.62271/pjc.16.3.1155.1172

Ramirez, F. (2022). The digital divide in the US criminal justice system. *New Media & Society*, 24(2), 514–529. https://doi.org/10.1177/14614448211063190

Riepina, I., Hrybinenko, O., Parieva, N., Parieva, O., Savenko, I., & Durbalova, N. (2019). Quantity assessment of the risk of investment projects. *International Journal of Recent Technology and Engineering*, 8(3), 7256–7260. https://doi.org/10.35940/ijrte.C6338.098319

Republic of Kazakhstan (2025). The Criminal Code of the Republic of Kazakhstan: Law of the Republic of Kazakhstan No. 167. https://www.warnathgroup.com/wp-content/uploads/2015/03/Kazakhstan-Criminal-Code.pdf

Runciman, B. (2020). Cybersecurity report 2020. *ITNOW*, 62(4), 28–29. https://doi.org/10.1093/itnow/bwaa103

Shukan, A., Erdogan, Y., & Karzhasova, G. (2025). The experience of the Republic of Turkey in combating cybercrime and issues of preventing criminal offenses in the field of information technologies. *Bulletin of the Karaganda University. Law Series*, 30(1), 80–86. https://doi.org/10.31489/2025l1/80-86

Smailov, N., Batyrgaliyev, A., Akhmediyarova, A., Seilova, N., Koshkinbayeva, M., Baigulbayeva, M., Romaniuk, R., Orunbekov, M., Assem, K., & Kotyra, A. (2021). Approaches to evaluating the quality of masking noise

interference. *International Journal of Electronics and Telecommunications*, 67(1), 59–64. https://doi.org/10.24425/ijet.2021.135944

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: Towards a 'digital criminology'? *International Journal for Crime, Justice and Social Democracy*, 6(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

Sysoyev, A. K., Umetov, A. U., Lakbayev, K. S., & Rysmagambetova, G. M. (2020). The crimes in the field of high technology: Concept, problems and methods of counteraction in Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, 12(4), 412. https://doi.org/10.1504/ijesdf.2020.10030688

UN System Chief Executives Board for Coordination (2025). Session report. https://unsceb.org/session-report-422

United Nations Office on Drugs and Crime (2024). Countering cybercrime. https://www.unodc.org/unodc/urban-safety/countering-cybercrime.html

Yerjanov, T. K., Baimagambetova, Z. M., Seralieva, A. M., Zhailau, Z., & Sairambaeva, Z. T. (2018). Legal issues related to combating cybercrime: Experience of the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics*, 8(7), 2286.

Yerkenov, B. (2024). Legal instruments of combating legalization (laundering) of proceeds of crime in conditions of digital evolution of the Republic of Kazakhstan. *Journal of Actual Problems of Jurisprudence*, 111(3), 119–128. https://doi.org/10.26577/japj2024-111-i3-013

Zhakenov, K., Kultemirova, L., & Ibraeva, A. (2024). Comparative analysis of the activities of authorities to ensure the prevention of offenses in the Republic of Kazakhstan and other world countries. *Security Journal*, 37(4), 1430–1446. https://doi.org/10.1057/s41284-024-00425-5

Publisher's Note: CRIBFB stays neutral about jurisdictional claims in published maps and institutional affiliations.