TRANSFORMATION OF PRE-TRIAL PROCEEDINGS MECHANISMS FOR CRIMES IN CYBERSPACE: THE EXPERIENCE OF POST-SOVIET STATES

DOI: 10.63407/738883

AYNURA SABYRBAEVA
Assoc.Prof.(Dr.), Department of Criminal Procedure Law Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract *The rapid digitalization of social relations and the globalization of the information environment across post-Soviet states have led to a qualitative transformation in transnational crime. Given the volatility and specific nature of digital traces, traditional convention-based mechanisms for international mutual legal assistance (specifically, the 1993 Minsk Convention and the 2002 Chisinau Convention) have exhausted their procedural efficacy. The execution time for requests, reaching up to twenty-one months in certain instances, effectively negates the possibility of prompt cybercrime investigations and holding perpetrators accountable. In this regard, the present article aims to conduct a comprehensive comparative legal analysis of pre-trial proceedings for crimes committed in cyberspace, focusing on the Russian Federation, the Republic of Belarus, the Republic of Kazakhstan, the Kyrgyz Republic, the Republic of Armenia, and Georgia.*

The research identifies and systematizes the most effective procedural tools introduced into the national legal systems of the examined countries. Particular attention is given to the experience of the Republic of Kazakhstan regarding its full-scale transition to an electronic criminal justice format, ensuring investigation transparency and minimizing the risk of evidence falsification. The study analyzes progressive norms within the criminal procedural legislation of the Russian Federation that regulate the procedure for seizing and copying digital information without the mandatory confiscation of physical devices (Article 164.1 of the Criminal Procedure Code of the Russian Federation). The advanced experience of the Republic of Belarus is examined, specifically the establishment of strict criminal liability for so-called «money mules» (drops)—individuals providing their financial details to launder criminal proceeds—as well as the operation of automated interbank control systems.Considerable scientific interest lies in the analysis of Georgian and Kyrgyz legislation regarding the legalization of special investigative actions in the cyber environment, including internet traffic monitoring, real-time surveillance of bank accounts, and the direct requisition of computer data from foreign jurisdictions, bypassing lengthy diplomatic procedures.Based on the conducted analysis, the author concludes that a conceptual modernization of pre-trial proceedings in CIS countries is necessary. The article substantiates the thesis that effective countermeasures against cybercrime require the harmonization of national legislations, the implementation of the electronic criminal case framework, the procedural legalization of cyber-search operations as full-fledged investigative actions, and the creation of a unified regional interagency platform for the secure and instant exchange of digital evidence. Implementing the reviewed foreign experience will help build a robust architecture for law enforcement cooperation and ensure the protection of states' sovereign interests in the digital world.

Keywords: *cybercrime, pre-trial proceedings, digital evidence, special investigative actions, international cooperation, comparative legal analysis, legal assistance, electronic criminal case, transnational crime, harmonization of legislation.*

Literature Review

The rapid digitalization of social relations across the post-Soviet space has naturally led to a transformation of criminal threats. Today, cybercrime exhibits a pronounced transnational character, necessitating an adequate and timely response from law enforcement systems. The scale of the problem is clearly illustrated by statistical data. «According to Searchinform data from 2020, 58% of surveyed respondents (companies) in the CIS countries faced information leaks, while in the Russian Federation, this figure was 55%» . According to an analytical report by F.A.C.C.T., «state-sponsored hacker groups most frequently attacked Russia (28 attacks) and Azerbaijan (6 attacks), as well as the Republic of Belarus, Kyrgyzstan, and Kazakhstan (4 attacks each). Their primary targets included government agencies, organizations linked to critical infrastructure, military institutions, and defense industry enterprises. In 2023, approximately 300 log clouds (Underground Clouds of Logs, UCL) were discovered, serving as conduits for streams of stolen data. A fivefold increase (from 496 to 2,300) was recorded in unique hosts where an account from at least one major bank in Russia and the CIS was compromised using a stealer. The source of these records was data derived from UCLs. In 2023, over 29,000 phishing domains were detected across Russia and the CIS, compared to only about 20,000 domains identified the previous year. The share of fraudulent resources hosted on Russian servers decreased from 73% to 41%» .

These figures highlight the urgent need to establish close cooperation among CIS countries to counter cybercrime through the adoption of joint international treaties and agreements. Historically, attempts to unify the legal framework have been undertaken since the early years of the Commonwealth's existence. The issue of countering cybercrime has been actively explored by leading legal scholars across various stages of integration. On February 17, 1996, during the VII plenary session of the Interparliamentary Assembly, the CIS Model Criminal Code was adopted, establishing regulations for computer-related crimes». Article 287 of the CIS Criminal Code lays the foundation

for correctly distinguishing between computer crimes and other related offenses, which also warrants a positive assessment» .

At the same time, the regulation of related domains remained fragmented for a prolonged period. «The CIS Model Law 'On Combating Terrorism' includes a chapter titled 'Information and Propaganda Support for Combating Terrorism.' However, it fails to address either the use of information technologies in suppressing cyberterrorism or their development». As accurately noted by E. V. Nikulchenkova, «legislation fails to keep pace with the rapid development of information technologies» .

It is noteworthy that «on June 1, 2001, the Agreement on Cooperation of the CIS Member States in Combating Crimes in the Sphere of Computer Information was concluded in Minsk» . According to P.N. Kobets, «among the shortcomings of this agreement is the narrowness of its regulatory scope, as illegal acts in the sphere of computer information serve as merely one structural element of cybercrime». Therefore, it is imperative to expand international cooperation by introducing innovative methods of information exchange and ensuring rapid, real-time responses to cybercrimes. However, such cooperation can only be effective if there is a high level of «trust» between the respective states.

Methodology and Scope of the Research

The methodological basis of the study was formed by a comprehensive approach based on general scientific methods (dialectics, systemic analysis, synthesis) and specific scientific methods of cognition. The leading method applied was the comparative legal method, which allowed for a detailed comparison of the norms of criminal and criminal procedural legislation of the Russian Federation, the Republic of Belarus, the Republic of Kazakhstan, the Kyrgyz Republic, the Republic of Armenia, and Georgia. The empirical and theoretical foundation (scope of the research) comprised international conventions, CIS model legislative acts, national codes, as well as statistical datasets and analytical reports from specialized organizations (F.A.C.C.T., Searchinform, NCSI) for the period from 2016 to 2024.

Main Research Hypothesis

The research hypothesis posits that traditional convention-based mechanisms for providing international mutual legal assistance have exhausted their procedural efficacy in the context of transnational digital crime. To ensure effective pre-trial proceedings, a conceptual departure from outdated diplomatic procedures is required in favor of creating a unified interagency platform for the rapid exchange of electronic evidence, alongside the integration of innovative mechanisms into national criminal procedure codes (such as the electronic criminal case format and special cyber-investigative actions).

Main Analysis

«Given the steady growth of crimes in this sphere across the territory of the CIS member states, there is an observable intensification in the interaction of CIS law enforcement agencies across several directions. Thus, the Concept of Cooperation of the CIS Member States in the Field of Information Security dated October 10, 2008; the Concept of Cooperation of the CIS Member States in Combating Crimes Committed Using Information Technologies dated October 25, 2013; and the Agreement on Cooperation of the CIS Member States in Combating Crimes in the Sphere of Information Technology dated September 28, 2018, have been approved and are actively being implemented» .

Alongside the regulatory framework, institutional and practical interaction is strengthening. «In 2014, the CSTO Advisory and Coordinating Center for Responding to Computer Incidents was established on the basis of the CSTO». For instance, in May 2016, law enforcement agencies from the Republic of Belarus, the Russian Federation, the Republic of Kazakhstan, the Kyrgyz Republic, and the Republic of Armenia, with the support of the CIS Anti-Terrorism Center, conducted joint anti-terrorism exercises named «Cyber-Antiterror-2016», one of the objectives of which was to identify and suppress cyberterrorism.

Despite the development of this partnership, the critically low speed of exchanging the evidentiary base remains the central problem of pre-trial proceedings. Furthermore, the «Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters» was signed between the CIS countries in Minsk in 1993, and a similar convention was adopted in Chisinau in 2002. However, considering the capabilities of cybercriminals to commit

offenses remotely and the shifting trends, these Conventions do not fully meet contemporary requirements, as countering cybercrime, along with the discovery and seizure of digital evidence, demands, first and foremost, promptness (a request takes an average of 3-4 months to be executed, if it is executed at all). For example, at the 74th session of the UN General Assembly, the Czech Republic noted that the average processing time for an international cybercrime request took 21 months (Myanmar and Portugal also highlighted this issue). Therefore, it is imperative to establish a unified platform within the CIS space for information exchange and the rapid, prompt provision of legal assistance in combating cybercrime.

The Experience of the Russian Federation

As highlighted by V.V. Kharin and T.V. Plotnikova, «Regarding the Criminal Code of the Russian Federation, it should be emphasized that cybercrimes are categorized into a distinct chapter—Chapter 28, "Crimes in the Sphere of Computer Information" we may qualify cyber-related offenses under conventional articles, such as libel (Article 128.1); violation of the privacy of correspondence, telephone conversations, postal, telegraphic, or other communications (Article 138); infringement of copyright and related rights (Article 146); and the unlawful acquisition or disclosure of information constituting commercial, tax, or banking secrets (Article 183)» . Furthermore, the Criminal Code of the Russian Federation contains specialized constituent elements of crimes, such as fraud in the sphere of computer information (Article 159.6) and fraud involving electronic payment instruments (Article 159.3). Nonetheless, some scholars have observed that «there is a persistent necessity for the thorough refinement of national legislation and international instruments providing for liability for the commission of cybercrimes» .

In addition, during a session of the Prosecutors General of the SCO member states, Prosecutor General Igor Krasnov noted that «legislative drafts have been prepared to clarify the constituent elements of crimes committed using specialized technical means (phishing, social engineering, cyber-extortion, and DDoS attacks) and to heighten the associated penalties, while also ensuring the preservation of electronic evidence for crimes in the sphere of information and telecommunications technologies, including those initiated at the request of foreign competent authorities» . Although the draft is currently undergoing refinement, the

introduction of these amendments may facilitate the improvement of the criminogenic situation and bolster international legal cooperation.

In contrast to our national legislation, the Criminal Procedure Code of the Russian Federation (CPC RF) establishes a procedure for the seizure of electronic media and the copying of information from them during investigative actions (Article 164.1), which provides the legal capability not only to seize but also to copy the data. Previously, during a search or seizure, particularly within large commercial organizations, an investigator would inspect, seal, and confiscate the physical device, subsequently recognizing it as material evidence and depositing it in an evidence storage facility. Naturally, this significantly disrupted the operational activities of individuals using the device (e.g., computers, laptops) for professional purposes, as there was no established procedure for merely extracting the resident information for subsequent forensic examination.

Furthermore, logistical issues regarding the transportation of these devices, servers, and related hardware had to be addressed. However, with the enactment of Federal Law No. 533-FZ dated December 27, 2018, Article 164.1 was incorporated into the CPC RF, strictly regulating the possibility of extracting and copying only the necessary information .

Nevertheless, despite these legislative amendments, «At the end of 2023 in the Russian Federation, 50.6% of cybercrimes were classified as grave and particularly grave categories (342.6 thousand; +25.9%), more than three-quarters (77.8%) were committed using the Internet (526.8 thousand; +38.2%), and nearly half (44.7%) involved the use of mobile communications (302.9 thousand; +42.2%).

According to the Main Information and Analytical Center of the Ministry of Internal Affairs of the Russian Federation (GIAC MVD RF), the vast majority of such crimes (70.2%) are committed through theft or fraud (475.3 thousand; +28.1%), while one in eight (12.0%) is committed for the purpose of illicit production, sale, or distribution of narcotic drugs (81.5 thousand; +31.0%).

In 2023, 677 thousand crimes committed using information and telecommunication technologies and in the sphere of computer information were registered in the RF, representing a 29.7% increase compared to the same period of the previous year» .

A primary catalyst for this trend in the RF, as well as in other CIS countries, is the activity of so-called «drops» (money mules), yet there is currently no specific criminal liability for providing bank cards to third parties, although «according to Sberbank statistics, approximately 500,000 individuals in Russia were identified in 2023 as having provided their accounts to third parties» .

In response, the Ministry of Internal Affairs of the Russian Federation has submitted a legislative draft to supplement the Criminal Code of the Russian Federation with Article 187.1, which establishes criminal liability for the «transfer, acquisition, or use of an electronic payment instrument or the provision of access to it, except in cases where actions performed with the electronic payment instrument are carried out in the legitimate interests of the holder of the said electronic payment instrument» .

A pivotal measure in countering cybercrime was the adoption of Federal Law No. 369-FZ «On Amendments to the Federal Law «On the National Payment System» dated July 24, 2023, which entered into force on June 25, 2024. This Law mandates banks to suspend all suspicious transfers for a period of two days based on information contained within the Bank of Russia's database (concerning instances and attempts of fraudulent operations).

In the event of non-compliance with this requirement, resulting in the facilitation of a fraudulent transfer, banking and other financial institutions are obligated to compensate the victims for their losses within one month out of their own corporate funds. Such sanctioning measures directed at the institutions themselves will optimize their operational protocols, compelling them to scrutinize every transaction more rigorously to mitigate their own financial liability.

On the exact day this Law entered into force, 30,000 suspicious operations were frozen, indicating that a significant portion of fraudulent transactions was successfully intercepted.

Furthermore, to counter cybercrime in Russia, forces and resources are being optimized. Thus, «a special detachment of cyber troops has been established in Russia. Officially, they are referred to as information operations troops, and they function within the framework of the Ministry of Defense of the Russian Federation» . In 2020, an Interdepartmental Working Group on Information Crime was established , comprising officials from the Prosecutor General's Office, the Ministry of Internal Affairs, the

Ministry of Foreign Affairs, the Federal Security Service, the Investigative Committee, and the Ministry of Justice. It is also worth noting that the Prosecutor General's Office of the Russian Federation engages in the extrajudicial blocking of Internet resources containing destructive information.

In 2017, the Russian Federation put forward an initiative to create a unified Convention under the auspices of the UN. In 2024, the first-ever Draft United Nations Convention against Cybercrime «Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes» was adopted.

In 2022, the Directorate for Organizing the Combating of the Unlawful Use of Information and Communication Technologies (UBK) was established within the Ministry of Internal Affairs (MIA)) . However, prior to this, the MIA of Russia already housed Directorate «K», whose history traces back to the USSR era when it was designated as Directorate «R» rather than «K», presumably because its primary mandate involved solving operational tasks by eliminating radio interference during unauthorized access to the information networks of the USSR. Nevertheless, the personnel of this directorate acquired the legal status of officers conducting operational-search activities only in 1997, following the introduction of a chapter dedicated to crimes in the sphere of computer information into the Criminal Code of the Russian Federation.

Moreover, in the same year, «Departments for combating crimes in the sphere of computer information and economics were established in the constituent entities of the federation. The Departments for Combating Economic Crimes (OBEP) were endowed with the powers of an agency of inquiry and collaborated closely with Directorate «K». Alongside this, in 1998, the Volgograd Academy of the MIA of Russia graduated its first specialists in the investigation of crimes in the sphere of computer information» . Furthermore, law enforcement agencies collaborate with private entities, such as Kaspersky Lab.

Additionally, specialized network security schools have been established to train relevant specialists in countering cybercrime.

According to V.A. Mikhailyuk, «the task of developing a cyber police force remains highly relevant, driven by the legal relations

emerging at the present stage and answering the needs of the information society» . «The Russian law enforcement system is experiencing a personnel shortage, particularly regarding highly qualified IT specialists, whose core objective should be combating cybercrime on behalf of the state authority» . Other scholars have also written on this subject .

The Experience of the Republic of Belarus

The Republic of Belarus is recognized as one of the leading nations within the post-Soviet space regarding the implementation of effective countermeasures against cybercrime. It distinguishes itself as the inaugural state to introduce legislative liability for «money mules» (commonly referred to as «drops»)—individuals who provide their personal data, bank cards, or authentication credentials to criminal entities for the subsequent concealment of illicit activities. Under Article 202 of the Criminal Code of Belarus, the illegal circulation of payment instruments and tools carries a potential penalty of up to ten years of imprisonment .

Section XII, Chapter 31 («Crimes against computer security») of the Criminal Code of the Republic of Belarus encompasses five distinct articles. A defining characteristic of the Belarusian legal framework, which differentiates it from the criminal legislation of many other jurisdictions, is that cyber-related offenses are not merely prosecuted under the aggravating factors of «traditional» norms (such as conventional fraud or theft). Instead, the legislature has established a specialized provision—Article 212, «Theft through the use of computer technology». This article comprehensively covers all offenses associated with the misappropriation of property, including digital variants of theft, fraud, and extortion.

The institutional framework for combating cyber-related offenses includes the Investigative Committee and the criminal police’s specialized units, such as the Main Directorate for Combating Cybercrime (Directorate «K»). Statistical indicators reflect the growing scale of the challenge: approximately 15.7 thousand such incidents were recorded since the beginning of 2023, representing an increase from the 14.8 thousand cases documented during the corresponding period in 2022 .

According to Dmitry Gora, Chairman of the Investigative Committee, crimes registered on online trading platforms saw a significant reduction in 2023, decreasing from 4,000 to 1,000

cases. This achievement is attributed to robust prevention strategies and interagency cooperation involving the Ministry of Internal Affairs, the Operations and Analysis Center (OAC), and other regulatory bodies . Furthermore, at the initiative of Directorate «K» the Academy of the Ministry of Internal Affairs of the Republic of Belarus has integrated a specialized curriculum focused on «Countering Cybercrime and Computer Intelligence».

In 2023, the regulatory framework was further strengthened by the decree «On Measures to Counteract Unauthorized Payment Operations». This instrument mandates that the National Bank organize structured information interaction between law enforcement agencies and payment service providers to exchange data on unauthorized transactions and attempted breaches. The processing, storage, and transfer of incident-related information are conducted via the National Bank's Automated Incident Processing System (ASOI), ensuring strict adherence to information security and data protection protocols . Most recently, on September 17, 2024, Decree No. 367 «On the Circulation of Digital Signs (Tokens)» was enacted, specifically aimed at suppressing the exploitation of crypto-assets in the commission of cybercrimes .

The Experience of the Republic of Kazakhstan

The Criminal Code of the Republic of Kazakhstan regulates the issue of criminal liability for cybercrimes within Chapter XII, «Criminal Offenses in the Sphere of Informatization and Communications» as well as by establishing qualifying elements for certain traditional types of crimes. Examples include fraud committed through deceit or the abuse of trust of an information system user (Paragraph 4, Part 2, Article 190) and theft committed through unlawful access to an information system or the alteration of information transmitted over telecommunication networks (Paragraph 4, Part 2, Article 188).

The «Concept of Legal Policy of the Republic of Kazakhstan until 2030» approved by the Decree of the President of the Republic of Kazakhstan No. 674 dated October 15, 2021, emphasizes the necessity of modernizing criminal legislation and utilizing innovative technologies to combat emerging types of crimes, including cybercrimes.

As noted by R.E. Dzhansarayeva and K. Aratuly, «In Kazakhstan, the work on identifying, suppressing, and solving cybercrimes, as

well as crimes committed using high technologies, is carried out by Directorate «K», established within the structure of the Ministry of Internal Affairs in 2003. Furthermore, for the systemic combating of cybercrimes, a National Contact Point for Combating Crimes in the Sphere of Information Technologies was established in 2006, which conducts continuous information exchange with CIS countries and states further abroad» .

It is noteworthy that the National Security Committee of Kazakhstan incorporates an Information and Cybersecurity Service, within the structure of which specialized groups have been formed to counter specific types of computer-related crimes . In 2022, an institutional cybersecurity center was established in Kazakhstan. In the same year, the «CyberPol» project and a system for identifying international calls to landline telephones were launched to combat internet fraud.

Additionally, a Center for Combating Cybercrime operates within the Criminal Police Department of the Ministry of Internal Affairs. The head of this Center, Zh. Suyinbay , noted that to combat cybercrimes in Kazakhstan, «the database of anti-fraud systems of cellular operators was integrated, which made it possible to block approximately 36 million calls».

According to statistical data, the proportion of cybercrimes within the total volume of crimes in Kazakhstan has increased 73-fold since 2016. While it accounted for 0.24% in 2016, by 2023, it had reached 17.5% . The heightened threat of internet fraud is also evidenced by statistical data, according to which «during the period from 2018 to 2021, 364 criminal offenses in the sphere of informatization and communications, along with 43,911 internet frauds, were committed in the Republic of Kazakhstan» .

A comparative legal analysis of cybercrime trends for the years 2016–2023, conducted by K.O. Karabekov , is presented in the following table.

Показатель	Год							
	2016	2017	2018	2019	2020	2021	2022	2023
Всего зарегистрированных преступлений в РФ	2160063	2058476	1991532	2024337	2044221	2004404	1966841	1947161
Темп прироста, %	–	-4,94	-3,36	1,65	0,98	-1,95	-1,84	-1,0
Всего зарегистрированных киберпреступлений в РФ	90722	142034	175254	294402	510447	517722	522065	676951
Темп прироста, %	–	56,56	23,39	67,99	73,38	1,43	0,8	29.66
Всего зарегистрированных уголовных правонарушений в РК	361689	316418	292286	243462	162783	157884	151241	140272
Темп прироста, %	–	-12,52	-7,63	-16,70	-33,14	-3,01	-4,21	-7.25
Всего зарегистрированных кибер уголовных правонарушений в РК	902	2869	5058	8522	14109	21479	20531	24506
Темп прироста, %	–	218	76,3	68,5	65,5	52,2	-4,5	19.36

According to O. Satiev, President of the Association of Legal Entities «Center for Analysis and Investigation of Cyber Attacks», «there is a requirement mandating that a bank or a microfinance organization (MFO), upon receiving an application from a client regarding the issuance of a fraudulent loan in their name, must appeal to law enforcement agencies. At present, this workflow has been established, and a memorandum of cooperation in this sphere has been concluded between the Agency for Regulation and Development of the Financial Market (ARDFM) and authorized bodies. This allows for monitoring the volume of such appeals and responding to them promptly» .

Furthermore, starting from the 2024-2025 academic year, three new specializations have been introduced at the Almaty Academy of the Ministry of Internal Affairs: «cybersecurity provision», «IT forensic support for the activities of internal affairs bodies», and «information systems», the graduates of which will be deployed to work within the «Cyberpol» units.

However, apart from the aforementioned measures, it is necessary to specifically emphasize the establishment of a system for conducting criminal proceedings in an electronic format. «In 2017, on the initiative of the Prosecutor General's Office of the Republic of Kazakhstan, the IT system of the electronic criminal case (E-criminal case) was developed.

The legislative consolidation of its procedural foundations was secured by amendments to the Criminal Procedure Code of the Republic of Kazakhstan (CPC RK) dated December 21, 2017, when

the legislator introduced the concept of the «Format of criminal proceedings» (Article 42-1).

The electronic criminal case enables the monitoring of actions and decisions of individuals conducting the criminal process, serving as a deterrent against various types of cover-ups, abuses of power, and evidence falsifications.

The entire process is transparent to supervisory bodies and officials. To ensure the full cycle of managing criminal cases in an electronic format, the information systems of criminal prosecution bodies (ERDR), prosecution bodies («Zandylyk»), and the judicial system («Torelik») were seamlessly integrated» . Sabit Nurlybay, Chairman of the Committee on Legal Statistics and Special Records of the Prosecutor General's Office, noted that in 2022, «more than 134 thousand criminal cases were investigated in electronic format, which constitutes over 90% of the total number of cases in the proceedings of pre-trial investigation bodies» .

Special attention should be drawn to a number of distinctive procedural features of the CPC of Kazakhstan.

Thus, pursuant to Article 120 of the CPC, upon an individual's petition—provided it does not prejudice the case—it is legally permissible to transfer copies of documents from electronic storage media to the said individual. Furthermore, a procedure is prescribed for the notarization of such documents, with the notary's services being remunerated directly by the petitioner. The Code additionally outlines the strict rules under which the application of scientific and technical means may be deemed admissible; it meticulously regulates the procedure for drafting the indictment protocol and documenting therein «scientific and technical means and electronic media, if they were utilized during the recording process or if traces of a criminal offense are recorded on them» . An expert's conclusion may also be formalized as an electronic document, while the search of residential premises is executed strictly upon the sanction of a court.

The Experience of the Republic of Armenia

The investigation of cybercrimes in the Republic of Armenia is conducted by the Directorate for the Investigation of Cybercrimes and High-Tech Crimes of the Investigative Committee. Since 2019, a computer forensics laboratory has been operating within the

Committee. Additionally, a specialized directorate for combating high-tech crimes has been established within the Police structure.

In 2008, Armenia acceded to and ratified the European Convention on Cybercrime, which serves as the legal framework for international cooperation with other states parties to the Convention.

R. Adilkhanian noted that «in Armenia, out of 10,000 hypothetical cases of cybercrimes, law enforcement agencies become aware of only 10 to 100, and a mere 1 to 10 are ultimately solved» .

A comparative legal analysis of the criminal legislation of Armenia demonstrates that, similarly to other CIS member states, it encompasses a dedicated Chapter 38, «Crimes Against the Security of Computer Systems and Computer Information» comprising seven articles. However, this chapter also establishes liability for emerging forms of cybercrime, such as grooming (Article 202) and computer theft (Article 257, which is analogous to Article 212 of the Criminal Code of Belarus). Furthermore, it introduces qualifying elements for traditional crimes committed «using information or communication technologies», encompassing lewd acts (Article 201) and even hooliganism (Article 297). Moreover, the mere storage of child pornography on a computer, as well as its viewing, is strictly criminalized (Article 300).

In June 2024, the Armenian Parliament passed, in its first reading, a legislative draft on cybercrimes and crypto-assets aimed at enhancing liability for offenses committed in cyberspace.

Regarding criminal procedural legislation, there are virtually no fundamental distinctions from the CPCs of other CIS countries.

The Experience of the Kyrgyz Republic

«The authorities of several post-Soviet states in the Central Asian region view the transition toward the state becoming the primary provider of internet content—thereby blocking access to cyberspace for external organizations—as a measure to combat cybercrime. Tajikistan and Kyrgyzstan, in particular, advocate for such measures» .

In 2021, the Kyrgyz Republic adopted a new Criminal Code, incorporating a novel chapter entitled «Crimes Against Cyber-Security» (Chapter 40). This chapter stipulates criminal liability

for unlawful access to electronic information (Article 319), the creation of malicious software products (Article 320), cyber-sabotage (Article 321), and the mass distribution of electronic messages (Article 322). It also introduces qualifying elements for specific categories of «conventional» crimes, such as theft from a bank account and theft of electronic money (in the absence of fraud indicators). However, cyber fraud is qualified as «conventional» fraud, lacking a specific qualifying element. The Kyrgyz Republic remains one of the few jurisdictions whose criminal legislation explicitly utilizes the prefix «cyber».

The new Criminal Procedure Code of the Kyrgyz Republic, much like that of Kazakhstan, provides for the legal capability of maintaining an electronic criminal case; however, its legislative formulation is exceptionally meticulous.

For instance, Article 89 specifies that «an electronic document is recognized as evidence equal in legal significance to written evidence... The original of an electronic document exists exclusively on a machine-readable medium». Such strict regulation effectively circumvents bureaucratic hurdles and prevents the flawed procedural practice where «a criminal case is recorded on paper, signed manually, and then scanned and entered into the system to become electronic»—a scenario observed during a pilot experiment conducted in Tashkent.

The procedure for the search and seizure of electronic media is also strictly regulated, albeit within the article governing conventional search and seizure operations. Furthermore, novel special investigative actions have been introduced, which are inherently operational-search activities. These include the «extraction of information from computers, servers, and other devices; audio and video surveillance of a person or location; observation of a person or location; covert entry and inspection of non-residential premises or other immovable property in the possession or disposal of an individual; infiltration into a criminal environment and (or) simulation of criminal activity; controlled delivery; and test purchasing» .

Moreover, in contrast to our domestic legislation, individuals participating in these actions may be interrogated as witnesses while preserving the strict confidentiality of their identities. However, even the seizure of postal and telegraphic communications and their subsequent inspection and (or) seizure, the extraction of samples for comparative forensic examination,

and the interception of communications are similarly classified as special investigative actions, despite having long been recognized as fully-fledged investigative actions in other CIS countries.

In addition, new specialized procedural roles have been instituted, including specialized investigators, prosecutors, judges, and defense attorneys for juvenile cases.

The Ministry of Internal Affairs of the Kyrgyz Republic serves as the primary agency responsible for solving and investigating cybercrimes, having established dedicated cybercrime departments alongside units for operational-technical support and social media monitoring. The State Committee for National Security (SCNS) of the Kyrgyz Republic also combats cybercrimes that encroach upon national security. In 2020, the SCNS Cybersecurity Coordination Center was established, which has successfully obtained CC-CERT accreditation.

Nevertheless, statistical data concerning cybercrimes in the Kyrgyz Republic remains classified, although law enforcement agencies publicly acknowledge a steady increase in their volume.

The Experience of Georgia

According to the National Cyber Security Index (NCSI), in 2024, Georgia ranked 22nd globally and 16th in Europe in terms of its cybersecurity level, achieving a 100% score in the category of combating cybercrime. This serves as a strong indicator of the correct trajectory of its established strategy for countering cyber-threats. «In the post-Soviet space, Georgia became the first country to establish criminal liability for terrorist crimes on the global network» , specifically cyberterrorism (Article 324.1). Furthermore, as official statistics from the Ministry of Internal Affairs of Georgia demonstrate, the volume of cybercrimes remains at a relatively low level: «in 2023, cybercrime in Georgia increased... victims reported 999 cases, which is 7% more than in 2022» . This indicator is significantly lower than in other jurisdictions. For instance, «in the Russian Federation, the share of cybercrimes in the overall structure of registered crimes increased 8-fold by 2023, amounting to 34.8% «.

A comparative legal analysis of Georgian criminal legislation revealed that criminal liability for cybercrimes is stipulated in Chapter 35 of the Criminal Code of Georgia, which comprises three articles (Articles 284–286).

However, the examination of its criminal procedural legislation elicits the greatest scientific interest. Thus, Article 124.1 of the Criminal Procedure Code (CPC) of Georgia regulates the procedure for monitoring bank accounts, which entails obtaining information on multiple bank accounts in real time with a court warrant. By way of comparison, in our country, obtaining information constituting a banking secret requires the sanction of a prosecutor, and the procedure for dispatching and executing such a request takes weeks.

The criminal procedural legislation of Georgia provides for specific types of covert investigative actions, such as real-time geolocation tracking. Chapter 16 of the CPC encompasses investigative actions related to computer data, such as requesting a document or information (Article 136), the real-time collection of internet traffic data (Article 137), and the «collection of content data» (Article 138). The introduction of these procedural actions represents a critical step in establishing the source of a cyberattack, the perpetrator's IP address, device location data, and related digital footprints.

Moreover, the introduction of the legal capability of «obtaining computer data or documents from a foreign state without submitting a request for mutual legal assistance» (Article 138.1) elevates Georgia to a fundamentally new level in terms of countering cybercrime, primarily because standard international requests typically require months for transmission and response.

«In 2010, the Data Exchange Agency (DEA) was established under the Ministry of Justice, whose mandate is to ensure the cybersecurity of the entire governmental network (excluding its military component), which comprises 36 critical infrastructure objects.

The Computer Emergency Response Team (CERT) operates under the supervision of the DEA, responsible for responding to cyber incidents and monitoring the operability of the Georgian governmental network.

The criminal prosecution and investigation of cybercrimes are conducted by the Cybercrime Division of the Central Criminal Police Department (under the Ministry of Internal Affairs). Within the Division, a 24/7 contact point operates, facilitating the exchange of cybercrime information with other parties to the Council of Europe Convention on Cybercrime» . Additionally, in

2022, a dedicated Cybercrime Department was established within the Prosecutor General's Office of Georgia.

Conclusion

The conducted comparative legal analysis of the pre-trial proceedings experiences in selected CIS countries (the Russian Federation, the Republic of Armenia, the Republic of Belarus, Georgia, the Republic of Kazakhstan, and the Kyrgyz Republic) has made it possible to identify the underlying trends in formulating a national strategy to combat cybercrime, as well as to extract their positive practices, which can be subsequently utilized to refine national criminal and criminal procedural legislation. In particular, the implementation and scaling of the electronic criminal case format, the legislative legalization of cyber-search operations within the procedural status of investigative actions, and the criminalization of the activities of individuals providing financial requisites for the laundering of criminal proceeds (so-called «drops» or money mules) serve as indispensable steps for the effective modernization of pre-trial proceedings and the protection of the sovereign interests of states within the digital space.

Refference

1. CIS Model Criminal Code. (1996). Retrieved from: http://www.cisatc.org//135/154/241 (in Russian).
2. Panfilov, E. I., & Popov, A. S. (1998). Model Criminal Code for the CIS states. Computer crimes, St. Petersburg, 195. (in Russian).
3. CIS Model Law on combating terrorism (new edition). (2004). Adopted by the resolution of the Interparliamentary Assembly of the CIS Member States on April 17, 2004, N 23-5. URL: http://docs.cntd.ru/document/901912313 (in Russian).
4. Bocharnikov, I. V. (2013). Information counteraction to terrorism in modern conditions. Security Problems, 3, 25-37. (in Russian).
5. Nikulchenkova, E. V. (2022). On the necessity of introducing the definition of «cybercrime» into the criminal law of the Russian Federation. Herald of Omsk University. Series. Law, 19(3), 98–107. https://doi.org/10.24147/1990-5173.2022.19(3).98-107 (in Russian).
6. Shkhagapsoev, Z. L., & Buraeva, L. A. (2018). On current issues of international cooperation in countering manifestations of extremism and terrorism in the Internet space. Gaps in Russian Legislation, 5, 251-254. (in Russian).
7. Shestak, V. A., & Adigamov, A. I. (2020). Modern approaches in the legislation of EU member states to criminal liability for crimes in cyberspace. Education and Law, 8. (in Russian).
8. F.A.C.C.T. (2024). Analytical report «Cybercrime in Russia and the CIS. Trends, analytics, forecasts 2023–2024». https://www.facct.ru/resources/research-hub/cybercrime-trends-annual-report-2023-2024/ (in Russian).

9. Agreement on cooperation of the CIS member states in combating crimes in the sphere of computer information. (2001). Commonwealth. Information bulletin of the Council of Heads of State and the Council of Heads of Government of the CIS, 1, 23–31. (in Russian).
10. Kobets, P. N. (2022). Improving the activities of law enforcement agencies of the CIS member states in combating cyberterrorism in the context of information globalization. Scientific Notes of the Kazan Law Institute of the MIA of Russia, 7(1), 53. (in Russian).
11. Lutovich, P. V., & Rudovich, N. I. (2020). Certain aspects of state cooperation in countering high-tech crimes. Theory and practice of combating computer crime: materials of the international scientific-practical conference. Academy of the MIA, Minsk, 59. (in Russian).
12. Kharin, V. V., & Plotnikova, T. V. (2018). Cybercrime as a threat to international security. Actual Problems of State and Law, 2(8), 96-107. DOI 10.20310/2587-9340-2018-2-8-96-107 (in Russian).
13. Dolzhenko, N. I., & Khmelevskaya, I. G. (2020). On the issue of the content aspects of cybercrime. NOMOTHETIKA: Philosophy. Sociology. Law, 45(2), 315–322. https://doi.org/10.18413/2712-746X-2020-44-2-315-322 (in Russian).
14. International Independent Institute for Investment Policy Analysis of the RF. (2024). Liability for cybercrimes intended to be tightened. https://xn--80aplem.xn--p1ai/news/Otvetstvennost-za-kiberprestuplenia-hotat-uzestocit/ (in Russian).
15. Criminal Procedure Code of the Russian Federation. (2001). (in Russian).
16. ConsultantPlus. (n.d.). https://www.consultant.ru/document/cons_doc_LAW_34481/a181248bd35e283bbf253a905940bfb32dd9923e/ (in Russian).
17. The state of crime in Russia (January–December 2023). (2024). URL: http://crimestat.ru/ (in Russian).
18. Moscow Bar Association «Sheriev and Partners». (n.d.). Liability of drops and drop-handlers. https://advokat-sheriev.ru/otvetstvennost-dropov.aspx (in Russian).
19. Ministry of Internal Affairs of the Russian Federation. (n.d.). The Ministry of Internal Affairs has developed a bill providing for criminal punishment for those who assist fraudsters in withdrawing funds stolen from Russian citizens' accounts. (in Russian).
20. Federal Law No. 369-FZ «On Amendments to the Federal Law 'On the National Payment System'«. (2023). http://publication.pravo.gov.ru/Document/View/0001202307240049 (in Russian).
21. Gyulalieva, R. A., & Aliev, A. R. (2023). Foreign experience in combating cybercrime. The World of Science and Ideas, 1, 117. (in Russian).
22. Ministry of Foreign Affairs of the Russian Federation. (n.d.). https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1773661/ (in Russian).
23. Order of the MIA of Russia N 1110 «On Approval of the Regulation on the Directorate for Organizing the Combating of the Unlawful Use of Information and Communication Technologies of the Ministry of Internal Affairs of the Russian Federation». (2022). https://www.consultant.ru/document/cons_doc_LAW_439373/ (in Russian).

24. Shikula, I. R., & Kurkin, E. N. (2023). Cybercrime in the Russian Federation: main methods of struggle and problems of counteraction. International Journal of Experimental Education, 1, 37-41. (in Russian).
25. Mikhailyuk, V. A. (2023). Cyberpolice as a modern law enforcement agency in the fight against Internet crime. Bulletin of the Ufa Law Institute of the MIA of Russia, 1(99), 74–79. (in Russian).
26. Shvyryaev, P. S. (2023). The problem of cybercrime in Russia: current state and prospects for solution. Living Standards of the Population in the Regions of Russia, 19(4), 625. (in Russian).
27. Osipenko, A. L., & Lugovik, V. F. (2021). Problems of law enforcement agencies' access to concealed computer information during crime investigation. Society and Law, 2(76), 60–68. (in Russian).
28. Criminal Code of the Republic of Belarus. (1999). https://pravo.by/document/?guid=3871&p0=hk9900275 (in Russian).
29. Statistics of the Main Directorate for Combating Cybercrime of the Ministry of Internal Affairs of the Republic of Belarus. (2023). Briefing at the BELTA press center. (in Russian).
30. Information on the decrease of cybercrime in the Republic of Belarus. (2024). Sputnik. https://sputnik.by/20240621/gora-chislo-kiberprestupleniy-znachitelno-snizilos-1087349548.html (in Russian).
31. Chernysheva, S. A. (2020). Combating computer crimes as a key link in ensuring information security. Theory and practice of combating computer crime: materials of the international scientific-practical conference. Academy of the MIA, Minsk, 100. (in Russian).
32. Decree of the President of the Republic of Belarus No. 269 «On measures to counteract unauthorized payment operations». (2023). https://president.gov.by/ru/documents/ukaz-no-269-ot-29-avgusta-2023-g (in Russian).
33. Decree of the President of the Republic of Belarus No. 367 «On the circulation of digital signs (tokens)». (2024). https://president.gov.by/ru/documents/ukaz-no-367-ot-17-sentabra-2024-g (in Russian).
34. Decree of the President of the Republic of Kazakhstan No. 674 «On approval of the Concept of Legal Policy of the Republic of Kazakhstan until 2030». (2021). https://adilet.zan.kz/rus/docs/U2100000674 (in Russian).
35. Dzhansarayeva, R. E., & Aratuly, K. (2012). Combating cybercrimes: a comparative analysis of the legislation of the CIS countries. Criminological Journal of Baikal National University of Economics and Law, 96. (in Russian).
36. Dadashov, R. F. (2023). Countering cybercrime in the Republic of Kazakhstan and foreign countries: criminological and victimological aspects. Criminological Journal, 3, 71-75. (in Russian).
37. Measures to combat cybercrime in Kazakhstan (MIA RK). (n.d.). https://www.zakon.kz/sobytiia/6400289-kak-borotsya-s-kiberprestupnostyu-v-kazakhstane-pridumali-v-mvd.html (in Russian).
38. Statistical data — information on criminal offenses for 2016–2023 (Kazakhstan). (2024). URL: https://qamqor.gov.kz (in Russian).
39. Statistical data — information on criminal offenses for 2018–2021 (Kazakhstan). (n.d.). URL: https://qamqor.gov.kz (in Russian).
40. Karabekov, K. O. (2024). The state and trends of cybercrime in the Russian Federation and the Republic of Kazakhstan. Scientific Herald of the Omsk Academy of the MIA of Russia, 30(2), 109. (in Russian).

41. Protection against cyber fraudsters: how to combat cybercrime in the RK. (n.d.). https://www.zakon.kz/finansy/6406916-zashchita-ot-kibermoshennikov-kak-borotsya-s-kiberprestupnostyu-v-rk.html (in Russian).
42. Balgyntayev, A. O. (n.d.). Electronic criminal proceedings in the Republic of Kazakhstan. https://online.zakon.kz/Document/?doc_id=34878697&pos=6;-106#pos=6;-106 (in Russian).
43. On the practice of investigating criminal cases in electronic format in Kazakhstan. (n.d.). https://www.gov.kz/memleket/entities/pravstat/press/news/details/416263?lang=ru (in Russian).
44. Criminal Procedure Code of the Republic of Kazakhstan. (2014). https://adilet.zan.kz/rus/docs/K1400000231 (in Russian).
45. Adilkhanian, R. (n.d.). Interview «The investigator presents» on the level of latency of cybercrimes. Iravaban.net. (in Russian).
46. Saidova, K. (n.d.). Tajikistan and Kyrgyzstan are seeking effective measures to combat cybercrime. Digital Report. (in Russian).
47. Criminal Procedure Code of the Kyrgyz Republic. (2021). https://mvd.gov.kg/rus/ministry/normative-bases/23 (in Russian).
48. Butkevich, S. A. (2018). Extremism and terrorism in cyberspace: detection, neutralization, and prevention. Herald of the Krasnodar University of the MIA of Russia, 1(39), 17-22. (in Russian).
49. Information on the growth of cybercrime in Georgia in 2023. (2024). Commersant.ge. (in Russian).
50. The state of crime in Russia (January–December 2023). (2024). http://crimestat.ru/ (in Russian).
51. Gotsiridze, A. (n.d.). Reliable cyber defense requires infrastructure, legal support, and multinational cooperation. Per Concordiam. (in Russian).