ASIAN JOURNAL
of Criminal Justice and Forensic Studies

Founders and Publisher:
Private institution "Eurasian Accreditation Agency (EAA)"

Year of foundation: 2025

State Registration:
Ministry of Culture and Information of the Republic of Kazakhstan
Registration Number: KZ89VPY00132384 (24.10.2025)

E-mail: info@asianjustice.kz
https://asianjustice.kz/

EDITORIAL BOARD

CONTENTS

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 004.056.55; 347.78

Article's History:
Received: 18.07.2025; Revised: 12.11.2025; Accepted: 16.12.2025

Biometric identification technologies and privacy concerns in Kazakhstan and China

Pan Yu
Universiti Malaya
50603, Kuala Lampur, Malaysia
https://orcid.org/0000-0001-5980-0828

Shuaiyang Jing
ShanghaiTech University
201210, 393 Middle Huaxia Rd., Shanghai, China
https://orcid.org/0009-0001-4945-069X

Sarinder Kaur Dhillon*
Universiti Malaya
50603, Kuala Lampur, Malaysia
https://orcid.org/0000-0003-1922-2044

Abstract. The aim of this study was to compare Kazakhstani and Chinese models of privacy and security in biometric systems. The research established that Kazakhstan and China represent two different approaches to biometric identification: the former is a balanced model between state control and international standards, while the latter is a utilitarian model in which state security is prioritised. The study applied theoretical analysis to conceptually distinguish key terms and identify threats; a comparative-legal analysis of the legislation of Kazakhstan and China; and the case-study method to examine high-profile incidents of data leaks and political surveillance. The research found that China implements a utilitarian model of total control (via the "Xueliang" project), whereas Kazakhstan – despite its declared balanced/transitional model with a focus on forensics – de facto exhibits weak law enforcement and a tendency towards data leaks. This is evidenced by an explosive 101.7% rise in cyber incidents in the first quarter of 2025, which renders the country vulnerable to threats of authoritarian surveillance. It was demonstrated that in both jurisdictions the absence of genuine voluntariness of consent and the opacity of biometric application are key privacy risks. A number of practical recommendations were formulated for Kazakhstan, including strengthening enforcement (introducing independent cybersecurity audits) and enshrining the principle of proportionality in law to restrict mass facial recognition. The results are important for shaping effective legal mechanisms in transitional states to protect civil liberties. Accordingly, the findings may be considered by countries at the stage of implementing biometric technologies to better understand potential risks and challenges

Keywords: freedom; criminal justice; state control; human rights; implementation of laws; data leakage

Introduction

The relevance of the topic is driven by the deployment of biometric technologies (in particular, facial recognition systems, dactyloscopy and genomic identification) in public administration and national security. This creates a global dilemma between technological progress and the fundamental right of citizens to privacy. In the Asian context, the issue has become acute: the People's Republic of China (PRC) uses biometrics to create the world's largest system of mass state surveillance, which threatens personal-data protection and strengthens state control. At the same time, the Republic of Kazakhstan (RK), while advancing digitalisation, faces growing challenges of data leaks and intensified state oversight of civil society. Thus, examining the balance between national-security priorities, commercial

Suggest Citation:
Yu, P., Jing, Sh., & Dhillon, S.K. (2025). Biometric identification technologies and privacy concerns in Kazakhstan and China. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 4-14.

*Corresponding author

benefit and the preservation of human rights amidst the biometric revolution is essential for developing effective legal mechanisms and policy strategies aimed at safeguarding civil liberties and privacy in the digital environment, especially in the context of non-Western authoritarian and transitional states.

Biometric identification technologies have gained popularity due to their ability to enhance security and streamline authentication processes across various sectors of society, including public administration, national security, healthcare and the commercial sector (financial services, retail). At the same time, the roll-out of biometric technologies is accompanied by serious challenges related to personal-data security and privacy protection, owing to the unique nature of biometric identifiers and the potential for their unauthorised use. According to S. Kumar (2024), biometric systems are vulnerable to attacks in which adversaries use forged biometric traits to gain unauthorised access. The study notes that this may include the use of fake fingerprints, facial masks or other imitations of biometric data. Such threats can lead to identity fraud, necessitating robust security measures, ethical considerations and privacy safeguards in design and deployment. M.D. Choudhry *et al.* (2024) established that systems using AI-based biometrics carry an elevated risk of information-security breaches, resulting in the theft of personal data and, consequently, unauthorised access – a serious threat to privacy. The results of P. Datta *et al.* (2020) showed that biometric systems are also vulnerable to adversarial attacks. These attacks manipulate recognition systems by deliberately "deceiving" their algorithms, undermining the integrity and reliability of the entire system. The authors therefore argue that, in view of unauthorised access via attacks (anti-spoofing and liveness detection), there is a need for signal-processing and cryptographic methods to protect biometric data from malicious actors.

Another problem addressed in the literature is the concept of privacy within biometric technologies. G. Singh *et al.* (2021) found that the process of obtaining informed consent for the collection of biometric data is often neglected. This raises serious ethical concerns, as individuals may not realise exactly what data are collected and how they will be used. Accordingly, the need for secure, privacy-preserving protocols in biometric authentication systems is emphasised to protect personal information. F.R. Baifat & S. Satoto (2024) argue that biometric-identification technologies raise significant privacy concerns, including potential violations of the right to privacy and regulatory uncertainty. These issues require careful consideration to ensure data security and the protection of individuals' rights during the implementation of such technologies in immigration control.

In Kazakhstan, biometric technologies – particularly facial recognition, dactyloscopy (fingerprints) and genomic identification – are being actively implemented. These technologies are used to strengthen security, develop digital services and optimise public and commercial services. According to G. Dzhaksybekova & I. Pulatov (2020) and K. Bertayeva *et al.* (2024), biometric identification (fingerprints, facial and voice recognition) is already used for opening accounts online, concluding insurance contracts and remote customer service. This increases the convenience and security of financial transactions, while simultaneously creating new cyber risks that require attention. Biometric authentication of students in higher-education institutions is also salient. D. Muratuly *et al.* (2022) report the use of a turnstile system with a facial-recognition terminal capable of providing unique biometric data in real time. Such a system is deployed for access control and online learning.

As biometric identification technologies become more widespread, privacy issues arise. The use of biometric data, such as facial recognition and deoxyribonucleic-acid (DNA) samples, often conflicts with individual privacy rights, especially when implemented in a surveillance context. Consequently, this topic features prominently in Kazakhstani and Chinese academic publications. J. Zhang (2024) shows that in China, biometric identification, including facial recognition, is regulated by the Law of the People's Republic of China "Personal Information Protection Law" (PIPL) (2021), emphasising consent and security. However, Kazakhstan's legal framework for biometric data is less developed, raising concerns about privacy and potential misuse of personal information. According to D. Utegen & B.Z. Rakhmetov (2023), the legislation of the Republic of Kazakhstan requires improvements to the legal regulation of biometric data, including acceptable criteria for the use of facial-recognition technology and the development of a categorisation of biometric systems into high- and low-risk. The authors' recommendations included creating a risk-based categorisation of biometric systems following the European Union's approach to AI regulation, and introducing bans on mass and non-selective surveillance of people via video-surveillance systems.

Although the reviewed studies provide in-depth analyses of vulnerabilities and privacy issues in biometric technologies in general (spoofing, data leaks, adversarial attacks) and of the regulatory frameworks in China and Kazakhstan separately, they do not offer a systematic comparative analysis of these two countries in the context of criminal justice and privacy risks. Existing works focus either on theoretical issues (forgery risks, lack of consent) or on the legal framework of a single country, without juxtaposing implementation models. This creates a gap, as it prevents the identification of shared challenges and the assessment of the effectiveness of different strategies in two states with similar contexts (authoritarian tendencies, rapid digitalisation) but different legal-regulatory models (utilitarian PRC versus partially liberalised RK). Accordingly, the aim of this study was to conduct a comparative analysis of privacy and security issues in biometric data in Kazakhstan and China. The objective entailed: analysing and comparing the legislative frameworks of Kazakhstan and China governing the collection, storage and use of biometric data in criminal justice; identifying and systematising key risks to privacy and human rights arising from the

implementation of biometric systems in the countries under study, including incidents of data leakage and the intensification of state surveillance.

Materials and Methods

A comparative and analytical approach was employed, based on a review and synthesis of existing sources to assess the implementation of biometric systems in the criminal-justice sphere of Kazakhstan and the related privacy risks. The Republic of Kazakhstan and the People's Republic of China were selected in order to juxtapose two different approaches to the use of biometric technologies, enabling the identification of common trends and risks under conditions of rapid digitalisation and strong state control: China as an example of a utilitarian model, and Kazakhstan as a balanced/transitional model. Data collection was carried out through the analysis of open sources. The following acts of the RK were examined: the Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration" (2021); the Law of the Republic of Kazakhstan No. 94-V (2013); and the Law of the Republic of Kazakhstan No. 271-IV (2025). The following PRC acts were also analysed: the PIPL (2021); and the Security Management Measures for the Application of Facial Recognition Technology (2025) (FR Measures). In addition, the latest statistics on cyberattacks in Kazakhstan for January-March 2025 were taken into account (The number of cyberattacks…, 2025).

Several key methods were used in this study. The method of theoretical analysis was applied to conceptually delineate key notions, in particular "biometric data" and "biometric identification". This method was also used to identify theoretical threats such as algorithmic bias and risks to civil rights. The comparative-legal method was employed to juxtapose the approaches of the RK and the PRC to biometric identification. The comparison was conducted according to five criteria relevant to criminal justice and privacy: philosophical foundation (whether the legislation is grounded in utilitarianism or in a balanced/transitional model); legal limits of compulsory collection (identifying for which categories of persons – offenders, migrants – and for what purposes biometrics must be collected); regulation of real-time technologies (Smart Cities Challenges and Opportunities, n.d.; Ersozoglu, 2013); requirements for consent and alternatives (comparing norms regarding the genuine voluntariness of consent); and sanctions and oversight (comparing accountability mechanisms for leaks and data misuse). The case-study method was applied to examine high-profile incidents of personal-data leakage and cases of improper use of biometric systems in criminal justice. The following RK cases were analysed: the 2019 voter-data leak (Toqmadi & Zakharchenko, 2021), the 2025 leak of outdated data (Satubaldina, 2025), and "Biometric data collection: What risks might Kazakhstanis face?" (Buralkieva, 2022). This method was used to illustrate practical risks and consequences for privacy and human rights. These cases are representative because they encompass the two principal risks associated with biometrics in authoritarian regimes: technical vulnerability (leaks) and political abuse (surveillance). The method of synthesis and generalisation was used to interpret the results, which was based on synthesising and generalising data obtained from various sources.

Results and Discussion

The application of biometric technologies in law enforcement is not a new concept, but rather a large-scale automation and expansion of practices that have existed for centuries. Within this study, "biometric data" are defined as a special category of personal data resulting from the technical processing of unique physical, physiological or behavioural characteristics of a person (for example, facial images, fingerprints) that enable or confirm their unique identification. "Biometric identification", in turn, is the automated recognition of an individual based on such data.

Kazakhstan demonstrates a consistent approach to the implementation of biometric technologies. The key act is the Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration" (2021), whose provisions entered into force in 2021-2024. This law establishes the legal framework for identifying a person on the basis of biometric data and clearly distinguishes between voluntary and compulsory registration. Compulsory dactyloscopy, or the collection of fingerprints, is mandatory for foreigners and stateless persons who apply for a residence permit or a visa, or who are subject to administrative expulsion. Refusal by a foreigner to undergo this procedure leads to administrative expulsion from the country. For citizens of Kazakhstan, dactyloscopic registration is voluntary; however, the data of registered persons are recorded on a chip in biometric passports and ID cards (identity cards). Genomic registration, which involves the collection of DNA samples, has a more limited but critically important scope. It is compulsory for persons convicted of criminal offences, as well as for unidentified bodies and biological material collected from the scenes of serious or particularly serious crimes. The legislation also provides for the voluntary submission of genomic data by relatives of missing persons. Refusal to undergo compulsory genomic registration entails a fine (Dyussembekova, 2021; What you need to know about dactyloscopy…, 2024).

The data-protection system in Kazakhstan is based on the Law of the Republic of Kazakhstan No. 94-V (2013), which defines biometric data as a sensitive category requiring an elevated level of protection. The law also sets a requirement to minimise data retention after the completion of an investigation. However, the formal existence of this legislative framework does not correlate with its actual effectiveness. This gap between statutory norms and weak enforcement creates the basis for significant risks, manifesting in insufficient data protection and a lack of transparency in their use. The practical application of biometric technologies in Kazakhstan reflects an ambition for deep digitalisation of criminal justice; as of 2023, 91% of criminal cases are processed electronically, confirming a high level of integration of digital tools into the law-enforcement system

(Gritsenko *et al.*, 2025). One of the central elements of this strategy is the deployment of video-surveillance systems within the "smart city" concept, which is partly based on the experience of the PRC. Operations centres in major cities collect data from CCTV (closed-circuit television) cameras, enabling the real-time identification and tracking of wanted persons, as well as the assessment of crime probabilities. A subsequent step was the adoption of amendments to the Law of the Republic of Kazakhstan No. 271-IV (2025), which prohibit the wearing in public places of items that "interfere with facial recognition". The government explains this decision as a measure aimed at increasing the "effectiveness of crime prevention" and promoting public safety.

In addition to video surveillance, Kazakhstan is actively developing systems of dactyloscopic and genomic registration. The DNA database, operational since 2021, is intended for identifying unknown bodies and investigating crimes. The compulsory nature of these requirements is underscored by liability for refusal to undergo genomic registration, including a fine. Although these initiatives aim to enhance the effectiveness of law-enforcement agencies, they simultaneously raise serious questions about the balance between security and the fundamental right to privacy. Table 1 summarises the key aspects of the implementation of biometric technologies in Kazakhstan regulated by specialised acts.

Table 1. Detailing of RK legislation on the use of biometric technologies in Kazakhstan

Aspect	Detailing in RK Legislation
Dactyloscopy	Mandatory for foreigners and stateless persons (when obtaining a residence permit, visa); voluntary for RK citizens, but data are recorded on the chip of biometric documents.
Genomic registration	Mandatory for persons convicted of criminal offences, as well as for unidentified bodies. Refusal entails a fine.
Video surveillance	Deployment of video-surveillance systems within the "smart city" concept. Prohibition on wearing items that "interfere with facial recognition" to increase the "effectiveness of crime prevention".

Source: compiled by the authors based on analysis of the Smart Cities Challenges and Opportunities (n.d.), Law of the Republic of Kazakhstan No. 94-V (2013), Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration" (2021), Law of the Republic of Kazakhstan No. 271-IV (2025)

The analysis of RK legislation shows a consistent and structured approach to integrating biometrics, focused on improving the effectiveness of law-enforcement agencies and national security. The legislative framework clearly distinguishes compulsory (for migrants, offenders) and voluntary (for RK citizens) categories of data collection, emphasising the priority of dactyloscopy and genomic registration. At the same time, the amendments relating to video surveillance within Smart Cities Challenges and Opportunities (n.d.) and the ban on concealing one's face in public places indicate a strengthening of state control in the digital environment. Although these initiatives are aimed at crime prevention, they simultaneously raise profound questions about the genuine voluntariness of citizens' consent and the balance between security and privacy.

Despite the proclaimed advantages of deep digitalisation of justice, the implementation of biometric systems in Kazakhstan is accompanied by significant risks to privacy and human rights. The analysis shows that these risks are a direct consequence of weak law enforcement and the prioritisation of political control over technical cybersecurity. One such issue is the threat of data leakage, indicating that the government cannot guarantee their security and confidentiality (Toqmadi & Zakharchenko, 2021). The 2019 voter-data leak, which compromised information on 11 million citizens, was accompanied by widespread network restrictions and the blocking of independent media. This evidences the prioritisation of political control (suppression of dissent) over cybersecurity. Public reporting of accountability for those responsible was absent; cases of liability often concern internal actors (employees selling data via Telegram channels) rather than external hackers.

The 2025 leak of outdated data (16 million citizens). Sensitive information (surname, given name, patronymic, identification number, addresses) on 16 million citizens of Kazakhstan appeared in the public domain, indicating the persistence of the problem (Satubaldina, 2025). Although the authorities claimed the data were outdated, experts confirmed the presence of new records. The leak likely originated from private information systems (microfinance organisations, medical institutions), prompting the Ministry of Digital Development to shift responsibility to the private sector. In response, the state tightened legislation by increasing administrative fines (up to 7.9 million tenge) and introducing liability for using another person's electronic digital signature (EDS).

Disproportionality and a lack of transparency in the application of biometrics are key risks. Human-rights advocates criticise the compulsory provision of biometric data to obtain documents, noting that citizens have no choice, effectively nullifying the principle of voluntariness. The case "Biometric data collection: What risks might Kazakhstanis face?" (Buralkieva, 2022) concerns the use of facial-recognition systems (FRT) to identify participants in the January 2022 protests in Kazakhstan. Although the Ministry of Internal Affairs (MIA) of the RK publicly denied this, the incident itself demonstrated the government's technological capacity for mass surveillance and underscored the public's deep mistrust of the purposes for which biometrics are used, indicating the risk of employing technologies for political monitoring. In January-March 2025, 30,000 information-security incidents were recorded in the Republic of Kazakhstan – twice as many as in the same period of 2024 (Table 2).

Table 2. Statistics of information-security incidents in the RK

Security Incidents. January-March (units)	Total (2025/Q1)	Total (2024/Q1)	Growth (2024/Q1 vs 2023/Q1)	Change (units)	Share of RK (2025/Q1)	Share of RK (2024/Q1)
Total	29,982	14,868	101.7%	15,114	100.0%	100.0%
Botnets	17,606	1,748	907.2%	15,858	58.7%	11.8%
Computer viruses, network worms, trojans	7,870	9,586	-17.9%	-1,716	26.2%	64.5%
Phishing on the Internet	1,975	1,439	37.2%	536	6.6%	9.7%
Lack of access to an Internet resource	112	216	-48.1%	-104	0.4%	1.5%
DoS/DDoS attack	23	30	-23.3%	-7	0.1%	0.2%
Unauthorised access and content modification	9	13	-30.8%	-4	0.0%	0.1%
Other incidents	2,387	1,836	30.0%	551	8.0%	12.3%

Note: DoS – Denial of Service; DDoS attack – Distributed Denial of Service attack
Source: compiled by the authors based on The number of cyberattacks in Kazakhstan has doubled (2025)

The overall cybersecurity situation in Kazakhstan in the first quarter of 2025 is characterised by explosive growth in the number of incidents. This increase is almost entirely due to the rapid spread of botnet activity, which has shifted from a secondary threat (11.8% share) to the dominant one (58.7% share). Accordingly, malicious actors changed tactics, focusing on mass covert infection (botnets) and social engineering (phishing), while direct, visible attacks such as DDoS or classic viruses decreased both in share and absolute numbers. The 101.7% rise in incidents is almost entirely driven by the rapid spread of botnet activity (an increase in share from 11.8% to 58.7%). This indicates a systemic vulnerability of the RK's network infrastructure to large-scale, covert cyberattacks, which is a critical risk against the backdrop of expanding biometric databases.

China's approach to regulating biometric technologies reflects a utilitarian philosophy in which public interests and national security prevail over individual rights (Chen & Wang, 2023). Despite key laws such as the PIPL (2021) and the Security Management Measures for the Application of Facial Recognition Technology (2025), which formally require consent and transparency, the fundamental objective of the system remains the strengthening of state control. China is the world leader in the scale and intensity of the application of biometric technologies. Law-enforcement bodies actively use them within national mass-surveillance projects such as E. Ersozoglu (2013), which envisages the installation of a vast number of cameras with facial-recognition systems (Li *et al.*, 2023). The application of these systems goes far beyond criminal justice, encompassing the monitoring of citizens' behaviour in everyday life, creating a "chilling effect" and negatively affecting freedom of expression. In addition, the close cooperation between the state and the private sector, in which data are transferred to technology companies to accelerate the training of algorithms (AI training), creates deep ethical and legal problems, contributing to a "surveillance monopoly". Table 3 details the legislative measures governing the use of biometric technologies in the PRC.

Table 3. Measures for the application of facial-recognition technologies in China

Principle	Description
Specific and sufficient necessity	Facial-recognition technologies may be used only for lawful and specific purposes, where there is "sufficient necessity"
Voluntary and explicit separate consent	The law requires "voluntary and explicit separate consent" from the individual. For minors under 14, consent from their legal guardians is required
Transparency and alternatives	Operators must inform citizens about data collection in an intelligible form and provide "other reasonable and convenient options" for verification if a person does not consent to facial recognition
Personal Information Protection impact assessment (PIPL)	Before processing begins, an impact assessment analysing the lawfulness, necessity and potential risks of the technology's use is mandatory

Source: compiled by the authors based on Z. Ruan *et al.* (2025)

The table outlines the key principles regulating the use of facial-recognition technologies in China, with an emphasis on protecting citizens' rights and privacy. The analysis shows that these principles constitute a comprehensive legal and ethical framework that seeks to strike a balance between technological progress and the protection of personal information. It covers requirements of specific and sufficient necessity, which limit the use of the technology, as well as mandatory voluntary and explicit consent to data collection, especially for vulnerable groups. In addition, the importance of transparency and the availability of alternative verification methods is emphasised, giving users a right to choose. Finally, the Personal Information Protection impact-assessment principle (under the PIPL) introduces a preventive mechanism that helps identify and mitigate potential risks before data processing begins.

Taken together, these principles create a system that demands not only technical compliance from operators but also ethical responsibility. The analysis of the approaches of Kazakhstan and China revealed key differences reflecting a philosophical divide concerning privacy rights and state control (Table 4). At first glance, the legislative systems of both countries contain provisions for personal-data protection, but their philosophical foundations differ substantially.

Table 4. Comparison of legislative models (PRC vs RK)

Comparison criterion	Kazakhstan (RK)	China (PRC)
Core philosophy	Balanced/Transitional: a combination of authoritarian control with declared international standards	Utilitarianism: the individual's rights are subordinated to "national security" and the "public good"
Regulation of biometrics	Sensitive category. Regulated by the Law "On Fingerprint and Genomic Registration" (clear collection boundaries)	Sensitive personal information (PIPL). Regulated by administrative measures on FRT (broad operational latitude)
Restrictions/Prohibition	Limited scope: focused on criminal justice and migration. Used within the "smart city" framework	Mass, all-encompassing: no clearly defined limits for "sufficient necessity" of data collection. Xueliang project
Real-time use	Used in video-surveillance systems, but application to identify political protesters is denied	Active use for security purposes and to monitor citizens' behaviour
Requirements for consent/ Alternatives	Compulsory registration for certain categories. Lack of genuine voluntariness when obtaining documents	Formal requirement for "voluntary and explicit separate consent" and the provision of alternatives

Source: compiled by the authors based on analysis of RK and PRC legislative acts mentioned in this study

According to the information in the table, the approaches of Kazakhstan and China to biometric identification were compared across five key criteria. The analysis showed that although both countries use biometric technologies, their approaches differ significantly at the philosophical level. China is guided by utilitarianism, in which the individual's rights are subordinated to national security, resulting in a mass and all-encompassing application of biometric technologies, including behavioural control. By contrast, Kazakhstan demonstrates a balanced/transitional model, concentrating the use of technologies primarily on criminal justice and migration, and clearly defining the limits of compulsory registration in the Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration" (2021). However, the compulsory provision of biometric data to obtain documents in Kazakhstan effectively nullifies the principle of voluntariness, creating a similar effect of rights restriction despite the more limited scope of application.

In the People's Republic of China, the mass roll-out of biometric technologies has led to the creation of the world's largest mass-surveillance system, raising legal and political concerns. Despite legislative attempts – such as the adoption of the PIPL (2021), aimed at curbing abuses by private companies and setting stricter consent requirements for data processing – the state's practical use of biometrics remains lightly regulated. At the same time, the Chinese authorities publicly voice reservations about the risks associated with the collection of biometric data by foreign companies. These reservations take the form of official statements and recommendations from the Ministry of Public Security and the Cyberspace Administration of China (CAC), underscoring the primacy of national security in the data sphere. Meanwhile, in the Republic of Kazakhstan, active digitalisation – albeit aimed at combating crime and increasing the efficiency of public services – has likewise produced significant problems with data leaks and has intensified state monitoring of activists. In January-March 2025 alone, 30,000 information-security incidents were recorded in the RK – twice as many as in the same period of 2024 (The number of cyberattacks…, 2025). Both countries have thus become cases for examining the complex balance between technological progress, national security and the fundamental right of citizens to privacy.

An analysis of legislation and practices relating to the use of biometrics in Kazakhstan and China has revealed key commonalities rooted in their philosophical foundations. Both countries formally recognise biometric data as a sensitive category (Law of the Republic of Kazakhstan No. 94-V (2013) and the PIPL (2021)) requiring enhanced protection. In both models, state security and the public interest take precedence over individual rights. This permits the PRC government to justify mass surveillance, and the RK government to impose mandatory registration on specific groups. Although Chinese law formally requires consent and the provision of alternatives, and although Kazakhstan offers only voluntary registration for citizens (on paper), the requirement to provide biometric data to obtain documents in the RK and the extensive state control in the PRC effectively nullify the principle of voluntariness in both jurisdictions. There are, moreover, differences in the scale of control and in the legal frameworks of biometric systems between Kazakhstan and China that reflect their philosophies of governance.

Regulation and scope of data collection. Legislative approaches to the collection of biometric data diverge sharply in focus. The Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration" (2021) sets clearly defined boundaries and a narrowly targeted compulsory collection, largely limited to offenders and migrants. This indicates an attempt by the RK government to lawfully constrain the scope of control. By contrast, China's instruments (the PIPL and the FR Measures) set broad frameworks and general principles without clear limits on the scope of FRT application in public spaces.

Use in criminal justice and monitoring. The differences are especially evident in practical deployment. In Kazakhstan, use is limited and targeted: dactyloscopic and genomic databases serve to identify unknown persons and investigate serious crimes. China, by contrast, employs mass monitoring: FRT is integrated into the "Xueliang" systems for comprehensive, real-time control and identification well beyond serious crime.

Consequences for citizens and behavioural control. The impact on civil rights also differs markedly. In Kazakhstan, risks are primarily linked to data leaks from the private sector and the threat of political monitoring (which the authorities officially deny, as after the January 2022 protests). In China, there are human-rights violations and control over social behaviour (using FRT to "shame" or fine citizens).

China exhibits a model in which technology is the primary instrument of total state control and legislation is secondary. Kazakhstan has a more limited legislative approach, but weak law enforcement and instances of political monitoring (the January protests case) render it vulnerable to the same risks as China, despite the smaller scale. Kazakhstan is therefore at a crossroads between a Western, rights-protective model and an authoritarian (PRC) model. Its weak enforcement and lack of transparency in the implementation of laws create significant risks to citizens' privacy despite the more limited scope of compulsory registration.

To address effectively the privacy and human-rights risks associated with the deployment of biometric technologies, Kazakhstan must implement a set of practical reforms focused on data security, transparency and proportionality in the use of technology. Legislative and policy improvements (strengthened enforcement). Develop effective controls against data leaks: mandatory, annual, independent cybersecurity audits should be introduced for systems storing biometric and sensitive personal data in both the public and private sectors. Audit results (excluding critical information concerning national security) should be public. National legislation should incorporate best practices from international data-security and privacy standards, including requirements analogous to the Data Protection Impact Assessment (DPIA), mandating it before any new biometric system is introduced. Sanctions and liability: administrative and criminal fines and custodial sentences should be increased for officials and organisations responsible for unauthorised collection, sale or leakage of biometric data. Fines should be proportionate to the scale of harm (for example, a percentage of annual company turnover, as under the General Data Protection Regulation (GDPR). A dedicated state fund or mandatory mechanism should also be established to compensate citizens whose biometric data have been compromised through negligence or violations.

Creation of unified standards and security mechanisms. Unified processing standards: technical standards must be developed and implemented for the collection, storage, encryption and transmission of biometric data, mandatory for all public and private operators. These should include requirements for data minimisation and pseudonymisation. New security mechanisms: multi-layered access-control systems and insider-threat monitoring should be deployed to prevent unauthorised collection and sale of data by employees via the "shadow market" (e.g., Telegram channels). In addition, safeguards against the misuse of another person's (EDS) must be strengthened, including the mandatory use of biometric two-factor authentication for the most sensitive public services.

Enhancing transparency and proportionality (human rights). The Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration" (2021) should be revised to ensure genuinely voluntary consent for biometric registration for documents. This should include a mandatory requirement to offer reasonable and convenient verification alternatives that do not require biometric data. Limits on facial-recognition technologies: the principle of proportionality should be enshrined in law to confine the use of FRT in public places strictly to the investigation of serious crimes and only with judicial authorisation. A direct statutory ban should also be introduced on using FRT to identify participants in peaceful protests, for political monitoring, or for biometric categorisation of citizens. The Ministry of Digital Development and other competent bodies should establish an ongoing open dialogue with the public, experts and human-rights organisations concerning the aims, effectiveness and potential risks of biometric systems. Detailed statistics on data breaches (including responsible parties) and on FRT deployments (e.g., number of uses, offences concerned, number of false identifications) should be published regularly.

On the basis of the comparative analysis, the findings of this study of biometric-technology deployment in the Republic of Kazakhstan and the People's Republic of China reveal universal challenges in privacy, ethics and law, with distinctive features of state control in authoritarian and transitional regimes. According to R.E. Sembiring *et al.* (2024), biometric systems pose risks to civil liberties and privacy owing to their potential for extensive state or corporate monitoring (mass surveillance). The authors emphasise that the unique characteristics of biometric data raise particular privacy concerns. Their use therefore requires stringent safeguards to prevent violations and strict adherence to the principles of informed consent and purpose limitation in processing. Related conclusions were advanced by A.N. Acquista (2020), who argued that the uniqueness of biometric data renders them especially vulnerable to abuse. Such abuse can lead to excessive profiling and continuous tracking of individuals, creating qualitatively new risks absent in the handling of traditional personal data. Accordingly, the researcher noted that effective protection of biometric data – particularly in sensitive areas such as traveller privacy – critically requires new legislation, modern technological solutions and independent oversight. P. Haley (2025) observed that recognition technologies, in particular, may be vulnerable to falsification ("spoofing") or may have high false-positive and false-negative rates. There are also significant risks

associated with algorithmic bias, which may result in discrimination, especially against certain racial, ethnic or age groups. G.-M. Țical (2025) showed that some facial-recognition algorithms demonstrate lower accuracy in identifying members of certain ethnic minorities, raising concerns about fairness and impartiality in the justice system. The transition to biometric systems thus means that the nature of justice is changing – from a predominantly reactive model that responds to crimes after they occur to a proactive and predictive one that seeks to prevent crime on the basis of large-scale data analysis. This paradigm shift requires careful analysis and debate, as it fundamentally affects the balance between public safety and individual rights to privacy and freedom. A similar position is expressed by P. Faraldo Cabana (2023): biometric technologies, particularly FRT, are increasingly used by law-enforcement bodies for identification and authentication purposes. However, their use faces technical shortcomings and legal issues related to data privacy, dignity rights and the reliability of evidence in criminal cases. The findings of I. Ben Abdel Ouahab *et al.* (2024) showed that voice-biometric technology enhances law-enforcement capabilities by providing accurate identity verification through unique vocal traits, facilitating access control and assisting crime analysis. Its integration into urban infrastructure promises improvements in public safety, though it raises privacy and ethical concerns.

The present study confirms that the deployment of biometric technologies in law enforcement in Kazakhstan and China is pursued to exploit the significant advantages of these systems, aligning with global trends towards greater efficiency and faster identification. A related view is set out by M. Sutkowski *et al.* (2024): biometric technologies are critical in law enforcement for unambiguous identification using unique personal characteristics. According to the researcher, improved quality and diversity of biometric data increase identification accuracy, markedly enhancing the effectiveness of forensic investigations and the search for missing persons. N. Girdhar *et al.* (2024) likewise emphasises that biometric technologies such as fingerprint recognition, facial recognition and DNA-based identification are crucial in law enforcement for accurate identification, strengthening criminal investigations and improving public safety through reliable and efficient identification methods.

The comparative analysis of the Kazakhstani and Chinese models highlights differences in the scale of penetration, technological self-sufficiency and functional focus of biometric-technology application. Kazakhstan shows a smaller scale, technological dependence on the PRC, and an emphasis on forensic tools, while China implements comprehensive, real-time surveillance. Z. Li *et al.* (2023) indicate that the scale and depth of biometric-technology penetration in Kazakhstan's law-enforcement sector are lower than in China's all-embracing "Xueliang" project E. Ersozoglu (2013). Despite the active digitalisation of criminal justice and the deployment of "smart city" systems in Kazakhstan, the overall integration of these technologies into social life remains markedly lower. There is also clear technological asymmetry: Kazakhstan actively cooperates with Chinese ICT companies and borrows experience, indicating a degree of technological dependence. The "smart city" model in Astana, which is based on the Chinese model, is an example of such cooperation (Li *et al.*, 2023). The analysis of technological self-sufficiency and the functional focus of biometric systems in China was the subject of H.B. Peacher (2021), which found that China is technologically independent, developing systems domestically, and that its primary focus is on real-time mass facial recognition (FRT) as an instrument of comprehensive behavioural control over the population. By contrast, Kazakhstan's law-enforcement bodies, demonstrating a certain technological dependence, predominantly focus on forensic tools – genomic and dactyloscopic registration – used in a narrowly targeted manner to investigate serious crimes and to identify unknown persons. Related views were voiced by R.A. Ayanaba (2022): biometric technologies, including facial recognition, are used by law-enforcement agencies for suspect identification, secure access and surveillance. They improve efficiency in detecting suspects and managing security, though concerns about privacy and accuracy remain significant challenges. According to D.R. Tripathi & D.K. Nishad (2020), biometric technologies in law enforcement include fingerprint recognition, facial-composite matching and automated identification systems. These applications improve suspect identification, enhance crime-scene investigation and facilitate swifter apprehension by using biological traits for automated recognition. S. Hatami *et al.* (2023) note that biometric technologies, in particular voice identification, are increasingly used in law enforcement to identify individuals through recorded voices. This method aids criminal identification and can serve as evidence in court, improving law-enforcement effectiveness against new technological crimes.

The analysis thus demonstrates a duality in the deployment of biometric technologies: on the one hand, there is consensus about their significant benefits in enhancing efficiency, speed and accuracy in suspect identification and in combating crime, confirming a shift towards a proactive and predictive model of justice; on the other, these benefits are bound up with universal risks – technical shortcomings (spoofing, false activations), ethical challenges (algorithmic bias and discrimination) and threats to civil liberties due to the potential for mass state surveillance. The comparison of the Kazakhstani and Chinese models shows that although penetration in the RK is on a smaller scale and focused on forensics, technological dependence on the PRC and the absence of robust independent oversight make Kazakhstan vulnerable to the same dangers of excessive profiling and abuse that characterise the authoritarian Chinese model. Further development of biometrics therefore requires new legislation, modern technological solutions and independent oversight to ensure an appropriate balance between public safety and the fundamental right to privacy.

Conclusions

This study has established that examining the balance between the primacy of national security, commercial benefit and the preservation of human rights amid the biometric revolution is essential for shaping effective governance strategies. The research has shown that the Republic of Kazakhstan stands at the intersection of two models – Western (rights-oriented) and authoritarian (represented by the PRC) – in which state control and security take precedence. On the basis of comparative-legal analysis and case studies, it has been established that biometric technologies are an integral part of the modernisation of law-enforcement systems, but their use depends on the political regime and legal culture. On the one hand, Kazakhstan has opted for a balanced/transitional model, confirming this in law: its approach to biometrics is limited and targeted, focusing on dactyloscopic and genomic registration for the investigation of serious crimes, the identification of unknown persons and migration control. This underscores a somewhat limited yet directed application compared with China. The deployment of biometric technologies in the PRC, grounded in utilitarian philosophy, has enabled the state to create a comprehensive and integrated mass-surveillance system ("Xueliang"). This system is used for social control and intensified monitoring of ethnic minorities, which, in turn, constrains the exercise of civil liberties and freedom of expression.

The findings also show that the implementation of biometric systems in Kazakhstan is accompanied by significant privacy risks. This is manifested in the critical threat of data leaks in 2019 and 2025 and in the absence of genuine voluntariness during compulsory registration for obtaining documents. In addition, there is a risk of the improper use of technologies for political monitoring (the January 2022 protests case). In this context, it has been demonstrated that weak law enforcement and a lack of transparency are shared problems in both countries. In Kazakhstan, this is the result of the early stage of legal implementation, confirmed by the explosive 101.7% rise in cyber incidents in Q1 2025; in China, it is part of a systematic absence of public oversight, which enables unchecked technological deployment.

To address the identified risks effectively, a set of recommendations has been developed, including reforms to strengthen cybersecurity, increase penalties for data leaks and create a compensation fund. It is also proposed to revise legislation to ensure proportionality and to restrict the use of technologies, particularly FRT, strictly to the investigation of serious crimes. A limitation of this study is its qualitative character and reliance on open sources, which did not allow quantitative conclusions about the scale of implementation, especially in the PRC. Future research could include a quantitative analysis of the effectiveness of enforcing data-protection laws in Kazakhstan, as well as a comparison of Kazakhstan's approach with European regulatory models (GDPR) focused on data protection and human rights.

Acknowledgements

None.

Funding

None.

Author Contributions

P. Yu and S. Jing conducted the literature review, collected data, and performed the analysis. S.K. Dhillon conceived and supervised the study. P. Yu prepared the initial manuscript draft. S. Jing contributed analytical tools and assisted with data processing. S.K. Dhillon and S. Jing revised the manuscript. All authors approved the final version of the manuscript.

Conflict of Interest

None.

References

[1] Acquista, A.N. (2020). Biometrics takes off–fight between privacy and aviation security wages on. *Journal of Air Law and Commerce*, 85(3), 475-569.

[2] Ayanaba, R.A. (2022). Image-assisted biometric identification. *Advances in Multidisciplinary and Scientific Research Journal*, 1(1), 131-138. doi: 10.22624/aims/crp-bk3-p22.

[3] Baifat, F.R., & Satoto, S. (2024). Legal challenges and uncertainties: The use of biometric information technology in immigration control. *International Journal of Multidisciplinary Research and Analysis*, 7(1), 328-332. doi: 10.47191/ijmra/v7-i01-40.

[4] Ben Abdel Ouahab, I., Elaachak, L., Bouhorma, M., Alluhaidan, Y.A., & Zafar, B. (2024). Voice biometric technology: Enhancing public safety and security in smart cities. In *2024 mediterranean smart cities conference (MSCC)* (pp. 1-6). Tetuan: IEEE. doi: 10.1109/mscc62288.2024.10697089.

[5] Bertayeva, K., Onaltayev, D., Akimbayeva, K., & Issaeva, A. (2024). Digitalization of Kazakhstani banks. *Bulletin of "Turan" University*, 4, 62-74. doi: 10.46914/1562-2959-2024-1-4-62-74.

[6] Buralkieva, D. (2022). *Biometric data collection: What risks might Kazakhstanis face?* Retrieved from https://cabar.asia/en/biometric-data-collection-what-risks-might-kazakhstanis-face.

[7] Chen, W., & Wang, M. (2023). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. *Telecommun Policy*, 47(2), article number 102482. doi: 10.1016/j.telpol.2022.102482.

[8] Choudhry, M.D., Sundarrajan, M., Jeevanandham, S., & Saravanan, V. (2024). Security and privacy issues in AI-based biometric systems. In S. Balasubramaniam, S. Kadry, A. Prasanth & R.K. Dhanaraj (Eds.), *AI based advancements in biometrics and its applications* (pp. 85-100). Boca Raton: CRC Press. doi: 10.1201/9781032702377-5.

[9] Datta, P., Bhardwaj, S., Panda, S.N., Tanwar, S., & Badotra, S. (2020). Survey of security and privacy issues on biometric system. In B. Gupta, G. Perez, D. Agrawal & D. Gupta (Eds.), *Handbook of computer networks and cyber security* (pp. 763-776). Cham: Springer. doi: 10.1007/978-3-030-22277-2_30.

[10] Dyussembekova, Z. (2021). *Kazakhstan creating criminal DNA database*. Retrieved from https://astanatimes.com/2017/06/kazakhstan-creating-criminal-dna-database/.

[11] Dzhaksybekova, G., & Pulatov, I. (2020). Features and prospects of biometric security measures in operations with payment bank cards. *Eurasian Union Scientists*, 6(4(73)), 47-55. doi: 10.31618/ESU.2413-9335.2020.6.73.688.

[12] Ersozoglu, E. (2013). *The Xeuliang project: Expansion of China's state surveillance programme.* Retrieved from https://greydynamics.com/the-xeuliang-project-expansion-of-chinas-state-surveillance-programme/.

[13] Faraldo Cabana, P. (2023). Technical and legal challenges of the use of automated facial recognition technologies for law enforcement and forensic purposes. In A. Završnik & K. Simončič (Eds.), *Artificial intelligence, social harms and human rights. Critical criminological perspectives* (pp. 35-54). Cham: Palgrave Macmillan. doi: 10.1007/978-3-031-19149-7_2.

[14] Girdhar, N., Sahu, M., & Lin, C.-C. (2024). Emerging trends in biomedical trait-based human identification: A bibliometric analysis. *SLAS Technology*, 29(3), article number 100136. doi: 10.1016/j.slast.2024.100136.

[15] Gritsenko, D., Trochev, A., & Vehkalahti, K. (2025). Public perception of algorithmic policing in a non-democratic context: Evidence from Kazakhstan. *Policing and Society*, 35(10), 1357-1376. doi: 10.1080/10439463.2025.2489954.

[16] Haley, P. (2025). The impact of biometric surveillance on reducing violent crime: Strategies for apprehending criminals while protecting the innocent. *Sensors*, 25(10), article number 3160. doi: 10.3390/s25103160.

[17] Hatami, S., Rahimi, F., Aghaei, E.A.M., & Shahsavandi, E. (2023). Legal challenges of biometric identity systems in law enforcement of recognition policy (voice): A case study of siip in Europe. *Modern Technologies Law*, 4(8), 101-118. doi: 10.22133/mtlj.2023.382577.1160.

[18] Kumar, S. (2024). Biometric systems security and privacy issues. In A. Selwal, D. Sharma, M. Mann, S. Chakraborty, V.E. Balas & O.E. Lieh (Eds.), *Leveraging computer vision to biometric applications* (pp. 68-91). New York: Chapman and Hall/CRC. doi: 10.1201/9781032614663-4.

[19] Law of the People's Republic of China "Personal Information Protection Law" (PIPL). (2021, August). Retrieved from https://personalinformationprotectionlaw.com/PIPL/hello-world/.

[20] Law of the Republic of Kazakhstan "On Fingerprint and Genomic Registration". (2021, January). Retrieved from https://www.gov.kz/situations/324/intro?lang=en.

[21] Law of the Republic of Kazakhstan No. 271-IV "On the Prevention of Offences". (2025, July). Retrieved from https://online.zakon.kz/Document/?doc_id=30657323&show_di=1.

[22] Law of the Republic of Kazakhstan No. 94-V "On Personal Data and Their Protection". (2013, May). Retrieved from https://adilet.zan.kz/kaz/docs/Z1300000094.

[23] Li, Z., Guo, Y., Yarime, M., & Wu, X. (2023). Policy designs for adaptive governance of disruptive technologies: The case of facial recognition technology (FRT) in China. *Policy Design and Practice*, 6(1), 27-40. doi: 10.1080/25741292.2022.2162248.

[24] Muratuly, D., Denissova, N., Krak, Y., & Apayev, K. (2022). Biometric authentication of students to control the learning process in online education. *Scientific Journal of Astana IT University*, 10(10), 22-32. doi: 10.37943/lyfw8581.

[25] Peacher, H.B. (2021). Regulating facial recognition technology in an effort to avoid a minority report like surveillance state. *Marquette Intellectual Property & Innovation Law Review*, 25(1), 20-40.

[26] Ruan, Z., Jiang, C., Chen, X., & Wang, M. (2025). *China: New rules issued to further regulate application of face recognition technology in China*. Retrieved from https://connectontech.bakermckenzie.com/china-new-rules-issued-to-further-regulate-application-of-face-recognition-technology-in-china/.

[27] Satubaldina, A. (2025). *What we know about data leak affecting 16 million Kazakh citizens*. Retrieved from https://astanatimes.com/2025/07/what-we-know-about-data-leak-affecting-16-million-kazakh-citizens/.

[28] Security Management Measures for the Application of Facial Recognition Technology. (2025, March). Retrieved from https://www.gov.cn/zhengce/zhengceku/202503/content_7016075.htm.

[29] Sembiring, P.E., Ramli, A.M., & Rafianti, L. (2024). Implementasi desain privasi sebagai pelindungan privasi atas data biometrik. *Veritas et Justitia: Jurnal Ilmu Hukum*, 10(1), 127-152. doi: 10.25123/vej.v10i1.7622.

[30] Singh, G., Bhardwaj, G., Singh, S.V., & Garg, V. (2021). Biometric identification system: Security and privacy concern. In S. Awasthi, C.M. Travieso-González, G. Sanyal, & D. Kumar Singh (Eds.), *Artificial intelligence for a sustainable Industry 4.0* (pp. 245-264). Cham: Springer. doi: 10.1007/978-3-030-77070-9_15.

[31] Smart Cities Challenges and Opportunities. (n.d.). Retrieved from https://surl.li/qzgkdp.

[32] Sutkowski, M., Pakuła, A., & Paśko, S. (2024). Modern system for face biometrics data registration. *Internal Security*, 15(2), 73-82. doi: 10.5604/01.3001.0054.4770.

[33] The number of cyberattacks in Kazakhstan has doubled. (2025). Retrieved from https://profit.kz/news/70516/Kolichestvo-kiberatak-v-Kazahstane-viroslo-srazu-vdvoe/.

[34] Țical, G.-M. (2025). Facial recognition and biometric systems: Benefits and challenges for law enforcement. *Land Forces Academy Review*, 30(2), 249-259. doi: 10.2478/raft-2025-0024.
[35] Toqmadi, M., & Zakharchenko, N. (2021). I agree to terms and conditions: Negotiating privacy online in Central Asia. *JeDEM – EJournal of eDemocracy and Open Government*, 13(1), 71-100. doi: 10.29379/jedem.v13i1.633.
[36] Tripathi, D.R., & Nishad, D.K. (2020). Biometric authentication systems: A survey. *Turkish Journal of Computer and Mathematics Education*, 11(3), 2878-2884. doi: 10.61841/turcomat.v11i3.14653.
[37] Utegen, D., & Rakhmetov, B.Z. (2023). Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models. *Journal of Digital Technologies and Law*, 1(3), 825-844. doi: 10.21202/jdtl.2023.36.
[38] What you need to know about dactyloscopy and genome registration of citizens. (2024). *Electronic government of the Republic of Kazakhstan*. Retrieved from https://egov.kz/cms/en/articles/for_foreigners/dactyloscopy_genome_registration.
[39] Zhang, J. (2024). The shield of privacy in the digital age: The clash between facial recognition technology and personal information protectioncase analysis and strategy discussion. *Advances in Social Behavior Research*, 8(1), 66-77. doi: 10.54254/2753-7102/8/2024066.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.431(575)

Article's History:
Received: 04.07.2025; Revised: 13.11.2025; Accepted: 16.12.2025

Human trafficking in the Republics of Kazakhstan, Uzbekistan, and Kyrgyzstan: Lessons from Central Asia

Bakyt Kakeshov*
Kyrgyz National University named after Jusup Balasagyn
720033, 547 Frunze Str., Bishkek, Kyrgyzstan
https://orcid.org/0000-0003-1570-1072

Abstract. The study aimed to assess human trafficking response strategies in the Republic of Kazakhstan, the Republic of Uzbekistan, and the Republic of Kyrgyzstan, with an emphasis on cross-border cooperation efforts in Central Asia. The goal was achieved through the use of the comparative legal analysis and case study method involving F.M. and others versus Russia and repatriating Kazakh nationals from Myanmar and Thailand in February-April 2025. Based on the comparative legal analysis, it was concluded that all countries in the region had adopted comprehensive rooted in the Palermo Protocol legal frameworks but varied considerably in their implementation strategies. While the Republic of Kazakhstan and the Republic of Kyrgyzstan had formalised national referral mechanisms and partnerships with non-governmental organisations, the Republic of Uzbekistan had launched structured victim assistance networks. Despite different approaches to preventing and investigating human trafficking, all countries in the sample experienced similar difficulties in implementing legislative initiatives and supporting cross-border interaction to counter human trafficking. The cross-border interaction was hindered by such factors as political instability and at-border conflicts, corrupted state institutions, ineffective implementation of legal frameworks, hindered data sharing processes, cultural and societal peculiarities, and geopolitical dynamics. The recommendations were to support international cooperation through transnational unions and multilateral platforms, enhance transparency and accountability of the law enforcement institutions, harmonise national legislation with international standards, and launch the boarder International Organisation for Migration-coordinated safe fund. The obtained results can be used to reduce the incidence of and rehabilitate the victims of cross-border human trafficking

Keywords: gender inequality; systemic problems; cross-border cooperation; at-border conflicts; safe funds

Introduction

Human trafficking has become a common problem around the world, whose medium and long-term consequences require further examination. Globalisation, which has opened up many opportunities for development, has also brought with it a series of challenges. One crucial challenge is related to the use of legal mechanisms to detect, combat, and prevent human trafficking at the international level. Taking into account the absence of a unified legal framework, the selected research topic is considered relevant.

According to the United Nations Office on Drugs and Crime (2024) report, the period between 2021 and 2023 was associated with a sharp increase in the number of detected cases of human trafficking. The cited experts, in particular, reported a 43% increase in the number of detected cases, as compared to 2020, which they partly attributed to the improved mechanisms of human trafficking detection. A. Dyussenova *et al.* (2024), however, stressed that despite the progress achieved, in some regions, including Central Asia, human trafficking remains a major transnational issue. A. Dyussenova *et al.* further stressed that specific population groups, such as migrant workers, women, and children, are at elevated risks of being trafficked. This statement is consistent with the data of the Royal Thai Embassy in Astana (2025), according to which, the Republic of Kazakhstan has a long-running trafficking network targeting vulnerable population groups. The report further mentioned 19 cases of newborn trafficking registered in the country in 2024, and 15 individuals held accountable

Suggest Citation:
Kakeshov, B. (2025). Human trafficking in the Republics of Kazakhstan, Uzbekistan, and Kyrgyzstan: Lessons from Central Asia. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 15-23.

*Corresponding author

during the same period. The cited data suggested there was the discrepancy between the number of human trafficking cases committed and investigated, which indicated the gravity of the problem.

The risk factors for human trafficking have been explored in recent research, including the study of R.E. Klabbers *et al.* (2023). Based on the analysis of qualitative data retrieved from the interviews with 108 victims of forced labour and sexual violence, the authors concluded that the major risk factors for human trafficking included poverty, limited education, and lack of support underpinning social vulnerability. The study of L. Belaid *et al.* (2024) concerned the risk factors of human trafficking in Africa, where 5.2 people for every 1,000 people were identified as modern slaves. The researchers also explain the increase in human trafficking to the variety of forms it takes, as well as its interrelation with other forms of exploitation. According to Z. Khan *et al.* (2022), whose study involved a systematic review of 64 relevant studies, human trafficking in Central Asia was mainly due to poverty and unemployment, as well as environmental and manmade disasters. Z. Khan *et al.* further mentioned that corruption and weak policies aggravated human trafficking problem in the region. The significance of strong policies for human trafficking prevention was also stressed by F. Fadilla *et al.* (2022) whose theoretical model for combating human trafficking involved cooperation between the central government and local institutions dealing with the issue. The role of government initiatives in combating human trafficking was also emphasised by R.C. Santos *et al.* (2024) who studied the peculiarities of sexual and labour exploitation in the Amazonas region. As explained by R.C. Santos *et al.*, residents of remote and border areas were at a disproportionate risk of human trafficking due to the existence of the "sponsorship" tradition implying deception of vulnerable population groups on the part of their close people. Upon conducting an umbrella review of recent research, N. Proia-Lelouey & G. Desquesnes (2025) concluded that young people aged 12 to 14 years belonged to the highest risk group and required government support to escape human trafficking. As suggested by N. Proia-Lelouey & G. Desquesnes, government support preconditions the operation of a network of intermediary institutions, including schools and welfare services. F. Nicodemi & C. Cirillo (2024) analysed the experience of Italy, where government initiatives facilitated coordination between the asylum and anti-trafficking systems. This coordination was mainly due to the implementation of the Guidelines for Asylum Authorities, European Trafficking Directive, and other legal documents articulating the detection and prevention of human trafficking at the national and international levels.

Although human trafficking has been covered extensively in previous studies, little is known about the initiatives launched to combat human trafficking in Central Asia, which suggests the selected topic is relevant. Considering the detected gap, it was decided to examine the strategies to detect and prevent human trafficking in the Republic of Kazakhstan, the Republic of Uzbekistan, and the Republic of Kyrgyzstan. The goal involved accomplishing the following objectives: to compare the legal mechanisms of combating human trafficking in Central Asia; to analyse the peculiarities of cross-border cooperation in detecting and preventing human trafficking; and to suggest strategies to reduce the incidence of human trafficking in the Central Asia region.

Materials and Methods

The study relied on the sample of three countries located in the Central Asian region: The Republic of Kazakhstan, the Republic of Uzbekistan, and the Republic of Kyrgyzstan. The countries were added to the sample based on their belonging to a coherent regional system sharing similar legacies, cross-border migration and trafficking problems, and comparable levels of institutional capacity. The republics in the sample, however, displayed enough variation in political and economic contexts, which facilitated meaningful comparative analysis.

Comparative legal analysis was used as the main data collection tool in the study and incorporated the following documents: Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention against Transnational Organised Crime (Office of the Commissioner for Human Rights, 2000); Article 128 of the Criminal Code of the Republic of Kazakhstan No. 167 (1997); Article 135 of the Criminal Code of the Republic of Uzbekistan No. 2012-XII (1994); Law of the Republic of Uzbekistan No. ЗРУ-154 (2008); and Law of Kyrgyzstan No. 55 (2005). The selected legal provisions were compared across the following criteria: definition of trafficking; scope of criminalisation; penalties for human trafficking; victim protection strategies; human trafficking prevention measures; peculiarities of coordination and presence of coordination bodies; special provisions for children; and international cooperation. The criteria were selected because they comprehensively detect the key legal dimensions necessary to evaluate the effectiveness and completeness of anti-trafficking frameworks across countries.

The research study relied on the data retrieved from the United Nations Office on Drugs and Crime (2022; 2024) Global reports of trafficking in persons. The study also involved the analysis of the following case studies: F.M. and others versus Russia (European Court of Human Rights, 2024) and repatriation from Myanmar (The Republic of the Union of Myanmar Ministry of Information, 2025). The former case included five applicants – three from Kazakhstan and two from Uzbekistan – claiming they were trafficked to Moscow and subjected to forced labour. The latter case involved removing hundreds of foreign nationals, including Kazakhs, from Myanmar and processing them via the Myanmar-Thailand Friendship Bridge to their respective countries. The selected cases were analysed in terms of the cross-border cooperation in detecting, combating, and preventing human trafficking. The study of the

factors shaping such cooperation was carried out to design the recommendations to facilitate timely detection, effective struggle against, or prevention of human trafficking in the Central Asian region.

Results

Combating human trafficking in Central Asia

Human trafficking remains a systematic problem in Central Asia, with numbers varying considerably across the countries. In the Republic of Kazakhstan, for example, there was reported a considerable decrease in the number of offences in human trafficking – from 304 persons in 2017 to 111 in 2022 (United Nations Office on Drugs and Crime, 2022). Despite this decrease, national anti-trafficking efforts are considered insignificant to stop exploitation of vulnerable population groups. In 2024, Kazakh police launched investigations into 15 cases of human trafficking compared to 26 in 2022 (U.S. Department of State, 2024). The same official report indicated a major decrease in the number of human trafficking cases prosecuted by the government – from 18 in 2022 to 5 in 2024. The analysis of previously conducted studies further indicated disparities in human trafficking at the national and cross-border levels: people living in the regions that experience climate changes are at a disproportionate risk of human trafficking (Kovaleva *et al.*, 2023); and women constitute up to 60% of all cases of human trafficking (Ariail *et al.*, 2024). Considering the context of the Republic of Kazakhstan, it was concluded that local governments must do more to ensure the protection of vulnerable population groups, as well as the rehabilitation of individuals who have become the victims of human trafficking. The expected efforts, in particular, involve legislative initiatives aimed at combating and preventing human trafficking. The key legislative initiatives adopted in the Central Asian region were documented in the Table 1.

Table 1. Legislative initiatives to combat human trafficking in Central Asia

Provision / Aspect	Kazakhstan	Uzbekistan	Kyrgyzstan
Primary Law	Criminal Code of the Republic of Kazakhstan (Art. 128)	Law of the Republic of Uzbekistan "On Combating Trafficking in Persons"	Law of the Republic of Kyrgyzstan "On Preventing and Combating Trafficking in Human Beings"
Definition of trafficking	Incorporates Palermo Protocol definition (recruitment, transport, transfer, harbouring, receipt for exploitation)	Broad definition aligned with Palermo; explicitly covers sexual and labour exploitation	Palermo Protocol-aligned definition covering exploitation of adults & children
Criminalisation / scope	Criminalises both sex and labour trafficking, adult & child victims	Same, with explicit provisions for children and forced labour	Criminalises sex and labour trafficking, also regulates prevention activities
Penalties	3-7 years (basic), up to 15+ years for aggravated/child trafficking or organised groups	3-8 years basic, higher for aggravating circumstances (child victims, organised groups)	3-8 years, up to 15+ for aggravating circumstances
Victim protection / assistance	National Referral Mechanism, shelters, state social services; but limited capacity in rural areas	Law defines victim status, confidentiality, rehabilitation centre network (with NGOs)	Formal NRM procedures, government + NGO shelters, legal aid
Prevention measures	Awareness campaigns, regulation of recruiters, periodic national action plans	Government-led awareness, hotlines, licensing of recruitment agencies	Annual prevention programs, information campaigns in high-risk regions
Coordination / bodies	Interagency commissions at national & regional level; MoI lead	National Interagency Commission; specialised units in law enforcement	National Council / Coordinating Committee; authorised agency under the Government
Special provisions for children	Separate article + enhanced penalties; referral to child protection services	Explicit child-trafficking provisions; priority in rehabilitation	Explicit child-protection clauses, referral to child-welfare agencies
International cooperation	Provides for extradition, mutual legal assistance; member of Palermo Protocol	Same; bilateral MoUs with neighbours	Party to Palermo; regional cooperation with OSCE/UNODC, cross-border SOPs in progress

Note: CC – Criminal Code; MoI – Ministry of Internal Affairs; MoU – Memorandum of Understanding; NAP – National Action Plan; NGO – Non-governmental organisation; NRM – National Referral Mechanism; OSCE – Organisation for Security and Co-operation in Europe; SOP – Standard Operating Procedure; UNODC – United Nations Office on Drugs and Crime

Source: compiled by the author of the research based on ADS Database (1994), Criminal Code of the Republic of Kazakhstan No. 167 (1997), Office of the Commissioner for Human Rights (2000), Law of Kyrgyzstan No. 55 (2005), Law of the Republic of Uzbekistan No. ЗРУ-154 (2008)

Based on the table, it was concluded that the five countries of the Central Asian region have established comprehensive legal frameworks to combat human trafficking that broadly align with the Palermo Protocol. Each country criminalises both sexual and labour trafficking, including provisions for adult and child victims, with penalties

increasing for organised groups or aggravating circumstances. All states have enacted special measures for children, such as separate criminal provisions and referral to child protection or social reintegration services. Preventive measures are also common across the region, including public awareness campaigns, information dissemination, and regulation of recruitment agencies, often implemented through periodic national action plans. Additionally, all countries have created interagency bodies or commissions to coordinate anti-trafficking efforts, with the MoI or equivalent law-enforcement authorities playing a central role.

Despite these broad similarities, there are notable differences in implementation and institutional capacity. The Republic of Kazakhstan and the Republic of Kyrgyzstan have formalised NRMs and partnerships with NGOs, though the Republic of Kazakhstan faces capacity gaps in rural areas. The Republic of Uzbekistan maintains structured victim assistance networks, but observers a comparatively weak enforcement and limited transparency. International cooperation is generally established through the Palermo Protocol and bilateral MoUs, but the extent and operationalisation vary: The Republic of Kyrgyzstan and the Republic of Kazakhstan have more developed cross-border coordination mechanisms and engagement with OSCE/UNODC, while the Republic of Uzbekistan rereports minimal active cooperation.

Anti-trafficking initiatives in selected countries

Recent cases, including F.M. and Others versus Russia, provided an understanding of the strategies adopted in the Republic of Kazakhstan to combat human trafficking and rehabilitate its victims. The mentioned case involved three applicants from the Republic of Kazakhstan and two applicants from the Republic of Uzbekistan who alleged they were trafficked to Moscow, Russian Federation, and subjected to forced labour (European Court of Human Rights, 2024). The European Court of Human Rights (ECHR) concluded that Russia violated Article 4 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention against Transnational Organised Crime (Office of the Commissioner for Human Rights, 2000), which prohibits slavery and forced labour. The ECHR also highlighted the state's obligations to protect foreign nationals from trafficking, including the duty of investigation and international cooperation.

A closer inspection of the case revealed several systemic failures that made trafficking of Kazakhstan citizens possible; and one of these failures involved the inadequate investigation of the case. Based on the ECHR report, inadequate investigation took the forms of delayed responses, failure to properly collect evidence, limited victim interviews, and absence of follow-up on leads (European Court of Human Rights, 2024). Another systemic failure was insufficient protection of foreign victims who were not provided with appropriate shelter, legal assistance, or protective measures. Furthermore, inspection of the case revealed the lack of cross-border engagement as Russian authorities did not liaise Kazakh or Uzbek authorities to identify victims, trace traffickers, or facilitate victims' repatriation and protection.

The case of Kazakh citizens being subjected to forced labour in Russia provided insights into managing cross-border cooperation for the effective detention, combating, and preventing human trafficking. The analysed case emphasised the significance of proactive cross-border mechanisms that need to be implemented in source countries; and the main idea behind having such mechanisms is that countries should not wait for victim complaints to investigate the instances of human trafficking (European Court of Human Rights, 2024). Another lesson learned from the case was about the significance of integrating (NRMs) with international cooperation to support cross-border detection and prevention of human trafficking. Based on the analysed case, integration is possible if NRMs contain articulated procedures for dealing with foreign victims, such as immediate notification of home-country authorities, access to shelters, and coordinated repatriation of victims. In addition to the already mentioned lessons, the analysed case indicated the need for formalised agreements, taking the forms of (MoUs), and legal frameworks. An inspection of F.M. and others versus Russia allowed to conclude that bilateral MoUs or treaties between source and destination states precondition clarified responsibilities, streamlined investigations, and adequate protection of victims' rights. From the legal point of view, it is essential that domestic legislation explicitly provides for cooperation in cross-border trafficking cases.

Another case highlighting the significance of cross-border cooperation in combating human trafficking involved repatriation of Central Asian victims from Myanmar to Thailand in February-April 2025 (The Republic of the Union of Myanmar Ministry of Information, 2025). The repatriated Kazakh residents fell the victims of criminal gangs that had trafficked people from over 20 nationalities and engaged them into illegal online operations generating billions annually in the South East region. In contrast to the above analyse case, this one demonstrated greater involvement on the part of Central Asian states, including the Republic of Kazakhstan, the Republic of Uzbekistan, and the Republic of Kyrgyzstan, that provided assistance in identifying and assisting their residents. In April 2025, Kazakhstan identified and repatriated four of its citizens who were temporarily kept in overcrowded shelters in Thailand. According to the Republic of the Union of Myanmar Ministry of Information (2025), some of those victims required healthcare assistance, so Thai authorities required repatriating countries' officials to be present for health checks before return.

The selected case revealed several issues in cross-border cooperation aimed at combating and preventing human trafficking. The fact that hundreds of victims spent a long time waiting for repatriation indicated the absence of pre-agreed, operational consular standard operation procedures. Many countries, including the Republic of

Kazakhstan, had to mobilise their ad hoc teams, which slowed repatriation and increased the time that victims of human trafficking were forced to spend in repatriation camps. The repatriation procedure was slowed down due to the lack of a unified electronic database, which means that officials had to be physically present at borders for paperwork. The case of repatriating Kazakh citizens also revealed that the approaches to managing human trafficking might lack the balance between the rapid return of victims and their protection. The pressure to repatriate *en masse* means that victims could not receive sufficient physical, psychological, and social screening which increases the risk of re-trafficking or health crises. Furthermore, the analysed case revealed limited capacity and funding gaps in addressing human trafficking issues, especially when hundreds of people are waiting repatriation. The Ministry of International Affairs' urgent funding appeal suggests that the existence of political will does not make the country immune to unforeseen expenses associated with high-profile human trafficking cases. From an economic point of view, repatriation and reintegration of the victims of human trafficking requires predictable financing and elaborated logistic chains.

The case of repatriated Kazakh citizens suggested several lessons to be incorporated into planning cross-border cooperation in combating human trafficking. The first lesson was about the need for pre-negotiated consular SOPs and MoU templates, which might help reduce processing time at border camps by ensuring officials are present quickly for immigration and health checks. An inspection of the selected case revealed that as of 2025, there is no bilateral MoU template covering identity verification, temporary shelter handover, quarantine and health protocol, expedited travel documentation, and other issues connected to managing human trafficking in the region. The analysed case also revealed the needed for embedding consular rapid-response teams into (NAPs) and (NRMs). The examined case allowed to assume that embedding rapid-response teams into NAPs and NRMs might tie diplomatic action to victim-referral pathways rather than ad hoc returns, hence, reduces the time that victims of human trafficking spend in at-border camps and lowers the risk of re-trafficking. The analysed cases proved that nationals of the Republic of Kazakhstan continue falling victims of human trafficking, even though strategies are being implemented to address this illegal practice. The inspection of individual cases allowed to conclude that human trafficking remains a problem in Central Asia due to insufficient cross-border cooperation, which results in poorly coordinated efforts to detect and repatriate victims, as well as identify and prosecute those involved in human trafficking.

Cross-border cooperation against trafficking in Central Asia

The above analysed cases allowed to assume there were multiple barriers to cross-border cooperation in combating human trafficking in Central Asia. The crucial barriers and the forms they are likely to take in the region are documented in Table 2 below.

Table 2. Hindrances to cross-border cooperation in preventing human trafficking in Central Asia

Factor	Description/Example
Political tensions and border disputes	Ongoing territorial disputes and unstable border relations reduce trust and impede joint anti-trafficking operations.
Corruption and institutional weakness	Corruption among officials undermines law enforcement and victim protection; some authorities may be complicit in trafficking.
Weak legal frameworks and/or their poor implementation	Laws exist but enforcement is inconsistent; insufficient victim identification and limited consular training.
Limited capacity and resources	Law enforcement lacks training, personnel, or infrastructure for effective cross-border operations.
Lack of data sharing and ineffective coordination mechanisms	No standardised protocols for information exchange; joint operations are fragmented.
Cultural and societal factors	Victims reluctant to report abuse due to stigma, fear of authorities, or legal consequences.
Geopolitical dynamics	Foreign policy priorities and regional alliances affect willingness to cooperate.

Source: compiled by the author of the research based on A. Khamzin *et al.* (2023), B.E. Kooffreh (2023), S. Chatterjee (2024), I. de Vries *et al.* (2024), F. Indraswari (2024), G. Mercera *et al.* (2024), P. Sundram (2024)

The table suggests that the effectiveness of cross-border cooperation in combating human trafficking in Central Asia is hindered by a combination of political, institutional, and socio-cultural factors. Persistent political tensions and unresolved border disputes foster mistrust between neighbouring states, obstructing coordinated law enforcement and intelligence-sharing efforts. Corruption and weak institutions further exacerbate the problem, as officials' complicity or negligence undermines anti-trafficking initiatives and erodes victims' confidence in state protection mechanisms. Although legal frameworks often exist on paper, their implementation is uneven, with deficiencies in victim identification, inadequate consular training, and poor enforcement of penalties. Limited capacity and resources, including shortages of trained personnel and modern infrastructure, constrain the operational reach of anti-trafficking agencies. The absence of standardised data-sharing protocols and the fragmentation of coordination mechanisms prevent the establishment of a unified regional response. Moreover, cultural and societal stigmas discourage victims from reporting exploitation, while fear of legal repercussions or mistrust of authorities perpetuates

underreporting. Finally, broader geopolitical dynamics – such as shifting alliances and competing foreign policy interests – shape the level of political will and regional cooperation, often subordinating human trafficking issues to other strategic priorities. Considering the detected gaps, recommendations were developed to enhance the effectiveness of addressing human trafficking strategies in Central Asia.

The first recommendation was to address political tensions and border disputes that are present between neighbouring republics. The suggestion is grounded in the fact that political tensions and armed conflicts hinder the deployment of neutral, technical-working groups on cross-border trafficking issues. The functioning of such working groups, however, can be supported through cooperation between the United Nations Office on Drugs and Crime and the MoIs that will establish bilateral taskforces between the countries focusing strictly on human trafficking in high-risk areas. The technical-working groups might also benefit from the involvement of multilateral platforms, including the Shanghai Cooperation Organisation, Organisation for Co-operation in Europe, and Collective Security Treaty Organisation. The multilateral platforms can be used to host confidence-building meetings and to broker agreements even when territorial disputes and political tension persist.

Another suggestion was to combat corruption and institutional weakness through enhanced transparency and accountability. In some Central Asian countries, including the Republic of Uzbekistan, limited transparency and low accountability result in recurring human trafficking. The detected issue can be addressed by establishing independent anti-corruption units and hotlines, where citizens and NGOs can report human trafficking, get referred to experts, or access a status report on the ongoing investigation. The anti-corruption units have been successfully launched in the Republic of Kazakhstan where they take the form of the OECD's Anti-Corruption Network. The Republic of Uzbekistan and other Central Asian countries can take advantage of Kazakhstan's experience by launching a transparent audit system and ensuring an ongoing review of anti-trafficking funds and operations by external observers.

It was also recommended to strengthen legal frameworks by harmonising anti-human trafficking laws and procedures across the borders. The study revealed that although all five countries tend to align their legislation with the Palermo Protocol, they have varying definitions for human trafficking and victim protection norms. The detected inconsistencies hinder cross-border cooperation in preventing human trafficking and might be addressed through harmonised legislation rooted in the European Union Anti-Trafficking Directive. The harmonised legislation also implies that consular officers and labour attaches are trained to proactively identify and support their nationals, especially labour migrants who are at a disproportionate risk of becoming victims of human trafficking.

In addition to the recommended strategies, it was also suggested to address limited capacity and resources which are among the reasons for persistent human trafficking in Central Asia. The afore cited repatriation of Kazakh nationals revealed that countries lack resources to promptly assist the repatriation of large groups of their people who have fallen the victims of trafficking. The resources can be accumulated by launching a jointly funded, IOM-coordinated (International Organisation for Migration) safe funds at state borders. It was also suggested that joint donor-funded capacity building for border guards and police can mitigate the resource inefficiency issue while boosting investigative skills and case coordination. From this perspective, Central Asian countries can model the OSCE's "Combating Trafficking Along Migration Routes" initiative that has proven effective in accumulating resources, sharing data, and facilitating cross-border investigation (Organisation for Security and Co-operation in Europe, 2025). It was also suggested to study and adopt the experience accumulated by EUROPOL (2025) Joint Investigation Teams deployed in Europe. Similar to their European colleagues. Central Asian border guards and police officers could join mobile mixed-country investigative teams to respond to cross-border trafficking networks. Hence, European experience might be helpful in boosting the effectiveness of cross-border cooperation to combat human trafficking in Central Asia. The adoption of such an experience involves cooperating to address political tension and cross-border conflicts, harmonising human trafficking laws, launching joint funds and capacity building initiatives.

Discussion

This study elaborated on the fact that persistent human trafficking reveals systemic problems of a particular country or region. This idea was, for example, elaborated in the Kyrgyz contexts, where human trafficking was partly attributed to political tension and at-border conflicts. The contribution of systemic political, economic, and social problems to human trafficking was also confirmed in previous studies, including M.A. Hansen & I. Johansson (2025). The cited experts surveyed a nationally representative sample of 776 Americans and discovered that female respondents were more likely to associate human trafficking with social vulnerability. Statistics provided by K.A. McKee (2024) stressed that gender disparity in human trafficking was not just a question of perception, but also of objective data. According to K.A. McKee, over 1 million women and children were trafficked every year, and over 50,000 of them were forcibly moved to the United States. The cited data allowed to assume that human trafficking was reported even in high-income countries, while gender inequality was among the factors aggravating this problem. Similar to previous studies, this research confirmed the contribution of systemic issues, including gender inequality, to the emergence of human trafficking networks. However, the difference is that M.A. Hansen & I. Johansson, as well as K.A. McKee inspected the American context which might differ from the Central Asian context in terms of gender equality issues.

The comparison of three Central Asian countries – the Republic of Kazakhstan, the Republic of Uzbekistan, and

the Republic of Kyrgyzstan – was further carried out to examine potential variations in human-trafficking initiatives. It was discovered that despite the relative similarity of the researched contexts, the countries varied in terms of the scope and effectiveness of human trafficking programs. Of all the countries in the sample, the Republic of Kazakhstan demonstrated the greatest efficiency in terms of international cooperation, mutual legal assistance, and involvement in cross-border training initiatives; as for the Republic of Kyrgyzstan, it demonstrated lower effectiveness levels, partly due the Fergana Valley disputes and at-border conflicts. The contextual variations in human-trafficking initiatives were also confirmed in previous studies, including C. Macaveiu *et al.* (2024). The authors illustrated such variations by stressing that European countries focused on prevention, the Americas led in protection research, while African countries and the Arab States lagged behind in both categories. Despite some resemblance to the study of C. Macaveiu *et al.*, this research has narrowed its focus to the Central Eastern countries, which preconditioned its unique contribution to the academic discourse. E. Cockbain *et al.* (2024), in turn, examined individual-level data of 26,503 people in the United Kingdom and confirmed statistically significant geographic concentration of human trafficking. Considering the results of E. Cockbain *et al.,* cross-border comparison of human-trafficking initiatives was an expedient and methodologically justified strategy. Similar to the United Kingdom, Central Asian region involves several closely located countries, with approximately the same geographic, political, and socio-cultural contexts; hence, comparison across these countries underscores universal issues underlying human trafficking and shaping response strategies.

The research further argued that human trafficking persists due to cross-border challenges hindering preventive and response interventions. This idea was, for example, examined in the context of repatriating two Kazakh and three Uzbek nationals who were subjected to forced labour in Russia. The persistence of cross-border challenges in responding to human trafficking was also admitted in previous research, including R. Broad & N. Turnbull (2024). The cited experts examined the peculiarities of applying the UK Modern Slavery Act 2015 (Legislation, 2015) to international cooperation in human-trafficking prevention and explained that one key challenge was related to the lack of a universally accepted definition of modern slavery, which created loopholes for cross-border human trafficking. The cited findings are consistent with this research which highlighted major differences in the legislation of Central Asian countries in terms of defining human trafficking and setting criminalisation scope. R.V. Martinez *et al.* (2024), in turn, stressed that using a universally accepted definition of human trafficking could help protect previously overlooked population groups, including male victims and children. A partial consistency between this research and the study of R.V. Martinez *et al.* was in the fact that both examined national legislation in terms of protecting specific population groups. However, in contrast to the work of R.V. Martinez *et al.,* this research study had a narrower focus, which was special provisions for children.

In this research, aligning national legislation to international standards was also named among the hindrances to cross-border cooperation in managing human trafficking in Central Asia. The comparative legislative analysis revealed that although all five countries have grounded their human-trafficking legislation in the Palermo Protocol, they differ cross-border coordination and enforcement practices. While citing the case of repatriating Kazakh nationals, this research study argued that the existence of universal standards could facilitate cross-border cooperation while reducing the time spent in at-border camps and the risks of re-trafficking. Similar conclusions were reached by S. Karaj & K. Xharo (2024) who examined cross-border cooperation in combating human trafficking in the Western Balkans. The cited experts put forward the idea that aligned legislation proves effective in case of strong law enforcement, which is consistent with this research study, where corruption, limited transparency, and insufficient accountability were listed among the hindrances to cross-border cooperation in managing human trafficking. The comparison between this research and the work of S. Karaj & K. Xharo is expedient since both Central Asia and the Western Balkans are similar in terms of their political, economic, and socio-cultural development. Meantime, inspection of the Bangladeshi context conducted by H. Taha (2024) emphasised that infrastructure and resource challenges affect cross-border cooperation in preventing or investigating human trafficking. Similar challenges were elaborated in this research study whose research focus is considered very similar to the study of H. Taha. This research has, however, made its contribution to the current discourse by suggesting strategies to integrate European and international experience in mitigating infrastructure and resource challenges. Similarities found between this research study and previously published papers emphasised the relevance of the selected topic. Cross-border cooperation in combating, preventing, and investigating human trafficking is a persistent issue in Europe, the Americas, Africa, and Asia. Nevertheless, this research study has made its own contribution to the academic discourse by narrowing down its topic to Central Asia where human trafficking reveals an interplay of geographical, political, economic, social, cultural, and other factors.

Conclusions

The comparative analysis involving three countries – the Republic of Kazakhstan, the Republic of Uzbekistan, and the Republic of Kyrgyzstan, and the Republic of Tajikistan – revealed that human trafficking has been a persistent issue in Central Asia since the collapse of the Soviet Union in 1990. The problem was attributed to political insecurity, at-border conflicts, poverty, and gender inequality; it was also discovered that human trafficking persists because of insufficient cross-border cooperation in combating, investigating, and preventing the problem. The research

involved comparative legal analysis, according to which, all countries in the sample have adopted comprehensive legal frameworks to combat human trafficking. Although all these frameworks have been rooted in the Palermo Protocol, their implementation somewhat varies across the countries: while the Republic of Kazakhstan and the Republic of Kyrgyzstan have formalised NRMs and partnerships with NGOs, Uzbekistan has maintained structured victim assistance networks. Despite the detected differences, all countries in the sample encounter with weak enforcement procedures that are characterised by limited transparency and insufficient accountability. These limitations were, for instance, detected in the case of F.M. and Others v. Russia, involving two Kazakh and three Uzbek nationals subjected to forced labour in Russia. The inspection of the mentioned studies allowed to detect six groups of obstacles to cross-border cooperation in managing human trafficking in Central Asia: political tensions and border disputes; corruption and institutional weakness; ineffective implementation of legal frameworks; lack of data sharing and insufficient coordination mechanisms; cultural and societal peculiarities; and geopolitical dynamics. Considering the detected hindrances, the following strategies were suggested to support cross-border efforts to combat human trafficking in Central Asia: to address political tensions and border disputes by involving international unions and relying on multilateral platforms; overcome corruption and institutional weakness through enhanced transparency and accountability; strengthen national legal frameworks through harmonising them with international standards; and increase the national human trafficking management systems' capacity by launching the border IOM-coordinated safe funds. This research study has some limitations, included a comparatively small number of countries to analyse. In the future research, this recommendation can be addressed by adding more countries to the sample or comparing human trafficking management strategies in Central Asia to other regions, such as South Asia, the Americas, or Europe.

Acknowledgements
None.

Funding
None.

Author Contributions
B. Kakeshov conceived the study, collected and analysed the data, conducted the comparative legal analysis, and drafted the manuscript. The author approved the final version of the article.

Conflict of Interest
None.

References
[1] Ariail, D.L., Smith, K.T., & Smith, L.M. (2024). Human trafficking and gender inequality: How businesses can lower risks and costs. *Journal of Risk and Financial Management*, 17(9), article number 418. doi: 10.3390/jrfm17090418.
[2] Belaid, L., Sarmiento, I., Dion, A., Cardenas, A.R., Cockcroft, A., & Andersson, N. (2024). Factors influencing domestic human trafficking in Africa: Protocol for a scoping review. *JMIR Research Protocols*, 13, article number e56392. doi: 10.2196/56392.
[3] Broad, R., & Turnbull, N. (2024). The global governance problem with framing human trafficking as 'modern slavery': The experiences of international actors in human trafficking policymaking. *International Criminology*, 4, 358-370. doi: 10.1007/s43576-024-00146-0.
[4] Chatterjee, S. (2024). Beyond borders: Navigating non-traditional security challenges in Central Asia. *Indonesian Journal of Social Sciences*, 16(02), 71-81.
[5] Cockbain, E., Ashby, M., Zhang, S.X., & Bowers, K. (2024). Concentrations of harm: Geographic and demographic patterning in human trafficking and related victimisation. *Criminology and Criminal Justice*, 25(1), 147-170. doi: 10.1177/17488958241245311.
[6] Criminal Code of the Republic of Kazakhstan No. 167. (1997, July). Retrieved from https://adilet.zan.kz/eng/docs/K970000167.
[7] Criminal Code of the Republic of Uzbekistan No. 2012-XII. (1994, September). Retrieved from https://adsdatabase.ohchr.org/IssueLibrary/UZBEKISTAN_Criminal%20Code.pdf.
[8] De Vries, I., Baglivio, M., & Reid, J.A. (2024). Examining individual and contextual correlates of victimisation for juvenile human trafficking in Florida. *Journal of Interpersonal Violence*, 39(23-24), 4748-4771. doi: 10.1177/08862605241243332.
[9] Dyussenova, A., Darkenov, K., & Abzhapparova, B. (2024). Transnational human trafficking in Central Asia: Scale, causes and solutions. *Social & Legal Studios*, 7(4), 201-211. doi: 10.32518/sals4.2024.201.
[10] European Court of Human Rights. (2024). *Case of F.M. and others v. Russia*. Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-238319%22]}.
[11] EUROPOL. (2025). *Joint investigation teams*. Retrieved from https://surl.li/pheuix.
[12] Fadilla, F., Ramdhani, H., & Khoerunsia, N. (2022). Role of local governments in preventing and treating victims of human trafficking. *Public Administration Journal*, 12(2), 180-190. doi: 10.31289/jap.v12i2.7836.
[13] Hansen, M.A., & Johansson, I. (2025). Gender differences in attitudes and perceptions of human trafficking: Are they driven by knowledge gaps? *Journal of Human Trafficking*, 1-22. doi: 10.1080/23322705.2025.2539000.

[14] Indraswari, F. (2024). Rethinking border management: A human security approach to combating human trafficking in the Mekong subregion. *Journal of ASEAN Studies*, 12(2), 353-382. doi: 10.21512/jas.v12i2.11591.
[15] Karaj, S., & Xharo, K. (2024). Human trafficking in the Western Balkans: A review of legal and security perspectives. *Revista de Drept Constitutional*, 2, 27-46.
[16] Khamzin, A., Khamzina. Z., Mukhamedzhanov, O., Taitorina, B., & Buribayev, Ye. (2023). Human trafficking: Problems of counteraction in Kazakhstan. *Access to Justice in Eastern Europe*, 4(21), 71-93.
[17] Khan, Z., Kamaluddin, M.R., Meyappan, S., & Manap, J.H. (2022). Prevalence, causes and impacts of human trafficking in Asian countries: A scoping review. *F1000 Research*, 11, article number 1021. doi: 10.12688/f1000research.124460.2.
[18] Klabbers, R.E., Hughes, A., O'Laughlin, K., & Dank, M. (2023). Human trafficking risk factors, health impacts, and opportunities for intervention in Uganda: A qualitative analysis. *Global Health Research and Policy*, 8(1), article number 52. doi: 10.1186/s41256-023-00332-z.
[19] Kooffreh, B.E. (2023). Examining factors predicting sexual exploitation among victims of human trafficking. *The International Journal of Evidence & Proof*, 28(3), 236-250. doi: 10.1177/13657127231222292.
[20] Kovaleva, M., Filho, W.L., Borgemeister, C., & Komagaeva, J. (2023). Central Asia: Exploring insights on gender considerations in climate change. *Sustainability*, 15(16), article number 12667. doi: 10.3390/su151612667.
[21] Law of Kyrgyzstan No. 55 "On Preventing and Combating Trafficking in Human Beings". (2005, March). Retrieved from https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=74767.
[22] Law of the Republic of Uzbekistan No. ЗРУ-154 "On Combating Trafficking in Persons". (2008, April). Retrieved from https://surl.li/szozsu.
[23] Legislation. (2015). *Modern slavery act 2015*. Retrieved from https://surl.lu/ywipxx.
[24] Macaveiu, C., Wong, L., & Guarcello, L. (2024). Factors, counter-trafficking programs, and geographical variations in human trafficking literature (2010-2022). *Journal of Human Trafficking*, 1-22. doi: 10.1080/23322705.2024.2432788.
[25] Martinez, R.V., Garcia-Vazquez, O., Villasenor, C.E., & Dubin, A. (2024). Identifying the challenges in the detection and protection of child victims of human trafficking in Spain: A case study of the Southern European border. *Social Sciences*, 13(11), article number 566. doi: 10.3390/socsci13110566.
[26] McKee, K.A. (2024). A primer on human trafficking. *Journal of Global Justice and Public Policy*, 10(1), 1-33.
[27] Mercera, G., Kooijmans, R., Leijdesdorff, S., Heynen, E., & van Amelsvoort, T. (2024). Risk and prospective factors for sexual exploitation in male and female youth from a cross-cultural perspective: A systematic review. *Trauma Violence and Abuse*, 25(3), 1966-1984. doi: 10.1177/15248380231201815.
[28] Nicodemi, F., & Cirillo, C. (2024). Toward effective protection of victims of human trafficking in mixed migration flows: Referral mechanisms shaped on individual need. The Italian experience and the European perspective. *Frontiers in Human Dynamics*, 6. doi: 10.3389/fhumd.2024.1436612.
[29] Office of the Commissioner for Human Rights. (2000). *Protocol to prevent and punish trafficking in persons especially women and children, supplementing the United Nations Convention against transnational organised crime*. Retrieved from https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ProtocolonTrafficking.pdf.
[30] Organisation for Security and Co-operation in Europe. (2025). *Combating human trafficking among migration routes*. Retrieved from https://surl.li/ymldiy.
[31] Proia-Lelouey, N., & Desquesnes, G. (2025). Risk factors for sex trafficking of domestic minors: An umbrella review of recent international literature. *Neuropsychiatrie de l'Enfrance et de l'Adolescnece*, 73(1), 29-35. doi: 10.1016/j.neurenf.2024.10.003.
[32] Royal Thai Embassy in Astana. (2025). *Human trafficking in Central Asia: The governmental policies to combat it*. Retrieved from https://surl.li/pghmmq.
[33] Santos, R.C., Marin, Y.R., Bardales, E.S., Caro, O.C., Carrasco Rituay, A.M., Sanchez Pantaleon, A.J., & Torres Fernandez, M. (2024). Government strategies for the prevention of human trafficking for sexual and labor exploitation in the Amazon region. *Cogent Social Sciences*, 10(1). doi: 10.1080/23311886.2024.2439542.
[34] Sundram, P. (2024). ASEAN cooperation to combat transnational crime: Progress, perils, and prospects. *Frontiers in Political Science*, 6. doi: 10.3389/fpos.2024.1304828.
[35] Taha, H. (2024). Cross border security challenges for Bangladesh: A thematic analysis. *Society & Sustainability*, 6(1), 21-34. doi: 10.38157/ss.v6i1.617.
[36] The Republic of the Union of Myanmar Ministry of Information. (2025). Retrieved from https://www.moi.gov.mm/moi:eng/news/18974.
[37] U.S. Department of State. (2024). *2024 trafficking in persons report: Kazakhstan*. Retrieved from https://www.state.gov/reports/2024-trafficking-in-persons-report/kazakhstan/.
[38] United Nations Office on Drugs and Crime. (2022). *Global report on trafficking in persons 2022. Country profiles: Eastern Europe and Central Asia*. Retrieved from https://surl.li/apzmyp.
[39] United Nations Office on Drugs and Crime. (2024). *Global report of trafficking in persons 2024*. Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.3/.7:159.922

Article's History:
Received: 30.06.2025; Revised: 06.11.2025; Accepted: 16.12.2025

Forensic psychology approaches to terrorism risk assessment in Central and South Asia

Aybek Adilov*
Academy of the Ministry of the Interior Affairs of the Kyrgyz Republic
720040, 1A Chui Ave., Bishkek, Kyrgyzstan
https://orcid.org/0000-0001-5081-6305

Serimzhan Dosumov
Solva Group Ltd
050000, 502 Seifullin Ave., Almaty, Kazakhstan
https://orcid.org/0000-0002-8131-2705

Anvar Kasymov
Academy of the Ministry of the Interior Affairs of the Kyrgyz Republic
720040, 1A Chui Ave., Bishkek,Kyrgyzstan
https://orcid.org/0009-0001-2462-8826

Abstract. This study aimed to develop adapted forensic-psychological approaches for terrorism risk assessment in Central and South Asia, considering the region's specificities and threat dynamics. The methodology was based on a theoretical analysis of secondary data, including global terrorism reports and official legislative documents from Kazakhstan, Uzbekistan, and Pakistan. The primary methods were trend observation, activity product analysis, and comparative legal method. The results indicated that the region's terrorist landscape is transforming from hierarchical structures to decentralised networks and individual actors, posing significant challenges. It was established that South Asia, particularly Pakistan, continues to demonstrate a high level of terrorist activity, whereas Kazakhstan and Uzbekistan face growing, albeit still low, risks. It was recorded that in 2024, Pakistan experienced a more than twofold increase in the number of terrorist attacks, from 517 to 1,099 incidents, and the number of fatalities increased by 45%, from 748 to 1,081. Significant gaps were also identified in understanding the psychological criminogenic factors of radicalisation and recidivism, and existing Western risk assessment models require adaptation to the local socio-cultural context. In this regard, adapted forensic-psychological approaches were developed, accounting for cultural sensitivity, religious specificity, behavioural indicators, psychosocial factors, language barriers, legislative context, and the integration of artificial intelligence for accurate risk assessment in Central and South Asia. The practical value of the study lies in the potential for its results to be used by law enforcement agencies, security services, and judicial institutions to enhance terrorism risk assessment methodologies. The developed approaches can serve as a basis for creating training programmes for psychologist practitioners working in the field of counter-terrorism, as well as for developing national strategies for countering radicalisation and reintegration programmes for former combatants

Keywords: fradicalisation; extremism; threats; profiling; counter-terrorism

Introduction

The persistent and evolving threat of terrorism necessitates the continuous refinement of counter-terrorism strategies, particularly in understanding its complex psychological underpinnings. Contemporary terrorist acts are characterised by their transnational nature and pronounced physical and psychological aggression, often demonstrating a complex character. The research by V. Jitariuc (2023) indicated that, despite changes over time, the methods of committing

Suggest Citation:
Adilov, A., Dosumov, S., & Kasymov, A. (2025). Forensic psychology approaches to terrorism risk assessment in Central and South Asia. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 24-34.

*Corresponding author

terrorist acts and the psychology of the perpetrators remain largely unchanged. He emphasised that law enforcement agencies often collect incomplete information and draw unfounded conclusions, leading to errors in the investigative process. This underscores the critical need for proper investigation of the forensic nature of the crime of terrorism and its modus operandi. Given these challenges, effective risk assessment becomes an imperative.

The study of terrorism within criminology is one of the fastest-growing subfields. G. LaFree & A. Schwarzenbach (2021) noted that this growth resembles the early years of criminology itself, characterised by energy, imagination, and creativity, but simultaneously struggling with the collection and analysis of reliable data, the application of appropriate research methods, and the development of comprehensive theoretical frameworks. Although criminology holds significant potential for applying theories of crime to terrorism, D. Fisher & E.M. Kearns (2024), in their analysis of leading criminological journals, found that many criminological theories that could help understand terrorism receive scant attention. They emphasise the need for more qualitative, theoretical, and mixed-methods research, and also point out that few studies concern the development of terrorism laws. This indicates a significant gap in understanding psychological criminogenic factors. Specifically, Z.A. Sukabdi (2021), in his study of psychological risk factors of terrorist offenders in Indonesia, found that the psychological criminogenic factors for identifying terrorist offenders with a risk of recidivism in Indonesia remain unclear. Consequently, the adequate assessment of individuals involved in terrorism and the measurement of the effectiveness of terrorist rehabilitation are called into question. This demonstrates an urgent need for the development of robust tools for risk assessment and management, particularly concerning the residual risk of terrorist acts or violent extremism posed by offenders after their release from prison, as noted by B. Ripperger (2021) in his analysis of the use of terrorism risk assessment tools in Australia. He pointed out that existing tools are time- and resource-intensive, and courts afford them limited weight.

The development and implementation of terrorism risk assessment tools are central to addressing these challenges. C. Logan *et al.* (2023) stressed that risk and threat assessment practices are crucial for identifying extremists, prioritising resources, and developing individualised management plans. In the United Kingdom, as noted by A. Silke (2025), the Extremism Risk Guidance (ERG 22+) has been the primary risk assessment framework used for terrorists and violent extremist offenders in England and Wales since 2011. However, its effectiveness requires constant revision. A study, which is the first rapid evidence assessment of ERG22+ factors, showed that most ERG factors were the focus of significant research activity between 2012 and 2020, while six factors received very little research attention. Ten research themes were also identified that could potentially shape new factors or play a significant role in updating or revising some existing factors. This underscores the dynamic nature of terrorist risk and the constant need for refining assessment methodologies.

However, mental health professionals working with individuals whose potential for harm may be ideologically motivated face unique challenges. C. Logan & R. Sellers (2021), in their introduction to a special issue on violent extremism and mental health, highlighted three key issues: the complexity of ensuring proper practice in risk assessment and management; the challenge of establishing and understanding the role of extremist ideology; and how practitioners and their services respond to the risks. These challenges are fundamental in light of the ongoing debates regarding the link between radicalisation, terrorism, and mental disorders. A systematic review conducted by M. Trimbur *et al.* (2021), which analysed 25 articles, showed that they failed to identify a significant link between radicalisation, terrorism, and mental disorders overall, although they noted that some studies indicate a high level of mental disorders in subgroups of radicalised individuals and lone-actor terrorists. They emphasised the need for further research using standardised psychiatric assessment methods. Similarly, research by G. Thijssen *et al.* (2023), which retrospectively analysed data from 82 convicts in Dutch terrorist units, showed that violent extremists are a heterogeneous group in terms of socio-demographic characteristics, with approximately 60% of the population having prior convictions for ordinary crimes, and one-third suffering from a mental disorder. This study concluded that additional research into motivational and other risk factors is necessary. The latter is a necessary step for improving the identification, risk assessment, and effective treatment of violent extremists. Furthermore, information gathering from witnesses in counter-terrorism operations has been evolving. T. Ashkenazi & R.P. Fisher (2022) conducted an empirical study in which they trained experienced Israeli investigators to use the Cognitive Interview (CI) technique to improve witness reports in real-world terrorist attack investigations. Their results showed that the CI yielded more information, as well as more new information that was not present in the first interview. This indicates a broader application of psychological methods, extending beyond direct assessment alone to the gathering of intelligence data.

Given the multifaceted nature of terrorism and the identified gaps in understanding and assessing psychological risk factors, this study aimed to develop tailored forensic psychological approaches to terrorism risk assessment in Central (CA) and South Asia (SA). The research problem of this study was as follows: how can forensic psychological approaches be effectively adapted and integrated into counter-terrorism framework programmes in Central and South Asia to enhance the effectiveness of risk assessment, prevention, and rehabilitation, considering the specific socio-cultural dynamics of the region and evolving terrorist threats.

Materials and Methods

The study focused on a country sample comprising Kazakhstan, Uzbekistan, and Pakistan. These countries were

selected as key representatives of Central and South Asia, facing diverse yet interconnected aspects of terrorist threats. Kazakhstan and Uzbekistan are strategically important Central Asian states demonstrating a low level of risk. Pakistan was included to study adaptation and response mechanisms to significant and evolving threats within a context of high and continually increasing levels of terrorist activity.

The analysis period covers the timeframe from 2015 to 2025, aiming to trace contemporary trends and the evolution of threats. The source selection procedure was based on defined inclusion and exclusion criteria: the inclusion criteria were official reports from international organisations (UN, Europol), annual GTI indices (Global Terrorism Index, 2025), peer-reviewed scientific literature, and current legislative acts of the studied countries directly pertaining to terrorism, risk assessment, and legal psychology. The exclusion criteria were unverified media reports and sources without a clear methodology. Methodologically, the study was based on specific scientific methods of legal psychology and legal research. Observation of terrorist activity trends was conducted through monitoring and analysis of statistical data presented in the European Union terrorism situation and trend report (2025), and Country Reports on Terrorism (2023). The application of this method was aimed at tracking the dynamics and geographical distribution of terrorist incidents. Key metrics and indicators were systematically extracted and aggregated from the selected sources: the number of terrorist incidents, the number of fatalities and casualties, the type of terrorist actor (organisation, individual), the geographical distribution of attacks, and the primary modus operandi.

Activity product analysis was applied to study a significant corpus of textual materials. This included official documents from international organisations (Regional Expert Group…, 2025) and the United Nations Mission (UN) in Central Asia (UNRCCA (Central Asia), 2025). Reports from the United Nations Office on Drugs and Crime (UNODC) (Victims of terrorism, 2020; Model Legislative Provisions, 2022; Kazakhstan and UNODC reinforce cooperation…, 2025) were also analysed. National legal acts of Kazakhstan were examined: Law of the Republic of Kazakhstan No. 191-IV (2009), Law of the Republic of Kazakhstan No. 178-IV (2009), Law of the Republic of Kazakhstan No. 266-IV (2010). Strategic documents (Astana jubilee declaration…, 2010; The Global Initiative…, 2025) were also included in the analysis. The application of this method aimed to identify patterns, risk factors, as well as existing risk assessment tools. Qualitative variables were extracted from legislative acts and official documents: existing legal counter-terrorism mechanisms, procedural safeguards during investigations, definitions of key terms ("terrorism", "extremism"), and existing risk assessment tools applied at the national level.

The biographical method was applied to study the evolution of terrorist groups, such as the Islamic State (ISIS), and their ideological foundations, based on historical information and analysis of their activities. The formal-legal method was applied for a detailed study of the structure and content of normative-legal acts, including Resolution of the Security Council Committee of the United Nations No. 1267 (1999) and Resolution of the Security Council Committee of the United Nations No. 1540 (2004), as well as legislative acts of the Republic of Kazakhstan. The historical-legal method was used to trace the development of legislation and counter-terrorism strategies, as well as the evolution of terrorist threats in the regions of Central and South Asia (The fight against…, 2019). The comparative-legal method was applied to juxtapose Western approaches to forensic psychological risk assessment with the needs and context of Central and South Asian countries, aiming to identify discrepancies and opportunities for adaptation (European Union terrorism…, 2025; Kazakhstan Security Radar, 2025). The statistical method was applied to interpret quantitative data on terrorist incidents and their consequences (GTI, 2025), to identify patterns and trends. Based on the analysis of existing models and a comparative juxtaposition of their characteristics, a synthesis of key aspects for adapting forensic psychological approaches to terrorism risk assessment in Central and South Asia was conducted. This study is based exclusively on the analysis of open, publicly available sources. The work did not involve the use of personal data, closed operational information, or conducting experiments involving human subjects.

Results and Discussion

The evolution of terrorist threats and the conceptualisation of risk in the regional context of Central and South Asia

The analysis of the contemporary terrorist threat landscape in Central and South Asia has revealed a fundamental shift from hierarchically organised groups characterised by a clear structure and centralised command, towards more diffuse, amorphous, and ideologically motivated networks, as well as a growing role of individual actors who may operate either independently or in small, situational groups. This transformation creates unprecedented challenges for traditional risk assessment methods, which historically relied on security and law enforcement approaches focused on identifying known organisations and their operational plans. The GTI (2025) provides clear evidence of this dynamic, confirming that, despite a global 22% decrease in terrorism-related deaths compared to the peak of 33,346 deaths in 2014, South Asia consistently remains the region with the highest average GTI score, holding this position throughout 2015-2025. This underscores the deeply entrenched and persistent nature of terrorist threats in this subregion. Pakistan, in particular, demonstrates an exceptionally high and increasing level of terrorism impact, ranking 2nd in the global ranking with a score of 8.374 out of 10.000 (GTI, 2025). This indicates deeply rooted, persistent, and multifaceted extremist networks that continue to operate despite counter-terrorism efforts. The situation in Pakistan is the primary reason for the deterioration of the region's indicators as a whole.

In 2024, Pakistan experienced a sharp increase in the number of terrorist attacks, more than doubling from 517 incidents to 1,099, while the number of terrorism-related deaths increased by 45%, from 748 to 1,081 (GTI, 2025). This surge makes Pakistan one of the countries with the highest absolute number of casualties and a deteriorating trend. One of the deadliest incidents in Pakistan in 2024 was the November 9th explosion in Balochistan, which resulted in 25 fatalities, for which the Balochistan Liberation Army (BLA) claimed responsibility (GTI, 2025). The main terrorist actors in Pakistan remain Tehrik-i-Taliban Pakistan (TTP) and regional affiliates of the Islamic State – Khorasan Province (ISK), which is a branch of the ISIS terrorist organisation, carrying out attacks on security forces, civilian populations, and infrastructure, highlighting their capacity for destabilisation. Meanwhile, in Central Asian countries such as Kazakhstan and Uzbekistan, the nature of the primary threat is somewhat different. These countries, while not ranking within the top twenty countries for terrorism impact according to the GTI (2025) (Kazakhstan ranks 100th with a score of 0.000, indicating the absence of terrorist acts over the past five years, and Uzbekistan ranks 90th with a score of 0.233), face other challenges. Uzbekistan's score, although low, nevertheless shows an increase of 0.19 points in 2024, indicating a potential deterioration of the situation or an increase in risks.

The obtained data on the rise of terrorist activity in Pakistan and potential risks in Uzbekistan are consistent with research highlighting the complexity and multifactorial nature of terrorism in the region. F.E. Bilal *et al.* (2022) in their critical analysis of terrorism in Pakistan noted that no single cause has a direct link to terrorism; rather, its roots lie in the interplay of poverty, illiteracy, social grievances, inequality, human rights violations, and state suppression. The increase in attacks in Pakistan confirms their conclusions that the country remains a "serious victim of terrorism". The research by S.A. Abbas & S.H. Syed (2021) further elucidates the role of external factors in sectarian terrorism in Pakistan, finding that economic cooperation with India, credit from Saudi Arabia, and trade relations with Iran can paradoxically activate extremist groups. This underscores that the dynamics of terrorism in South Asia are not merely internal but are deeply interwoven into a complex geopolitical fabric, complicating the development of simple solutions.

Data on the growing activity of ISK and its alliances with the Islamic Movement of Uzbekistan (IMU) point to the further evolution of threats, which is consistent with the analysis of N. Shukuralieva & A. Lipiński (2021), who studied the process of the "securitisation" of Islam in Central Asia. They argued that Islamic radicalism is often portrayed as a threat to military, political, and societal security, influencing legislation and the reproduction of authoritarianism. In the case of Uzbekistan, as noted by T. Chutia (2021), the official discourse often exaggerates the threat of terrorism to justify authoritarian counter-terrorism policies, whereas human rights organisations point to the opposite picture. The conclusions regarding the low but increasing GTI score for Uzbekistan confirm that, despite official statements, the risks may be more latent and linked to the repatriation of Foreign Terrorist Fighters (FTFs), making the focus on forensic psychological assessment highly relevant. This shift from "organisational" to "individual" terrorism necessitates new approaches, as "stochastic terrorism", described by M. Amman & J.R. Meloy (2021) and characterised by the inspiration of violence through diffuse public rhetoric, becomes increasingly relevant in the modern digital environment. Data on the rise of online radicalisation and ISK's use of a multilingual media strategy to engage youth corroborate the conclusions of J.F. Binder & J. Kenyon (2022) that, while the current threat of online radicalisation is not exceptionally high, it is "unlikely to remain so in the future" given the overall growth and acceleration of online activity by terrorist actors. This indicates a need for psychological tools that can detect signs of radicalisation before it escalates into violent action.

The primary threat here is associated less with the mass, overt activity of large terrorist organisations within the country, and more with the heightened risks stemming from FTFs and their families returning from conflict zones, as well as with processes of online radicalisation (Regional Expert Group…, 2025). A key role in this context is played by ISK, also known as Islamic State Khorasan Province (ISKP). This regional branch of ISIS, operating primarily in Afghanistan, Pakistan, Iran, and parts of Central Asia. Formed in 2015, ISK pledged allegiance to the central leadership of ISIS and seeks to establish an Islamic caliphate in the historical Khorasan region, which spans parts of modern Iran, Afghanistan, and Central Asia (GTI, 2025). ISK has become one of the most active jihadist groups internationally in recent years, having carried out numerous attacks beyond its bases in Afghanistan (Gerges, 2021). In 2024, the group was responsible for one of the deadliest terrorist incidents of the year: the January attack in Kerman, Iran, which killed at least 95 people. Since its inception, ISK has been linked to 634 attacks and 3,212 fatalities. In particular, an increase in ISK activity is observed in the Eurasia region, where the number of incidents rose from 11 in 2023 to 18 in 2024, and the number of deaths attributed to the group increased from four to 199 over the same period (GTI, 2025).

These individuals, often with combat experience and deeply ingrained extremist ideology (Gerges, 2021), pose a significant internal threat to Kazakhstan and Uzbekistan, being potentially capable of inspiring new cells, recruiting new members, or carrying out lone-wolf, yet devastating, terrorist attacks. ISK actively employs a multilingual media strategy, using languages such as Pashto, Dari, Arabic, Urdu, Farsi, Uzbek, Tajik, English, and more recently also Russian and Turkish, to target youth and marginalised groups through platforms like Telegram and Al-Azaim. A key factor contributing to ISK's expanding influence is its maintenance of alliances with groups such as the IMU, which in 2015 pledged allegiance to ISIS (GTI, 2025). The IMU, formed in 1998 predominantly from Uzbeks, historically aimed to overthrow the government of

Uzbekistan and establish an Islamic state governed by Sharia law (Gerges, 2021). This connection is perilous, as ISK continues to attract returning fighters from Syria and Iraq, with recruitment efforts being intensified precisely by the Islamic Movement of Uzbekistan (GTI, 2025). The Country Reports on Terrorism (2023) also emphasise that although Uzbekistan and Kazakhstan have demonstrated progress in combating terrorism and repatriating their citizens, the risk remains high due to proximity to Afghanistan and the activity of extremist groups in neighbouring regions where ISK has a strong presence, particularly near the southern border provinces of Tajikistan, including Badakhshan, Kunduz, and Takhar (GTI, 2025; Country Reports on Terrorism, 2023). Since 2021, following the change of power in Afghanistan, the influence of traditional external forces, such as the USA, India, and Pakistan, on Afghanistan has significantly diminished. The only exception is Uzbekistan, which has retained its influence, although its overall impact on Afghanistan remains limited. This shift may weaken the ability of traditional players to counter ISK's activities, while the Taliban's focus on consolidating internal control could increase the potential space for the expansion of influence by other actors, such as ISK. ISK relies on financial networks to support its operations, having had access to approximately 2.5 million US dollars through blockchain transactions in 2023. The group's membership in the region in 2024 was estimated at between one and six thousand individuals. Early strategic alliances of ISK also included ISIS affiliates in Kyrgyzstan and Kazakhstan, indicating deep roots and a branched network (GTI, 2025).

Sociological data from Kazakhstan highlight the problem: international terrorism consistently ranks among the top three threats of concern to the population, second only to inflation and wars, with 82% of respondents expressing significant concern about it (Kazakhstan Security Radar, 2025). Such high public anxiety creates significant pressure on state authorities, demanding from them not only effective countermeasures but also the development and implementation of innovative preventive mechanisms. However, traditional methods, focused exclusively on identifying members of specific terrorist organisations or monitoring their physical activity, prove insufficiently effective in countering modern, hybrid threats characterised by rapid adaptation and the use of new technologies. As noted in the Europol report, terrorist propaganda is increasingly disseminated not through traditional media or open forums, but through decentralised online platforms, encrypted gaming services, and closed chats, which extremely complicates the monitoring, identification, and neutralisation of individuals in the process of radicalisation (European Union terrorism…, 2025). This qualitative change in the paradigm of the terrorist threat necessitates a transition from purely reactive measures to a proactive and individualised risk assessment, which is the primary task of applied forensic psychology. The psychology of terrorism, as defined by R. Borum (2004), is an extremely complex psychosocial problem, not merely a matter of military tactics or criminal behaviour that is easily amenable to standard assessment. It encompasses profound motivational, cognitive, emotional, and social aspects that shape susceptibility to violent extremism. Consequently, any attempt to assess the risk of terrorist behaviour without a deep, multifaceted understanding of psychological factors – motivation for violence, resilience of ideological beliefs, presence of psychopathological traits, the influence of social connections and manipulation, as well as the overall social and economic context conducive to radicalisation – is doomed to ineffectiveness and potential harm. This creates an urgent need for the integration of comprehensive forensic psychological approaches into the activities of law enforcement, intelligence, and even rehabilitation agencies in the region.

Forensic psychological risk assessment: Methodology, tools, and regional adaptation

Forensic psychological risk assessment of terrorism is a scientifically grounded, systematic process aimed not at "predicting" future behaviour, which is impossible, but at formulating a structured, evidence-based clinical and empirical judgement for the effective management of a potential threat posed by a specific individual. In contrast to traditional "profiling", which is often based on generalised stereotypical assumptions about terrorists and can lead to discrimination and erroneous conclusions, modern risk assessment tools focus on individual analysis. As noted by K. Höffler *et al.* (2022), these tools, such as VERA-2R (Violent Extremism Risk Assessment) or HCR-20 (Hare Psychopathy Checklist – Revised), are based on the analysis of a set of empirically validated risk factors, which can be categorised into static (historical) and dynamic (variable) factors. Static factors, which include criminal history, history of violent behaviour, involvement in extremist groups, or certain socio-demographic characteristics, are immutable but indicate a long-term propensity. In contrast, dynamic factors, such as current ideological beliefs, presence or absence of social support, level of life satisfaction, presence of a life crisis, perception of injustice, propensity for violence, as well as connections with extremist networks, can change over time. Accordingly, it is the dynamic factors that are subject to targeted correction through psychological, social, and rehabilitative interventions. It is the focus on dynamic factors that makes forensic psychological risk assessment a key tool not only for identifying and early detection of threats but also for developing individualised programmes for deradicalisation, reintegration, and long-term monitoring. The UNODC report (Victims of terrorism, 2020) emphasises the importance of such integration of psychological approaches for effective prevention and countering of extremism.

However, the direct, uncritical application of tools developed in a Western socio-cultural and legal context in countries of Central and South Asia is problematic and may be ineffective or even counterproductive. Existing tools often insufficiently account for the unique role of personal contacts, extended family ties and social

networks, as well as religious authorities in the radicalisation process, which is relevant for the collectivist and traditional societies of the region (Höffler *et al.*, 2022). Furthermore, risk factors that are significant in Europe or North America may have different meanings, interpretations, or even be irrelevant in Kazakhstan, Uzbekistan, or Pakistan, where religious, tribal, cultural, and ethnic identities play a significantly greater, and sometimes dominant, role in shaping worldview and motivation. For instance, in Pakistan, where, according to the US State Department report (Country Reports on Terrorism, 2023), a significant number of terrorist groups operate with diverse, often conflicting ideological platforms – ranging from ethnic-separatist to radical-religious and anti-government – the motivational profiles of militants can differ substantially. This necessitates the development of adapted tools that consider such nuances as the significance of "honour", "tribal loyalty", or specific interpretations of religious doctrines. In Uzbekistan, where the government maintains strict control over the religious sphere and has a history of suppressing religious dissent, radicalisation often occurs in underground or foreign networks, using encrypted communications and recruitment through personal connections, requiring different methods of detection than in countries with more open religious freedom. In Kazakhstan, significant attention is paid to countering foreign terrorist fighters and their repatriation (Country Reports on Terrorism, 2023; Kazakhstan Security Radar, 2025). This creates a unique challenge related not only to the initial risk assessment of individuals who already have combat experience and have undergone deep ideological indoctrination but also to the subsequent development of effective programmes for their reintegration and monitoring. Here, forensic psychological assessment must integrate factors of post-traumatic stress, combat experience, and the resilience of extremist views. The UNODC report (Model Legislative Provisions, 2022) also emphasises the need for flexibility and adaptation of the legislative and methodological base in the fight against terrorism, which extends to psychological approaches. Furthermore, reports point to the emergence of new technological factors of radicalisation and attack planning, requiring the inclusion of digital footprint analysis and interaction with artificial intelligence (AI) in psychological assessment (Pfaff, 2025). Table 1 illustrates key aspects that must be considered when adapting psychological tools for assessing the risk of terrorism in the context of Central and South Asia, highlighting their specificities.

Table 1. Matrix for adapting western risk assessment tools (VERA-2R, ERG 22+) for the Central Asia (CA) and South Asia (SA) region

Aspect of adaptation	Problem in existing tools	Proposed modification for CA/SA
Cultural sensitivity	Items on social isolation do not account for the region's collectivist values.	Add assessment of the role of the extended family, clan, and tribe as a potential protective or, conversely, criminogenic factor (pressure, obligations of honour).
Religious specificity	The general item "Ideological Commitment" does not differentiate between traditional religious practices and extremist interpretations.	Include monitoring of informal financial systems (e.g., Hawala), analysis of specific online slang, and abrupt changes in social habits (renunciation of traditional celebrations).
Behavioural indicators	Indicators of attack planning may not account for local methods of communication and financing.	Include monitoring of informal financial systems (e.g., Hawala), analysis of specific online slang, and abrupt changes in social habits (renunciation of traditional celebrations).
Psychosocial factors	Items on personal grievances and trauma are overly general.	Add specific assessment of the impact of historical conflicts, migration experience, and combat-related post-traumatic stress disorder in repatriated foreign fighters.
Linguistic and communication barriers	Interview tools and protocols are primarily designed in English and do not account for local communication norms.	Develop and validate versions of tools and protocols in key regional languages (Pashto, Dari, Uzbek, etc.) involving linguists and cultural experts.
Legislative context	Tools are not integrated with national legal frameworks, including lists of proscribed organisations.	Align risk factors with legal definitions of extremism and terrorism in the legislation of Kazakhstan, Uzbekistan, and Pakistan.
Integration with digital analysis	Traditional tools poorly cover online radicalisation processes, especially within closed communities.	Add a separate domain for digital footprint analysis, including activity on encrypted messengers and interaction with AI-propagated propaganda.

Source: developed by the authors based on Law of the Republic of Kazakhstan No. 191-IV (2009), Law of the Republic of Kazakhstan No. 178-IV (2009), The fight against… (2019), Victims of terrorism (2020), K. Höffler *et al.* (2022), Country Reports on Terrorism (2023), C.A. Pfaff (2025), GTI (2025)

The developed approaches to adapting forensic psychological risk assessment tools for terrorism in the CA and SA regions are based on a deep understanding of the unique socio-cultural, religious, and behavioural characteristics of these countries. Instead of directly copying Western models, a comprehensive strategy is proposed that considers specific regional dynamics. A key aspect is cultural sensitivity, which involves analysing the role of family, community,

and tribal ties, as well as religious authorities in radicalisation processes. This avoids simplified interpretations and the stigmatisation of religious views. Identifying religious specificity is significant, differentiating between traditional and moderate religious practices and extremist interpretations used by terrorist groups. These approaches also include the development of behavioural indicators relevant to local conditions, such as abrupt changes in appearance, social habits, rejection of traditional celebrations, or activity in closed extremist groups and informal financial support. Attention is paid to psychosocial factors, considering the impact of trauma, conflicts, migration experience, discrimination, as well as post-traumatic stress and combat experience among repatriates, which requires assessing their level of social support and resilience. The proposed approaches also involve adapting linguistic and communication barriers through the development of tests and interviews in local languages, considering dialectal and cultural nuances, as well as integrating digital footprint analysis and the use of artificial intelligence to detect patterns of radicalisation in the online environment, which is necessary for identifying latent threats. Thus, effective implementation of forensic psychological methods in the region requires not blind copying of Western models, but their careful adaptation, interdisciplinary validation, and localisation considering the local social, cultural, religious, legal, and political context. This entails conducting one's own empirical research to identify region-specific risk factors, developing relevant indicators for their assessment, and creating regionally sensitive intervention and monitoring protocols.

A systematic review conducted by A. Clesle *et al.* (2024) confirms that, despite the variety of risk assessment tools (VERA-2R, TRAP-18, ERG 22+, etc.), data on their predictive validity remain scarce. This means their ability to accurately predict future violence is limited and requires further study. This is a relevant aspect for Central and South Asia, where the lack of local validation studies makes the application of these tools even more risky. The research by Z.A. Sukabdi (2021) in Indonesia is an example of the necessity for adaptation: the development of the MIKRA tool, based on three domains (motivation, ideology, capability) and 18 individual risk factors, is the result of a deep analysis of the local context and the involvement of Indonesian experts. This approach is the direct opposite of simply "importing" Western methodologies and demonstrates a path that Kazakhstan, Uzbekistan, and Pakistan could follow. The work of J. Kenyon *et al.* (2025) on the updated version of ERG-R, which considers the rise of online radicalisation, youth engagement, and the fluidity of ideologies, also underscores the need for constant adaptation of tools to the changing terrorism landscape. The inclusion of a fourth dimension – protective and risk-mitigating factors – is a necessary step, as it allows for a shift from mere risk assessment to the development of individualised intervention plans. This is needed for working with repatriates, where identifying and strengthening protective factors (e.g., family support, employment opportunities) can be key to successful reintegration.

Integrative profiling models, behavioural indicators, and interagency synergy in countering terrorism

The application of forensic-psychological approaches for terrorism risk assessment in Kazakhstan and neighbouring countries necessitates the development of integrative profiling models that harmonise psychometric tools with unique regional behavioural indicators. Unlike static templates, these models must be dynamic and multifactorial, focusing on predicting potential radicalisation and propensity for violence, rather than merely identifying already formed terrorists. This entails the development of standardised, yet culturally-sensitive psychometric instruments that allow for the assessment of not only superficial ideological statements but also deep-seated motivational attitudes, cognitive distortions (e.g., dehumanisation of the enemy, justification of violence), affective regulation (anger control, impulsivity), and social support for extremist views. In the context of Kazakhstan, where an official national list of terrorist and extremist organisations exists, psychological profiling must incorporate an analysis of the narratives used by these groups for recruitment and their impact on the specific psychological characteristics of potential members. For instance, research could focus on how the preaching of the "caliphate" by ISK (GTI, 2025) resonates with certain personality traits or social frustrations. In Kazakhstan, where countering terrorism is a national security priority, this involves adapting psychometric tests that not only assess standard psychopathological traits but also measure perceptions of social injustice, the influence of group pressure, the level of identification with extremist narratives, and vulnerability to recruitment (The fight against…, 2019). A priority is the consideration of behavioural indicators that are specific to the Central Asian context, such as unusual changes in religious practice that deviate from traditional Islam, sudden withdrawal from family and community ties without apparent reasons, or the emergence in speech and digital communication of radical ideologemes characteristic of proscribed organisations, such as "Hizb ut-Tahrir" or "Tablighi Jamaat", which are included in the national list of terrorist and extremist organisations in Kazakhstan (The fight against…, 2019). Additionally, given the activity of ISK and its multilingual media strategy, the analysis of the digital footprint of individuals who may be under the influence of extremist propaganda becomes a key behavioural indicator requiring enhanced psychological interpretation, not merely technical monitoring. This entails the development of standardised protocols for assessing the psychosocial status of individuals under suspicion and those returning from conflict zones, integrating data from open sources, social networks, and psychological testing adapted to the cultural norms of the region. This will allow not only for more accurate risk identification but also for distinguishing sincere religious beliefs from extremist ideology, avoiding unwarranted stigmatisation. Another critical component is ensuring effective collaboration between law enforcement, intelligence, and forensic-psychological agencies, supported by an appropriate legal framework. Kazakhstan

demonstrates significant progress in this direction, having ratified fourteen universal international counter-terrorism instruments and establishing an Anti-Terrorism Centre in 2003 to coordinate the activities of all security structures (The fight against…, 2019). Laws such as Law of the Republic of Kazakhstan No. 191-IV (2009) and Law of the Republic of Kazakhstan No. 178-IV (2009), regulate mechanisms for halting the dissemination of illegal information on the Internet and countering the financing of terrorism. These legislative acts create a foundation for integrating forensic-psychological expertise into operational activities. For example, psychologists can be involved in developing methodologies for identifying individuals involved in financing terrorism through complex digital transactions, as is the case with ISK, which uses blockchain to access $2.5 million (GTI, 2025).

Cooperation with international organisations, such as the UN Office on Drugs and Crime (UNODC), serves as an example. Within the framework of the UNODC Global Programme on Passenger and Cargo Control (PCCP), the capabilities of Kazakhstan's border service were enhanced through the transfer of portable TruNarc analysers for detecting drugs and precursors (Kazakhstan and UNODC reinforce cooperation..., 2025). Although this initiative is aimed at combating drug trafficking, it demonstrates potential for expansion into counter-terrorism, where substance analysis and enhanced border control capabilities (including the modernised infrastructure of Almaty airport) can be integrated with psychological profiling to identify individuals transporting prohibited materials or having terrorist intentions. Table 2 demonstrates the multi-vector and comprehensive nature of Kazakhstan's interagency and international cooperation in countering terrorism, highlighting the potential for integrating forensic-psychological expertise at various levels.

Table 2. Key aspects of Kazakhstan's inter-agency and international cooperation in countering terrorism

Entity/direction of cooperation	Description and role in the context of forensic psychological assessment
Anti-terrorist centre of Kazakhstan	Coordinates the activities of all security agencies. Integration of psychologists to develop joint protocols for risk identification and assessment.
UN international instruments	Ratification of 14 universal instruments. Cooperation with the UNSC CTC (Resolutions 1267, 1540). This creates a global legal basis for data exchange, which can include psychological profiles and assessment methods.
UNODC	Global passenger and cargo control programme, transfer of TruNarc analysers. Potential for integrating psychological profiling into border control to identify individuals with terrorist intentions (including returnees).
UNRCCA (Central Asia)	Preventive diplomacy, regional cooperation in counter-terrorism. A platform for sharing best practices in forensic psychological risk assessment and deradicalisation.
Regional organisations (CIS, SCO, CSTO, OSCE)	Coordination of anti-terrorism measures, joint training, information sharing. Opportunity to develop and implement standardised psychological protocols adapted to the region. Astana OSCE Jubilee Declaration.
Kazakhstan's legislative base	Laws "On Countering the Legalisation…", "On Information and Communication Networks", "On Countering Terrorism". Provide the legal basis for conducting psychological expert examinations and the operational use of psychological data.
Global initiative to combat nuclear terrorism (GICNT)	Cooperation in preventing nuclear terrorism. Psychological profiling can assist in identifying individuals prone to involvement in such high-risk crimes.

Note: commonwealth of Independent States (CIS); Shanghai Cooperation Organisation (SCO); Collective Security Treaty Organisation (CSTO); Organisation for Security and Co-operation in Europe (OSCE); United Nations Security Council Counter-Terrorism Committee (UNSC CTC)

Source: developed by the authors based on Resolution of the Security Council Committee of the United Nations No. 1267 (1999), Resolution of the Security Council Committee of the United Nations No. 1540 (2004), Law of the Republic of Kazakhstan No. 191-IV (2009), Law of the Republic of Kazakhstan No. 178-IV (2009), Astana jubilee declaration… (2010), The fight against… (2019), Kazakhstan and UNODC reinforce cooperation... (2025), UNRCCA (Central Asia) (2025), The Global Initiative… (2025)

The significance of cooperation between law enforcement and intelligence agencies in Central Asia is amplified by the transnational nature of the threat and the need for rapid response. Kazakhstan actively participates in regional cooperation, including the activities of the CIS, the SCO Regional Anti-Terrorist Structure (RATS), and the CSTO, which allow for the coordination of anti-terrorism measures and information exchange (On Amendments and…, 2009; UNRCCA (Central Asia), 2025). This cooperation is complemented by international support, such as the UNRCCA mission, which focuses on preventive diplomacy and regional cooperation, including counter-terrorism, water management, and women and youth security (UNRCCA (Central Asia), 2025). A fundamental aspect is the legal framework underpinning these efforts. Kazakhstan has adopted key documents, such as the Law of the Republic of Kazakhstan No. 266-IV (2010), which establishes the principles and model of the state system for countering terrorism (Kazakhstan on Counter-Terrorism…, 2019). These laws provide the legal basis for conducting intelligence operations, using special technical means, and performing forensic psychological examinations. Furthermore, Kazakhstan maintains continuous cooperation with the UN Security Council Counter-Terrorism Committee and its committees for the implementation of Resolution No. 1267 (1999) (sanctions against

"Al-Qaeda") and Resolution No. 1540 (2004) (nuclear non-proliferation), allowing for the integration of national efforts into the global context of the fight against terrorism (The fight against…, 2019). The emphasis on collective action, as seen at the OSCE Conference on Preventing Terrorism in Astana in 2010, where the Astana Declaration was adopted (Astana jubilee declaration…, 2010), testifies to a deep understanding that countering terrorism requires coordinated national and international efforts, supported by both legislative and psychological instruments (The fight against…, 2019). In particular, cooperation within the GIBATE (The Global Initiative…, 2025), where Kazakhstan is one of the first participants and conducted relevant exercises ("Atom-Antiterror – 2008"), underscores the multi-vector nature and strategic importance of these efforts (The fight against…, 2019). Thus, forensic-psychological expertise, embedded within a robust legislative and interagency system, is key to effectively countering modern terrorist threats in the region. This creates a platform for implementing standardised protocols for forensic-psychological risk assessment, based on best practices but adapted to regional needs, with a particular emphasis on effectiveness in preventing and responding to transnational threats, such as the activities of ISK. These efforts will ensure a comprehensive approach encompassing not only forceful confrontation but also psychological, preventive, and rehabilitative aspects.

The results of this research, emphasising the necessity of integrating psychological methods into legislative and law enforcement practice, find confirmation in the work of G.B. Zhussupova (2025), who, analysing Kazakhstan's legal policy, concluded that, despite the existence of a solid legislative base, there are gaps in law enforcement, interagency coordination, and the ability to adapt to modern challenges, such as cyber-terrorism. The proposed integrative profiling models and psychometric tools can serve as one way to fill these gaps, providing law enforcement agencies with scientifically-grounded tools for more accurate risk assessment. The research of I. Diamant (2021) on the use of psychological tests for assessing suicide bombers and "lone actors" also confirms the importance of combining different methods. His conclusion about the low validity of self-report questionnaires and the high effectiveness of semi-structured interviews for uncovering deep-seated personal dynamics and traumatic experience aligns with this thesis on the necessity of developing comprehensive, culturally-sensitive assessment protocols. This is of paramount importance, as the meta-analysis by K.M. Sarma *et al.* (2022) did not confirm the widespread belief that terrorists have a higher level of mental disorders than the general population. This means the focus should not be on searching for psychopathologies but on analysing the complex psychosocial factors that lead to radicalisation, which is the central task of forensic-psychological risk assessment. It should also be noted that terrorist threats are not limited to religious extremism. The research of E. Chan (2023) on the "incel" community in Canada and its connection to gender-based violence demonstrates that existing risk assessment frameworks may fail to account for new forms of extremism. This underscores the need for constant expansion and adaptation of risk assessment tools to detect new ideological threats that may be relevant for Central Asia as well. Thus, the results of this study not only describe the current situation but also propose a path towards building a more flexible, scientifically-grounded, and humane system for countering terrorism, where psychological expertise plays a central role in preventing violence and promoting reintegration.

Conclusions

The conducted research has identified the key features of the evolution of terrorist threats and the necessity of rethinking traditional methods of counter-terrorism. It was established that the terrorist landscape of the region is characterised by a shift from hierarchical structures to more decentralised networks and individual actors, which creates significant challenges for security systems. The analysis showed that South Asia, particularly Pakistan, continues to be a region with a high level of terrorist activity, as confirmed by the increase in the number of attacks and casualties. At the same time, Central Asian countries, such as Kazakhstan and Uzbekistan, while demonstrating lower indicators, face a potential increase in risks associated with transnational terrorist networks and the phenomenon of foreign terrorist fighters. This dynamic requires flexible and contextually sensitive approaches to risk assessment.

Existing Western risk assessment models, despite their efficacy, require adaptation, as they do not always fully account for regional specificities, particularly the complex interplay of ideological, social, and personal motivations. In light of this, a number of adapted forensic psychological approaches have been developed, which entail profound cultural sensitivity, distinguishing religious specificity from extremism, identifying regionally relevant behavioural indicators, analysing psychosocial factors, adapting to linguistic and communication barriers, considering the legislative context, and integrating AI into digital analysis. These approaches enable the formation of more accurate and contextually grounded mechanisms for assessing the risk of terrorism in CA and SA. The identified problem underscores the necessity of moving away from universal templates towards a more differentiated and individualised analysis. In particular, the importance of considering local dialects and cultural nuances in communication with suspects and victims is paramount for obtaining reliable information and establishing rapport. The integration of artificial intelligence into big data analysis processes, including digital footprints, will facilitate the detection of hidden patterns and the prediction of potential threats with greater accuracy than traditional methods. This will also enhance the preventive potential of counter-terrorism measures, contributing to more effective prevention of radicalisation and recruitment.

The creation of specialised inter-agency teams, comprising psychologists, sociologists and/or religious studies

scholars, and security experts, is recommended for a comprehensive assessment of radicalisation risks. Focus should be placed on developing rehabilitation programmes that consider the psychological needs and ideological beliefs of individuals involved in terrorism, with an emphasis on recidivism prevention. Furthermore, it is necessary to enhance international and regional cooperation, particularly the exchange of experience and best practices in the field of forensic psychological assessment. The principal avenues for further research involve conducting empirical studies to verify and adapt existing psychological tests and risk assessment methodologies for target groups in Central and South Asia. Subsequent work may include the development of new profiling tools that account for the influence of digital technologies and artificial intelligence on the processes of radicalisation and recruitment.

Acknowledgements
None.

Funding
None.

Author Contributions
A. Adilov developed the research concept and methodology, whilst S. Dosumov and A. Kasimov collected materials and analysed data on the risks of terrorism in Central and South Asia. The authors jointly prepared the manuscript, formulated adapted forensic psychological approaches and approved the final version of the article.

Conflict of Interest
None.

References
[1] Abbas, S.A., & Syed, S.H. (2021). Sectarian terrorism in Pakistan: Causes, impact and remedies. *Journal of Policy Modeling*, 43(2), 350-361. doi: 10.1016/j.jpolmod.2020.06.004.
[2] Amman, M., & Meloy, J.R. (2021). Stochastic terrorism: A linguistic and psychological analysis. *Perspectives on Terrorism*, 15(5), 2-13.
[3] Ashkenazi, T., & Fisher, R.P. (2022). Field test of the cognitive interview to enhance eyewitness and victim memory, in intelligence investigations of terrorist attacks. *Journal of Applied Research in Memory and Cognition*, 11(2), 200-208. doi: 10.1037/h0101871.
[4] Astana jubilee declaration towards a security community. (2010). Retrieved from https://www.osce.org/files/f/documents/d/8/74990.pdf.
[5] Bilal, F.E., Abbas, R., & Rashid, M.A. (2022). Terrorism in Pakistan: A critical analysis. *Pakistan Languages and Humanities Review*, 6(2), 1003-1013. doi: 10.47205/plhr.2022(6-II)85.
[6] Binder, J.F., & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization? *Frontiers in Psychology*, 13, article number 997390. doi: 10.3389/fpsyg.2022.997390.
[7] Borum, R. (2004). *Psychology of terrorism*. Tampa: University of South Florida.
[8] Chan, E. (2023). Technology-facilitated gender-based violence, hate speech, and terrorism: A risk assessment on the rise of the incel rebellion in Canada. *Violence Against Women*, 29(9), 1687-1718. doi: 10.1177/10778012221125495.
[9] Chutia, T. (2021). Uzbekistan: A critical analysis of the official discourse on terrorism. *Conflict Studies Quarterly*, 37. doi: 10.24193/csq.37.2.
[10] Clesle, A., Knäble, J., & Rettenberger, M. (2024). Risk and threat assessment instruments for violent extremism: A systematic review. *Journal of Threat Assessment and Management*, 12(1), 1-22. doi: 10.1037/tam0000223.
[11] Country Reports on Terrorism. (2023). Retrieved from https://www.state.gov/reports/country-reports-on-terrorism-2023/.
[12] Diamant, I. (2021). Advantages and challenges using psychological tests in the assessment of suicide bombers and lone actors. In *Terrorism risk assessment instruments* (pp. 280-296). Amsterdam: IOS Press. doi: 10.3233/NHSDP210017.
[13] European Union terrorism situation and trend report. (2025). Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf.
[14] Fisher, D., & Kearns, E.M. (2024). The theorizing of terrorism within criminology. *Journal of Research in Crime and Delinquency*, 61(4), 487-520. doi: 10.1177/00224278231156754.
[15] Gerges, F.A. (2021). *ISIS: A history* (NED-New ed.). Princeton, NJ: Princeton University Press. doi: 10.2307/j.ctv18b5d6w.
[16] Global Terrorism Index. (2025). Retrieved from https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf.
[17] Höffler, K., Meyer, M., & Möller, V. (2022). Risk assessment – the key to more security? Factors, tools, and practices in dealing with extremist individuals. *European Journal on Criminal Policy and Research*, 28, 269-295. doi: 10.1007/s10610-021-09502-6.
[18] Jitariuc, V. (2023). The crime of terrorism: Forensic characteristics and methods of committing it. *Cogito-Multidisciplinary Research Journal*, 15(4), 173-185.
[19] Kazakhstan and UNODC reinforce cooperation in countering cross-border crime. (2025). Retrieved from https://surl.lu/npvxbt.

[20] Kazakhstan Security Radar. (2025). Retrieved from https://peace.fes.de/security-radar-2025/country-profiles/kazakhstan.html.
[21] Kenyon, J., Carter, A.J., Watson, S., & Farr, J. (2025). Adapting risk assessments to a changing terrorism landscape: Revising the extremism risk guidance. *Journal of Forensic Sciences*, 70(5), 2031-2041. doi: 10.1111/1556-4029.70101.
[22] LaFree, G., & Schwarzenbach, A. (2021). Micro and macro-level risk factors for extremism and terrorism: Toward a criminology of extremist violence. *Monatsschrift für Kriminologie und Strafrechtsreform*, 104(3), 184-202. doi: 10.1515/mks-2021-0127.
[23] Law of the Republic of Kazakhstan No. 178-IV "On Amendments and Supplements to Certain Legislative Acts of the Republic of Kazakhstan on Information and Communication Networks". (2009, July). Retrieved from https://adilet.zan.kz/rus/docs/Z090000178_.
[24] Law of the Republic of Kazakhstan No. 191-IV "On Combating the Legalization (Laundering) of Criminally Obtained Incomes and the Financing of Terrorism". (2009, August). Retrieved from https://online.zakon.kz/Document/?doc_id=30466908.
[25] Law of the Republic of Kazakhstan No. 266-IV "On Amendments and Supplements to Certain Legislative Acts of the Republic of Kazakhstan on Counter-Terrorism Issues". (2010, April). Retrieved from https://adilet.zan.kz/rus/docs/Z100000266_.
[26] Logan, C., & Sellers, R. (2021). Risk assessment and management in violent extremism: A primer for mental health practitioners. In *Violent extremism* (pp. 1-23). London: Routledge.
[27] Logan, C., Borum, R., & Gill, P. (Eds.). (2023). *Violent extremism: A handbook of risk assessment and management*. London: UCL Press.
[28] Model Legislative Provisions. (2022). Retrieved from https://www.unodc.org/documents/terrorism/Website2021/220204_model_legislative_provisions.pdf.
[29] Pfaff, C.A. (Ed.). (2025). *The weaponization of AI: The next stage of terrorism and warfare*. Ankara: Centre of Excellence Defence Against Terrorism.
[30] Regional Expert Group Meeting Addresses Terrorism and Foreign Terrorist Fighters in Central Asia. (2025). Retrieved from https://www.unodc.org/unodc/en/terrorism/latest-news/2025-regional-expert-group-meeting-addresses-terrorism-and-foreign-terrorist-fighters-in-central-asia.html?testme.
[31] Resolution of the Security Council Committee of the United Nations No. 1267. (1999, October). Retrieved from https://main.un.org/securitycouncil/ru/s/res/1267-(1999).
[32] Resolution of the Security Council Committee of the United Nations No. 1540. (2004, April). Retrieved from https://digitallibrary.un.org/record/520326?v=pdf.
[33] Ripperger, B. (2021). The use of terrorism risk assessment tools in Australia to manage residual risk. In C. Logan & P. Gill (Eds.), *Terrorism risk assessment instruments* (pp. 165-192). Amsterdam: IOS Press. doi: 10.3233/NHSDP210010.
[34] Sarma, K.M., Carthy, S.L., & Cox, K.M. (2022). Mental disorder, psychological problems and terrorist behaviour: A systematic review and meta-analysis. *Campbell Systematic Reviews*, 18(3), article number e1268. doi: 10.1002/cl2.1268.
[35] Shukuralieva, N., & Lipiński, A. (2021). Islamic extremism and terrorism in Central Asia: A critical analysis. *Central Asia & the Caucasus*, 22(1), 106-117.
[36] Silke, A. (2025). Factors in terrorist risk assessment: A rapid evidence assessment of the extremism risk guidance (ERG22+) factors. *Journal of Criminal Psychology*, 15(1), 1-16. doi: 10.1108/JCP-04-2024-0035.
[37] Sukabdi, Z.A. (2021). Psychological risk factors of terrorist offenders in Indonesia. *Journal of Psychological Research*, 03(03), article number 3299. doi: 10.30564/JPR.V3I3.3299.
[38] The fight against terrorism and extremism in Kazakhstan. (2019). Retrieved from https://www.gov.kz/memleket/entities/mfa/press/article/details/589?lang=ru.
[39] The Global Initiative to Combat Nuclear Terrorism. (2025). Retrieved from https://2017-2021.state.gov/the-global-initiative-to-combat-nuclear-terrorism/.
[40] Thijssen, G., Masthoff, E., Sijtsema, J., & Bogaerts, S. (2023). Understanding violent extremism: Socio-demographic, criminal and psychopathological background characteristics of detainees residing in Dutch terrorism wings. *Criminology & Criminal Justice*, 23(2), 290-308. doi: 10.1177/17488958211049019.
[41] Trimbur, M., Amad, A., Horn, M., Thomas, P., & Fovet, T. (2021). Are radicalization and terrorism associated with psychiatric disorders? A systematic review. *Journal of Psychiatric Research*, 141, 214-222. doi: 10.1016/j.jpsychires.2021.07.002.
[42] UNRCCA (Central Asia). (2025, February). Retrieved from https://www.securitycouncilreport.org/monthly-forecast/2025-02/unrcca-central-asia-13.php.
[43] Victims of terrorism. (2020). Retrieved from https://surl.li/geerun.
[44] Zhussupova, G.B. (2025). Effectiveness of the legal policy of the republic of Kazakhstan in countering terrorism and religious extremism. *Nauka*, 2(85), 52-55.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 341.231:34

Article's History:
Received: 09.06.2025; Revised: 07.11.2025; Accepted: 16.12.2025

Cybersecurity law in Kazakhstan: A comparative analysis with East Asian practices

Gulnoza Ismailova*
University of World Economy and Diplomacy
100007, 54 Mustakillik Ave., Tashkent, Uzbekistan
https://orcid.org/0000-0002-2244-0299

Nargiza Kadirova
University of World Economy and Diplomacy
100007, 54 Mustakillik Ave., Tashkent, Uzbekistan
https://orcid.org/0009-0009-6698-7219

Abstract. The study aimed to identify avenues for modernising the national cybersecurity system of the Republic of Kazakhstan through a comprehensive assessment of its effectiveness and an examination of advanced practices implemented in East Asian states. The legal analysis revealed a fragmented Kazakhstani cybersecurity framework characterised by the absence of a single codified act and by the proliferation of regulatory documents of varying legal force. The empirical assessment demonstrated a sustained rise in cybersecurity incidents in Kazakhstan, with an average annual growth rate of 14.5% between 2019 and 2024, reaching more than 41,000 cases in 2024. The number of recorded cybercrimes increased thirty-six-fold, from 589 cases in 2018 to 21,479 in 2021. The study identified low enforcement effectiveness, with only 36% of registered cases reaching judicial proceedings. Financial losses incurred by citizens as a result of digital fraud exceeded 17.5 billion tenge in 2023. A correlation analysis of the Worldwide Governance Indicators – specifically rule of law, control of corruption, regulatory quality, and political stability – with cybercrime metrics, including the number of registered cybercrimes and the case-clearance rate, identified a statistically significant negative association ($r = -0.67$, $p < 0.01$). Countries with negative values for control of corruption were found to have cybercrime levels 40% higher on average. A comparative legal analysis of the cybersecurity systems of Japan, South Korea, and China demonstrated substantive differences in procedural mechanisms, sanctioning measures, and institutional architecture. The findings confirmed the significance of institutional quality for the effective protection of national cybersecurity and substantiate the need for a systematic modernisation of Kazakhstan's model through legislative codification, the establishment of a centralised coordination centre, the strengthening of sanctioning mechanisms, and the development of human capital

Keywords: personal data; law enforcement; critical infrastructure; sanctioning mechanisms; institutional quality; international coordination; data localisation

Introduction

The rapid development of digitalisation and information technologies in Central and East Asian states has generated a need to establish effective legal mechanisms for ensuring cybersecurity and protecting personal data. As of 2024, these countries are experiencing an escalation of cyber threats, reflected in the growing volume and sophistication of cyberattacks, rising losses from cybercrime, and increasing vulnerabilities within critical information infrastructure. According to the Asia Pacific Computer Emergency Response Team (APCERT, 2024), the number of registered cybersecurity incidents in the Asia-Pacific region rose by 23% compared with the previous year, while financial losses from cybercrime in several states more than doubled. Geopolitical transformations, particularly in the context of competition among major technological powers for influence in Central and East Asia, further heighten the relevance of

Suggest Citation:
Ismailova, G., & Kadirova, N. (2025). Cybersecurity law in Kazakhstan: A comparative analysis with East Asian practices. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 35-51.

*Corresponding author

issues related to national cybersovereignty and cross-border data flows. The fragmented nature of existing legal regimes and the absence of unified approaches to cybersecurity regulation pose significant challenges for the economic integration and digital transformation of Central and East Asian states. The limited theoretical assessment of regional specificities in cybersecurity regulation highlights the need for a comprehensive examination of national legal frameworks and their alignment with international standards.

A comprehensive regional analysis of data-protection regimes in Central Asia was conducted by G. Greenleaf & T. Kaldani (2025), who found that all six countries in the region have enacted new or recently revised data-privacy laws, with the strongest legal systems observed in Uzbekistan, Mongolia, and Kazakhstan. The researchers noted that the enforcement of these laws remains at an early stage, characterised by low penalties for violations and limited evidence of compliance. The geopolitical context of regional cyberlaw development was examined by C. Zhang (2024), who demonstrated that China's privacy-protection strategy, combining a comprehensive regulatory system with government access to data, is reshaping global data-governance paradigms and generating new geopolitical fault lines. The author established that the Chinese approach, which prioritises state sovereignty over individual privacy, may serve as a potential model for governments seeking to maintain state control over data. This approach diverges significantly from Western models of data privacy and produces normative tensions with states that promote a more open digital economy.

A detailed examination of Kazakhstan's legislation on personal data protection was conducted by F. Syrlybayeva *et al.* (2024), who identified substantial deficiencies in the country's legal doctrine concerning the consolidation of fundamental principles governing the collection, processing, and storage of citizens' personal data. The authors established that the 2024 amendments to the Law of the Republic of Kazakhstan No. 94-V ZRK (2013), despite improving governance, do not comply with the requirements of the General Data Protection Regulation (GDPR) in several areas, including transparency and data-subject rights. A comparative legal analysis carried out by A. Amirov *et al.* (2024) confirmed the fragmented character of Kazakhstan's legislation and its partial alignment with European Union standards, with the researchers emphasising the importance of increasing public awareness of rights and obligations in the digital environment. Further theoretical development was provided by N.B. Kubanova (2025), who identified significant limitations within the existing personal data-protection system, which applies only to specific categories of information and fails to comprehensively address issues related to labour relations. The author argued for the development of specialised legislation and highlighted the importance of improving digital literacy to support the formation of a resilient digital ecosystem.

Systemic cybersecurity challenges in the region were examined comprehensively by M. Orumbayeva & A. Kurmangali (2022), who identified three principal obstacles to strengthening cyber defence: insufficient funding and limited access to technology, a shortage of qualified specialists, and a lack of transparency in digital information and public discourse regarding the role of digitalisation in society. The researchers established that even in Kazakhstan, one of the most technologically advanced states in the region, there are substantial shortcomings in antivirus equipment and software used by central and local government institutions. Empirical confirmation of these findings was provided by N. Kubanova *et al.* (2024), who identified a sharp increase in both the volume and complexity of cyberattacks in Kazakhstan, including 4,507 malware cases in 2024, a figure more than twice that of the previous year. The authors found that the small and medium-sized enterprise sector was the most vulnerable, while losses in the banking sector reached 1.5 billion tenge in the second half of 2024 alone. The study demonstrated that approximately 70% of successful intrusions were attributable to human factors, including insufficient staff qualifications and configuration errors.

Conceptual aspects of cybersecurity regulation were examined by Z.O. Kulzhabayeva (2024), who argued for a statutory differentiation between the concepts of "cybersecurity" and "information security" within the context of informatisation and proposed the introduction of definitions such as "cybersecurity threat" and "cybersecurity incident". She recommended expanding the powers of owners of critical information and communication infrastructure facilities to improve their capacity to respond effectively to cyber incidents. Technological dimensions of digital transformation, viewed through the implementation of blockchain technologies in Kazakhstan, were analysed by S. Zhamburbayeva & G.A. Ilsasova (2024), who identified potential applications of blockchain to enhance transparency, security, and data reliability across various sectors. The researchers identified the need to develop new legislative acts and to adapt existing regulatory documents in order to create an enabling legal environment for blockchain, emphasising the importance of international cooperation and the exchange of best practices in this domain. They also highlighted the advantages of blockchain technologies, including the reduction of human-error-related risks, lower operational costs, and enhanced security in data transmission.

An alternative perspective on the evolution of cyber strategy was presented by N. Katagiri (2022) through an examination of Japan's cybersecurity policy between 2017 and 2020. The author concluded that policy changes remained moderate due to the resilience of existing constraints on the use of force. The analysis demonstrated that Japan's traditionally defensive posture continued to underpin the deterrent nature of its cyber strategy, evident in the legal system's status-quo orientation and in the country's adherence to international expectations regarding responsible state behaviour in cyberspace. The study showed that structural influences on governmental cybersecurity activity are likely to emerge only in the long term, given Japan's preference for a fragmented approach to addressing persistent challenges in

cyberspace. This conservative stance stands in marked contrast to the more assertive cybersecurity strategies developing in Central Asian states and illustrates the diversity of national models for regulating cyberspace across the Asian region. At the same time, issues concerning the harmonisation of national cybersecurity legislation and the mechanisms of international cooperation among states in the region to counter cross-border cyber threats have remained insufficiently explored. This research aimed to identify avenues for modernising the national cybersecurity system of the Republic of Kazakhstan. The objectives were as follows:

1. To analyse the current state of Kazakhstan's national cybersecurity system, including its legal framework and the effectiveness of law enforcement;

2. To examine cybersecurity practices in Japan, South Korea, and China in order to identify successful elements suitable for adaptation;

3. To develop recommendations for modernising Kazakhstan's national cybersecurity system on the basis of the conducted analysis.

Materials and Methods

The study employed a comprehensive legal approach grounded in the conceptual frameworks of international law and comparative jurisprudence, supplemented by theoretical foundations in public administration and institutional analysis. Its theoretical basis was formed by doctrinal principles concerning the implementation of international cybersecurity standards in national legal systems and by concepts addressing the relationship between governance quality and the effectiveness of national cyber-defence systems. The research materials included Kazakhstan's regulatory acts on cybersecurity, official statistical data issued by state authorities, international rankings and indices, legislation of Asia-Pacific states, reports of national computer emergency response teams, as well as analytical publications produced by international organisations and leading law firms. The methodological framework was informed by theories of legal transformation in post-Soviet states, which enabled an assessment of the transition from fragmented to comprehensive cybersecurity systems under conditions of institutional reform.

The study was conducted in three sequential stages in accordance with its stated objectives. The first stage involved a legal analysis of Kazakhstan's cybersecurity regulatory landscape using the formal-legal method to examine the structure and content of the core legislative acts. The analysis covered the provisions of the Law of the Republic of Kazakhstan No. 418-V ZRK (2015), the Law of the Republic of Kazakhstan No. 94-V ZRK (2013) as amended in 2024, and the relevant chapters of the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014). Additional attention was given to the Code of the Republic of Kazakhstan No. 235-V KRK (2014) to assess administrative sanctions for violations in the field of cybersecurity, and to the Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ (2014) to understand procedural aspects of cybercrime investigations. Strategic documents, including Government Decree of the Republic of Kazakhstan No. 407 (2017) and Government Decree of the Republic of Kazakhstan No. 269 (2023), were examined. Analytical publications from leading law firms, including AEQUITAS Law Firm (2024) reports on doing business in Kazakhstan and S. Akhmetova (2024) materials on state supervision of personal data protection, were also utilised to assess enforcement practices and recent legislative developments. This comprehensive analysis aimed to identify gaps in legal regulation, evaluate the system of sanctioning mechanisms, and determine the extent to which national legislation corresponds to contemporary cybersecurity challenges.

The second stage involved an empirical analysis of the effectiveness of Kazakhstan's cybersecurity system using statistical and correlation-based methods. A quantitative assessment of the dynamics of cyber incidents was conducted on the basis of official data from the national response centre KZ-CERT, published by the Forum of Incident Response and Security Teams (n.d.). Statistical materials from the OSCE (Organization for Security and Co-operation in Europe) M. Stickings & J. Nosal (2024) concerning countercybercrime efforts in Central Asia were also examined. Official statistics from the State Technical Service (Cyber attacks of 2024…, 2025) on cyberattacks recorded in 2024, as well as judicial statistics reported by the Less than half of criminal cases… (2025), were processed. Additional data were drawn from the Committee for National Security of the Republic of Kazakhstan (2021) on the prevention of cyberattacks and from the F. Mukhametgali (2024) on court verdicts in cybercrime cases. A correlation analysis was employed to identify statistically significant associations between four key governance-quality indicators from the Worldwide Governance Indicators – Regulatory Quality, Rule of Law, Control of Corruption, and Political Stability and Absence of Violence/Terrorism (Worldwide Governance Indicators, 2024) – and cybercrime metrics, including the number of registered cybercrimes per 100,000 population and the percentage of cases resulting in convictions. Data from the NCSI (National Cyber Security Index, n.d.) were used to evaluate the overall condition of the national cybersecurity system. Official media reports on Kazakhstan's position in the 2024 Global Cybersecurity Index were examined (Abuova, 2024). The Global Cybercrime Report 2024… (2024) and ITU (International Telecommunication Union, 2020) data on international cybersecurity indicators for Asia-Pacific states were also analysed, enabling an assessment of Kazakhstan's standing relative to other countries in the region in terms of cyber-threat levels. Analytical materials on the economic losses caused by cybercrime, prepared by the Eurasian Research Institute (2025) and S. Kergroach *et al.* (2024), along with global statistics from Evolve Security on the cost of cybercrime, were reviewed. The regional report of the Asia Pacific Computer Emergency Response Team (APCERT, 2024) was additionally analysed to contextualise Kazakhstan's indicators within the broader Asia-Pacific cybersecurity landscape.

Data from the Ministry of Education and Science of the Republic of Kazakhstan on the number of cybersecurity education programmes available on the Univision.kz platform (n.d.a; n.d.b) as of 2024 were used to assess the state of human-capital development in this field.

The third stage involved a comparative legal analysis of national cybersecurity systems to identify key elements of successful regulatory models. Japan's legal system was examined through an analysis of the Act of Japan No. 104 (2014) as amended in 2019, the Act of Japan No. 57 (2003) together with the official Guidelines of the Personal Information Protection Commission (2022), and the Act of Japan No. 128 (1999) to understand the criminal-law mechanisms involved. Official documents of the Government of Japan (n.d.) concerning policies for the protection of critical infrastructure were examined. South Korean legislation was analysed, including the Act of the Republic of Korea No. 14080 (2016), Act of the Republic of Korea No. 14122 (2016) and Act of the Republic of Korea No. 19234 (2023), which together form the basis of the Data 3 Act package of 2020, with the most recent amendments in 2024. The national cybersecurity strategy of South Korea was reviewed using materials from the South Korea's 2024 Cyber Strategy: A Primer (2024). Chinese legislation was studied through a review of key laws, including the Cybersecurity Law of the People's Republic of China (Creemers *et al.*, 2018), Data Security Law of the People's Republic of China No. 84 (2021), and Personal Information Protection Law of the People's Republic of China No. 91 (2021), as well as regulatory documents issued by the CAC (Cyberspace Administration of China) (Regulations on the Management of Online Data…, 2021) and relevant provisions of the Criminal Law of the People's Republic of China (1979) concerning criminal liability for cyber offences. Analytical materials from international law firms, including Baker McKenzie (2025), were utilised to understand practical aspects of legislative implementation. Documents from the Council of Europe (2022; 2023; 2024) were examined to assess Kazakhstan's status with regard to the Budapest Convention on Cybercrime and mechanisms of international legal assistance, including materials on the network of 24-hour contact points and the Second Additional Protocol on electronic evidence. The bilateral agreement on mutual legal assistance between Kazakhstan and the United States of America was examined (International treaty UK/Kazakhstan TS No. 25/2016, 2016). A comparative analysis of operational models of incident response centres was conducted through a study of the Japan Computer Emergency Response Team Coordination Center (JPCERT, 2024) based on the organisation's official information and international cybersecurity indicators for Japan (National Cyber Security Index, n.d.; International Telecommunication Union, 2020), as well as statistical reports from the Coordination Center. The South Korean centre KrCERT/CC was analysed using the NATO Cooperative Cyber Defence Centre of Excellence (Cho, 2022) report, alongside the activities of Kazakhstan's KZ-CERT, drawing on materials from, which allowed for an evaluation of operational capabilities, resource provision, and the effectiveness of national incident response systems from a comparative perspective.

Results

Legal framework and law enforcement in Kazakhstan

An analysis of current legislation in the Republic of Kazakhstan revealed a fragmented legal system, characterised by the absence of a single codified act and a multiplicity of regulatory documents with varying legal force. The legal foundation of Kazakhstan's cybersecurity framework is formed by two primary legislative acts: the Law of the Republic of Kazakhstan No. 418-V ZRK (2015) of 24 November 2015, and the Law of the Republic of Kazakhstan No. 94-V ZRK (2013) of 21 May 2013, as amended in 2024. The Law of the Republic of Kazakhstan No. 418-V ZRK (2015) establishes the legal foundations for the creation, operation, and protection of information systems. It defines the concept of critical information infrastructure (CII), obliges CII operators to register, develop and implement security policies, and to report incidents to the authorised body. Article 1 of the Law defines information security as the state of protection of information and information systems against unauthorised access, use, disclosure, destruction, modification, or loss. Article 29 stipulates that owners of information systems are required to ensure the protection of information in accordance with the legal requirements on information security and personal data. At the same time, legal analysis reveals that the Law contains numerous references to subordinate regulations and grants wide discretion to executive authorities regarding specific technical standards. Notably, the text does not include provisions on cyber incidents, procedures for their investigation, or mechanisms for interagency coordination in responding to cyberattacks (AEQUITAS Law Firm, 2024).

The Law of the Republic of Kazakhstan No. 94-V ZRK (2013) establishes a regime for the localisation of personal data within Kazakhstan and introduces mechanisms for reporting security breaches. Article 15 provides that the personal data of citizens of the Republic of Kazakhstan must be stored in personal data databases located on Kazakhstani territory, while Article 17 permits the transfer of personal data abroad only if the receiving state provides an adequate level of data protection or if the data subject has provided written consent. The 2024 amendments introduced the concept of a "personal data security breach", obliging organisations to report leaks to the Ministry of Digital Development and Innovations, prohibiting the collection of physical document copies, and establishing a 33-point checklist to verify compliance with requirements (Akhmetova, 2024). Article 191 of the Law, in its revised version, requires personal data operators to notify the authorised body of a security breach within one working day of its detection. The notification must include information on the nature of the breach, the number of data subjects affected, potential consequences, and measures taken to address the

incident (AEQUITAS Law Firm, 2024). However, enforcement practice reveals a lack of effective mechanisms to ensure compliance with localisation requirements, including audit procedures for data centres, the maintenance of storage registries, and the application of sanctions for violations.

Strategic planning in the field of cybersecurity is carried out through the national programmes set out in Government Decree of the Republic of Kazakhstan No. 407 (2017) for 2017-2021 and Government Decree of the Republic of Kazakhstan No. 269 (2023) for 2023-2029. The 2017 Cyber Shield of Kazakhstan concept defines cybersecurity as a key condition for joining the club of the most developed nations and sets out objectives to raise public awareness, develop domestic information and communication technology (ICT) products, improve law enforcement operations, and establish an adaptive information-security management system for critical information infrastructure. The 2023-2029 strategy envisages the implementation of a risk-based approach to cybersecurity management, the development of public-private partnerships, and the harmonisation of national legislation with international standards, including the establishment of a unified national centre for cyber-threat monitoring. The digital transformation concept allocates responsibilities among ministries and records achievements such as near-complete internet coverage, growth in e-commerce, and the launch of digital farms. However, as a government decree, it can be easily amended and does not carry the force of law (Government Decree of the Republic of Kazakhstan No. 269, 2023). Legal analysis of these documents indicates a largely declarative character, as they lack measurable performance indicators and specific mechanisms for achieving the stated objectives. Kazakhstan's criminal legislation contains a dedicated Chapter 9, "Criminal Offences in the Field of Information Technologies", which includes Articles 205-207 of the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014). The structure of criminal and administrative liability for cybercrime in Kazakhstan is summarised in Table 1.

Table 1. Sanctioning provisions of Kazakhstan's criminal and administrative legislation in the field of cybersecurity

0,25 пт	Qualification	Sanction	Typical verdicts/examples
Art. 205-1, Criminal Code of the Republic of Kazakhstan (2014)	Unauthorised access to computer information (basic form)	Fine of 200-500 monthly calculation indices (MCI), or corrective labour up to 1 year, or restriction of liberty up to 2 years	In 2024, 24 incidents were prosecuted under Art. 205, nearly half carried over from previous years
Art. 205-2, Criminal Code of the Republic of Kazakhstan	Unauthorised access for material gain or by a group of persons	Fine of 500-1000 MCI, or restriction of liberty for 2-4 years, or detention up to 6 months	In January 2025, the Taldykorgan court fined two individuals 300 MCI each for unauthorised access to the Ministry of Health information systems
Art. 205-3, Criminal Code of the Republic of Kazakhstan	Unauthorised access causing significant damage or committed against CII	Fine of 1000-2000 MCI, or restriction of liberty for 3-5 years, or imprisonment up to 5 years	Specific verdicts under this provision are not publicly available
Art. 205-4, Criminal Code of the Republic of Kazakhstan	Unlawful destruction or modification of information relating to CII with serious consequences	Imprisonment for 4-6 years	In 2024, 24 cases were registered under all parts of the Art. 205, but only a portion were brought to court
Art. 207-1, Criminal Code of the Republic of Kazakhstan	Violation of rules for operating computer systems or their networks (basic form)	Fine of 100-200 MCI, or corrective labour up to 1 year, or restriction of liberty up to 2 years	In 2024, only five incidents were prosecuted under Art. 207
Art. 207-2, Criminal Code of the Republic of Kazakhstan (2014)	Violation of system operation causing significant damage or affecting CII	Fine of 200-500 MCI, or restriction of liberty for 2-5 years, or imprisonment up to 4 years	In December 2020, the Saryarkinsky District Court sentenced an individual for a coordinated distributed denialofservice attack on the electronic public procurement system to 2 years' restriction of liberty and barred him from participating in electronic public procurement activities for 3 years
Art. 210, Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014)	Creation, use, or distribution of malicious computer programs or software products	Fine of 200-500 MCI, or corrective labour up to 1 year, or restriction of liberty up to 3 years	In August 2024, the Kostanay Regional Court sentenced a 24year-old resident for distributing malware to 1 year's restriction of liberty, 100 hours of compulsory labour, a fine of 15 MCI, and confiscation of computer equipment
Arts. 79, 641, Code of the Republic of Kazakhstan No. 235-V KRK (2014)	Violation of legislation on personal data and its protection, including rules on the storage and processing of personal data	Fine for individuals: 10-20 MCI; for officials: 30-50 MCI; for organisations: up to 2000 MCI	Statistics on the application of administrative sanctions are limited in publicly available sources

Note: as of 2024, 1 MCI equals 3,692 KZT (approximately 7.70 USD at the November 2024 exchange rate)
Source: compiled by the authors based on Al-Farabi Kazakh National University (n.d.), Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014), Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ (2014), Committee for National Security of the Republic of Kazakhstan (2021), F. Mukhametgali (2024), Less than half of criminal cases… (2025), Committee of National Security of the Republic of Kazakhstan (2025)

Analysis of Table 1 indicates that sanctions for cybercrime in Kazakhstan are relatively mild compared with the potential losses caused by such offences. Basic offences carry fines ranging from 200 to 500 MCI (approximately 1,540 USD to 3,850 USD) or restriction of liberty for up to two years, while harsher penalties are applied only in the presence of aggravating circumstances. Judicial practice demonstrates a predominance of suspended sentences and restrictions of liberty over actual imprisonment, which diminishes the deterrent effect of criminal sanctions. For example, even in a high-profile case involving a distributed denial-of-service (DDoS) attack on the electronic public procurement system, which caused economic losses by delaying 7,901 government procurements worth 164 billion KZT, the offender received only two years' restriction of liberty without actual incarceration (Committee for National Security of the Republic of Kazakhstan, 2021).

The institutional structure for cybersecurity is characterised by a multi-level organisation with functions distributed across various state bodies, lacking a clearly defined central coordinator. The Committee for Information Security under the Ministry of Digital Development, Innovations, and Aerospace Industry (MDDIAI) sets policy, develops standards, monitors compliance, and coordinates the activities of the national centre KZ-CERT (National Cyber Security Index, n.d.). The national company State Technical Service acts as the operator of the national cyber-attack response centre, monitoring Kazakhstan's segment of the Internet, analysing malicious software, and coordinating responses to cyber incidents. Within this structure, KZ-CERT collects and analyses information on cyber incidents, provides recommendations for addressing vulnerabilities, and conducts educational outreach among users of information systems. The Committee for National Security is responsible for cryptographic protection and countering cyber-espionage, as well as the security of facilities containing state secrets. It conducts operational and investigative activities and pre-trial investigations of cybercrime in accordance with the Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ (2014). In the field of personal data, the authorised body is the Committee for Information Security of the MDDIAI, which, under the Law of the Republic of Kazakhstan No. 94-V ZRK (2013) and the Code of the Republic of Kazakhstan No. 235-V KRK (2014), supervises compliance, considers complaints from data subjects, and initiates administrative proceedings against violators. However, Kazakhstan lacks a single, centralised coordination centre comparable to Japan's National Information Security Centre (NISC) and does not have an overarching cybersecurity strategy. As a result, the functions of different agencies often overlap, leading to inefficient use of resources and slower responses to cyber incidents.

Kazakhstan is not yet a Party to the 2001 Budapest Convention on Cybercrime: on 19 April 2023, the country was invited to accede (Council of Europe, 2023), with the invitation valid until April 2028. As of November 2025, the ratification instrument has not been deposited, so Kazakhstan is not yet part of the Convention's network of 24/7 points of contact (POC) and cannot sign the Second Additional Protocol on Electronic Evidence (Council of Europe, 2022). Nevertheless, the MDDIAI and the Ministry of Internal Affairs are cooperating with the Council of Europe under the Octopus project to align national legislation with the Convention and to establish a national 24/7 POC (Council of Europe, 2024). For international legal assistance (MLAT), Kazakhstan relies on regional agreements within the Commonwealth of Independent States (CIS) and bilateral treaties on mutual legal assistance, including with the United States of America (signed 20 February 2015, entered into force 6 December 2016) (International treaty UK/Kazakhstan TS No.25/2016, 2016), while urgent requests are processed through the National Central Bureau of INTERPOL and KZ-CERT channels.

Trends in cyber incidents and investigations (2019-2024)

KZ-CERT statistics demonstrate a sustained increase in the number of cyber incidents in Kazakhstan between 2019 and 2024, with an average annual growth rate of 14.5%, significantly outpacing the pace of the country's digitalisation of the economy. According to the OSCE (Stickings & Nosal, 2024), the number of registered cybercrimes in Kazakhstan rose from 589 cases in 2018 to 21,479 in 2021, representing an increase of more than 36-fold. In 2019, 20,800 incidents were recorded, of which 17,300 involved botnet activity, 201 were DDoS attacks, and the remainder comprised other types of cyber threats, including phishing, malware, and attempts at unauthorised access. Official data from the Cyber attacks of 2024… (2025) for 2024 records over 41,000 incidents, approximately 66% of which involved malware infections, around 20% were phishing campaigns, 8% were DDoS attacks, and 6% consisted of other threat types. According to the Cyber and Digital Security forum organised by the State Technical Service in 2024, 740 million cyberattacks were blocked, and more than 6,500 DDoS attacks on critical information infrastructure were successfully repelled. Sectoral analysis shows that the most targeted sectors are financial services (28% of incidents), public administration (22%), telecommunications (18%), and energy (15%) (Nguyen *et al.*, 2021).

Financial losses from cybercrime illustrate the scale of the problem for Kazakhstan's economy. The 2025 report of the Eurasian Research Institute provides specific figures: in 2023, citizens lost over 17.5 billion KZT (approximately 37 million USD) due to digital fraud, and in 2024, 11,765 cases of online fraud were registered, only 152 more than in 2023, representing an increase of 1.31% (Eurasian Research Institute, 2025). Frauds included phishing, counterfeit banking websites, investment scams, and credential theft. Compared with a population of approximately 20 million, these figures may appear modest; however, experts consider the actual number of incidents to be substantially higher due to the low rate of reporting to the police. Global losses from cybercrime exceeded 8 trillion USD in 2022 and are projected to reach 10.5 trillion USD by 2025, reflecting an

annual growth rate of 15% (Hernandez, n.d.). At the enterprise level, according to the OECD, the median cost of a ransomware attack can reach up to 1.2 million USD, while a data breach may incur losses of up to 1.6 million USD (Kergroach *et al*., 2024).

Judicial statistics confirm systemic problems in law enforcement and cybercrime investigation, with a low proportion of cases reaching court. According to the Less than half of criminal cases… (2025), in 2024, 99 criminal offences in the information and communication technology sector were registered in Kazakhstan; however, only 44 were investigated, and merely 36 cases were referred to court, representing 36% of the registered incidents. The largest share of registered offences comprised 70 cases of information destruction or modification, whereas only five incidents were prosecuted under Article 207 of the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014) for disrupting the operation of an information system or telecommunications network, and 24 cases under Article 205 for unauthorised access to an information system, with nearly half of these cases carried over from previous years. Twenty-eight cases were closed due to statute of limitations or the inability to identify the perpetrator, highlighting difficulties in tracing offenders and collecting digital evidence.

A detailed analysis of individual court cases illustrates characteristic issues within Kazakhstan's criminal justice system regarding cybercrime. In December 2020, the Saryarkinsky District Court of Nur-Sultan convicted an individual for a coordinated DDoS attack on the electronic government procurement system in May of the same year (Committee for National Security of the Republic of Kazakhstan, 2021). The cyberattack caused the goszakup.gov.kz platform to become non-operational, resulting in the postponement of 7,901 government procurement procedures valued at 164 billion tenge due to the technical impossibility of conducting electronic tenders as scheduled. The perpetrator, who sought to gain advantages in government procurement, was identified by the Committee for National Security with the assistance of the Electronic Finance Centre. Following a computer-technical examination, the defendant was found guilty under Part 2, Paragraph 1 of Article 207 of the Criminal Code and sentenced to two years of restricted liberty, with a three-year prohibition on engaging in activities related to electronic government procurement (Committee for National Security of the Republic of Kazakhstan, 2021). Notably, even in the face of significant economic damage, the court imposed a relatively lenient sentence without actual imprisonment.

Another case occurred in the Kostanay Region in August 2024, where a local court convicted a 24-year-old resident for distributing malicious software online. The perpetrator, whose activities involved spreading viruses to harvest users' personal data and offering paid tutorials on creating malware, was stopped by the Department of the Committee for National Security and the Police Department. The court found him guilty under Part 1 of Article 210 of the Criminal Code and imposed a sentence of one year of restricted liberty, 100 hours of compulsory labour, a fine of fifteen MCI, and the confiscation of computer equipment (Mukhametgali, 2024). This case illustrates a typical pattern: even when guilt is established and the offender identified, courts often impose suspended or lenient sentences, which do not generate a sufficient deterrent effect.

Formally, criminal liability for unauthorised access, the distribution of malicious software, and fraud is established in the Criminal Code; however, the number of convictions for cybercrimes recorded in the judicial registry remains limited. This indicates challenges in the organisation of investigations, the insufficiency of specialised units, and difficulties in collecting digital evidence. Enforcement effectiveness is further undermined by the lack of specialised training for investigators, the limited technical capacity of expert institutions, and the complexity of international cooperation in investigating cross-border cybercrime.

Correlation between governance quality and cybercrime levels

Governance indicators in Kazakhstan reveal systemic deficiencies in institutional capacity within the cybersecurity sector, negatively affecting the effectiveness of measures to combat cybercrime (Table 2). The correlation between the number of cybercrimes and governance indicators shows a statistically significant negative relationship ($r = -0.67$, $p < 0.01$). This suggests that countries with low rule of law and regulatory quality scores experience higher success rates of cyberattacks and lower effectiveness of law enforcement in investigating cybercrime. Countries with a "Control of Corruption" indicator below zero exhibit, on average, a 40% higher level of cybercrime compared with countries displaying positive values for this indicator.

Table 2. Comparative assessment of Worldwide Governance Indicators, 2023

Country/ Indicator	Regulatory Quality	Rule of Law	Control of Corruption	Political Stability & Absence of Violence/Terrorism
Kazakhstan	+0.07% / 53.3% (+3.3 pp)	-0.45% / 36.8% (-13.2 pp)	-0.27% / 47.2% (-2.8 pp)	-0.27% / 36.5% (-13.5 pp)
Japan	+1.47% / 92.5% (+42.5 pp)	+1.54% / 92.5% (+42.5 pp)	+1.40% / 90.1% (+40.1 pp)	+0.95% / 81.5% (+31.5 pp)
South Korea	+1.12% / 84.9% (+34.9 pp)	+1.25% / 85.8% (+35.8 pp)	+0.89% / 79.7% (+29.7 pp)	+0.61% / 68.2% (+18.2 pp)
China	-0.36% / 38.7% (-11.3 pp)	-0.04% / 52.8% (+2.8 pp)	-0.01% / 54.2% (+4.2 pp)	-0.51% / 25.1% (-24.9 pp)

Note: values are presented as Estimate (range -2.5 to +2.5) / Percentile Rank (0-100%), with deviations from the median percentile (50%) shown in parentheses. Percentile ranks indicate the proportion of countries with lower scores; higher values correspond to better governance quality. Deviations exceeding ±25 percentile points (pp) from the global median are analytically significant for the formulation of policy recommendations

Source: compiled by the authors based on Worldwide Governance Indicators (2024)

A comparative analysis of the Worldwide Governance Indicators presented in Table 2 reveals notable differences in the quality of the institutional environment among the countries studied, which directly correlates with the effectiveness of their cybersecurity systems. Japan and South Korea exhibit high governance quality across all dimensions, creating a favourable institutional environment for effective law enforcement and coordination between the public and private sectors in the field of cybersecurity. Kazakhstan, by contrast, displays predominantly negative values for most indicators, particularly in terms of rule of law, control of corruption, and political stability. This reflects structural institutional weaknesses that hinder the effective implementation of cybersecurity policy and reduce business confidence in state initiatives. The low rule of law indicates difficulties in ensuring legislative compliance and the efficiency of the judicial system. China occupies an intermediate position, with relatively stronger institutional quality indicators than Kazakhstan. This partly explains the Chinese system's ability to maintain centralised control over cyberspace, despite limitations in political stability.

International cybersecurity rankings place Kazakhstan at an average level, indicating scope for significant improvement. According to the 2024 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU), Kazakhstan scored 94.04 out of a possible 100 points, placing it in the second group of "emerging countries". The country achieved full marks of 20 for legal and cooperative measures, 19.38 for technical measures, 18.3 for organisational measures, and 16.36 for capacity development (Abuova, 2024). This outcome indicates that the state has invested in building a regulatory and coordination framework, but requires strengthening of human resources, as the lowest score was recorded in capacity development. According to the NCSI, Kazakhstan ranks 38th with a score of 73.33, below the East Asian countries: South Korea ranks 22nd with 83.33 points, while China is 53rd with 60.00 points (National Cyber Security Index, n.d.). For Japan, the International Telecommunication Union (2020) places the country 7th in the Global Cybersecurity Index with a score of 97.82. NCSI reports a score of 63.64 for Japan, corresponding to 52nd in the global ranking. The MixMode analytical report, based on a comprehensive analysis of four indices, indicates Japan's cyber resilience index at 82.29 and an overall cybersecurity score of 88.77, reflecting the country's strong technical and organisational base (Global Cybercrime Report 2024…, 2024).

Sociological research on public awareness in Kazakhstan indicates relatively high levels of citizen knowledge about cyber threats, albeit with a notable gap between knowledge and behaviour. A 2023 government survey found that 80.4% of respondents were aware of the existence of cyber threats, 74.64% could identify phishing messages, and 90.52% possessed skills to protect personal data on social networks (Eurasian Research Institute, 2025). In 2024, the Ministry of Digital Development launched an interactive platform, Cyberlabyrinth, where schoolchildren and university students learn the basics of cyber hygiene through gamified activities and receive certificates. The programme has become popular and contributed to growing interest in information technology careers. Cybersecurity weeks are also actively conducted, involving banks, telecom operators, and civil society organisations. However, high awareness does not necessarily translate into behavioural change, as many citizens continue to use weak passwords, install pirated software, and connect to unsecured Wi-Fi networks. According to the Ministry of Education and Science (Univision.kz, n.d.a, n.d.b), by 2024, Kazakhstan offered only 12 undergraduate and eight postgraduate programmes in information security, which does not meet labour market demand. At the same time, there were approximately 1,500 certified cybersecurity specialists, an insufficient number to meet the needs of both the public and private sectors.

Comparative legal analysis of the cybersecurity systems of Kazakhstan, Japan, South Korea, and China

The Japanese cybersecurity model is founded on comprehensive legislation with centralised coordination and principles of shared responsibility. Act of Japan No. 104 (2014), as amended in 2019, establishes the fundamental principles and identifies responsible entities, emphasising the protection of citizens' lives and rights, economic prosperity, and national security, while promoting the free and secure flow of information. Between 2020 and 2022, the Act on the Protection of Personal Information (APPI) was significantly updated. Amendments effective from 1 April 2022 expanded obligations regarding data breach notifications, tightened requirements for cross-border transfers of personal information, and substantially increased the maximum fines for legal entities (up to 100 million JPY) for non-compliance with directives issued by the Personal Information Protection Commission (PPC). Article 1 of the Act establishes the aim of ensuring a safe and peaceful society through comprehensive and effective cybersecurity measures, while Article 2 defines cybersecurity as the prevention of leaks, loss, destruction, and other incidents concerning electronic information and information systems, as well as the maintenance of stable system operations and their effective utilisation. The law allocates responsibilities among the national government, local authorities, operators of critical information infrastructure, enterprises, and citizens, delineating the role of each. It also mandates the development of a national cybersecurity strategy and establishes a Cybersecurity Headquarters under the Cabinet of Ministers. In practice, these functions are carried out by the National Centre of Incident Response and Strategic Coordination (NISC), which coordinates policy, develops standards for government systems, conducts audits, and manages the government network monitoring centre (Government of Japan, n.d.). In 2024, the Japanese government updated the Critical Infrastructure Protection Policy, adding ports and harbours to the list of critical sectors, thereby expanding the scope of responsibility for logistics service providers. According to JPCERT/CC (Japan Computer

Emergency Response Team Coordination Center), in 2023 alone, the organisation received 65,669 reports of computerrelated incidents from Japan and abroad, reflecting both the scale of cyberattacks and the key role of the national Computer Security Incident Response Team (CSIRT) in the practical implementation of state cybersecurity policy (JPCERT Coordination Center, 2024).

The South Korean system is characterised by comprehensive regulatory governance through a combination of specialised laws, mandatory standards, and active international cooperation. The legal framework is centred on three principal data laws: the Personal Information Protection Act (PIPA), including Act of the Republic of Korea No. 19234 (2023); the Information and Communications Network Act (Network Act), with one of the key versions being Act of the Republic of Korea No. 14080 (2016); and the Credit Information Use and Protection Act (Act of the Republic of Korea No. 14122, 2016). The 2020 amendments to these three acts, known collectively as the Data 3 Act package, centralised regulatory authority over privacy by transferring the previously fragmented functions of the Ministry of the Interior and the Korea Communications Commission to the unified Personal Information Protection Commission (PIPC), elevating its status as the central supervisory body for personal information protection. The PIPA serves as the foundational privacy law, establishing principles of data minimisation, legality, and transparency, as well as requirements for obtaining consent from data subjects. The Network Act, in turn, regulates the activities of telecommunications service providers, obliging them to implement measures to prevent data leaks, combat spam, follow incident reporting procedures, and granting authorities the power to issue orders to rectify violations (Baker McKenzie, 2025). Following the amendments to the Network Act, network operators and online service providers are required to notify affected users immediately in the event of a personal data breach and submit an initial report to the Korea Communications Commission or the Korea Internet & Security Agency within 24 hours of detecting the incident. Under the general PIPA framework, a report must be submitted to the PIPC and data subjects informed no later than 72 hours after the breach is discovered. Article 44-7 of the Information and Communications Network Act (ICNA) prohibits the dissemination of unlawful information that harms minors or infringes the rights of third parties, granting the Korea Communications Commission the authority to issue orders for its removal. Article 45 establishes obligations for information and communications service providers to implement technical and administrative measures to protect users' personal information (Anderson *et al*., 2015). In 2024, amendments to the Network Act strengthened measures against illegal spam, simplified the certification process for the Information Security Management System (ISMS), and granted authorities the power to issue orders to rectify violations and impose fines on non-compliant operators. The same year, the National Cybersecurity Strategy 2024 was adopted, explicitly identifying North Korea as a primary threat and emphasising the zero-trust principle. The strategy introduces a classification of incidents by severity and obliges organisations to report breaches within prescribed timeframes (South Korea's 2024 Cyber Strategy: A Primer, 2024).

The Chinese cybersecurity model is characterised by a centralised regulatory approach to cyberspace, underpinned by a comprehensive legislative framework that includes the Cybersecurity Law of the People's Republic of China (Creemers *et al*., 2018), the Law of the People's Republic of China No. 84 (2021), and the Personal Information Protection Law of the People's Republic of China No. 91 (2021). The central coordinator of China's cybersecurity framework is the CAC, which holds extensive authority over oversight, certification, and enforcement of sanctions. The Chinese model imposes stringent data localisation requirements: operators of critical information infrastructure must store personal data and "important information" collected within the territory of the People's Republic of China on servers located domestically. Cross-border data transfers are permitted only after undergoing a state security assessment, creating additional barriers and costs for international companies providing digital services to Chinese users. These restrictions are directly linked to the doctrine of "cyber sovereignty" enshrined in the Cybersecurity Law, under which the state asserts full sovereignty over its national cyberspace and uses data flow regulation as a tool to protect national security and establish domestic rules for the global digital order. The Multi-Level Protection Scheme (MLPS 2.0) establishes a graduated classification of information systems across five levels of criticality, with corresponding requirements for certification, technical protection, and regular inspections (Regulations on the Management of Online Data…, 2021). A comparative analysis of procedural and sanctioning mechanisms in the cybersecurity legal frameworks of the countries studied is summarised in Table 3. The comparative analysis of procedural mechanisms in Table 3 reveals fundamental differences in approaches to ensuring cybersecurity and their alignment with the maturity of legal systems. The South Korean and Chinese systems are the most structured, featuring clear procedural frameworks with specific deadlines and enforcement mechanisms. The Chinese model additionally relies on data localisation requirements and the principle of cyber sovereignty, which significantly affect the ability of international companies to transfer user data abroad. The Japanese model is characterised by greater flexibility and an emphasis on voluntary cooperation, reflecting a high level of trust between the state and the private sector. Kazakhstan's system exhibits the greatest fragmentation in procedural mechanisms, with reporting deadlines limited solely to the sphere of personal data and lacking comprehensive requirements for CII. A pronounced disparity exists between the potential scale of damage from cyber incidents and the sanctioning mechanisms in Kazakhstan: the maximum administrative

fine is only 15,200 USD, whereas in South Korea and China, fines may reach millions of dollars or a percentage of a company's global turnover. This underscores the need for a fundamental overhaul of approaches to deterring cybercrime and ensuring operator accountability for compliance with cybersecurity requirements.

Table 3. Comparative analysis of procedural and sanctioning mechanisms in cybersecurity legal frameworks

Country	Mandatory incident notification period	Maximum administrative fine for organisations	Maximum criminal penalty for unauthorised access	Personal data localisation requirement	Central coordinator/ regulator	Sources
Kazakhstan	1 working day to the Ministry of Digital Development, Innovation and Aerospace Industry	Up to 2,000 monthly calculation indices – approximately 7.3 million KZT (≈ 15,200 USD) for serious personal data violations	Imprisonment up to 7 years	Yes; storage restricted to the territory of the Republic of Kazakhstan	Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry + KZCERT	Arts. 19-1, 15 Law of the Republic of Kazakhstan No. 94-V ZRK (2013); Arts. 79, 641 Code of the Republic of Kazakhstan No. 235-V KRK (2014); Art. 205(4) Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014)
Japan	Preliminary notification: 3-5 days; final notification: up to 30 days	100 million JPY (≈ 660,000 USD) for corporations	Up to 3 years' imprisonment or a fine of up to 1 million JPY (≈ 6,600 USD)	No; crossborder transfers allowed with consent and recipient obligations	Cybersecurity Strategic Headquarters of the Cabinet + Personal Information Protection Commission	Guidelines of the Personal Information Protection Commission for the Act on the Protection of Personal Information (2022); Art. 832 Act of Japan No. 57 (2003); Art. 11 Act of Japan No. 128 (1999); Act of Japan No. 104 (2014); Government of Japan (n.d.)
South Korea	Immediate to users; within 24 hours to the Korea Communications Commission / Korea Internet & Security Agency (Network Act); within 72 hours to the PIPA	Up to 3% of global turnover or 3 billion KRW (≈ 2 million USD) for serious violations	Up to 5 years' imprisonment or a fine of 50 million KRW (≈ 35,700 USD)	No general requirement; consent of the data subject and specific contractual guarantees are required	Korea Internet & Security Agency / PIPC	Arts. 64-2, 71 Act of the Republic of Korea No. 14080 (2016, amended 2024); Act of the Republic of Korea No. 19234 (2023)
China (PRC)	Initial notification within 8 hours; full report within 5 working days	Up to 50 million CNY or 5% of annual turnover (≈ 7 million USD)	5-7 years' imprisonment for serious cyberattacks	Yes; for critical information infrastructure – storage within China and prior state security assessment for export	CAC	Regulations on the Management of Online Data... (2021); Art. 40, 66 Personal Information Protection Law of the People's Republic of China No. 91 (2021); Art. 286 Criminal Law of the People's Republic of China (1979); Art. 37 Cybersecurity Law of the People's Republic of China (Creemers *et al.*, 2018)

Note: maximum sanctions listed relate to the basic offence of "unauthorised access" and may increase under aggravating circumstances. The Act on the Protection of Personal Information refers to the Japanese law on the protection of personal information

Source: compiled by the authors

Functional analysis of incident response centres highlights significant differences in operational capacity, resource allocation, and overall effectiveness compared with Kazakhstan's KZ-CERT. Japan's JPCERT/CC, established in 1996, was the country's first Computer Security Incident Response Team (CSIRT) and effectively functions as a national "CSIRT centre". It coordinates interaction among network service providers, software developers, government agencies, and industry associations and played a key role in forming the Asia Pacific Computer Emergency Response Team (APCERT) network. The organisation receives information on incidents and malware from global partners, conducts technical and threat analyses, rapidly disseminates relevant data to stakeholders, and coordinates responses with national and international CSIRTs. JPCERT/CC operates as a neutral and independent entity, free from governmental control (Japan Computer Emergency Response Team Coordination Center, n.d.). Its statistics demonstrate the effectiveness of Japan's system: in 2023, the centre received 65,690 incident reports and handled 19,720 coordination cases, reflecting a highquality filtering and response process with a 30% handling rate (JPCERT Coordination Center, 2024).

South Korea's KrCERT/CC (Korea Computer Emergency Response Team Coordination Center), operating under the Korea Internet & Security Agency (KISA), offers a wide range of services. It provides consultation and receives reports on vulnerabilities and incidents, issues timely recommendations for vulnerability remediation to the private sector, assists with inspections of personal computers and Internet of Things (IoT) devices, supports small and medium-sized enterprises, strengthens website security, organises cyber training, and shares threat intelligence with private companies and academic institutions (Cho, 2022). KrCERT also monitors malware infections on over four million Korean websites and employs an automated Cyber Threat Analysis System (C-TAS) for data sharing. By comparison, Kazakhstan's KZ-CERT holds national and governmental authority and is responsible for every host or subnet connected to the Kazakh segment of the Internet (Forum of Incident Response and Security Teams, n.d.). However, it suffers from limited human and financial resources, lacks its own earlywarning system, and publishes insufficient information on incidents.

Recommendations for modernising Kazakhstan'snational cybersecurity system

The results of the comparative analysis allow the identification of key elements of successful cybersecurity systems in East Asian countries and inform concrete recommendations for Kazakhstan. All three countries demonstrate the presence of comprehensive framework laws or interconnected legislative acts covering both cybersecurity and personal data protection. Japan and China have enacted separate statutes that define core principles and establish coordinating authorities, whereas South Korea relies on several specialised laws complemented by a national strategy. The central role of a specialised coordinating body is evident in the functioning of Japan's NISC for strategic planning and coordination, the Cybersecurity Council under the President in South Korea, and CAC, all of which have the authority to issue binding directives, conduct audits, and allocate resources. Mandatory certification and standardisation systems are characterised by differing approaches: South Korea has implemented compulsory ISMS certification for network operators, China has introduced the MLPS, and Japan sets standards for government systems. Based on these observed patterns and the identified differences between national cybersecurity regulatory models, the following priority directions are proposed for modernising Kazakhstan's system.

The foremost task in modernising the national cybersecurity system is the codification of legislation to eliminate fragmented regulation and establish a unified legal framework. By the end of 2026, it is advisable to draft and submit to Parliament a single foundational law, On Cybersecurity, which integrates provisions of the current Law of the Republic of Kazakhstan No. 418-V ZRK (2015) and Law of the Republic of Kazakhstan No. 94-V ZRK (2013), supplemented with specific provisions on cyber-incident response procedures, interagency coordination mechanisms, and requirements for operators of CII. The proposed legislation should set clear deadlines for reporting different types of incidents, specifically no more than 24 hours for CII and 72 hours for other sectors, alongside a graduated classification system for incidents based on severity and corresponding response procedures. The anticipated outcome of this codification is the creation of a unified legal framework that addresses gaps and overlaps, enhances the predictability of regulation, and simplifies compliance for economic actors.

A second critical area of modernisation is the establishment of an effective institutional architecture to coordinate the efforts of different agencies in the field of cybersecurity. By mid-2026, it will be necessary to establish a National Cybersecurity Headquarters within the Office of the Prime Minister, with authority for strategic planning, coordinating the activities of all agencies in cybersecurity, approving mandatory standards for CII, and allocating budgetary resources. The proposed structure should include representatives from the MDDIAI, the Committee for National Security, the Ministry of Internal Affairs, the Ministry of Defence, and the private sector, thereby ensuring interagency coordination and public-private partnership, following the model of Japan's NISC. Concurrently, KZ-CERT should be reorganised into a fully-fledged national incident response centre with expanded powers, an increased staff of up to 100 specialists by 2028, and a budget sufficient to implement early threat detection systems and automated analysis. This approach would eliminate the duplication of functions across agencies, increase the speed of response to cyber incidents by 40%, and improve coordination between the public and private sectors.

A third priority is the strengthening of sanctions mechanisms and the introduction of an objective system for monitoring the effectiveness of law enforcement activities in combating cybercrime. By 2027, amendments should be made to the Criminal Code of the Republic of Kazakhstan No. 226-V KRZ (2014), raising maximum penalties for cybercrimes to levels commensurate with the potential losses arising from such offences. The proposed amendments envisage the introduction of fines for organisations of up to 10,000 MCI or 3% of annual turnover, whichever is higher, custodial sentences of up to seven years for basic offences, and up to 12 years for aggravated offences involving CII, thereby aligning Kazakhstan's legislation more closely with the standards of South Korea and China. Simultaneously, it is necessary to establish mandatory KPIs for law enforcement agencies, including a target of 50% for the proportion of cybercrimes solved by 2028, an average time from detection to suspect apprehension of 30 days for internal affairs cases, and a target of 60% for cases brought to a guilty verdict by 2028. To achieve these targets, specialised cyber-police units should be established in each regional directorate of the Ministry of Internal Affairs, staffed with a minimum of 15 certified specialists who have completed international training in digital forensics. Implementing this package of measures will enhance the preventive effect of criminal

sanctions, increase the proportion of solved cybercrimes from the current 36% to 50%, and strengthen citizen and business confidence in the effectiveness of the law enforcement system.

A fourth strategic priority is the systematic development of human capital in cybersecurity, identified as the weakest link in Kazakhstan's system according to international rankings. By 2027, the Ministry of Education and Science should increase the number of cybersecurity and related programmes to 25 undergraduate and 15 postgraduate courses in leading national universities, representing more than a twofold increase from the current level. In parallel with the expansion of formal education, it is advisable to introduce a state programme for the training and certification of cybersecurity specialists, targeting 5,000 certified professionals by 2028. This would more than triple the current number of approximately 1,500 specialists. To support continuous professional development, a national centre for advanced training should be established for civil servants and employees of CII, with mandatory cybersecurity courses every two years. An additional incentive to attract young talent to the cybersecurity field could be the introduction of scholarship programmes for students in relevant disciplines, with a compulsory service period of at least three years in government bodies or at CII facilities. Comprehensive implementation of these measures will ensure the labour market has sufficient qualified personnel, reduce dependence on foreign consultants, and raise the overall level of cybersecurity awareness across society.

The proposed measures can be applied by the MDDIAI and the State Technical Service to draft a unified cybersecurity law and establish a centralised coordination centre. Strengthening the training of investigators and specialised cyber-police units will contribute to an increased rate of accountability for cybercrime and enhance the overall effectiveness of law enforcement. The findings of this study may also serve as a reference for private-sector entities in developing corporate cybersecurity strategies and provide a model for other Central Asian countries currently modernising their cybersecurity systems.

Discussion

The identified fragmentation of Kazakhstan's cybersecurity legal framework is corroborated by global trends analysed by international researchers. A. Marotta & S. Madnick (2025) examined over 170 cybersecurity regulations across different world regions and identified inconsistencies between national approaches to cyberspace governance. Their study revealed that organisations operating in international environments face a complex web of international, national, and local regulations, complicating compliance due to variations in scope, stringency, and enforcement. These findings align with the situation in Kazakhstan, where the absence of a single codified law and the coexistence of multiple regulatory instruments of varying legal authority reflect similar challenges. Moreover, the study demonstrates that regulatory fragmentation is not limited to transitional economies but is also characteristic of developed jurisdictions, indicating that this is a systemic global challenge.

The observed rise in cyber incidents in Kazakhstan, with an average annual growth rate of 14.5%, mirrors the global escalation of cyber threats, as confirmed by European studies. N. Vandezande (2024) analysed European Union statistics and found that the proportion of enterprises affected by cyber incidents increased from 12% in 2018 to 22% in 2021, reflecting a similar trend in threat growth. The research also recorded a 41% increase in ransomware attacks in 2022 and a 48% rise in email-based attacks, correlating with Kazakhstani data showing the predominance of malware (66% of incidents) and phishing campaigns (20% of incidents). R. Pellreddy (2025) highlights the growing vulnerability of CII to cyber threats, corroborating Kazakhstani data that identify the most frequently targeted sectors: financial services, public administration, telecommunications, and energy. D. Markopoulou & V. Papakonstantinou (2021) analysed the concept of CII in the context of cyber threats and found that the increasing dependence of CII on ICT for operational functionality creates complex challenges for both infrastructure operators and policymakers. This convergence of findings indicates that cybersecurity challenges are universal, irrespective of a country's level of economic development.

The low effectiveness of law enforcement in Kazakhstan, with only 36% of cases reaching prosecution, finds parallels in studies of incident response systems in other jurisdictions. S. Busetti & F.M. Scanni (2025) examined the operation of incident reporting systems in Italy and identified mixed outcomes in their effectiveness. The researchers noted difficulties in detecting and reporting incidents due to organisational capacity constraints, reluctance to report breaches, and limited ability to respond to complex incidents. At the same time, the study shows that even with improvements in reporting system design, from NIS1 to NIS2, the connection between incident reporting and the learning process remains weak due to inertia at both central and local levels. These conclusions align closely with Kazakhstani challenges in pre-trial investigation, the insufficiency of specialised units, and difficulties in identifying perpetrators and collecting digital evidence.

The statistically negative correlation identified between governance quality indicators and the level of cybercrime in Kazakhstan is supported by studies of corporate cybersecurity governance in other countries. W. Tan *et al.* (2025) examined the relationship between corporate cybersecurity governance and the market value of Chinese companies, finding that effective cybersecurity governance enhances trust among investors and suppliers through a reputation-building mechanism. The researchers noted that the reputational effect is particularly pronounced in companies with non-myopic management, stronger protection of trade secrets, and greater media attention to environmental, social, and corporate governance issues. These findings underscore the importance of institutional quality not only

at the state level but also within corporations to ensure effective cybersecurity. E. McCoy (2025) analysed the regulatory landscape of the financial sector in the United States of America, the United Kingdom, and the European Union, highlighting challenges arising from policy inconsistencies across governance levels, which complicate the effective regulation of cybersecurity.

A comparative analysis of the Kazakhstani system against Asian practices revealed fundamental differences in procedural mechanisms and institutional architecture, corroborated by research on the evolution of regional cybersecurity approaches. K. Komiyama (2025) examined Japan's proactive cyber defence reforms and identified the complexities involved in transitioning from a traditionally defensive stance to proactive cybersecurity strategies. The Japanese experience illustrates the critical role of legislative reform in expanding the authority of cybersecurity bodies and establishing centralised coordination among multiple government agencies. D.H. Kim & D.H. Park (2024) compared South Korea's PIPA with the European General Data Protection Regulation and identified shortcomings in the protection of fundamental rights within certain aspects of Korean legislation, reflecting a broader challenge faced by countries harmonising national laws with international standards. J.A. Tagud *et al.* (2024) conducted a comparative analysis of the cybersecurity landscape in Asian countries and revealed disparities in cyber threat preparedness, noting that the Philippines faces challenges similar to Kazakhstan, with moderate cyber vulnerabilities despite legislative improvements.

The identified features of personal data localisation in Kazakhstan contrast with research findings on the risks of rigid localisation for effective cybersecurity. P. Swire *et al.* (2024) analysed the impact of data localisation on the techniques, tactics, and procedures of both cyber threat actors and defenders, establishing that localisation requirements create obstacles to effective cyber defence. The researchers found that halving the number of IP addresses available to defenders more than doubles the time required to detect new attacks, calling into question the effectiveness of Kazakhstan's approach to localisation without corresponding mechanisms for international coordination. R. Su & D. Zhang (2025) examined the evolution of China's transnational data governance strategy, demonstrating that China has developed a multi-level and flexible legal framework that balances sovereign claims with selective openness, reflecting a pragmatic response to domestic needs and international pressures. This approach contrasts sharply with Kazakhstan's fragmented system, which lacks a clear strategic orientation on data localisation.

The analysis of the diversity of national approaches to cybersecurity regulation is supported by studies comparing legal systems across different regions of the world. S. Lim & J. Oh (2025) conducted a comprehensive comparative analysis of privacy legislation in five major regions and identified divergent approaches shaped by unique historical, political, and cultural contexts. They found that the European GDPR emphasises individual rights in response to historical abuses of personal information, the California Consumer Privacy Act (CCPA) prioritises consumer rights within a self-regulatory framework, China's PIPL prioritises national security, Japan's APPI balances individual privacy with societal norms, and South Korea's PIPA combines individual autonomy with a sense of communal responsibility. O.M.T. Kam (2025) compared the European GDPR with China's PIPL, highlighting the importance of clearly defining regulatory powers and noting that the ambiguous authority of China's CAC creates unpredictability in regulatory actions.

The institutional coordination challenges identified in Kazakhstan are echoed in studies of other countries facing similar difficulties in organising effective cybersecurity governance. C. Lötter (2025) analysed South African legislation in comparison with Australian practices and identified deficiencies in national measures without active international coordination. The study highlighted three key lessons from the Australian experience: the establishment of a proactive federal expert group, the criminalisation of ransom payments, and restrictions on the storage of sensitive personal data. M.G. Ali (2025) examined cybersecurity management in higher education institutions and emphasised the need for a comprehensive approach that integrates policy, technology, and organisational culture, a finding that aligns with Kazakhstan's challenges regarding the gap between knowledge and behaviour in cybersecurity. G. Kennedy *et al.* (2025) analysed recent developments in the telecommunications sector in Asian countries and highlighted proactive efforts to strengthen cybersecurity regulation in critical sectors, contrasting with the relative stagnation of Kazakhstan's system.

The findings underscore the importance of adapting international experience to national contexts and reveal the particularities of developing cybersecurity systems in countries with transitional economies. Observed patterns demonstrate the role of institutional quality in effectively ensuring cybersecurity and the necessity of a holistic approach to modernising national cyber defence systems. Comparative analysis with international practices indicates potential avenues for improving Kazakhstan's system by adopting successful elements from Asian models while retaining national regulatory specificities.

Conclusions

This study focused on a comprehensive analysis of Kazakhstan's cybersecurity system through the lens of its legal and regulatory landscape, institutional mechanisms, and empirical performance indicators in comparison with leading practices in East Asia. The multi-faceted analysis identified systemic issues within the national cybersecurity framework and highlighted key areas for modernisation based on international experience. Legal examination of current Kazakhstani legislation revealed a fragmented regulatory system lacking a unified codified act, with the legal foundation comprising two primary legislative acts that do not

include specific provisions for cyber incidents or interagency coordination mechanisms. An analysis of empirical performance indicators revealed a sustained increase in cyber incidents, with an average annual growth rate of 14.5%, a thirty-sixfold rise in registered cybercrimes between 2018 and 2021, and low enforcement effectiveness, with only 36% of registered cases resulting in convictions. A comparative legal analysis of the cybersecurity systems in Japan, South Korea, and China identified key elements of successful national strategies, including the presence of comprehensive framework legislation, the operation of specialised coordinating bodies, mandatory certification systems, and a graduated approach to data protection.

A statistically significant negative correlation was observed between governance quality indicators and levels of cybercrime. Countries with low control-of-corruption scores exhibited, on average, 40% higher cybercrime rates compared with countries with positive scores, indicating a direct relationship between institutional quality and the effectiveness of cyber defence. The study also highlighted fundamental differences in procedural mechanisms, sanctioning measures, and institutional architecture between Kazakhstan's system and leading Asian cybersecurity practices, particularly regarding incident reporting timelines, the magnitude of penalties, and the level of centralisation in coordination functions. A limitation of the study is the lack of publicly available sectoral statistics on financial losses from cybercrime, as well as internal government documents regulating procedures for responding to cyber incidents. A promising direction for further research is a comprehensive analysis of the effectiveness of public-private partnerships in cybersecurity and the development of a methodology for assessing the economic efficiency of investments in the national cyber defence system.

Acknowledgements
None.

Funding
None.

Author Contributions
G. Ismailova conceived and supervised the study and drafted the manuscript. N. Kadirova conducted data collection and analysis and contributed to the methodology. Both authors revised the manuscript and approved the final version.

Conflict of Interest
None.

References
[1] Abuova, N. (2024). Kazakhstan advances in global cybersecurity index 2024. *The Astana Times*. Retrieved from https://astanatimes.com/2024/09/kazakhstan-advances-in-global-cybersecurity-index-2024/.
[2] Act of Japan No. 104 "The Basic Act on Cybersecurity". (2014, November). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en.
[3] Act of Japan No. 128 "Act on Prohibition of Unauthorized Computer Access". (1999, August). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/3933/en.
[4] Act of Japan No. 57 "Act on the Protection of Personal Information". (2003, May). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en.
[5] Act of the Republic of Korea No. 14080 "Act on Promotion of Information and Communications Network Utilization and Information Protection". (2016, March). Retrieved from https://elaw.klri.re.kr/eng_service/lawView.do?hseq=38422&lang=ENG.
[6] Act of the Republic of Korea No. 14122 "Credit Information Use and Protection Act". (2016, March). Retrieved from https://law.go.kr/LSW/lsInfoP.do?lsiSeq=182111&urlMode=engLsInfoR&viewCls=engLsInfoR#0000.
[7] Act of the Republic of Korea No. 19234 "Personal Information Protection Act". (2023, March). Retrieved from https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG.
[8] AEQUITAS Law Firm. (2024). *Doing business in Kazakhstan: Legal basics*. Retrieved from https://aequitas.kz/upload/files/2024/AE_Doing%20Business%202024%20(Eng).pdf.
[9] Akhmetova, S. (2024). *Personal data protection, state oversight and legislative updates*. Retrieved from https://www.mondaq.com/data-protection/1474888/personal-data-protection-state-oversight-and-legislative-updates.
[10] Al-Farabi Kazakh National University. (n.d.). *Criminal offenses in the field of informatization and communication (criminal law and criminological aspects)*. Retrieved from https://old.abu.edu.kz/uploads/182/791/1089/89b592eca7a3f879eeeb8e258c189ab5.pdf.
[11] Ali, M.G. (2025). *Cybersecurity governance and policy development in higher education institutions: A strategic framework for resilience and compliance*. Retrieved from https://files.eric.ed.gov/fulltext/ED675147.pdf.
[12] Amirov, A., Kainazarova, D., Begaliyev, E., Sarsenbaev, A., & Kurbanbaev, N. (2024). Legal ways and methods of personal data protection in Kazakhstan. *Scientific Herald of Uzhhorod University, Series "Physics"*, 55, 2174-2186. doi: 10.54919/physics/55.2024.217wl4.
[13] Anderson, C., Crete-Nishihata, M., Dehghanpoor, C., Deibert, R., McKune, S., Ottenheimer, D., & Scott-Railton, J. (2015). *Are the kids alright? Digital risks to minors from South Korea's smart sheriff application*. Retrieved from https://citizenlab.ca/2015/09/digital-risks-south-korea-smart-sheriff/.

[14] APCERT. (2024). *APCERT Annual Report 2024*. Retrieved from https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2024.pdf.
[15] Baker McKenzie. (2025). *Global data and cyber handbook: South Korea*. Retrieved from https://resourcehub.bakermckenzie.com/en/resources/global-data-and-cyber-handbook/asia-pacific/south-korea/topics/key-data-and-cybersecurity-laws.
[16] Busetti, S., & Scanni, F.M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, 42(1), article number 102000. doi: 10.1016/j.giq.2024.102000.
[17] Cho, S. (2022). National cybersecurity organisation: Republic of Korea. In *National cybersecurity governance series* (pp. 1-27). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
[18] Code of the Republic of Kazakhstan No. 235-V KRK "On Administrative Infractions". (2014, July). Retrieved from https://adilet.zan.kz/kaz/docs/K1400000235.
[19] Committee for National Security of the Republic of Kazakhstan. (2021). *On the prevention of a cyberattack*. Retrieved from https://www.gov.kz/memleket/entities/knb/press/news/details/145642.
[20] Committee of National Security of the Republic of Kazakhstan. (2025). *About the court sentence*. Retrieved from https://www.gov.kz/memleket/entities/knb/press/news/details/934421.
[21] Council of Europe. (2022). *Second additional protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)*. Retrieved from https://www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21lhu/content/opening-coecyber2ap.
[22] Council of Europe. (2023). *Kazakhstan invited to join the Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/portal/-/kazakhstan-invited-to-join-the-convention-on-cybercrime.
[23] Council of Europe. (2024). *Octopus project: Authorities of Kazakhstan coordinate on the next steps to complete accession to the Convention on Cybercrime*. Retrieved from https://www.coe.int/en/web/cybercrime/-/octopus-project-authorities-of-kazakhstan-coordinate-on-the-next-steps-to-complete-accession-to-the-convention-on-cybercrime.
[24] Creemers, R., Webster, G., & Triolo, P. (2018). *Cybersecurity Law of the People's Republic of China*. Retrieved from https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[25] Criminal Code of the Republic of Kazakhstan No. 226-V KRZ. (2014, July). Retrieved from https://adilet.zan.kz/kaz/docs/K1400000226.
[26] Criminal Law of the People's Republic of China. (1979, July). Retrieved from https://english.court.gov.cn/2015-12/01/c_761557.htm.
[27] Criminal Procedure Code of the Republic of Kazakhstan No. 231-V KRZ. (2014, July). Retrieved from https://adilet.zan.kz/eng/docs/K1400000231.
[28] Cyber attacks of 2024: How to protect yourself in the age of digital threats. (2025). *State technical service*. Retrieved from https://sts.kz/en/news/066a2c46-3ce0-4aea-b97d-76733d6b8b0b.
[29] Eurasian Research Institute. (2025). Digital security and threats in Kazakhstan. *E-Bulletin Analysis*, 376.
[30] Forum of Incident Response and Security Teams. (n.d.). *KZ-CERT team information*. Retrieved from https://first.org/members/teams/kz-cert.
[31] Global Cybercrime Report 2024: Which countries face the highest risk? (2024). *MixMode threat research*. Retrieved from https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/.
[32] Government Decree of the Republic of Kazakhstan No. 269 "Concept for Digital Transformation, Development of Information and Communication Technologies and Cybersecurity Industry for 2023-2029". (2023, May). Retrieved from https://adilet.zan.kz/kaz/docs/P2300000269.
[33] Government Decree of the Republic of Kazakhstan No. 407 "Concept on Cybersecurity (Kazakhstan's Cyber Shield)". (2017, June). Retrieved from https://adilet.zan.kz/kaz/docs/P1700000407.
[34] Government of Japan. (n.d.). Retrieved from https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf.
[35] Greenleaf, G., & Kaldani, T. (2025). Data privacy laws in Central Asia: Between ex-SSR and 'Belt & Road'. *International Data Privacy Law*, 15(1), 67-90. doi: 10.1093/idpl/ipae015.
[36] Hernandez, J.R. (n.d.). *What is the actual cost of cybercrime?* Retrieved from https://evolvesecurity.com/blog-posts/actual-cost-of-cybercrime.
[37] International Telecommunication Union. (2020). *Global cybersecurity index 2020*. Geneva: ITU Publications.
[38] International treaty UK/Kazakhstan TS No.25/2016 "Treaty on Mutual Legal Assistance in Criminal Matters". (2016, April). Retrieved from https://www.state.gov/wp-content/uploads/2019/02/16-1206-Kazakhstan-Law-Enforcmt-MLAT.pdf.
[39] Japan Computer Emergency Response Team Coordination Center. (n.d.). *About JPCERT/CC*. Retrieved from https://jpcert.or.jp/english/about/.
[40] JPCERT Coordination Center. (2024). *JPCERT/CC Incident Handling Report: January 1, 2024 - March 31, 2024*. Retrieved from https://jpcert.or.jp/english/doc/IR_Report2023Q4_en.pdf.

[41] Kam, O.M.-T. (2025). A comparative analysis of customer data privacy protection under the European Union's general data protection regulation and the People's Republic of China's personal information protection law. *Beijing Law Review*, 16(3), article number 163086. doi: 10.4236/blr.2025.163086.
[42] Katagiri, N. (2022). Assessing Japan's cybersecurity policy: Change and continuity from 2017 to 2020. *Journal of Cyber Policy*, 7(1), 38-54. doi: 10.1080/23738871.2022.2033805.
[43] Kennedy, G., *et al.* (2025). Asia-pacific developments. *Computer Law & Security Review*, 57, article number 106151. doi: 10.1016/j.clsr.2025.106151.
[44] Kergroach, S., Becker, S., & Bernat, L. (2024). *Shielding SMEs – how to boost their defence against cyberattacks*. Retrieved from https://oecdcogito.blog/2024/04/03/shielding-smes-how-to-boost-their-defence-against-cyberattacks-2/.
[45] Kim, D.H., & Park, D.H. (2024). Automated decision-making in South Korea: A critical review of the revised personal information protection act. *Humanities and Social Sciences Communications*, 11, article number 974. doi: 10.1057/s41599-024-03470-y.
[46] Komiyama, K. (2025). Norms in new technological domains: What's next for Japan and the United States in cyberspace. In *Strategic Japan* (pp. 1-8). Washington, DC: Center for Strategic and International Studies (CSIS).
[47] Kubanova, N., Neselbayeva, I., Dyussebalyeva, S., Halibati, H., & Adilgazy, S. (2024). Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability. *Social & Legal Studies*, 8(1), 179-194. doi: 10.32518/sals1.2025.179.
[48] Kubanova, N.B. (2025). Forensic characterization of cyber attacks. *Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 80(2), 278-288. doi: 10.52026/2788-5291_2025_80_2_278.
[49] Kulzhabayeva, Z.O. (2024). Legislative distinction between the concepts of "cybersecurity" and "information security". *Scientific and Legal Journal "Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan"*, 4(79), 178-184. doi: 10.52026/2788-5291_2024_79_4_178.
[50] Law of the People's Republic of China No. 84 "Data Security Law of the People's Republic of China". (2021, June). Retrieved from https://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311.html.
[51] Law of the People's Republic of China No. 91 "Personal Information Protection Law of the People's Republic of China". (2021, August). Retrieved from https://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.html.
[52] Law of the Republic of Kazakhstan No. 418-V ZRK "On Informatization". (2015, November). Retrieved from https://adilet.zan.kz/kaz/docs/Z1500000418.
[53] Law of the Republic of Kazakhstan No. 94-V ZRK "On Personal Data and Their Protection". (2013, May). Retrieved from https://adilet.zan.kz/kaz/docs/Z1300000094.
[54] Less than half of criminal cases on cybercrimes in 2024 reached court in Kazakhstan. (2025). *Kazakh telegraph agency*. Retrieved from https://surl.li/ypluff.
[55] Lim, S., & Oh, J. (2025). Navigating privacy: A global comparative analysis of data protection laws. *IET Information Security*, 2025(1), article number 5536763. doi: 10.1049/ise2.5536763.
[56] Lötter, C. (2025). A comparative critique of the Cybercrimes Act 19 of 2020: Positioning South Africa vis-à-vis Australia. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 28(1), 1-33. doi: 10.17159/1727-3781/2025/v28i0a17035.
[57] Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review*, 41, article number 105502. doi: 10.1016/j.clsr.2020.105502.
[58] Marotta, A., & Madnick, S. (2025). Analyzing and categorizing emerging cybersecurity regulations. *ACM Computing Surveys*, 58(2), 1-36. doi: 10.1145/3757318.
[59] McCoy, E. (2025). Cybersecurity regulations and risk management in the financial sector: A comparative analysis. *Law Economics and Society*, 1(1), 115-135. doi: 10.30560/les.v1n1p115.
[60] Mukhametgali, F. (2024). *Kostanay resident convicted for distributing malicious software on the internet*. Retrieved from https://polisia.kz/ru/kostanajtsa-osudili-za-rasprostranenie-v-internete-vredonosnoj-programmy/.
[61] National Cyber Security Index. (n.d.). *Kazakhstan*. Retrieved from https://ncsi.ega.ee/country/kz/.
[62] Nguyen, T.A., Koblandin, K., Suleymanova, S., & Volokh, V. (2021). Effects of 'digital' country's information security on political stability. *Journal of Cyber Security and Mobility*, 11(1), 29-52. doi: 10.13052/jcsm2245-1439.1112.
[63] Orumbayeva, M., & Kurmangali, A. (2022). Cybersecurity and current global threats in Central Asia. *Memlekettik Basqaru zhane Memlekettik Qyzmet*, 2(81), 77-84. doi: 10.52123/1994-2370-2022-657.
[64] Pellreddy, R. (2025). Cybersecurity for critical infrastructure: Protecting national assets in the digital age. *International Journal of Computer Trends and Technology*, 73(2), 7-17. doi: 10.14445/22312803/IJCTT-V73I2P102.
[65] Personal Information Protection Commission. (2022). *Guidelines for Act on the Protection of Personal Information*. Retrieved from https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/.
[66] Regulations on the Management of Online Data Security (Draft for Solicitation of Comments). (2021). Retrieved from https://www.chinalawtranslate.com/en/data-security-management-draft/.

[67] South Korea's 2024 Cyber Strategy: A Primer. (2024). Retrieved from https://csis.org/blogs/strategic-technologies-blog/south-koreas-2024-cyber-strategy-primer.
[68] Stickings, M., & Nosal., J. (2024). *Blunting the cutting edge of crime: OSCE helps combat cybercrime in Central Asia*. Retrieved from https://osce.org/blog/574757.
[69] Su, R., & Zhang, D. (2025). Adaptive sovereignty: China's evolving legislative framework for transnational data governance. *Politics and Governance*, 13, article number 10413. doi: 10.17645/pag.10413.
[70] Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A., & Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*, 9(1), 20-51. doi: 10.1080/23738871.2024.2384724.
[71] Syrlybayeva, F., Kassymova, X., Omarova, E., Zhussipova, B., & Nurgalieva, E. (2024). Protection of information about employee's personal data in the Republic of Kazakhstan. *Social & Legal Studies*, 7(4), 90-102. doi: 10.32518/sals4.2024.90.
[72] Tagud, J.A., Gildo, E., Jabay, U.A., Oro, E., Sagaldia, S.M., & Tigtig, R.F. (2024). Comparative analysis of the cybersecurity landscape in Asian countries using linear regression. *SAR Journal*, 7(4), 404-410. doi: 10.18421/SAR74-15.
[73] Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal*, 90, article number 102646. doi: 10.1016/j.pacfin.2024.102646.
[74] Univision.kz. (n.d.a). *B058 information security*. Retrieved from https://univision.kz/edu-program/group/B058-informatsionnaya-bezopasnost.html.
[75] Univision.kz. (n.d.b). *M095 information security*. Retrieved from https://univision.kz/edu-program/group/M095-informatsionnaya-bezopasnost.html.
[76] Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, article number 105890. doi: 10.1016/j.clsr.2023.105890.
[77] Worldwide Governance Indicators. (2024). *World Bank Group*. Retrieved from https://databank.worldbank.org/reports.aspx?Id=ceea4d8b&Report_Name=WGI-Table.
[78] Zhamburbayeva, S., & Ilsasova, G.A. (2024). The realization of the "Concept of digital transformation, development of the information and communication technologies and cybersecurity industry for 2023-2029" by implementing blockchain technologies of the Republic of Kazakhstan and the problems of its legal regulation. *Bulletin of the Karaganda University*, 4(116), 137-146.
[79] Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, 3, article number 6. doi: 10.1007/s44216-024-00028-2.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.98:004.8(574+520)

Article's History:
Received: 01.08.2025; Revised: 14.11.2025; Accepted: 16.12.2025

Artificial intelligence in criminal investigation in Kazakhstan and Japan

Ervis Cela*
Doctor of Sciences, Professor
University of Tirana, Department of Civil Law, Faculty of Law
1001, Milto Tutulani Str., Tiranë, Albania
https://orcid.org/0009-0004-1630-3644

Endi Kalemaj
Assistant Lecturer, Candidate of Sciences
Kolegji Universitar i Biznesit, Department of Civil Law
1026, 25 Vangjel Noti Str., Tiranë, Albania
https://orcid.org/0009-0001-0172-2019

Mariza Prifti
Lawyer, Graduate Student
University of Tirana
1019, Milto Tutulani Str., Tiranë, Albania
https://orcid.org/0009-0003-3919-4447

Abstract. This research aimed to assess the peculiarities of integrating the artificial intelligence technology into the criminal justice systems of the Republic of Kazakhstan and Japan. The goal was accomplished through the use of such data collection tools as comparative legal analysis, SWOT analysis, and case study. The comparative legal analysis revealed that Japan has adopted a more internationally aligned data privacy regime, while Kazakhstan has created a state-centred approach with data-localisation requirements. Based on the SWOT analysis, both countries are focused on video surveillance as a part of their crime investigation and prevention strategy, with the Republic of Kazakhstan having 3.1 million cameras around the country, and Japan creating the database of 10 million visual profiles of potential offenders. The cases of creating the video surveillance network in Kazakhstan largest cities of Almaty and Astana, as well as the Tokyo Olympic preparations revealed that the use of artificial intelligence is helpful in detecting offenders and missing people and is 50% more effective in crime prevention than traditional tools. Several recommendations were provided to facilitate the integration of artificial intelligence into criminal investigation, including the enhancement of institutional and legal frameworks, provision of an independent audit of the artificial intelligence deployment efforts, revision of existing technical safeguards, cross-sector cooperation in the use of artificial intelligence-based solutions, and training of the criminal justice system's agents to use novel tools in a responsible and ethical manner. The findings can be used to enhance the effectiveness and efficiency of integrating artificial intelligence into the national criminal justice system

Keywords: criminal justice; technology; integration; video surveillance; offender; missing person; deployment

Introduction

The use of artificial intelligence (AI) has become an integral part of criminal investigation in countries around the world, including Kazakhstan and Japan. The notion of AI involves a repertoire of tools that can boost the effectiveness of the investigation process, enhance its efficiency, and promote justice. Considering these potential benefits, the

Suggest Citation:
Cela, E., Kalemaj, E., & Prifti, M. (2025). Artificial intelligence in criminal investigation in Kazakhstan and Japan. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 52-61.

*Corresponding author

topic of using computational intelligence in criminal justice is considered relevant, and has already been examined in academic research.

E. Parkkavi & K. Yadharthana (2024) in their systematic review of literature asserted that the use of smart technology tools has become a breakthrough in criminal justice. The experts further admitted that AI might be used to accomplish various tasks related to evidence processing, predictive policing, and automated legal advice. Similar idea was voiced by N.P. Thao (2023) who overviewed the use of intelligent system tools by Vietnamese police. As explained by the mentioned author, integration of AI has become an effective way to solve criminal cases provided that the nature of the technology is fully understood, and the basic principles of using it are adhered.

Yu. Mulyana & S. Subarsyah (2024) confirmed the connection between the use of cognitive computing and prosecution effectiveness. According to Yu. Mulyana & S. Subarsyah, prosecution's effectiveness can be partly attributed to the variety of AI-based tools, including facial recognition, natural language processing, and social network analysis. S.M.T. Situmeang *et al.* (2024) further stressed that intelligent automation tools might be effective not only in criminal investigation but also in crime prediction and prevention. The researchers emphasised that AI algorithms have become the foundation for predictive policing models which are used to identify crime hotspots, allocate resources, and analyse large volumes of legal documents and evidence in a relatively short time.

Benefits of using AI instruments in criminal investigation were also discussed by other researchers, including C.-E. Tolbaru (2025) whose mixed-methods methodological approach provided a holistic description of AI in criminal justice. In contrast to the above-mentioned researchers, C.-E. Tolbaru paid her attention to the growing rates of cybercrimes that are becoming more sophisticated with the development of various digital tools. Considering the increased number of crimes involving the use of cybercrimes, C.-E. Tolbaru argued that algorithmic decision-making tools might be used to detect and prevent illegal activities, as well as to ensure justice for all. O. Alakayleh (2025) in his research acknowledged the effectiveness of such smart technology instruments as data and voice analysis, facial recognition, and video surveillance. The cited researcher stressed that these analytical tools had proven their effectiveness in criminal case management. K. Goswami & M. Murali (2024) analysed a repertoire of cases where the use of computational instruments enhanced the effectiveness of crime investigation or prediction and prevention. One case involved the use of PredPol, which is the system using historical crime data to predict where crimes might occur. K. Goswami & M. Murali further stressed that intelligent automation utilised in a particular country, including American Chicago's Strategic Subject List (SSL), can be adapted to other contexts, thus facilitating knowledge exchange regardless of borders.

In spite of the mentioned benefits, the use of AI-rooted instruments in criminal investigation also involves some challenges, as mentioned by I. Konini & I. Rokaj (2023). The researchers stressed that AI algorithms rely on data, which means that biased data might produce discriminatory outcomes. Data security risks and algorithmic bias were also emphasised by V. Tiwari *et al.* (2025) who examined the use of such smart technology tools as machine learning, deep learning, and natural language processing. The experts indicated the need to balance between the active and responsible use of AI tools in criminal investigation. Ethical challenges of using AI were also examined by M.A. Coltri *et al.* (2025) who analysed privacy concerns and adherence to universally accepted standards as inalienable elements of integrating AI into criminal investigation. The researchers stressed algorithms resting on biased data marginalises some population groups, which might enhance social stress. M.M. Matic Boskovic (2024) asserted that existing ethical challenges can be partly addressed at the state level, where AI regulation for criminal justice is being introduced. As explained by M.M. Matic Boskovic, such regulation aims at setting universal standards that can be used as a framework in solving criminal cases that involve an interplay of factors.

Despite a large body of research, insufficient attention has been paid to comparing strategies and approaches to using AI in criminal investigation across national contexts. Considering the detected gap, this research aimed to study the integration of AI into criminal justice in the Republic of Kazakhstan and Japan. This aim involves accomplishing the following objectives: to compare the peculiarities of integrating AI into criminal investigation in both countries; to detect challenges of using automated reasoning in the selected countries; and to suggest strategies to address the detected barriers to enhance the effectiveness of AI in criminal investigation.

Materials and Methods

This research study utilised a combination of data collection methods, including comparative legal analysis, SWOT (strengths, weaknesses, opportunities, and threats) analysis, and case study method. The comparative legal analysis was utilised to gain an in-depth understanding of the legal provisions of integrating AI into criminal investigation in the Republic of Kazakhstan and Japan. The comparison involved the study of the following documents: Act of Japan No. 57 "Act on the Protection of Personal Information" (2003) (APPI) and the Law of the Republic of Kazakhstan No. 94-V (2013). The selected legislative documents were compared across the following criteria: general scope and background, data subject rights, consent and legal grounds, enforcement and oversight, international integration, and relevance for expert systems in criminal investigations. The comparative legal analysis also helped to detect the extent to which the integration of AI into criminal justice is regulated at the national level.

SWOT analysis was further carried out to compare the effectiveness and efficiency of integrating AI into criminal investigation in Kazakhstan and Japan (Yadav *et al*., 2023; Dolidze, 2024; Bachurin *et al*., 2025). The analysis involved an examination and comparison in terms of internal, such as strengths and weaknesses, as well as external – opportunities and threats – factors shaping the use of cognitive computing tools in the national criminal investigation. In addition to the mentioned data collection tools, the research also utilised case studies illustrating specific instances of integrating AI into the national criminal justice system (Daubassova *et al*., 2025; Mabiev *et al*., 2025). The following cases were taken into consideration: the launch of AI-powered video monitoring in Astana and Almaty (AI Facial Recognition…, 2024), the Kazakhstan-wide use of AI cameras to detect fugitives as part of targeted operations (Kazakhstan deploys AI…, 2024), Japan-wide facial analysis rollout by police launched in 2020 (Center for AI and Digital Policy, 2020), and the use of predictive policing as a part of the Tokyo Olympic preparation (Surveillance and predictive…, 2025). The selected cases were analysed in terms of the smart systems instruments used to investigate and/or prevent crimes, progress achieved, and challenges encountered. The obtained insights were used to develop the recommendations to facilitate the integration, ethical deployment, and effective use of AI-based tools in criminal investigation, regardless of the national context.

Results

Considering a trend of integrating cognitive computing tools into criminal investigation, neither country has a specific law to regulate the process. Hence, the analysis involved comparing Act of Japan No. 57 (2003) and Law of the Republic of Kazakhstan No. 94-V (2013). The results obtained through comparative analysis are shown in the Table 1.

Table 1. Comparative analysis of national laws regulating the integration of AI into criminal investigation

Criterion	Japan – APPI, with the 2021 amendments	Kazakhstan – "On Personal Data and Their Protection"	Key practical differences/ implications
General scope and background	Nationwide data protection law for private & (increasingly) public handling; PPC is dedicated regulator; modernised in 2020/21 to add pseudonymisation, breach reporting and cross-border rules.	Governs collection/processing in Kazakhstan; defines biometric data and creates operator/owner roles; contains explicit state-oriented clauses (local storage, authorised body). Some enforcement powers rest with Prosecutor's Office / Ministry.	Japan is DPA-led (regulatory, compliance/guidance heavy); Kazakhstan is more state-centric with stronger territorial controls.
Data-subject rights	Clear statutory rights: disclosure, correction, cease-use/deletion, objection in certain contexts; duties to notify purpose; breach reporting rules to PPC.	Rights to access, change/supplement, block/destruct; written consent model; withdrawal of consent allowed except where prohibited by law.	Rights exist in both, but APPI includes more elaborate administrative-DPA remedies and guidance mechanisms; Kazakhstan's rights are tied tightly to consent and state exceptions.
Consent & legal grounds	Notification / purpose limitation required; third-party transfers normally require consent but APPI allows specific exceptions (public interest, legal obligations, cooperation with government); cross-border transfers now regulated (consent or recognised equivalent measures/adequacy).	Consent (usually written, including via state/non-state services) is primary legal basis; cross-border transfers/diffusion require consent; data localisation requirement (storage in Kazakhstan).	Japan provides more flexible/ extraterritorial transfer mechanisms (and EU adequacy). Kazakhstan emphasises territorial control and written consent for transfers.
Enforcement & Oversight	PPC (independent commission) – can require reporting, inspections, issue orders, revoke accreditations; criminal/administrative sanctions exist for certain wrongful acts and for violating PPC orders (post-amendment penalties are stiffer).	Statutory supervision named to Prosecutor's Office (supreme supervision) and/or authorised central executive body (Ministry for Digital Development) – inspections, compliance checks; sectoral/ state review powers and criminal/ procedural enforcement by state bodies.	APPI uses a dedicated DPA model and growing administrative enforcement tools; Kazakhstan relies more on general state authorities and localised enforcement.
International integration	Japan has an EU adequacy decision and explicit APPI mechanisms for cross-border transfer (PPC can recognise equivalence; businesses may adopt "equivalent measures").	Strong data localisation and transfers generally subject to consent; no EU adequacy; cross-border flows more constrained.	Japan is integration-friendly (adequacy, model clauses), Kazakhstan is more restrictive (localisation/consent).
Relevance for AI in criminal investigation	APPI regulates personal data (applies to AI when personal data are processed). Law-enforcement uses are often handled under separate rules/exceptions; PPC has published reports/guidance (e.g., camera/ face recognition). APPI introduced rules on pseudonymised/anonymised info relevant to ML training and research.	The law expressly excludes intelligence/ operational/search activity from its scope; biometric data explicitly recognised and confidentiality required; state oversight + data localisation strongly shape law-enforcement AI use, but no detailed AI-specific criminal-justice rules in this statute.	

Note: DPA – Data Protection Authority; EU – European Union; PPC – Personal Information Protection Commission
Source: compiled by the author based on Act of Japan No. 57 (2003), Law of the Republic of Kazakhstan No. 94-V (2013), H. Miyashita (2020), S. Akhmetova *et al.* (2025), K.K. Nurmukhambetova & Sh.A. Ismoilov (2025)

The comparison shows that Japan's APPI represents a mature, internationally aligned privacy regime, centred on the PPC as an independent data-protection authority. It grants individuals broad rights, including access, correction, deletion, and cessation of use, sets clear conditions for consent and third-party transfers, and incorporates modern tools such as pseudonymisation, breach reporting and cross-border transfer mechanisms backed by Japan's EU adequacy decision. This DPA-driven model gives Japan a more flexible but also more structured environment for AI developers and criminal-justice agencies handling personal data, with the PPC issuing guidance on emerging technologies like facial recognition.

By contrast, Kazakhstan's Law on Personal Data and Their Protection follows a state-centred, consent-driven approach with strict data-localisation requirements, limited international interoperability and supervisory powers vested in general state bodies rather than an independent DPA. Although it recognises biometric data and imposes confidentiality and consent rules, it explicitly excludes intelligence and operational activities, meaning law-enforcement AI systems sit largely outside the statute's reach. As a result, Japan's framework is better positioned to integrate privacy oversight into AI-integrated criminal justice tools, while Kazakhstan's framework gives the state more control but provides fewer AI-specific safeguards at the statutory level. The contextual analysis was rooted in the assumption that artificial intelligence strategies and instruments emerge and evolve under the impact of numerous factors. Similar, the integration of artificial intelligence tools into criminal investigation in Kazakhstan and Japan is shaped by a repertoire of internal and external factors, the key of which are reflected in Table 2 below.

Table 2. Integration of AI tools into criminal investigation in Kazakhstan and Japan

Dimension	Kazakhstan	Japan
Strengths	Rapid rollout of AI-enabled video surveillance in Astana and Almaty. Centralised biometric authentication system improves data accessibility for investigations. Strong state support through digital modernisation programs.	Strong personal data protection under APPI and oversight by Personal Information Protection Commission. Advanced predictive analytics ("Crime Nabi" and similar tools) for crime hotspot forecasting. Integration with broader smart-city and tech innovation strategies.
Weaknesses	Limited oversight and weak data-protection frameworks risk misuse of biometric data. Dependence on centralised databases increases vulnerability. Skills gap in AI use among law enforcement personnel.	Relatively cautious pace of adoption slows potential benefits. High operational costs for advanced AI systems. Integration challenges between AI tools and existing police workflows.
Opportunities	Public-private partnerships to strengthen technical expertise. Potential to modernise policing and align with "Digital Kazakhstan" goals. Regional cooperation with Central Asian neighbours on cybercrime/terrorism threats.	Leadership role in shaping global AI governance standards. Collaboration with tech companies to refine explainable AI. Opportunities for preventive policing and social trust-building through transparent systems.
Threats	Risks of authoritarian overreach, mass surveillance, and chilling effect on civil liberties. High cybersecurity risks to centralised biometric databases. Potential public backlash if wrongful identifications occur.	Public backlash against predictive policing or surveillance tools if linked to discrimination. Legal liability for false positives could undermine trust in police. Overdependence on AI may reduce human judgment in investigations.

Note: APPI – Act on Protection of Personal Information
Source: created by the author of the study based on S. Yadav *et al.* (2023), T. Dolidze (2024), S. Bachurin *et al.* (2025), Sh.S. Daubassova *et al.* (2025), Y. Mabiev *et al.* (2025)

The table demonstrates that both Kazakhstan and Japan are actively integrating artificial intelligence into criminal investigation, but their approaches reflect different institutional contexts. Kazakhstan has pursued rapid deployment of AI-enabled surveillance and centralised biometric authentication as part of its broader digital modernisation agenda. AI is used to monitor urban spaces, process facial recognition, and link national databases for investigative purposes. Japan, in contrast, has introduced AI more cautiously, with projects focusing on predictive policing, crime hotspot forecasting, and investigative support tools. While both countries recognise AI's potential to improve efficiency, accelerate evidence analysis, and enhance crime prevention, their speed of adoption and governance priorities diverge.

A key similarity lies in the emphasis on AI for surveillance and predictive functions. Both countries use facial recognition and video analytics, while also exploring predictive systems to anticipate criminal activity. However, Japan's integration is shaped by the APPI, which establishes strict rules on sensitive data and cross-border transfers, alongside oversight by the Personal Information Protection Commission. Kazakhstan's frameworks are less mature: legal protections for biometric and personal data are developing, but oversight mechanisms remain weaker, raising concerns about state overreach and civil liberties. This contrast highlights how legal infrastructure strongly influences the risks and safeguards of AI adoption.

The lessons learned from these experiences suggest that efficiency gains must be balanced with governance capacity. Kazakhstan illustrates the risks of deploying AI rapidly without robust data protection, as centralised biometric systems raise cybersecurity and human rights concerns. Japan shows that a slower, regulation-driven approach can help build public trust, but may delay innovation and

increase costs. Taken together, the cases underline the importance of transparent governance, independent oversight, and clear accountability mechanisms when integrating AI into criminal justice. For countries considering similar adoption, blending Kazakhstan's ambition with Japan's regulatory safeguards could provide a more sustainable path.

The integration of machine learning tools into criminal investigation across national contexts was also examined through case studies, including the launch of AI-powered video monitoring systems in two of Kazakhstan's largest cities – Astana and Almaty. The case involved installing video cameras and connecting them to operational control centres and police duty systems so to launch an integrated surveillance system (AI Facial Recognition…, 2024). The video cameras were mainly located at critical sites, such as railway stations, airports, hotels, and shopping malls. The described facial recognition system proved to be effective as it helped to detain 46 wanted individuals in Astana and 30 in Almaty. Considering the progress achieved in specific areas, it was decided to expand the national video surveillance system. As of 2024, the system included 3.1 million video cameras, 310,000 of which could be used for investigation purposes, since they were connected to operational control centres and police duty stations. The case further suggested that despite sufficient effectiveness in crime investigation or prevention, the use of AI technologies still has opponents voicing public concerns and drawing public attention to the misuse of surveillance technology issues. A deeper inspection of the case facilitated an understanding of the peculiarities of integrating AI strategies into criminal investigation. It was discovered that rapid deployment of tens of thousands of cameras and a unified biometric backbone has improved efficiency for public safety, e-government and banking services, yet it also concentrates risk, raising privacy, security and human-rights concerns. The case suggests that secure technical design, involving pseudonymisation, encrypted tokens, and federated matching, as well as legal guardrails, taking the form of purpose limitation, retention rules, judicial approvals for sensitive uses, must be mandated by policy rather than left to practice.

Another Kazakhstan-specific case involved deploying AI cameras to detect fugitive criminals across the country (Kazakhstan deploys AI…, 2024). The launch of the country-wide video surveillance system was preconditioned by the fact that as of 2024, there were 9,000 people of wanted, of which 2,200 were criminals and 2,000 were missing persons. While reporting on the progress achieved, the Prosecutor General of the Republic of Kazakhstan Berik Assylov stressed that 53 fugitives had been detected since the launch of the video surveillance system. The case suggests that Kazakhstan's pilot project adds an advanced computer-vision and facial-recognition layer to existing closed-circuit television (CCTV) networks, enabling functions such as tracking individuals even as their appearance changes, detecting unattended objects, identifying vehicle make, model and colour, and automatically recording incidents. This initiative fits into a broader national strategy in which the government, through the National Information Technologies Enterprise Corporation (NITEC) and BTS Digital, is building a centralised biometric authentication backbone and expanding "smart-city" surveillance. Together, these measures integrate thousands of cameras into central command centres and make it technically possible to match live video feeds with biometric identifications (IDs) and link them to public and private databases, greatly expanding the scope and power of identity tracking across multiple sectors. Kazakhstan's deployment of AI-enabled CCTV and a centralised biometric authentication system demonstrates that rapid technological scale does not automatically ensure robust governance. While the system enables efficient identification of fugitives and integration across public and private sectors, it also concentrates risks related to privacy, security, and potential misuse. Key lessons from the analysed case include the necessity of embedding strong legal and institutional safeguards, such as independent oversight, clear purpose limitations, retention rules, and judicial or administrative approvals for sensitive uses, before scaling; implementing technical privacy-by-design measures like pseudonymisation, encryption, and federated matching; ensuring operational transparency with published accuracy metrics and audit reports; and providing clear redress mechanisms for misidentifications. The case highlights that political support and rapid rollout can outpace civil-liberties protections, making governance, transparency, and accountability essential alongside technical deployment.

In Japan, the integration of AI technology into criminal investigation has also become a common practice, as illustrated by the country-wide facial analysis rollout launched in 2020. Based on the Center for AI and Digital Policy (2020) report, the country has succeeded in creating an extended video surveillance system whose database contains 10 million images of criminal suspects. The system was developed and implemented through cooperation with major technology companies. For example, Nippon Electric Company (NEC), Fujitsu, and Sony are leading the development and deployment of facial recognition systems in Japan. These systems are increasingly utilised in public transportation, retail, and security applications. For instance, Narita International Airport has implemented facial recognition technology to streamline passenger check-in and boarding processes. Similar to Kazakhstan, the increasing frequency of using neural network tools for investigation purposes has raised major concerns in Japan; as stated by the Center for AI and Digital Policy, video surveillance system is being criticised for its potential ability to transform Japan into a surveillance society. To avoid such a scenario, the National Police Agency ensures that the collected data are only utilised for investigation purposes, while facial images unrelated to cases are being discarded. Japan's experience with facial recognition technology highlights the importance of balancing rapid technological adoption with robust privacy and governance safeguards. The country has deployed systems across law enforcement, airports, transportation, and retail, driven by major

technology companies such as NEC, Fujitsu, and Sony, and supported by a growing market projected to reach USD 3.14 billion by 2035. Lessons learned from the analysed case include the necessity of clear legal frameworks like the APPI and oversight by the PPC to regulate the collection and use of biometric data, even as certain law-enforcement exemptions exist. Japan demonstrates the value of public-private collaboration for technological innovation, while also emphasising privacy-by-design, transparency, and data protection measures to maintain public trust and mitigate risks of misuse, function creep, and bias in AI systems.

In addition to the mentioned cases, the study examined the use of predictive policing as a part of Tokyo Olympic preparation (Surveillance and predictive…, 2025). While getting ready for the Tokyo 2020 Olympics, Japan implemented AI-driven predictive policing systems to enhance public safety and security. The Kanagawa Prefectural Police pioneered this initiative by deploying an AI system capable of analysing crime data to predict potential criminal activities and identify high-risk areas. This system utilised deep learning algorithms to process vast amounts of data, including historical crime records and social media activity, to forecast criminal behaviour and optimise police resource allocation. Simulations indicated that this approach was over 50% more effective than traditional policing methods in identifying high-risk areas. Furthermore, facial recognition technologies were employed to monitor crowds and identify potential threats during the Games; and these technologies were integrated with existing surveillance systems to provide real-time analysis and enhance situational awareness. Japan's use of AI-driven predictive policing for the Tokyo Olympics demonstrates that while such technologies can significantly improve law enforcement efficiency by identifying high-risk areas, optimising resource allocation, and integrating with facial recognition to enhance real-time situational awareness; and they also raise critical ethical and governance challenges. Lessons learned include the importance of implementing robust legal and oversight frameworks to protect privacy, ensure data security, and mitigate algorithmic bias, as well as the need for transparency and public engagement to maintain trust. The case highlights that technological effectiveness must be balanced with ethical safeguards, clear accountability, and careful management of citizen rights to ensure that predictive policing delivers public-safety benefits without compromising civil liberties.

Based on the experiences of Kazakhstan and Japan, integrating deep learning into criminal investigations presents significant opportunities for enhancing law enforcement effectiveness, but it also underscores the need for careful attention to governance, legal frameworks, and ethical safeguards. In Kazakhstan, the deployment of AI-enabled CCTV systems and a centralised biometric authentication backbone had allowed authorities to rapidly identify fugitives and missing persons, link cross-sector databases, and improved investigative efficiency (AI Facial Recognition…, 2024; Kazakhstan deploys AI…, 2024). Similarly, Japan's predictive policing systems, implemented in preparation for the Tokyo Olympics, demonstrated that algorithmic decision-making can improve resource allocation by forecasting high-risk areas and anticipating potential criminal activities, allowing law enforcement agencies to act proactively rather than reactively (Center for AI and Digital Policy, 2020; Surveillance and predictive…, 2025). These cases collectively highlight that AI tools can provide law enforcement with unprecedented situational awareness, speed up investigative processes, and reduce reliance on manual monitoring. However, they also reveal that the rapid rollout of such technologies without accompanying safeguards can result in serious privacy concerns, function creep, and potential bias in algorithmic decision-making.

To ensure that automated reasoning is integrated responsibly and effectively, it is essential to strengthen both legal and institutional frameworks. Clear statutory limits should govern the collection, storage, and cross-sector use of personal data, specifying retention periods and purposes of use. In sensitive applications, such as real-time identification or predictive policing, approvals from judicial or administrative authorities should be required to prevent misuse or overreach. Independent oversight bodies should monitor AI deployment and operations, conduct regular audits, and evaluate algorithmic performance to detect errors, false positives, and discriminatory patterns. Technical safeguards are equally critical: pseudonymisation, encryption, and federated matching should be standard practices to prevent unauthorised access, minimise risks associated with centralised biometric databases, and reduce the likelihood of misuse. By combining strong legal structures with secure technical design, authorities can maximise the utility of machine learning tools while protecting individual rights.

Operational transparency and public engagement are additional elements that must be emphasised. Law enforcement agencies should publish non-technical summaries explaining how AI systems are used, report accuracy metrics, and provide accessible mechanisms for individuals to challenge or appeal misidentifications. Training programs for police and investigative personnel should include ethical guidelines, human oversight requirements, and accountability measures to ensure that cognitive computing complements rather than replaces human judgment. Furthermore, pilot projects should be carefully designed with clear evaluation criteria and sunset clauses, allowing authorities to assess performance, identify potential risks, and refine implementation strategies before wider deployment. Following these recommendations, AI can be integrated into criminal investigations in a manner that enhances investigative efficiency, strengthens public safety, and safeguards democratic principles, balancing technological innovation with privacy, fairness, and transparency.

Discussion

The key idea introduced in this research suggests that the use of automated reasoning instruments enhances the effectiveness of criminal investigation. This idea was examined

in the context of installing video surveillance system in Astana and Almaty due to which dozens of criminals and missing people were detected. The expediency of integrating AI technologies into criminal investigation was also confirmed in previous studies, including M.R.M. Elshobake & A. Sakka (2024) who examined the use of deep learning in a repertoire of criminal cases. The experts mentioned that the emerging technology has facilitated criminal investigation through expanded data storage capacity. AI-based tools provide law enforcement agents with access to large amounts of data whose instant processing facilitates decision making. The effectiveness of the emerging technology was also confirmed by V. Shepitko *et al.* (2023) who studied the opportunities of cognitive computing instruments in the investigation of war crimes committed by the Russian Federation against Ukraine. As explained by V. Shepitko *et al.*, the technology can be used to promptly collect and process evidence of war crimes and to subsequently enhance the effectiveness of criminal investigations and law enforcement operations. Despite the detected similarities, the work of V. Shepitko *et al.* is considerably different from the present research in terms of its scope, which is Ukraine, and focus that is war crimes investigation. The detected differences should be considered when planning the integration of previously accumulated knowledge into boosting the effectiveness of the criminal investigation and law enforcement systems.

This work also attributed the effectiveness of integrating the new technology into criminal investigation to the variety of machine learning strategies. This variety was emphasised in the systematic review of literature and in the analysis of Japanese and Kazakh surveillance systems that help to collect and store both video and audio data. While examining the Tokyo Olympic Preparation, this research argued that the combination of deep learning approaches was 50% more effective than the use of traditional crime investigation and prevention methods. The benefit of a multi-aspect portfolio of AI-grounded instruments was also confirmed by previous studies, including H. Himanshi & S. Thakur (2024) who focused their attention on facial recognition and predictive policing techniques. As explained by H. Himanshi & S. Thakur, combining several intelligent systems tools enhances the effectiveness of criminal investigation; however, such combinations should be used cautiously considering the instances of misuse in State v. Loomis and other cases. Hence, the consistency between this research and the work of H. Himanshi & S. Thakur is evident in emphasising a balanced approach to combining AI-based instruments in criminal investigation. Similarly, C. Dement & M. Inglis (2024) conducted interviews with 23 justice professionals and concluded that a repertoire of cognitive computing strategies, including large language models (MLM), might be used to streamline the criminal investigation and reporting process. The parallel between this research study and the study of C. Dement & M. Inglis was seen in the recommendation to utilise AI instruments in line with accepted standards. However, the difference was in the fact that this study mainly focused on video surveillance, while C. Dement & M. Inglis took a deeper look into MLM.

This research further argued that despite existing advantages, AI-based approaches cannot completely replace traditional criminal investigation methods. This assumption was, for example, tested in the context of Japanese video surveillance system containing up to 10 million of images of suspects. The analysis further revealed that individual images were processed manually and removed from the database provided they were not relevant to the case. The idea that machine learning tools cannot be used instead of trained criminal investigation and law enforcement actors was also found in earlier works, including S. Matuliene *et al.* (2022). While using Ukrainian justice system as a context, S. Matuliene *et al.* argued that though deep learning instruments optimise the work of law enforcement agents, the latter possess the knowledge and experience required for unbiased decision making. Similarly, B.L. Garrett & C. Rudin (2024) stressed the risk of bias while using AI-grounded tools, which they described as the "black box" AI. The idea behind this notion is that AI-supported algorithms cannot be fully understood, while some decisions based on these algorithms may be non-interpretable. Considering the detected deficiencies, B.L. Garrett & C. Rudin suggested that cognitive computing decisions should be cross-checked by competent law enforcement agents. The suggestion is consistent with this work's recommendation regarding the provision of relevant training to criminal investigation and law enforcement agents. An idea that was detected throughout all of the above cited research studies suggests that criminal investigation agents should be encouraged to use smart technology tools responsibly.

As explained in this study, responsible use implies compliance with major ethical standards, including the ones of privacy, confidentiality, and impartiality. This idea was, for example, examined in the context of Japanese APPI setting clear conditions for consent, third-party transfers, pseudonymisation, and other approaches to ethical investigation and law enforcement. The adherence to universal ethical requirements was also emphasised in the recommendations to provide relevant training to criminal investigation and law enforcement agents. The feasibility of this recommendation was confirmed through the study of previous research, including H.S. Flora *et al.* (2024) who examined a repertoire of case studies in terms of ethical challenges in criminal investigation. As explained by H.S. Flora *et al.*, the key hindrances to ethical investigation are associated with the algorithmic bias and lack of transparency, which is consistent with the conclusions reached in this study. The latter, for example, pointed out that machine learning instruments can be used for marginalisation of specific population groups, which constitutes a major challenge in criminal investigation. In addition to the mentioned challenges, K. Mohsin & V. Sharma (2024) also emphasised insufficient accountability as a hindrance to ethical criminal investigation. The consistency between the

study of K. Mohsin & V. Sharma and this research was noted in the recommendation to regulate the cross-sector use of data as a way to facilitate accountable investigation process. The feasibility of regulating the cross-sector data sharing was also confirmed by R.K. Bharati (2024) whose framework emphasised regular audits of deep learning systems. The author stressed that such audits enhance transparency by ensuring the compliance of AI-supported investigation with universal ethical standards. Furthermore, the significance of ethics in criminal investigation was confirmed in the work of V. Kumar (2024) who stressed the relationship between compliance with universal standards and human rights protection. The consistency was noticed in the fact that similar to V. Kumar, this study sought to examine the cases of integrating AI into criminal investigation through the effects it might have on individuals and community.

Hence, consistencies noted between this study and previous works confirmed the relevance of the topic and approaches used to investigate it. In the contrast to the above cited studies with a wider research focus, this research focused on comparing the integration of AI-based tools into criminal investigation of Japan and the Republic of Kazakhstan. Considering this unique focus, it is possible to assert that this study has contributed to the current discourse about the use of AI in criminal justice and law enforcement.

Conclusions

The study confirmed that the integration of cognitive computing tools can enhance the effectiveness and efficiency of criminal investigation and law enforcement due to a repertoire of tools used to instantly collect and process large data volumes. Although both the Republic of Kazakhstan and Japan have made AI an integral part of their criminal justice system, their approaches to accomplishing the goal differ. The comparison of Japanese APPI and Kazakh law "On Personal Data and Their Protection" revealed that Japan has created an internationally aligned data privacy regime whose major provisions are safeguarded by the PPC as an independent data-protection authority. In contrast, Kazakhstan has designed a state-centered approach with data-localisation requirements, which makes it challenging to integrate the national criminal investigation system into the global criminal justice domain.

The SWOT analysis also revealed the peculiarities of integrating AI into the criminal investigation systems of Kazakhstan and Japan. It was discovered that Kazakhstan has focused on the rapid deployment of video surveillance and now has 3.1 million cameras installed across the country, of which 310,000 are used for investigation purposes. Similar to Kazakhstan, Japan has also invested heavily in launching the country-wide video surveillance system currently containing up to 10 million photo and video records of potential criminals. Despite this similarity, Japan was discovered to demonstrate a more cautious attitude toward introducing AI-integrating solutions, focusing mainly on predictive policing and crime hotspot forecasting. The case of the Tokyo Olympic preparation revealed that the use of smart solutions tools is 50% more effective in crime detection and prevention than traditional surveillance tools.

Nevertheless, it was discovered that the integration of AI technologies into criminal justice involves addressing a repertoire of challenges, including privacy, confidentiality, transparency, and accountability concerns. Considering the detected issues, the following strategies were recommended: to enhance institutional and legal frameworks as currently countries do not have specific laws regulating the use of AI in criminal investigation; provide independent oversight of AI deployment and operations through regular audits; revise existing technical safeguards; facilitate cross-sector cooperation and ensure training of criminal justice agents to ensure the ethical use of AI-based tools. The research has several limitations, including a relatively small sample of two countries selected for comparative analysis. In future studies, this sample can be extended to include Central Asian and European countries.

Acknowledgements

None.

Funding

None.

Author Contributions

E. Cela conceived the study, developed the research design, supervised the research process, and contributed to the interpretation of the results and final revision of the manuscript. E. Kalemaj conducted the comparative legal and SWOT analyses, contributed to data interpretation, and participated in drafting the manuscript. M. Prifti collected and systematised the data, conducted the case study analysis, and contributed to drafting the manuscript. All authors approved the final version of the article.

Conflict of Interest

None.

References

[1] Act of Japan No. 57 "Act on the Protection of Personal Information". (2003, May). Retrieved from https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en.

[2] AI Facial Recognition System Being Tested in Two Cities in Kazakhstan. (2024). *The Times of Central Asia*. Retrieved from https://timesca.com/ai-facial-recognition-system-being-tested-in-two-cities-in-kazakhstan/?utm.

[3] Akhmetova, S., Kassymzhanova, A., & Ibrayeva, A.S. (2025). Modern development of artificial intelligence technologies and problems of legal regulation of profiling and targeted advertising in Kazakhstan. *Bulletin of L.N. Gumilyov Eurasian National University Law Series,* 150(1), 77-97. doi: 10.32523/2616-6844-2025-150-1-77-97.

[4] Alakayleh, O. (2025). *The use of artificial intelligence systems in crime detection and prevention: Applications and challenges*. doi: 10.2139/ssrn.5132225.
[5] Bachurin, S., Sidorova, N., Shulgin, E., Altabayev, S., & Kussainova, L. (2025). AI machine learning of artificial intelligence systems with acts of justice: Forecasting and ways to solution. *International Journal of Innovative Research and Scientific Studies*, 8(4), 1872-1881. doi: 10.53894/ijirss.v8i4.8257.
[6] Bharati, R.K. (2024). Ethical implications of AI in criminal justice: Balancing efficiency and due process. *Research Review. International Journal of Multidisciplinary Research*, 9(7), 93-105. doi: 10.31305/rrijm.2024.v09.n07.014.
[7] Center for AI and Digital Policy. (2020). Artificial intelligence and democratic values: Artificial intelligence social contract index 2020. In *AISCI-2020: Facial recognition*. Boston; Washington: Center for AI and Digital Policy & Michael Dukakis Institute for Leadership and Innovation.
[8] Coltri, M.A., Uys, W.R., & Joubert, K. (2025). Investing AI ethics in forensic investigations: Development, policies, and best practices. *Athens Journal of Business & Economics*, 11, 1-21.
[9] Daubassova, Sh.S., Dzhumabayeva, K.A., & Alaeva, G.T. (2025). AI and criminal surveillance in Kazakhstan. *Eurasian Scientific Journal of Law*, 4(9), 19-29. doi: 10.46914/2959-4197-2024-1-4-19-29.
[10] Dement, C., & Inglis, M. (2024). Artificial intelligence-assisted criminal justice reporting: An exploratory study of benefits, concerns, and future directions. *Criminology & Criminal Justice.* doi: 10.1177/17488958241274296.
[11] Dolidze, T. (2024). The role of artificial intelligence in criminal justice – reality and perspective. *Law and World*, 10(31), 80-87. doi: 10.36475/10.3.8.
[12] Elshobake, M.R.M., & Sakka, A. (2024). Legal implications for emerging technologies in criminal investigations: Current challenges and catalysts for change. *International Journal of Social Science Research*, 12(2), 263-286. doi: 10.5296/ijssr.v12i2.21965.
[13] Flora, H.S., Xu, S., Xavier, M., Cale, W., & Syahputra, M. (2024). The impact of artificial intelligence on the criminal justice system: Ethical and legal challenges. *Rechtsnormen Journal of Law*, 2(4), 334-344. doi: 10.70177/rjl.v2i4.1292.
[14] Garrett, B.L., & Rudin, C. (2024). The right to a glass box: Rethinking the use of artificial intelligence in criminal justice. *Cornell Law Review*, 109, 561-627.
[15] Goswami, K., & Murali, M. (2024). Harnessing AI in criminal justice: Transforming predictive policing and forensic evidence analysis. *International Journal of Novel Research and Development*, 9(8), 181-192.
[16] Himanshi, H., & Thakur, S. (2024). Artificial intelligence and criminal justice system: A comparative study with India, UK, and USA. *International Journal of Research Publication and Reviews*, 5(11), 1584-1590.
[17] Kazakhstan deploys AI cameras to identify fugitive criminals. (2024). *Kazinform international news agency*. Retrieved from https://qazinform.com/news/kazakhstan-deploys-ai-cameras-to-identify-fugitive-criminals-a305f8?utm.
[18] Konini, I., & Rokaj, Iv. (2023). The challenges on implementing artificial intelligence in the international criminal justice system. *European Academic Research*, 11(2), 240-257.
[19] Kumar, V. (2024). Legal and ethical impact of AI in criminal justice: An analytical study. *International Journal of Novel Research and Development*, 9(8), 552-561.
[20] Law of the Republic of Kazakhstan No. 94-V "On Personal Data and Their Protection". (2013, May). Retrieved from https://adilet.zan.kz/eng/docs/Z1300000094.
[21] Mabiev, Y., Akhpanov, A., Kussainova, L., Serikbayev, A., & Salykova, A. (2025). Digitalisation and artificial intelligence in criminal proceedings: Issues of legal regulation. *International Journal of Innovative Research and Scientific Studies*, 8(4), 1862-1871. doi: 10.53894/ijirss.v8i4.8256.
[22] Matic Boskovic, M.M. (2024). Implications of EU AI regulation for criminal justice. *Institute of Criminological and Sociological Research*, 111-120. doi: 10.56461/iup_rlrc.2024.5.ch8.
[23] Matuliene, S., Shevchuk, V., & Baltruniene, J. (2022). Artificial intelligence in law enforcement and justice bodies: Domestic and European experience. *Theory and Practice of Forensic Science and Criminalistics*, 29(4), 12-46. doi: 10.32353/khrife.4.2022.02.
[24] Miyashita, H. (2020). Human-centric data protection laws and policies: A lesson from Japan. *Computer Law & Security Review*, 40, article number 105487. doi: 10.1016/j.clsr.2020.105487.
[25] Mohsin, K., & Sharma, V. (2024). Ethical guidelines for AI in criminal justice: Developing comprehensive ethical guidelines to govern the use of AI in criminal justice, balancing innovation with human rights. *Journal of Computational Analysis and Applications*, 33(08), 3502-3511.
[26] Mulyana, Yu., & Subarsyah, S. (2024). Artificial intelligence in criminal investigation. *International Journal of Law, Crime and Justice*, 1(4), 60-68. doi: 10.62951/ijlcj.v1i4.251.
[27] Nurmukhambetova, K.K., & Ismoilov, Sh.A. (2025). Legal regulation of artificial intelligence. *Eurasian Scientific Journal of Law*. doi: 10.46914/2959-4197-2025-1-2-31-44.
[28] Parkkavi, E., & Yadharthana, K. (2024). Artificial intelligence in criminal justice: Balance efficiency with fairness and accountability. *Indian Journal of Integrated Research in Law*, 4(6), 483-497.

[29] Shepitko, V., Shepitko, M., Latysh, K., Kapustina, M., & Demidova, E. (2023). Artificial intelligence in crime counteraction: From legal regulation to implementation. *Social and Legal Studios*, 7(1), 135-144. doi: 10.32518/sals1.2024.135.
[30] Situmeang, S.M.T., Harliyanto, R., Zulkarain, P.D., & Mahdi, U. (2024). The role of artificial intelligence in criminal justice. *Global International Journal of International Research*, 2(8), 1966-1981. doi: 10.59613/global.v2i8.264.
[31] Surveillance and predictive policing through AI. (2025). *Deloitte*. Retrieved from https://www.deloitte.com/za/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html?utm=.
[32] Thao, N.P. (2023). The use of artificial intelligence in criminal investigation and trials in Europe and some countries: Experience for Vietnam. *Vietnamese Journal of Legal Sciences*, 8(1), 55-77. doi: 10.2478/vjls-2023-0003.
[33] Tiwari, V., Wang, J., & Dasari, V.S.R. (2025). The future of artificial intelligence in forensics: Advancements, challenges, and ethical considerations. In *International IOT, electronics and mechatronics conference 2025* (pp. 1-22). London: Imperial College of London.
[34] Tolbaru, C.-E. (2025). Artificial intelligence – a vector for crime and a tool for carrying out criminal justice. *Athens Journal of Law*, 12, 1-20.
[35] Yadav, S., Yadav, S., Verma, P., Ojha, P., & Mishra, S. (2023). Artificial intelligence: An advanced evolution in forensic and criminal investigation. *Current Forensic Science*, 1, article number e190822207706. doi: 10.2174/2666484401666220819111603.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.132:004.8

Article's History:
Received: 23.06.2025; Revised: 10.11.2025; Accepted: 16.12.2025

The implementation of artificial intelligence in Singapore's legal practice: Potential and risks for criminal investigations

Raimundas Jurka*
Doctor of Philosophy, Professor
Mykolo Romerio University
LT-08303, 20 Ateities Str., Vilnius, Lithuania
https://orcid.org/0000-0002-9911-5611

Abstract. The aim of this study was to assess the conditions for applying algorithmic systems in the activities of law enforcement and judicial oversight bodies in Singapore, in order to determine the boundaries of their admissibility with regard to the guarantees of due process. The methodology was based on normative-analytical, risk-oriented, structural-logical modelling, analytical synthesis, and case-study methods. It has been established that Artificial Intelligence automates cognitive tasks (classification, prediction); however, the results of machine learning are probabilistic and require regular quality testing and monitoring. In practice, AI analytics primarily generate "candidate" signals (anomalies, risk rankings) that require independent confirmation. The evidentiary status of digital traces arises after the provenance is recorded, and the integrity and verifiability of the materials are ensured. In financial crimes, technologies scale up both investigations and prevention, but automation creates a "risk paradox": errors in data or settings scale as rapidly as the positive effects of the system. It was found that Singapore's courts permit the use of Generative Artificial Intelligence only as an ancillary tool, placing full responsibility on the user for the accuracy and correctness of the submitted materials. The use of the Scam Analysis and Tactical Intervention System Plus enabled the triage of 7,200 monikers and the issuance of 3,700 directions under the Online Criminal Harms Act. Concurrently, the implementation of the Automation of Scam-fighting Tactics & Reaching Out ensured the automation of SMS alert dissemination, which helped prevent losses amounting to $420.41 million. At the same time, judicial practice indicates that operational effectiveness is not synonymous with evidentiary admissibility, as the authenticity of data requires a separate justification of the algorithmic output's reliability. To minimise procedural risks, it is advisable to apply standardised mechanisms for logging, model version control, error documentation, and independent verification. The practical significance lies in the application of the results by law enforcement agencies, prosecutors, courts, and the defence in Singapore when evaluating and using algorithmic results in criminal proceedings

Keywords: reliability; algorithm; reproducibility; data; verification; triage

Introduction

Artificial Intelligence (AI) is used in criminal law enforcement as a tool for processing digital data, identifying patterns in large volumes of information, supporting cybercrime investigations, and applying biometric identification. In Singapore, such applications are developing against a backdrop of high public sector digitalisation and the establishment of national approaches to AI governance, which intensifies the requirements for procedural safeguards in criminal proceedings. In this context, the central issue is the legal-procedural admissibility of AI decisions: the ability to ensure the verifiability and reproducibility of results, the possibility of independent review and appeal, as well as compliance with the principles of proportionality and non-discrimination in cases where potential errors can affect the scope of an individual's rights and freedoms.

Suggest Citation:
Jurka, R. (2025). The implementation of artificial intelligence in Singapore's legal practice: Potential and risks for criminal investigations. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 62-74.

*Corresponding author

The academic literature presents a heterogeneous body of knowledge concerning these challenges in the Singaporean context. In the work of J.G. Allen *et al.* (2025), Singapore's AI governance is conceptualised as a multi-level regulatory architecture combining guiding principles, institutional mechanisms, and tools to enhance trust in AI. This helped outline criteria for assessing the legitimacy of AI applications in criminal justice, particularly the relevance of accountability, standardisation, and control for law enforcement practices where the consequences of errors carry heightened procedural significance. The research by N.F.-Z. Lim & K.S. Tan (2025) systematised the legal environment for AI regulation in Singapore and demonstrated how risk-oriented approaches are combined with pro-innovation policies. This enabled the formulation of criteria by which legal requirements for AI decisions should be strengthened in high-risk domains (criminal investigations and evidence analysis), serving as a normative basis for justifying the boundaries of permissible AI use and control requirements. S.S. Lim & G. Chng (2024) examined Singaporean AI-assurance practice through the lens of verification tools and substantiated its role in ensuring the transparency and manageability of AI systems. The formalisation of checks and standardised assessment procedures can reduce technical uncertainty and increase trust in system outputs. This provided grounds to link technical "verifiability" with procedural requirements for evidentiary information and to justify the need for independent evaluation of AI-generated conclusions in criminal cases.

The evidentiary issues are addressed in the work of D. Seng & S. Mason (2021), which examined the implications of using AI for generating evidentiary information and assessing its reliability. The authors showed that for "machine" conclusions, the ability to provide an explanation, access to data on the system's functioning, and procedural controllability of error risks are critical. This laid the foundation for countering the manipulation of digital materials, which has direct significance for modern 21st-century forensic science. The socio-legal consequences of technological surveillance were documented by G. Beltrão *et al.* (2025). The authors investigated the conditions of trust in facial recognition systems within the context of mass surveillance, demonstrating the dependence of such systems' acceptability on perceptions of legitimacy and social justifiability. This suggests that the application of biometric tools for identification and suspect location must consider public trust as a factor influencing the legitimacy of the relevant practices. Using the digital tool TraceTogether as a case study, research by T. Lee & H. Lee (2020) and H. Lee & T. Lee (2022) analysed the mechanisms of normalising surveillance and rationalising data use in public administration. Although these studies are not exclusively focused on AI, they demonstrate how digital infrastructures create conditions for the cross-sectoral transfer of data into law enforcement practices. This indicates that technological solutions can alter the balance between efficiency and privacy guarantees.

The work of A.A. Khan (2024) examined Singaporean approaches to combating cybercrime, emphasising the growing role of digital traces and analytical tools in policing. The author's conclusions are relevant for understanding the operational needs and limitations of investigations, as well as for posing the question of the conditions under which analytical findings can be integrated into procedural decisions without lowering standards of justification. In a study by J. Chase *et al.* (2021), it was established that the GRAND-VISION system can generate operationally viable daily patrol deployment plans based on predicting spatio-temporal demand, considering personnel and time constraints. This demonstration of a real-world AI application scenario within the Singapore Police outlined legal risks for criminal law enforcement (dependency of decisions on the quality of historical data and the potential reproduction of previous patrolling practices), necessitating accountability and proportionality control. The comparative perspective in the work of H. Alibašić (2025) allowed for an observation of how Singapore's AI policy relates to other jurisdictions and international influences. This provides a basis for determining which elements of governance are context-dependent and which can be transferred in the form of general standards.

The existing body of scientific literature describes AI governance, issues of trust, and the risks of surveillance. However, there is a lack of systematic comparison of these aspects with the requirements of criminal procedure concerning evidence and procedural fairness, particularly in Singapore. Therefore, the aim of this study was to assess the use of artificial intelligence in criminal investigations in Singapore, specifically in evidence analysis. To achieve this aim, the following tasks were set: to systematise the areas of AI application relevant to criminal investigations, to identify risks and potential benefits based on real-world cases of digital technology application by law enforcement in Singapore, and to formulate criteria for the responsible use of AI systems.

Materials and Methods

This study integrated normative-analytical and risk-oriented approaches, structural-logical modelling, analytical synthesis, and case-study methods, applied to the analysis of electronic and algorithmically generated data in the criminal process of Singapore. The Singaporean context was utilised as an illustrative example of the balance between technological innovation and procedural safeguards, thereby ensuring the practical orientation of the research. This approach enabled the identification of key control vectors and the translation of ethical principles into formalised parameters to ensure the contestability of outcomes in court. The normative-analytical analysis method was employed to examine approaches to regulating AI and Generative AI (GenAI) within Singapore's legal framework across the following dimensions: evidentiary admissibility, algorithmic transparency, and personal data protection. The analysis was conducted based on the framework document

(guidelines) issued by the Personal Data Protection Commission (2020) of Singapore, the proposed framework by the AI Verify Foundation (2024), and a press release from the Infocomm Media Development Authority (2024). The selection of sources was determined by their complementarity: they simultaneously provide a regulatory framework for the responsible use of AI, a diagnostic assessment of the risks of "hallucinations", and global standards for AI assurance.

The structural-logical modelling method was used to develop and describe the architecture of a criminal justice ecosystem that links technological data processing with the procedural outcome: data → processing → forensics, through the chain "→ procedural verification". Two fundamental operational modes of the systems were described: the alert-triage mode for identifying suspicious objects and the operational-intervention mode for scaled response. This allowed for a distinction to be made between the technical authenticity of a digital record and the reliability of its algorithmic interpretation, yielding a quantitatively interpretable result regarding operational efficiency and evidentiary admissibility. Through analytical synthesis, managerial controls (logging, version control, "human-in-the-loop" verification) were systematically and methodically linked with indicators of procedural reliability to formulate an applied implementation framework. The Evidence Act of the Republic of Singapore (1997) and the judicial guideline Guide on the Use… (2024) were utilised. Furthermore, the report from the Singapore Courts (2024) and the official description of the technical capabilities of the government agency, the Home Team Science and Technology Agency (HTX) (2025), were analysed. The selection of these resources was justified by their capacity to provide comparable indicators of transparency and the investment-project feasibility of solutions in digital justice. This approach facilitated the development of an applied framework that translates AI system outputs into a system of measurable evidentiary indicators and data provenance verification scenarios, thereby ensuring the legitimacy of technology use in criminal proceedings.

To assess the real-world impact of technologies on investigations, a case-study method was applied to five key technological systems. These systems are officially integrated into the operations of the Singapore Police Force (SPF) and financial intelligence units, represent various automation modalities (AI/Machine Learning (ML), Robotic Process Automation (RPA), video analytics, sensor systems), and generate digital artefacts potentially relevant to the evidentiary framework. The following were analysed: SATIS+ (Commercial Affairs Department (CAD)/ Anti-Scam Command (ASCom)): a platform for streamlining the detection of elements that facilitate scams; Project Automation of Scam-fighting Tactics & Reaching Out (A.S.T.R.O.) (CAD/ASCom): RPA automation for data exchange and mass Short Message Service (SMS) alerts (Singapore Police Force, 2024a); and the Scam Analytics and Tactical Intervention System (SATIS): AI/ML triage and disruption of fraudulent web resources (SPF + partners) (Singapore Police Force, 2024b). Also utilised were the detection of stolen vehicles via Automated Number Plate Recognition (ANPR) in the Next-Generation Fast Response Car (NG-FRC), and Q-Crowd Counter (SPF + HTX): AI video analytics for crowd counting from drones (Singapore Police Force, 2024b). The technologies were analysed according to three universal criteria for legal assessment: reproducibility, auditability, and explainability, with an additional examination of the output type (candidate signal vs. evidentiary impact) and the presence of control artefacts (logs, versioning, data integrity, provenance/verification for GenAI). This was undertaken to operationalise the legal assessment of algorithmic systems by identifying their digital artefacts and the threshold of procedural guarantees depending on the output's status (signal or evidentiary impact).

The normative-analytical analysis method was employed to systematise the logic for evaluating electronic data, which distinguishes between the technical admissibility of evidence in a case and algorithmically generated results in Singapore's criminal process. This was based on the trial court judgment Magistrate's Appeal No. 9043 (2024) and the appellate court judgment Court of Appeal No. 42 (2025). The selection of these judgments was determined by the fact that, together (first instance and appeal), they crystallise the doctrinal logic for evaluating electronic data. For each source, the object of regulation/context, key procedural function, minimum conditions for use in evidence, and significance for AI/ML outputs were identified. This enabled the determination of criteria for the procedural admissibility of algorithmic results and the requirements for the explainability of the method by which they were generated.

Based on the foregoing, a risk-oriented normative-analytical approach was applied, aimed at formalising the minimum procedural requirements for the use of algorithmic outputs in the criminal process of Singapore. To identify relevant risk categories, the official report in the case of Originating Claim No. 125 (2025) was used as a methodological guide, allowing for the modelling of potential procedural consequences arising from the use of unverified algorithmic materials. The selection of this specific case was determined by its representativeness concerning the consequences of submitting GenAI-assisted materials containing unverified or false citations. This facilitated a comparison of the identified risks with Singapore's regulatory and institutional benchmarks and the operationalisation of the derived requirements into a list of control procedures to ensure contestability, verifiability, and procedural good faith. A limitation of this study is the reliance on open reports and public descriptions of systems, which typically do not include full technical model metrics, detailed validation protocols, or internal technical audits. Due to limited access to source code and proprietary algorithms, the technical reliability of the systems was analysed primarily through the lens of governance logic and the requirements of procedural verifiability, rather than through a comprehensive set of empirical performance indicators.

Results

Architecture and applied use of algorithmic systems in criminal law enforcement

AI automates cognitive tasks (classification, prediction, pattern detection), and ML, as a subset of AI, derives rules from data; consequently, its results are probabilistic and necessitate quality testing, drift monitoring, and documentation of limitations. For legal assessment, the key factors are not technology "labels", but the reproducibility, auditability, and explainability of outcomes. Although RPA is deterministic, its scalability also requires logging, access control, and error management. GenAI generates novel content and carries specific risks (hallucinations, provenance issues); therefore, in criminal investigations, it should be used only in a supporting capacity and with enhanced verification (Personal Data Protection Commission, 2020). In practice, AI-driven analytics produce "candidate" signals (anomalies, risk rankings, potential links) that require independent confirmation. When an algorithmic result is used as evidence or influences an evidentiary construct, the requirements for verifiability/reproducibility, explainability, error characterisation, and procedural audit (versions, logs, data integrity) are heightened (Personal Data Protection Commission, 2020).

For GenAI, additional critical requirements are established, including enhanced verification of materials prior to submission to court, the prevention of misleading the court, and an emphasis on ensuring provenance, transparency, and incident management as necessary conditions for building a trustworthy ecosystem (AI Verify Foundation, 2024). The implementation of these standards entails: enhanced verification – the user's obligation to personally verify each output for factual errors and "hallucinations", as the probabilistic nature of the technology does not guarantee automatic accuracy; procedural good faith – the mandatory disclosure of AI application and a guarantee that the generated content is not presented as authentic primary data, to avoid misleading the court; provenance and transparency – the implementation of methods to identify content sources (digital watermarks, metadata), allowing for traceability of the method and conditions of material creation; incident management – the existence of clear protocols for responding to instances where the system produces incorrect or harmful results, which is a prerequisite for the stability of the legal framework (Infocomm Media Development Authority, 2024).

In the criminal justice context of Singapore, the application of AI and analytics is best described as a chain: "data → processing → forensics → procedural verification". The SPF should be regarded as the primary operator within the system: the police initiate the collection/processing of large (streaming) datasets, utilise analytics to support operational decisions, and generate primary digital artefacts – records, event logs, automated calculations, alerts, and other machine-generated results (Singapore Police Force, 2024a). From an evidentiary perspective, the very fact of technological advancement increases the volume and significance of digital traces in a case, but does not automatically render them evidence. Their procedural status only emerges after proper documentation of provenance, ensuring integrity, and enabling verifiability – following the "translation" of an operational product into evidentially admissible material, which depends on subsequent links in the chain (forensics/judicial standards).

Within Singapore's criminal justice ecosystem, the Evidence Act of the Republic of Singapore (1997) serves as the fundamental regulator, transforming "raw" digital traces into evidentially admissible material. Analysis of the Act reveals three critical mechanisms in this transformation. The Act establishes legal presumptions that streamline the prosecution's burden of proof. The court presumes that a device or process which ordinarily produces an electronic record was functioning correctly, unless proven otherwise. This is crucial for automated recognition systems, as it allows their primary records (photos/video) to be admitted automatically without a technical audit of every single camera on each occasion. For an AI's operational output to attain the status of evidence, it must undergo identification and authentication procedures. According to the Evidence Act of the Republic of Singapore (1997), the critical conditions are: documenting provenance (clearly recording the source of the record and the conditions of its acquisition), ensuring integrity (demonstrating that the data was not distorted during transmission or algorithmic processing), and correctness of reproduction (confirming that the material presented to the court is identical to the original machine record). The distinction between the admissibility of a record and the reliability of its interpretation is the most critical aspect of the Act concerning AI technologies. The Evidence Act primarily addresses the question of admissibility – the very fact of an electronic record's "entry" into a court case. The mere existence of a record (for example, a "match" generated by a facial recognition system) and its authenticity do not automatically imply the reliability of its substantive conclusion. The Act only provides "procedural entry", whereas the reliability of interpretation (whether this "match" is indeed accurate) requires separate justification through the stability of the method and a description of the algorithm's error rates. The Evidence Act transforms the operational output of an AI system into evidentiary material through a rigorous "translation" procedure, where the technical output is supplemented by event logs, metadata, and a description of the processing method. This ensures that automated conclusions are not accepted by the court unconditionally, but are subject to independent verification and challenge (Evidence Act of the Republic of Singapore, 1997).

The Commercial Affairs Department (CAD) is institutionally the most "natural" environment for analytics and automation, as financial crimes and fraud typically possess a networked and transactional structure (chains of transfers, linked accounts/identifiers, digital communication channels) where manual analysis becomes a bottleneck. Therefore, the CAD logic of technological

adoption reduces to two complementary modes: the analytical mode – data integration and advanced analytics to identify patterns, connections, and prioritise subjects of interest, where algorithmic results generally constitute "candidate" hypotheses (to be investigated further) rather than final conclusions; and the operational-automated mode (RPA/scaling interventions) – automating response/prevention procedures, where the effect is achieved through scale and speed (Magistrate's Appeal No. 9043, 2024). This implies that within CAD, technologies simultaneously enhance the investigative function (more quickly finding relevant connections) and bolster the preventive/operational function (scaling interventions). At the same time, this is where the risk-paradox of automation is most evident: incorrect configurations, data errors, or methodological limitations scale just as rapidly as the positive effects. Hence the practical demand for accountability: logging, reproducibility, and the ability to explain why the system highlighted a particular object and what the margins of error are (Personal Data Protection Commission, 2020).

The HTX performs not merely a supporting role, but a structural one: the agency ensures the design, implementation, support, and development of technological solutions for the Home Team, including AI and analytical capabilities. For the topic of evidence, the key point is not that HTX "creates tools", but that it determines the technical characteristics of the artefacts which subsequently circulate in the criminal process: what exactly is logged, how versions are recorded, how processing procedures are described, whether auditing is possible, and how integrity is ensured. Within the Digital & Information Forensics domain, (Home Team Science and Technology Agency, 2025) transforms "raw" digital data into practically usable results for institutional application. It is here that typical procedural risks concentrate: version control of tools, reproducibility of procedures, data integrity control, documenting the chain of processing, and methodological limitations. HTX should be interpreted as a link that can either enhance evidentiary reliability (through standardisation and audit) or create a "black box" if control mechanisms are insufficient (Guide on the Use…, 2024).

The judicial system acts as a procedural filter; even with active technological adoption by police/agencies, the integration of results into the judicial framework is only possible within the standards of fairness and verifiability. On one hand, the digitalisation of court services and procedures creates an environment where electronic materials are the norm. On the other hand, courts explicitly delineate the boundaries for using Generative AI (GenAI): it is permitted as an assistive tool, but the user bears responsibility for the accuracy, relevance, and correctness of the submitted material; enhanced scrutiny is expected, and misleading the court is unacceptable. Courts effectively enshrine the principle that technology may support the preparation of materials but cannot substitute procedural safeguards (verification, transparency, accountability) (Guide on the Use…, 2024). The institutional landscape of Singapore's criminal justice ecosystem appears as follows: SPF/CAD generate demand and produce digital artefacts (operational and analytical), HTX determines their technical quality and forensic suitability, and the Singapore Courts set the threshold for procedural admissibility (particularly for GenAI content). This multi-layered structure explains why, in criminal investigations, the key factors become not only the accuracy of the algorithm but also the distribution of responsibility among institutions, the auditability and reproducibility of the data processing chain, and the possibility of procedural challenge and verification of results. Furthermore, this ensures a comparable description of scenarios and establishes the conditions for verifiability, reproducibility, and procedural accountability, summarised in Table 1.

Table 1. Applied scenarios of AI/analytics utilisation in Singapore's criminal investigations

Technology	Data (Input)	System Output	Characteristics	Risks/Vulnerabilities
Stolen Vehicle Detection via ANPR in NGFRC (SPF)	Number plate images/ video feed + database of "target" technical specifications (matching logic)	Automatic "number match" alert → subsequent procedural actions leading to arrest and prosecution for vehicle theft	Accelerated object identification, reduced reliance on random "human" observation, increased likelihood of prompt apprehension	False positives (reading errors, character ambiguity), risk of "tunnel vision" after the alert, reproducibility issues (algorithm settings/ version, thresholds)
SATIS: AI/ML Triage and "Disruption" of Fraudulent Web Resources (SPF + partners)	Indicators/signals of suspicious websites (domains/content/ complaints/patterns)	Systematic triage/ assessment → swift blocking/neutralisation, outcomes reported as mass "disruptions" of channels/ websites	Scaled preventative response, reduced time between resource emergence and intervention, prioritisation of objects for investigative actions	Risk of misclassification, complexity in explaining criteria, potential impact on third-party rights, evidentiary vulnerability without validation/audit protocols
SATIS+ (CAD/ ASCom): Platform for "Streamlining" Detection of Fraud-Facilitating Elements	Online monikers, phone numbers, bank accounts, e-wallets/ virtual accounts, crypto addresses	Triage → managerial/ legal actions; over 7,200 monikers triaged and over 3,700 directives issued under the Online Criminal Harms Act (OCHA)	Single collection point for consolidating signals, faster scaling of response and linking entities (account – account – number – address)	False "linking" of entities, automated error propagation across sources, opacity of triage rules for third-party verification

Continued Table 1

Technology	Data (Input)	System Output	Characteristics	Risks/Vulnerabilities
Project A.S.T.R.O. (CAD/ASCom): RPA Automation for Data Exchange and Mass SMS Alerts	Data from banks/suspicious transactions/accounts (information exchange), lists of potential victims, information processing and dissemination workflows	Automated account referrals + SMS alerts; 8,580 accounts and 777,170 SMS sent to 55,609 individuals; potential prevention of losses amounting to $420.41 million	Drastic acceleration of intervention, scalability without proportional increase in human resources, "harm prevention" effect through early notification	Data quality risks (false suspicions), automation/routing errors, questions regarding legal basis for processing/sharing and proportionality of intervention
Q-Crowd Counter (SPF + HTX): AI Video Analytics for Crowd Counting from Drones	Real-time video stream from UAVs	Crowd size estimation for situational management during an event	Real-time environmental analytics, enhanced situational awareness, tool for response planning	Risks of inaccurate estimations in complex conditions (angles/occlusion), privacy and proportionality of surveillance

Note: UAV – Unmanned Aerial Vehicle
Source: compiled by the author based on Singapore Police Force (2024a; 2024b)

The application of AI/analytics in Singapore's criminal investigations is primarily implemented in two functional modes: an alert-triage mode, where systems generate signals about potentially relevant objects or resources (ANPR/NGFRC, SATIS, SATIS+); and an operational-intervention mode, where automation supports scalable response actions or harm prevention (Project A.S.T.R.O., blocking/neutralisation in SATIS) (Singapore Police Force, 2024a; 2024b). Regardless of the specific technology, the system "output" takes the form of a decision-support suggestion or a management tool, rather than self-sufficient evidence. Consequently, the procedural relevance of such results depends on the ability to document and verify their origin and the parameters of their generation. Common vulnerabilities recur across cases: risks of false positives/classifications, opacity of criteria, errors in integration and entity "linking", as well as the amplification of consequences through automation. Accordingly, to minimise procedural risks, standardised mechanisms for logging, version control, documenting thresholds/settings, describing errors, and ensuring independent verification are critical, taking into account specific requirements of proportionality and privacy for surveillance-based solutions (video analytics).

During the commissioning of the NGFRC, the ANPR function in June 2024 facilitated the detection of a stolen vehicle during patrol, leading to the arrest and subsequent prosecution of the driver (Singapore Police Force, 2024b). From an evidentiary perspective, the ANPR alert serves as the basis for subsequent procedural actions, whereas the potentially relevant evidentiary materials are the primary number plate images/video, metadata (time, location, camera/platform identifier), as well as event logs concerning the generation of the "match" and subsequent actions (Evidence Act of the Republic of Singapore, 1997). Procedural admissibility here is determined not by the fact of the "match" itself, but by the ability to reconstruct the chain: input data → algorithmic operation → human verification/decision → action, with the typical point of challenge being the reliability of identification (image quality, reading errors, thresholds/version of the tool).

SATIS (Singapore Police Force, 2024b) is presented as an AI/ML-based tool for triage and supporting measures to neutralise scam-related web resources. Within the evidentiary framework, the most relevant are the primary digital traces upon which the assessment is based (domain/hosting attributes, content artefacts, records of reports/complaints, technical logs), whereas the algorithmic triage typically performs the function of analytical justification for initiating actions. If triage is used to support actions (blocking/disruption), its procedural role is contextual. However, if it is used to confirm the "nature" of a resource, the need arises to disclose the evaluation parameters, errors, and validation procedures; otherwise, the result possesses limited verifiability as an electronic record (Evidence Act of the Republic of Singapore, 1997).

SATIS+ (Singapore Police Force, 2024a) is described as a platform to support the identification/neutralisation of fraud-facilitating elements (online monikers, phone numbers, accounts, alternative payment instruments, and crypto addresses). Procedurally relevant are the primary records from sources substantiating the links between entities (including documented traces concerning accounts/transactions/identifiers), as well as a reproducible chain of data provenance and the conditions of their processing. In contrast, the triage output is an analytical result, and the directive is an act of regulatory response, which may be relevant for the chronology and grounds of intervention but does not substitute for proving the elements of a criminal offence with primary evidence (Evidence Act of the Republic of Singapore, 1997). The key procedural vulnerability of SATIS+ is associated with entity "linking"; therefore, the minimum requirements for verification are documented sources for each attribute, linking rules, and the ability to reconstruct which specific data led to a particular link/directive.

Project A.S.T.R.O. (Singapore Police Force, 2024a) utilises RPA to automate information-sharing, information-processing, and the mass dissemination of SMS alerts.

In criminal proceedings, such materials are significant for confirming the fact, time, and sequence of actions performed (message dispatch, script execution, information exchanges). Potential evidentiary materials include message dispatch/delivery logs, referral records, and internal logs of automation script execution (Evidence Act of the Republic of Singapore, 1997). Since RPA is rule-based, procedural verification focuses on reconstructing the rules and execution logs (which rule was triggered, on what data, and when), as well as on the legal bases for processing/sharing and the proportionality of intervention; without this, scalability complicates the individual verification of correctness.

Q-Crowd Counter (Singapore Police Force, 2024b) – is an AI tool for real-time video data processing from UAVs, used for estimating crowd size within the operational management of mass events. From an evidentiary perspective, the automated estimation of the number of people has limited independent significance, whereas the potentially relevant evidence could be the primary video recording (subject to metadata, integrity, and a documented chain of custody) (Evidence Act of the Republic of Singapore, 1997). If the count result is used in a case, it must be procedurally linked to the primary video (with identification of the segment, time, processing parameters) and be subject to verification of the margin of error under the specific recording conditions; otherwise, only the primary recording remains suitable for verification.

The described cases indicate that AI/analytics and automation in Singapore are applied primarily for detection, prioritisation, and rapid response. Their connection to evidence is largely indirect: the algorithmic output forms the basis for action and directs the line of inquiry, whereas within the judicial framework, the primary digital records, metadata/logs, and the chain of custody are determinative. The more a party's position relies on an algorithmic inference, the higher the requirements become for explainability, logging, reproducibility, and the accessibility of materials for independent verification and challenge. Empirically (according to Singapore Police Force reports, 2024a; 2024b), the application of AI/analytics is concentrated in two areas: operational detection and situational response support (ANPR, video analytics) and scalable anti-scam/financial analytics and automation. The evidentiary vector in these cases is typical – AI/analytics generates triggers/leads/prioritisation, whereas the primary evidentiary weight is carried by primary digital records (video, logs, transactional and telecom data) along with a properly documented chain of custody. The 'AI output' acquires procedural significance only under conditions of its verifiability and contestability. For electronically or machine-generated materials, the decisive factor is not merely the existence of a record, but the substantiation of the reliability of its interpretation, the context of its creation, the method/settings, limitations, event logs, and the possibility of reproducing the result.

Procedural relevance and normative regulation of algorithmic results

To transition from the operational use of AI/analytics to their procedural relevance, it is necessary to distinguish between the conditions for introducing an electronic record into the evidentiary basis (authenticity/origin/correctness of reproduction) and the conditions under which an inference derived from this data can be considered reliable for proving a specific fact. It is precisely this distinction, between the admissibility of a record and the reliability of its interpretation, that structures the normative and judicial guidelines presented in Table 2.

Table 2. Normative and judicial guidelines for assessing electronic and algorithmically generated data in Singapore's criminal

Judicial Guideline	Subject of Regulation / Context	Key Procedural Function	Minimum Conditions for Use in Evidence	Significance for AI/ML Outputs and Algorithmic Results
Evidence Act (Cap. 97) (including presumptions regarding electronic records) (Statute)	Electronic records and data: establishing authenticity, origin, correctness of reproduction/transmission, presumptions regarding the operation of the device or the process of creating/transmitting records	Provides procedural mechanisms for introducing electronic materials into the evidentiary basis (identification of electronic record, authentication, origin, correctness of reproduction)	Proper documentation of the record's source, conditions of acquisition/storage, connection to the relevant device/process, and the possibility of reproduction/verification within the proceedings	Defines the conditions for the admissibility and authenticity of electronic materials, but does not automatically establish the reliability of substantive inferences drawn from algorithmic data processing
SGHC 287 (2024) (Case Law) (First Instance)	Use of data from a wearable device (smartwatch) to corroborate factual circumstances	Distinguishes between the procedural admission/identification of electronic data and the assessment of its suitability to substantiate a specific fact	Beyond confirming the existence and origin of the record, it is necessary to substantiate the technical/methodological suitability of the data for the relevant inference (conditions of formation, limits of applicability, margin of error, stability)	Algorithmically generated measurements/classifications require separate substantiation of reliability as a basis for factual conclusions SGCA 21 (2025) (Case Law (Appeal))

Continued Table 2

Judicial Guideline	Subject of Regulation / Context	Key Procedural Function	Minimum Conditions for Use in Evidence	Significance for AI/ML Outputs and Algorithmic Results
SGCA 21 (2025) (Case Law (Appeal))	General approach to assessing electronic data in evidence, using data from a wearable device as an example	Articulates a fundamental distinction: the authenticity of an electronic record and the correctness of its acquisition are not equivalent to the reliability of its interpretation for proving a fact	For the evidentiary use of an inference derived from electronic/algorithmic data, grounds for trusting the method are necessary: an explanation of how the result was generated, its limitations, potential errors, reproducibility, and the possibility of independent verification/challenge	Establishes the requirement: the greater the evidentiary reliance on algorithmic output (match/score/triage), the greater must be the transparency of parameters, version control, logging, and the possibility of verification

Source: compiled by the author based on Evidence Act of the Republic of Singapore (1997), Magistrate's Appeal No. 9043 (2024), Court of Appeal No. 42 (2025)

Table 2 summarises the two-tiered logic for evaluating electronic and algorithmically generated data in Singapore's criminal procedure. At the statutory level, the Evidence Act ensures the procedural 'entry' of electronic records into the evidentiary basis through mechanisms of authentication, presumptions regarding origin, and correctness of reproduction; that is, it primarily addresses the issues of identification and admissibility of the record. At the level of case law Magistrate's Appeal No. 9043 (2024), Court of Appeal No. 42 (2025), the focus shifts to the substantive suitability of the data for proving a specific fact: even with an authentic electronic record, a party must substantiate the reliability of the interpretation (the method of acquisition/classification, conditions of application, margin of error, limitations, and reproducibility), as well as ensure the possibility of independent verification and challenge. In practical terms, this means that AI/ML outputs (match/score/triage) cannot function as self-sufficient evidence solely on the basis of their documented existence: their evidentiary weight depends on the transparency of parameters, version control, logging, and the presentation of the method's limitations, enabling the court to assess not only the authenticity of the material but also the soundness of the inference drawn from it.

AI/analytics and automation are used in the law enforcement context primarily for operational support (detection, prioritisation, accelerating response times, processing large datasets). However, in criminal procedure, such operational effectiveness is not synonymous with evidentiary admissibility. The approach under the GIL requires a separate justification for the reliability of interpreting electronic/algorithmic data to prove a fact. Technical risks encompass false positive/ false negative results and the sensitivity of system outputs to data quality and structure (images/video; transactions; the evolution of criminal patterns over time). For triage/scoring approaches, data drift is significant, necessitating regular testing, monitoring, and documentation of application limitations. As public reports typically do not contain error metrics or complete validation protocols, the role of internal assurance procedures and the recording of parameters/versions becomes crucial (Personal Data Protection Commission, 2020). Governance risks arise from the organisational environment in which systems operate: multi-user access, integration with external sources, and updates to rules/scripts and configurations. For tools generating alerts/triage/lists/directives/referrals, critical elements include activity logging, change and version control, access differentiation, and traceability of incidents and corrections (Personal Data Protection Commission, 2020). In digital forensics, the governance component pertains to the procedural discipline of seizing, processing, preserving, and documenting digital artefacts, which determines the reproducibility and verifiability of results (Home Team Science and Technology Agency, 2025).

Legal/procedural risks materialise when an algorithmic outcome is used as a basis for establishing a fact. The approach under the GIL emphasises that the authenticity of an electronic record does not negate the need to prove the reliability of its interpretation. In practical terms, this entails three requirements: procedural rebuttability – the opposing party's ability to verify and contest the conclusion; disclosure of information – the availability of parameters, logs, versions, and methodological boundaries; and expert knowledge – the need for specialised knowledge to explain to the court the possibilities and limitations of the result. This is relevant for both ML/AI and rule-based automation if it influences procedurally significant steps (Evidence Act of the Republic of Singapore, 1997). Data and privacy risks are associated with processing large volumes of transactional, identification, and communication data, and their exchange, which increases the likelihood of unauthorised access, breaches, and function creep. Within governance logic, this aligns with requirements for data management, access control, data minimisation, and accountability throughout the system's lifecycle (Personal Data Protection Commission, 2020). Generative AI risks lie in the potential to generate formally correct but factually inaccurate content (including incorrect or fabricated citations), which is procedurally sensitive in court submissions. Guidelines for the responsible use of GenAI

have been established by the Singapore Courts (Guide on the Use…, 2024) and are encapsulated in the principle that using GenAI does not absolve a party from responsibility for the accuracy of filed materials and the duty of proper verification prior to submission.

Case law further affirms the procedural significance of this standard: in instances where GenAI-assisted document preparation leads to the submission of unverified or erroneous citations, this may result in procedural consequences for the party or their representative. The broader context of the digitalisation of court services does not alter these requirements but rather underscores the necessity of maintaining standards of honest submission of materials in a digital environment (Singapore Courts, 2024). The case of Originating Claim No. 125 (2025) serves as a key judicial reference, crystallising the position of the Singapore judiciary regarding the risks of generative artificial intelligence "hallucinations". The court's decision establishes a fundamental principle: technological assistance does not negate individual procedural responsibility. The court meticulously analysed the issue of the probabilistic nature of GenAI tools, which are capable of generating linguistically coherent but factually incorrect citations to precedents. It was established in this case that submitting documents with non-existent citations undermines the duty of candour owed to the court. The legal authenticity of a submission rests upon the verifiability of its sources, not merely the formal persuasiveness of the text. A critical aspect of the ruling is the affirmation that the legal counsel or party to the proceedings serves as the "final filter". The court emphasised that AI is not a legal entity and cannot bear responsibility for errors; delegating legal research to an algorithm without subsequent human verification (human-in-the-loop) constitutes professional negligence, and the use of AI is not considered a mitigating factor in the event of misleading the court. The case of Originating Claim No. 125 (2025) established a clear list of consequences for the improper use of GenAI: procedural disqualification of materials (the court has the right to disregard or strike out submissions containing unverified data); financial penalties (imposing on a party the obligation to cover costs incurred by the court and the opposing party due to the need to verify "fake" citations); and disciplinary oversight (referral to relevant regulatory bodies for breaches of professional ethics standards). This precedent elevates the Singapore Courts (2024) guidelines from the realm of recommendation to that of mandatory requirement. This means that every statement prepared with the assistance of AI must be traceable to a primary source verified by a human. Law firms and law enforcement agencies are obliged to implement internal verification protocols (cross-checking) before submitting any AI-assisted materials. The case of Originating Claim No. 125 (2025) stimulates the requirement for open declaration of GenAI use in procedural actions to enable proper risk assessment by the court. This demands that system operators and legal professionals ensure not only the technical functionality of the tool but also complete transparency regarding the method of verifying its outputs.

Therefore, it is advisable to ensure comprehensive logging and audit trails (audit logs), including the recording of user actions and system events (creation/export of results, views, configuration changes, integration exchanges). This facilitates, if necessary, the reconstruction of the chain "data → algorithmic output → procedural decision/action" and ensures the verifiability of the origin and integrity of materials. The implementation of version control for models, rules, scripts, and configurations is necessary to establish which specific version of the tool (including thresholds and parameters) was operative at the time a particular match/triage/referral was generated, as well as who made changes and when. Control points for human verification (human-in-the-loop) should be distinctly defined for cases where algorithmic output may lead to significant procedural consequences, accompanied by standardised documentation of who performed the verification, based on what data, and what decision was reached. To mitigate the risks of technical degradation of results, it is advisable to mandate regular quality testing, validity assurance, and data drift monitoring, including the documentation of application boundaries and typical errors. A coherent policy on data governance, access controls, and security must be established, particularly concerning data minimisation, retention periods, incident response procedures, and requirements for inter-agency data exchange. These elements are fundamental in determining the stability and evidentiary admissibility of digital artefacts in subsequent proceedings.

In using GenAI in legal work, it is advisable to proceed from the presumption that the tool is assistive, and that responsibility for the content and correctness of submissions remains entirely with the participant in the proceedings; therefore, any material prepared with the use of GenAI must undergo mandatory verification of facts, citations, and references before submission to the court. In practice, this should be supplemented by internal controls that prevent the inclusion of unverified or erroneous references to precedents or sources, as case law demonstrates that submitting such materials may entail procedural consequences for the party or their representative. Confidentiality requires separate attention: inputting sensitive or procedurally significant data into GenAI tools is justified only if there are clear guarantees regarding the processing and storage of information, consistent with general data management requirements and judicial guidelines on the responsible use of GenAI. To ensure the procedural verifiability of algorithmic outputs, it is recommended to retain primary records and metadata (video/photo, transactional data, telecom logs, system journals) along with documented data provenance and the chain of custody/transmission. Furthermore, it is necessary to document the description of the method and the limits of application: what exactly the system does, under which conditions the result is correct, what typical errors and limitations are known, and how these are accounted for in practical use.

Discussion

The research findings demonstrated that within Singapore's law enforcement system, artificial intelligence is transforming from a tool for automating routine tasks into a multi-layered architecture for operational triage and decision support. The formation of functional modes (alert-triage and operational-intervention) enables law enforcement agencies to scale response measures, particularly in the fight against fraud, where algorithmic systems ensure the prioritisation of subjects of attention. This approach aligns with the conclusions of N. Lettieri *et al.* (2023), who theoretically substantiated the human-machine collaboration strategy as a means of overcoming AI's "blind spots", where the algorithm acts as an analytical filter, while the final procedural decision rests with the human. Concurrently, the emphasis on the need for independent verification and contestability of algorithmic conclusions, identified in this study, correlates with the concept of "contestable AI" in the work of F. Maoro & M. Geierhos (2025), where the transparency of semantic modelling is considered a key condition for making informed decisions in criminal intelligence. The transformation of AI into a multi-layered decision-support architecture confirms the shift towards a human-machine strategy, where the effectiveness of scaling response measures is combined with the critical necessity of transparency and human control to ensure the contestability and validity of procedural conclusions.

Research by T. Greene *et al.* (2022) showed that a key vulnerability of algorithmic risk assessment tools is their predictive inconsistency, arising from model sensitivity to the structure of input data. This confirms the "risk paradox" of automation identified in the current study: incorrect settings or data errors in systems such as ANPR or SATIS scale as rapidly as the positive effect of their implementation. The authors also emphasised the risks of "tunnel vision" when using predictive systems, which corresponds to the results of the analysis of Singaporean cases regarding potential bias and the need to account for errors when generating "match" signals. In this context, the conclusions of A.S. Almasoud & J.A. Idowu (2024) regarding algorithmic fairness in predictive policing reinforce the thesis that without regular monitoring of data drift and auditing of model parameters, operational efficiency may conflict with the principles of non-discrimination.

The work of T. Douglas *et al.* (2021) revealed that a fundamental condition for the effectiveness of algorithmic risk assessment tools in criminal justice is not only the mathematical sophistication of the models but also the quality and representativeness of the input data. The authors noted that a deficit of reliable data leads to systemic errors that are subsequently difficult to identify in "machine" conclusions. This correlates with the current study's findings on the functioning of ANPR and SATIS systems (Singapore Police Force, 2024b), where the "risk paradox" of automation was identified: incorrect settings or methodological limitations based on historical data scale as rapidly as the operational benefit of the system. Parallels between these studies indicate that the identified problems of decision dependence on data structure necessitate systemic audit and regular monitoring of data drift. Concurrently, R.A. Berk *et al.* (2022) proposed methods for improving the fairness of algorithmic assessments through conformal prediction, which aligns with the current study's conclusions on the need to transition from probabilistic AI "candidate" signals to independent human confirmation of each result (human-in-the-loop). The "risk paradox" of automation necessitates systemic audit and data monitoring to prevent the scaling of errors and guarantee algorithmic fairness.

Research by M.-P. Sandoval *et al.* (2024) and S.M. Qureshi *et al.* (2024) demonstrated that systemic threats from deepfakes to criminal justice arise from the difficulty of identifying manipulations in multimodal data. This correlates with the current study, which identified specific risks of Generative AI (hallucinations, provenance issues) that necessitate mandatory enhanced verification of digital materials before their submission to court. The authors also emphasised that the technical sophistication of deepfakes can undermine trust in digital evidence overall, which corresponds to the results of the analysis of Singaporean guidelines: GenAI technology may support the preparation of materials, but responsibility for their accuracy and correctness invariably rests with the user. Parallels between the results and the Singaporean case indicate that the use of unverified algorithmic results or fabricated precedents leads to real procedural consequences for parties and their representatives. This further substantiates the need for the evolution of the control system towards a model of institutionally formalised oversight over the entire data processing cycle, from the primary artefact to the court submission, as the sole condition for maintaining trust in digital justice. Ensuring institutional control over the data lifecycle, combined with the personal responsibility of the user, is a critical prerequisite for the legitimate use of Generative AI in criminal justice.

The findings established that, unlike purely operational systems, the evidentiary framework in Singapore is based on the structuring role of the HTX agency, which embeds control elements directly into the technical architecture of forensic instruments. The technical properties of artefacts (logging standardisation, model version control, and documentation of the processing chain) are determined at the design stage, enabling the transformation of "raw" digital data into procedurally admissible materials with guaranteed integrity. This approach correlates with the conclusions of D. Dunsin *et al.* (2024), who demonstrated that the integration of AI and ML in contemporary 21st-century digital forensics requires new standards of transparency and incident audit to maintain trust in investigation outcomes. Furthermore, the emphasis identified in this study on the necessity of content provenance traceability corresponds with the position of J. Loovens & H. Tinmaz (2025), who noted that amidst the growing threat from deepfakes, only systematic verification and transparency of processing methods allow for the preservation of the evidentiary value of digital

materials. The implementation of explainable AI and the standardisation of forensic procedures enable the transformation of the algorithmic "black box" into a transparent evidentiary tool, ensuring the procedural reliability of justice.

The research by D. Purves (2022) documented that the expansion of algorithmic policing carries ambiguous implications for the fairness of justice. On one hand, automation allows for the processing of vast information arrays; on the other hand, without robust accountability mechanisms, it can exacerbate discriminatory practices. This corresponds with the current study's findings regarding the alert-triage mode of operation of the SPF and CAD, where the scaling of anti-scam interventions (as in the A.S.T.R.O. project (Singapore Police Force, 2024a)) is accompanied by risks of misclassification and potential impact on the rights of third parties. The author also emphasised the need for transparency in selection criteria, which aligns with the requirements identified in the study for the explainability of algorithmic outputs and access to event logs for independent verification. Thus, the transformation of AI in Singapore into a multi-level decision-support architecture allows for the critical scaling of law enforcement measures; however, its safety depends on the implementation of a "human-in-the-loop" strategy and the prevention of the "risk paradox" of automation through systematic audit and control of data bias. The procedural reliability of algorithmic results is achieved through the introduction of explainable AI and institutional control over the complete data lifecycle, enabling the court to distinguish between the technical authenticity of a digital record and the validity of its intellectual interpretation.

Conclusions

The research findings established that RPA technologies, despite their deterministic nature, require equally strict logging and access control as AI, due to the risks of large-scale error propagation. The Singapore Police Force (SPF) acts as the primary operator of the ecosystem, initiating the "data → processing" chain and producing primary digital artefacts for investigations. The networked and transactional nature of contemporary 21st-century financial crime makes automation within CAD an indispensable tool for overcoming the limitations of manual analysis. The logic of technologisation in financial crime fighting units is based on distinguishing between the analytical mode of hypothesis generation and the operational-automated mode of rapid interventions. The HTX agency performs a structuring role, determining the technical properties of evidence (model versions, logging parameters) already at the design stage of law enforcement systems. Within the realm of digital forensics, HTX ensures the critical transformation of "raw" data into procedurally admissible results, ready for judicial use. The judicial system functions as a "procedural filter", admitting technological results only on condition that they meet standards of integrity and verifiability. Normative regulation (Evidence Act) provides only the "entry" of electronic records into the evidentiary base, but does not guarantee the reliability of substantive conclusions drawn by algorithms. Judicial practice formulates the requirement for the prosecution to substantiate the technical suitability and stability of the data acquisition method, not merely the fact of its existence.

The practical effectiveness of algorithmic solutions is confirmed by the successful use of ANPR systems for real-time detection of stolen vehicles and the large-scale application of SATIS and SATIS+ tools, through which over 7,200 suspicious objects were triaged. At the same time, judicial precedents, notably the case of Tajudin bin Gulam Rasul and Mohamed Ghouse v. Suriaya bte Haja Mohideen, demonstrate the real procedural risks of improper use of generative AI, leading to the submission of unverified materials and corresponding sanctions for the parties involved. These examples underscore that high operational effectiveness in Singapore is invariably accompanied by strict requirements for the verification of each automated inference. The contestability of an algorithmic inference in criminal proceedings directly depends on the disclosure of the system's parameters, event logs, and the limits of the applied analytical methodology. "Human-in-the-loop" mandates the documentation of the verifier's identity, the list of data used by them, and the justification for the decision made based on the AI. To enable independent verification, law enforcement agencies are obliged to preserve primary records and metadata alongside a detailed description of the method of their processing. Future research should usefully focus on developing standardised protocols for the judicial audit of algorithmic results and improving mechanisms for the traceability of digital material provenance to ensure the contestability and reproducibility of evidence in criminal justice, particularly in Singapore.

Acknowledgements

None.

Funding

None.

Author Contributions

R. Jurka conceived and supervised the study, designed the methodology, and conducted data analysis. The author also drafted and revised the manuscript.

Conflict of Interest

None.

References

[1] AI Verify Foundation. (2024). *Proposed Model AI Governance Framework for Generative AI: Fostering a trusted ecosystem*. Retrieved from https://aiverifyfoundation.sg/downloads/Proposed_MGF_Gen_AI_2024.pdf.

[2] Alibašić, H. (2025). Harmonizing artificial intelligence (AI) governance: A comparative analysis of Singapore and France's AI policies and the influence of international organizations. *Global Public Policy and Governance*, 5, 93-113. doi: 10.1007/s43508-025-00116-w.
[3] Allen, J.G., Loo, J., & Luna, J.L. (2025). Governing intelligence: Singapore's evolving AI governance framework. *Cambridge Forum on AI: Law and Governance*, 1, article number e12. doi: 10.1017/cfl.2024.12.
[4] Almasoud, A.S., & Idowu, J.A. (2024). Algorithmic fairness in predictive policing. *AI and Ethics*, 5, 2323-2337. doi: 10.1007/s43681-024-00541-3.
[5] Beltrão, G., Goh, S.T., Sousa, S., & Lamas, D. (2025). Community, identity & stability? Building trust in facial recognition systems for mass surveillance. *Journal of Responsible Technology*, 24, article number 100139. doi: 10.1016/j.jrt.2025.100139.
[6] Berk, R.A., Kuchibhotla, A.K., & Tchetgen Tchetgen, E. (2021). Improving fairness in criminal justice algorithmic risk assessments using optimal transport and conformal prediction sets. *ArXiv*. doi: 10.48550/arXiv.2111.09211.
[7] Chase, J., Phong, T., Long, K., Le, T., & Lau, H.C. (2021). Grand-vision: An intelligent system for optimized deployment scheduling of law enforcement agents. *Proceedings of the International Conference on Automated Planning and Scheduling*, 31(1), 459-467. doi: 10.1609/icaps.v31i1.15992.
[8] Court of Appeal No. 42 "GIL v Public Prosecutor". (2025, May). Retrieved from https://www.elitigation.sg/gdviewer/s/2025_SGCA_21.
[9] Douglas, T., Davies, B., Pugh, J., Brown, R., Hass, B., Forsberg, L., Mishra, A., Singh, I., Savulescu, J., & Fazel, S. (2021). *Algorithmic risk assessment tools in criminal justice: The need for better data*. Oxford: University of Oxford.
[10] Dunsin, D., Ghanem, M.C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, 48, article number 301675. doi: 10.1016/j.fsidi.2023.301675.
[11] Evidence Act of the Republic of Singapore. (1997, December). Retrieved from https://sso.agc.gov.sg/Act-Rev/97/Published?DocDate=19971220&ProvIds=pr76-.
[12] Greene, T., Shmueli, G., Fell, J., Lin, C.-F., & Liu, H.-W. (2022). Forks over knives: Predictive inconsistency in criminal justice algorithmic risk assessment tools. *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, 185(2), 692-723. doi: 10.1111/rssa.12966.
[13] Guide on the Use of Generative Artificial Intelligence Tools by Court Users. (2024). Retrieved from https://surl.li/elcwmu.
[14] Home Team Science and Technology Agency. (2025). *Digital & information forensics*. Retrieved from https://www.htx.gov.sg/who-we-are/what-we-do/our-expertise/digital-information-forensics.
[15] Infocomm Media Development Authority. (2024). *Singapore proposes framework to foster trusted Generative AI development*. Retrieved from https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai.
[16] Khan, A.A. (2024). Reconceptualizing policing for cybercrime: Perspectives from Singapore. *Laws*, 13(4), article number 44. doi: 10.3390/laws13040044.
[17] Lee, H., & Lee, T. (2022). The tracetogether matrix has you – surveillance, rationalisation and tactics of governance in Singapore's COVID-19 app. *Platform: Journal of Media and Communication*, 9(2), 77-91.
[18] Lee, T., & Lee, H. (2020). Tracing surveillance and auto-regulation in Singapore: 'Smart' responses to COVID-19. *Media International Australia*, 177(1), 47-60. doi: 10.1177/1329878X20949545.
[19] Lettieri, N., Guarino, A., Zaccagnino, R., & Malandrino, D. (2023). Keeping judges in the loop: A human-machine collaboration strategy against the blind spots of AI in criminal justice. *Soft Computing*, 27, 11275-11293. doi: 10.1007/s00500-023-08604-z.
[20] Lim, N.F.-Z., & Tan, K.S. (2025). The new frontier: Regulating artificial intelligence in Singapore. *Singapore Academy of Law Journal*, 37, 436-463.
[21] Lim, S.S., & Chng, G. (2024). Verifying AI: Will Singapore's experiment with AI governance set the benchmark? *Communication Research and Practice*, 10(3), 297-306. doi: 10.1080/22041451.2024.2346416.
[22] Loovens, J., & Tinmaz, H. (2025). A systematic literature review of deepfakes in forensic science. *Forensic Imaging*, 43, article number 200647. doi: 10.1016/j.fri.2025.200647.
[23] Magistrate's Appeal No. 9043 "GIL v Public Prosecutor". (2024, November). Retrieved from https://www.elitigation.sg/gd/s/2024_SGHC_287.
[24] Maoro, F., & Geierhos, M. (2025). Contestable AI for criminal intelligence analysis: Improving decision-making through semantic modeling and human oversight. *Frontiers in Artificial Intelligence*, 8, article number 1602998. doi: 10.3389/frai.2025.1602998.
[25] Originating Claim No. 125 (Summons No. 1240 of 2025) "Tajudin bin Gulam Rasul and Mohamed Ghouse v. Suriaya bte Haja Mohideen". (2025, September). Retrieved from https://www.elitigation.sg/gd/s/2025_SGHCR_33.

[26] Personal Data Protection Commission. (2020). *Model AI governance framework*. Retrieved from https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf.
[27] Purves, D. (2022). Fairness in algorithmic policing. *Journal of the American Philosophical Association*, 8(4), 741-761. doi: 10.1017/apa.2021.39.
[28] Qureshi, S.M., Saeed, A., Almotiri, S.H., Ahmad, F., & Al Ghamdi, M.A. (2024). Deepfake forensics: A survey of digital forensic methods for multimodal deepfake identification on social media. *PeerJ Computer Science*, 10, article number e2037. doi: 10.7717/peerj-cs.2037.
[29] Sandoval, M.-P., Vau, M. de A., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, 13, article number 41. doi: 10.1186/s40163-024-00239-1.
[30] Seng, D., & Mason, S. (2021). Artificial intelligence and evidence. *Singapore Academy of Law Journal*, 33, 241-279.
[31] Singapore Courts. (2024). Strengthening justice, safeguarding society. In *Singapore courts annual report 2023*. Singapore: The Judiciary.
[32] Singapore Police Force. (2024a). *CAD report 2024*. Retrieved from https://www.police.gov.sg/-/media/SPF/Media-Room/Publications/CAD-Report-2024/CAD-Report-2024.pdf.
[33] Singapore Police Force. (2024b). *A future-ready Singapore Police Force: Cyber and beyond*. Retrieved from https://www.police.gov.sg/-/media/SPF/Files/Publications/PDF/SPF-Annual-Report-2024.pdf.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.352:004.42(574+519.5)

Article's History:
Received: 31.07.2025; Revised: 17.11.2025; Accepted: 16.12.2025

Digital forensics in combating cryptocurrency-related crimes in Kazakhstan and South Korea

Andrejs Vilks*
PhD, Professor
Riga Stradins University
LV-1007, 16 Dzirciema Str., Riga, Latvia
https://orcid.org/0000-0002-5161-0760

Aldona Kipane
PhD, Associate Professor
Riga Stradins University
LV-1007, 16 Dzirciema Str., Riga, Latvia
https://orcid.org/0000-0001-6408-3456

Anatolijs Krivins
PhD, Associate Professor
Daugavpils University
LV-5401, 13 Vienibas Str., Daugavpils, Latvia
https://orcid.org/0000-0003-1764-4091

Abstract. The purpose of this study was to identify the specific features of national approaches to the use of digital forensics in the investigation of cryptocurrency-related crimes in the Republic of Kazakhstan and the Republic of Korea. The methodological basis was a comparative analysis of regulatory and legal acts, practical approaches and the outcomes of law enforcement activities in both jurisdictions in the context of the transnational nature of cryptocurrency crime. The study revealed fundamental differences between the regulatory approaches: the Kazakhstani model is oriented towards the legalisation of the crypto industry through licensing and the creation of special regimes within the Astana International Financial Centre, whereas the Korean approach is characterised by strict financial supervision and preventive monitoring through specialised legislation on the protection of virtual asset users. An analysis of practical results for 2024 showed a significant asymmetry in the scale of law enforcement activity: Kazakhstan achieved initial success through the dismantling of 36 illegal cryptocurrency exchanges with a turnover of more than 110 million US dollars, the freesing of 4.8 million stablecoins and the return of 545 thousand stablecoins to victims, while in 2024 Korean law enforcement agencies continued to receive an increasing number of reports of suspicious cryptocurrency transactions, indicating the intensification of the financial monitoring system. The findings conceptualise two trajectories in the development of national digital forensics systems and confirm the critical role of the regulatory and legal framework in creating an effective evidentiary trail in cross-border investigations of cryptocurrency-related crimes. The practical significance of the study lies in identifying the preconditions for the successful functioning of digital forensics and the potential for mutual learning between jurisdictions with differing experience in regulating cryptocurrency markets, which may be used by regulatory and law enforcement bodies to improve national systems for countering cryptocurrency-related crime

Keywords: blockchain analysis; virtual assets; law enforcement agencies; international cooperation; regulatory mechanisms; law enforcement practice

Suggest Citation:
Vilks, A., Kipane, A., & Krivins, A. (2025). Digital forensics in combating cryptocurrency-related crimes in Kazakhstan and South Korea. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 75-89.

*Corresponding author

Introduction

With the increase in the volume of cryptocurrency transactions globally, the number of crimes involving digital assets is also growing. The challenges of investigating such crimes are becoming increasingly relevant for law enforcement agencies, as cryptocurrencies are used for money laundering, terrorist financing and fraud. Countries that are actively developing digital technologies and financial innovations, such as the Republic of Korea and Kazakhstan, are faced with the need to improve legal mechanisms and technical tools to combat cryptocurrency crime. This requires the development of specialised approaches to the collection and analysis of digital evidence, as well as the improvement of international cooperation in the field of cryptocurrency investigations.

The technological aspects of digital forensics have undergone significant development thanks to the research of N. Apsimet *et al.* (2024), who found a 40-60% increase in the accuracy of processing digital traces when using artificial intelligence compared with traditional methods. Their results confirmed the critical role of automated analysis of network traffic in identifying the sources of cyber-attacks and reducing human error in processing large data sets. A practical contribution to the development of cryptocurrency forensics was made by A. Park *et al.* (2023), who developed the first systematised three-phase methodology for examining cryptocurrency wallets, capable of ensuring effective investigation even in the absence of prior information on addresses or private keys. Experimental testing demonstrated a 35-50% reduction in the time required to identify cryptocurrency assets and an increase in the reliability of analytical results. Advances in automated fraud detection were demonstrated by U. Agarwal *et al.* (2023), whose system achieved the highest accuracy among existing solutions, at 97.5% when using a random forest algorithm, processing more than 10,000 transactions per minute with minimal false positives.

Structural problems in the sector were identified in the studies of S. Dudani *et al.* (2023), who found that 87% of academic works focus exclusively on Bitcoin, while the analysis of alternative cryptocurrencies remains underdeveloped. A review of 156 publications revealed critical gaps in inter-agency coordination and a lag of 3-5 years in the technological provision of forensic units compared with the pace of development of cryptocurrency technologies. The forensic features of specific categories of crime were examined by S. Choi *et al.* (2024), who identified eleven key scenarios of criminal activity in cryptocurrency Ponzi schemes and established that 73% of victims are persons over the age of 55 with limited knowledge of digital technologies. The results of their study showed that early detection of indicators of Ponzi schemes can prevent losses of up to 2.3 billion US dollars annually on a global scale. The issue of online fraud in the context of national security was addressed by A. Kaliyev (2024), who identified a critical correlation between the level of digital literacy in the population and the effectiveness of countering cybercrime, establishing that 65% of victims do not possess basic cyber security skills. The author demonstrated that a systemic approach to personnel training can increase the clearance rate of online crimes by 40-50% within five years.

The national context of the development of digital forensics in Kazakhstan has been studied by several research groups from different methodological standpoints. The legal foundations of coordination between public and private actors engaged in forensic activity were substantiated by Y. Alimkulov *et al.* (2023), whose findings formed the basis for the draft Law "On Private Detective Activity in the Republic of Kazakhstan". The state of development of the sector was assessed by Y. Saniyazova *et al.* (2024), who recorded a 15-fold increase in the number of cybercrimes over the past five years alongside a decline in clearance rates to 23%, due to a critical shortage of qualified experts and technical equipment. The prospects for technological modernisation of the criminal justice system were analysed by A. Abuova *et al.* (2025), whose forecasts suggest a reduction in the duration of criminal proceedings by 20-25% and an increase in the accuracy of evidence analysis to 90% with the implementation of a national platform for the management of digital evidence using artificial intelligence. Despite the broad range of existing studies, the practical implementation of cross-border cooperation between Kazakhstan and South Korea in the field of cryptocurrency investigations remains insufficiently explored.

The purpose of this study was to identify the specific features of national approaches to the use of digital forensics in the investigation of cryptocurrency-related crimes in the Republic of Kazakhstan and the Republic of Korea. The research objectives were as follows:

1. To examine the regulatory and legal foundations and mechanisms that constitute the legal basis for the functioning of digital forensics in the field of cryptocurrency-related crimes in both jurisdictions;

2. To analyse the practical approaches, institutional capacities and results of the application of digital forensic methods by the law enforcement agencies of kazakhstan and the republic of korea in the investigation of cryptocurrency-related offences;

3. To systematise existing mechanisms of international cooperation between the countries under study and to determine the prospects for the development of bilateral cooperation in countering cross-border cryptocurrency-related crime.

Materials and Methods

The methodological framework consisted of the international standards of the Financial Action Task Force (2025) (FATF) on the regulation of virtual asset service providers (VASP), in particular Recommendation 15 on new technologies and the Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Financial Action Task Force, 2021), which sets out the definition of VASP as entities that conduct exchange

between virtual assets and fiat currencies, transfer, safekeeping or administration of virtual assets. This provided unified criteria for assessing national approaches to countering cryptocurrency-related crime. The theoretical framework was formed by the conceptual foundations of digital forensics in the cryptocurrency sphere, based on comprehensive analysis of blockchain data, including address clustering for grouping wallets, heuristic algorithms for identifying behavioural patterns, analysis of time stamps and correlation analysis for detecting links between different addresses and services (Kubanova *et al.*, 2025).

The comparative legal method was used to systematically compare the regulatory approaches of the Republic of Kazakhstan and the Republic of Korea through an analysis of national legislative acts forming the legal basis for the functioning of digital forensics in the field of virtual assets, including the Act of the Republic of Korea No. 14839 (2017), the Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), and the Act of the Republic of Korea No. 19563 (2024) as well as subordinate legislation and regulatory documents governing special legal regimes, in particular the Rules and Mechanisms of Cooperation of Unbacked Digital Asset Exchanges with Second-Tier Banks of the Republic of Kazakhstan issued by the AIFC – Astana International Financial Centre (2023), and regulatory acts of the financial authorities of the Republic of Korea issued by the FSC – Financial Services Commission of Korea (2023; 2024a; 2024b) and the KoFIU – Korea Financial Intelligence Unit (n.d.). Structural and functional analysis was used to identify interconnections between different elements of national law enforcement systems, including coordination between regulatory authorities, financial intelligence units and law enforcement structures in both jurisdictions, with a view to identifying the specific features of organisational models for countering cryptocurrency-related crime and assessing promising areas for bilateral cooperation in this sphere.

Statistical analysis was applied to process quantitative indicators of the effectiveness of law enforcement activities, using analytical reports from the international platform Chainalysis (2024; 2025) on the volume of illegal cryptocurrency transactions, data from the Agency of the Republic of Kazakhstan for Financial Monitoring (2025a) on the dismantling of money laundering structures operating through cryptocurrency in 2024, and statistics from the State Revenue Committee… (2025) on the regulation of digital mining, as well as statistical indicators of the activities of the specialised investigative task force for cryptocurrency-related crimes in the Republic of Korea for 2023-2024 from the Seoul Southern District Prosecutors' Office (2024). The method of systematisation was used to create structured tables of regulatory requirements and mechanisms of international cooperation, which provided a clear representation of complex regulatory constructs and made it possible to identify a gradation from basic financial monitoring standards to specialised supervisory regimes for virtual assets. This facilitated systematic comparison of practices and the identification of specific features of national models for countering cryptocurrency-related crime.

The case-study method was used to examine instances in which national courts in the Republic of Kazakhstan recognised digital evidence obtained through blockchain analysis in criminal cases concerning the unlawful circulation of digital assets. The materials for analysis were official communications from the Agency of the Republic of Kazakhstan for Financial Monitoring (2025b) on court verdicts in cases of illegal cryptocurrency exchange in the cities of Astana and Almaty for the period 2024-2025, and an official communication from the Prosecutor's Office of Astana (2024) on the outcomes of court proceedings in cases relating to cryptocurrency-related crimes. This method made it possible to identify the courts' approaches to assessing the admissibility and reliability of electronic evidence in cases involving virtual assets and to establish practical evidential standards in cryptocurrency cases.

The international legal framework consisted of bilateral treaties on extradition and mutual legal assistance between Kazakhstan and the Republic of Korea concluded by the Ministry of Foreign Affairs of the Republic of Korea (2003), which establish a formal mechanism for the surrender of offenders and the exchange of evidential information in criminal matters. The analytical basis consisted of reports from international organisations, including materials from the INTERPOL (2023; 2024a; 2024b; 2025) HAECHI series of operations targeting online fraud and cryptocurrency scams, and the capacity-building programmes of the OSCE – Organisation for Security and Co-operation in Europe (2023; 2025) in the field of combating cybercrime, which together provided a comprehensive understanding of institutional mechanisms and practical outcomes of international cooperation in countering cryptocurrency-related crime.

Results

The growth in the volume of cryptocurrency transactions on a global scale is accompanied by a parallel increase in criminal offences involving the use of digital assets. As of 2024, law enforcement agencies in various countries are facing new challenges in investigating crimes in which cryptocurrencies are used as an instrument for laundering criminal proceeds, financing terrorism and conducting fraudulent schemes. In the Republic of Korea, a specialised investigative task force on cryptocurrency-related crimes, in the course of its activities in 2024, initiated more than 30 criminal cases, brought charges against 41 individuals and confiscated assets totalling 846 billion Korean won, of which 564 billion were virtual assets (Seoul Southern District Prosecutors' Office, 2024). In Kazakhstan, tax audits conducted during 2024 revealed violations in the field of cryptocurrency mining, which led to additional tax assessments amounting to 4.9 billion tenge, and also established cases of under-reporting income from the sale of cryptocurrency with additional assessments of personal income tax totalling 4.3 billion tenge, demonstrating the scale of

tax evasion in the cryptocurrency sector (State Revenue Committee…, 2025). The effectiveness of combating such offences directly depends on the capacity of law enforcement systems to adapt to technological change and to implement modern methods of digital forensics.

Regulatory and legal framework and the context of the problem of digital forensics. The global growth of crime in the field of cryptocurrencies is creating new challenges for law enforcement agencies in national jurisdictions, requiring the development of specialised methodological approaches and institutional mechanisms. According to analytical data from the specialised platform Chainalysis (2024; 2025), the volume of detected illegal cryptocurrency transactions worldwide in 2024 amounted to 40.9 billion US dollars under current metrics for identifying illicit addresses; however, taking into account historical trends in retrospective recalculation, this figure may reach 51 billion dollars after further identification of additional illicit addresses over the following year. For comparison, the initial estimate for 2023 amounted to 24.2 billion dollars at the time of publication of the preliminary report, but one year later, after additional identification of illicit addresses, this figure rose to 46.1 billion dollars, which demonstrates the need to take account of methodological particularities in the assessment of cryptocurrency-related crime. The share of criminal operations in 2024 was 0.14% of the total volume of cryptocurrency transactions, reflecting a decrease compared with 0.61% in 2023; however, this share is also expected to increase after retrospective recalculation. These statistical indicators confirm the need for the development of specialised approaches to countering cryptocurrency-related crime at the national level. An additional challenge in 2024 was the shift in the structure of cryptocurrency assets used in criminal activity: stablecoins accounted for 63% of all illicit transactions, reflecting a broader ecosystem-wide trend towards increased use of stablecoins, with the volume of operations involving them rising by 77% compared with the previous year (Chainalysis, 2025).

The dynamics of the development of cryptocurrency-related crime demonstrate a trend towards the complication and diversification of criminal schemes, evolving from early forms of investment fraud to complex multi-layered money laundering operations through decentralised finance protocols and transaction mixing services. Traditional categories of cryptocurrency crime include theft from centralised exchanges, fraudulent investment schemes and pyramids, ransomware demanding payment in cryptocurrencies, drug trafficking and other illicit goods on darknet platforms, as well as the use of crypto-assets to finance terrorism and circumvent international sanctions. Alongside traditional forms of criminality, new forms of offences specific to the decentralised financial ecosystem are emerging, including manipulation of decentralised exchanges, fraud involving non-fungible tokens, abuses within decentralised autonomous organisations and the exploitation of smart contract vulnerabilities for the unlawful appropriation of assets. This evolution of criminality requires law enforcement agencies to continuously adapt to new forms of criminalisation of the digital space and to develop appropriate methodological tools for counteraction.

The response to these challenges is the development of digital forensics in the field of cryptocurrencies, an interdisciplinary domain that integrates methods from information security, cryptography, financial analysis and criminal procedure law in order to identify, document and interpret electronic traces of criminal activity in blockchain ecosystems. The methodology of digital forensics in the cryptocurrency sphere is based on comprehensive analysis of blockchain data, including address clustering to group wallets belonging to a single user, heuristic algorithms to identify behavioural patterns, time-stamp analysis to establish the sequence of events and correlation analysis to detect links between different addresses and services (Kubanova *et al*., 2025). The technical basis of these methods consists of specialised tools such as Chainalysis Reactor, Elliptic Investigator and CipherTrace Inspector, which enable law enforcement agencies to visualise cryptocurrency flows, identify high-risk addresses and services, and automate the tracking of funds through complex money-laundering schemes. The practical application of these methodological approaches depends to a large extent on the existence of an appropriate regulatory and legal framework and institutional mechanisms in national jurisdictions.

In the context of creating such a legal framework, the Republic of Kazakhstan, in response to the development of the crypto industry and the potential risks of money laundering, adopted the comprehensive Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), which entered into force on 1 April 2023 and created the legal basis for regulating all aspects of activity in the field of virtual assets. For the first time at the national level, this legislative act defined the concept of a digital asset as a digital expression of value or contractual rights that can be transferred and stored in electronic form using distributed ledger technology or similar technology. Structurally, the Law establishes a distinction between backed digital assets, which comply with established regulatory requirements and are backed by real assets or issued on licensed platforms, and unbacked digital assets, which encompass all other virtual assets.

The institutional mechanism for implementing Kazakhstan's legislation provides for the creation of a system of inter-agency coordination under the leadership of an authorised body that is responsible for licensing activity in the field of digital mining and monitoring compliance with the legislation. In accordance with Article 4 of the Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), the authorised body carries out state control in the field of digital assets, including supervision of compliance by entities engaged in the issuance and circulation of digital assets with legislation in the sphere of anti-money laundering (AML) and countering the financing of terrorism. In addition, the legislation creates a special legal regime within the Astana International Financial Centre (2023), where licensed cryptocurrency exchanges operate under the supervision of the

Astana Financial Services Authority (AFSA), providing an additional level of control and oversight over the activities of market participants. The practical implementation of the regulatory model provides for mandatory licensing of mining activity, the use exclusively of accredited national mining pools, the obligation to sell part of mined cryptocurrency via Kazakhstani exchanges in the amount of 50% in 2024 with a subsequent increase to 75% from 2025, and the payment of tax at a rate of 15% on income (Crypto license in Kazakhstan, n.d.; Greshnikov, 2025).

In contrast to the Kazakhstani approach, the Republic of Korea has developed a phased approach to regulating the cryptocurrency market, characterised by systematic and consistent implementation of regulatory measures. The first stage was the reform in March 2021 of the Act of the Republic of Korea No. 14839 (2017), as amended in 2024, which introduced mandatory registration of VASP with the financial regulator and implemented the Financial Action Task Force travel rule for the transmission of information on the sender and recipient in cryptocurrency transfers exceeding 1 million won in order to prevent money laundering (Financial Services Commission of Korea, 2024a). As a result of these measures, more than 60 small cryptocurrency exchanges that failed to meet the enhanced compliance requirements, including mandatory partnerships with banks for the safekeeping of clients' fiat deposits, were closed, leading to market concentration around a small number of large licensed platforms with the corresponding supervisory and control infrastructure.

The current culmination of the development of the regulatory system was the adoption on 18 July 2023 by the National Assembly of the Republic of Korea of the Act of the Republic of Korea No. 19563 (2024), which consolidated provisions from 19 different bills and entered into force on 19 July 2024 after a one-year transition period for industry adaptation. This legislative act establishes a comprehensive supervisory regime aimed at ensuring user protection and creating an orderly virtual asset market through four key regulatory blocks: measures to protect client assets, prohibitions and sanctions against unfair trading, the granting of supervisory and sanctioning powers to financial regulators in respect of VASP, and mechanisms for cooperation between financial regulators and law enforcement agencies in investigating crimes on the virtual asset market. The regulatory component of the Act obliges VASP to ensure the segregation of clients' fiat funds and cryptocurrencies in banking institutions, to accrue interest for users on fiat deposits, and to maintain full (100%) reserves of cryptocurrencies belonging to clients (Financial Services Commission of Korea, 2024a).

The sanctions component of Korean legislation includes a wide range of supervisory and enforcement mechanisms that ensure effective law enforcement in the field of virtual assets. The Financial Supervisory Service (FSS) has been granted the right to conduct inspections and audits of compliance with user protection requirements, while the FSC ssion may impose administrative penalties, including orders to remedy violations, fines of up to 5 billion won for corporations, suspension of activities and revocation of registration (Financial Services Commission of Korea, 2024b). Criminal liability of up to five years' imprisonment is provided for in cases of systematic or particularly serious offences. Both jurisdictions, despite different emphases in their regulatory approaches, adhere to international Financial Action Task Force standards and implement regulatory mechanisms to ensure the transparency of cryptocurrency operations, recognising the necessity of coordinating global efforts to combat cybercrime and cryptocurrency-related offences (Kubanova *et al.*, 2025). The systematisation of regulatory requirements that constitute the legal basis for digital forensics in both countries is presented in Table 1.

Table 1. Regulatory requirements directly strengthening digital forensics

Jurisdiction	Instrument (year / status)	Key obligations of VASPs/exchanges relevant to forensics (data, access, control)	Supervisory authority
Kazakhstan	Law "On Digital Assets" No. 193-VII (adopted 06.02.2023; in force; amended 05.09.2024) – defines digital assets, introduces state control and coordination of AML/CFT in the field of digital assets	Requirement to comply with AML/CFT: KYC, STR, state control over issuance/circulation; consolidation of the powers of the authorised body for supervision and inter-agency coordination – legal basis for obtaining transactional data and logs from market participants	Authorised body of the Republic of Kazakhstan in the field of digital assets; cooperation with the financial intelligence unit
Kazakhstan (AIFC regime)	AIFC/AFSA: "Rules and mechanisms of cooperation of Unbacked Digital Asset Exchanges ... with second-tier banks of the Republic of Kazakhstan" (current version, PDF) – regulates interaction between exchanges and banks	Operational mechanisms for data exchange between cryptocurrency exchanges/operators of digital assets and second-tier banks: facilitates tracing of fiat on/off-ramps, retention and access to records of fund movements (bank logs plus on-chain references)	AFSA (AIFC regulator)
South Korea	Virtual Asset User Protection Act (VAUPA) (adopted 18.07.2023; in force since 19.07.2024) + drafts/detailed rules of the FSC	Segregation of clients' fiat funds in banks; 100% reserve of clients' crypto-assets; mandatory insurance/reserve fund for compensation of losses; continuous transaction monitoring and immediate reporting to the FSS of indicators of market manipulation/insider trading; enhanced inspections and sanctions by the FSC/FSS – together forming a complete evidentiary "trail" (logs, records, inspection reports)	FSC / FSS / KoFIU

Continued Table 1

Jurisdiction	Instrument (year / status)	Key obligations of VASPs/exchanges relevant to forensics (data, access, control)	Supervisory authority
South Korea (AML / Travel Rule)	Implementation of the FATF Travel Rule through KoFIU / the special act on financial information (2021); CDD for certain transactions; 1 million KRW threshold for transfers (wire transfers) in the AML system	Formalises KYC/CDD and inter-institutional data exchange on senders/recipients; ensures the availability of named information for rapid forensic analysis and ML screening of transfers through threshold-based procedures	KoFIU (financial intelligence unit)

Note: CFT – Combating the Financing of Terrorism; KYC – Know Your Customer; CDD – Customer Due Diligence; STR – Suspicious Transaction Reports; Travel Rule – the rule on the transfer of information on transaction participants
Source: compiled by the authors on the basis of the Korea Financial Intelligence Unit (n.d.), Law of the Republic of Kazakhstan No. 193-VII ZRK (2023), Astana International Financial Centre (2023), Financial Services Commission of Korea (2023), Financial Action Task Force (2021; 2025)

Table 1 systematises regulatory requirements that directly affect the effectiveness of digital forensics in both jurisdictions, demonstrating an evolution from basic AML/CFT standards to comprehensive supervisory mechanisms for virtual assets. Comparative analysis of the regulatory instruments presented reveals a gradation from general financial monitoring requirements in Kazakhstan's core legislation to the specialised regimes of the AIFC and the Korean system for protecting virtual asset users. The Korean model integrates preventive mechanisms for transaction monitoring and immediate reporting of suspicious operations directly into the obligations of service providers, whereas the Kazakhstani approach focuses on ensuring the basic infrastructure for the collection and exchange of information between regulatory bodies. Travel Rule mechanisms in both jurisdictions create the technical basis for international data exchange on cryptocurrency transfers, which is critically important for cross-border investigations, while the difference in threshold values reflects differing approaches to balancing user privacy and law enforcement needs.

Application of digital forensics: Investigation of cryptocurrency-related crimes in Kazakhstan and Korea. The practical implementation of the theoretical foundations of digital forensics depends on the capacity of law enforcement agencies to apply methods of tracing blockchain transactions and de-anonymising offenders, which requires the creation of specialised institutional structures and the development of appropriate technical competences. In both jurisdictions, specialised institutional capacities for conducting such investigations are being formed; however, their scale and organisational structure differ in line with national particularities of the cryptocurrency market and the law enforcement system. Kazakhstan demonstrates an initial stage of systematic implementation of digital forensics, receiving expert support from international organisations in building national capacities through specialised training programmes and the exchange of best practices. A concrete example of such cooperation was the joint training course held in Astana in June 2023 by the Organisation for Security and Co-operation in Europe (2023) and the United Nations Office on Drugs and Crime (UNODC) for Kazakhstani law enforcement officers, devoted to the investigation of crimes involving cryptocurrencies and the functioning of the darknet.

The structure of the training programme covered a wide range of theoretical and practical aspects of digital forensics, creating the necessary foundation for effective investigation of cryptocurrency-related crimes. Approximately 20 representatives of the Ministry of Internal Affairs, the Academy of the Ministry of Internal Affairs and the Academy of Law Enforcement Agencies under the Prosecutor General's Office took part in the programme, while international experts from Germany and Ukraine provided instruction on modern methodological approaches to cryptocurrency forensics. The practical component of the programme included key concepts of blockchain technologies and the functioning of cryptocurrencies, practical methods for profiling users, techniques for tracing transactions and procedures for seising crypto-assets, with participants practising practical skills in clustering cryptocurrency wallets, identifying linked addresses and analysing anomalies in transaction sequences (Organisation for Security and Co-operation in Europe, 2023). In addition, the programme included a demonstration by a representative of the cryptocurrency exchange Binance of the possibilities for cooperation between exchanges and law enforcement agencies in tracking transactions and disclosing information on suspects, as well as the study of anonymisation technologies, including the Tor network and Darknet platforms.

The technical component of digital forensics requires specialised knowledge and procedural skills, including the seizure of hardware devices storing private keys, the creation of forensic images of electronic data carriers, analysis of network activity logs and reconstruction of transaction chains in blockchain networks. In response to these requirements, Kazakhstani law enforcement agencies are introducing specialised protocols for preserving the integrity of digital evidence, including the use of cryptographic hash functions to confirm the immutability of data and the application of chain-of-custody procedures to document all stages of work with evidence (Kubanova *et al.*, 2025). The results of the practical application of the knowledge acquired by Kazakhstani law enforcement agencies are

confirmed by concrete outcomes in 2024 and the creation of judicial precedents for the use of digital evidence. According to the Agency of the Republic of Kazakhstan for Financial Monitoring (2025a), during 2024 the activities of 36 illegal cryptocurrency exchanges were detected and terminated, with a total turnover of approximately 60 billion tenge, equivalent to more than 110 million US dollars.

The characteristics of the offences uncovered indicate the systemic nature of the illegal activity and the need for a comprehensive approach to counteraction. These illegal exchanges operated without the necessary licences and outside the legal framework; some of them functioned as online services masquerading as peer-to-peer exchanges, did not carry out client identification procedures and, as investigations established, were widely used by organised criminal groups for laundering proceeds from cyber fraud and drug trafficking. The operational activities of law enforcement agencies demonstrated growing effectiveness through coordinated actions by different departments and the use of modern technical means. The Agency of the Republic of Kazakhstan for Financial Monitoring (2025a), with the support of the National Security Committee, conducted a comprehensive operation to block more than 3,500 web resources of illegal online exchanges, making access to their services more difficult for the public. The financial results of the operations included the freesing and confiscation of assets totalling 4.8 million USDT, equivalent to approximately 2.5 billion tenge, in the course of investigating these cases, which indicates that Kazakhstani authorities have mastered mechanisms for seising cryptocurrency assets by obtaining access to wallet private keys or through court orders for compulsory transfer of assets via exchange platforms.

The expansion of law enforcement activities has covered different types of cryptocurrency-related crime, including pyramid schemes and investment fraud. In 2024 the Agency of the Republic of Kazakhstan for Financial Monitoring (2025a) uncovered two pyramid schemes that had attracted investments in cryptocurrencies; law enforcement agencies were able to return approximately 545 thousand USDT to victims and additionally freeze 120 thousand USDT in the accounts of the organisers of the fraudulent schemes. Judicial practice has demonstrated the readiness of Kazakhstan's national legal system to recognise digital evidence obtained through blockchain analytics in criminal proceedings. In January 2024, a court in Astana convicted two individuals, A.V. Kuchukov and E.T. Sadirov, under Article 214 of the Criminal Code of the Republic of Kazakhstan for carrying out illegal cryptocurrency exchange operations with a turnover of 15 billion tenge; Kuchukov was sentenced to three years' imprisonment with confiscation of property, and Sadirov to two years and six months with confiscation of property, with 22,894.5 USDT, 328 thousand US dollars and almost 7 million tenge confiscated in favour of the state. In December 2024, a court in Astana delivered a verdict in a case concerning illegal entrepreneurial activity related to cryptocurrency exchange totalling more than 7 billion tenge, in which digital evidence of transactions served as the key evidential basis for the prosecution, and the Prosecutor's Office of Astana (2024), acting in the interests of the state, initiated four civil claims totalling 7.9 billion tenge, which were satisfied by court decisions with full recovery of the damage from the defendants. In March 2025, a court in Almaty convicted an individual under subparagraph 2 of paragraph 2 of Article 214 of the Criminal Code, imposing a sentence of two years and six months' restriction of liberty for the unlawful circulation of digital assets without the necessary permits totalling 5.6 billion tenge over the period from 2021 to 2024, with 5,172 USDT and a Mitsubishi motor car confiscated in favour of the state (Agency of the Republic of Kazakhstan for Financial Monitoring, 2025b). The above-mentioned court decisions create a body of precedent in which national courts recognise the admissibility and reliability of digital evidence obtained through the analysis of blockchain transactions, confirming the legal system's capacity to apply digital forensic methods effectively in proving cryptocurrency-related crimes.

In contrast to the initial stage of development in Kazakhstan, the Republic of Korea demonstrates one of the highest levels of institutional capacity in countering cryptocurrency-related crime globally, as a result of many years of experience and systematic investment in the development of relevant competences and technical capabilities. The historical development of the Korean system for combating cryptocurrency-related crime began in 2017-2018 with the establishment of specialised investigative teams to investigate cryptocurrency offences, including fraudulent initial coin offerings (ICO) and hacking attacks on local exchanges. The current stage of institutional development is characterised by the creation on 9 January 2024 by the FSS of two new departments devoted exclusively to virtual assets: the Virtual Asset Supervision Department and the Virtual Asset Investigation Department (Recent trends in virtual…, 2024). The functional division between the departments provides that the first is responsible for ongoing supervision, market monitoring and inspections of VASP, while the second is responsible for planning and conducting investigations and providing analytical support in uncovering criminal schemes.

The technological modernisation of Korea's financial monitoring system includes the implementation of new technological solutions announced by the KoFIU in 2024 for tracking cryptocurrency flows through the deployment of a system for the analysis and tracing of fund movements in the virtual asset sphere, which will integrate data from exchange platforms, banking institutions and blockchain scanners for the prompt detection of suspicious transactions (Recent trends in virtual…, 2024). An innovative element of the system is the potential introduction of a proactive mechanism for suspending suspicious transactions, which would allow the temporary blocking of fund movements prior to the commencement of a formal prosecution investigation in cases of reasonable suspicion of money

laundering or fraud. The comprehensive infrastructure includes integration with databases of all licensed cryptocurrency exchanges, automated real-time transaction monitoring and the use of machine learning algorithms to detect suspicious activity patterns; the system is capable of tracing transaction chains across multiple exchanges and wallets, identifying attempts to circumvent withdrawal limits through the creation of multiple accounts, and detecting correlations between the activities of different users in order to identify possible conspiracies or coordinated actions (Hassan, 2025).

Statistical performance indicators show an increase in the activity of law enforcement agencies in detecting and investigating cryptocurrency-related crime, reflecting both the growth in the scale of criminal activity and the improved effectiveness of monitoring and analytical systems. In 2023, the KoFIU received 16,076 reports of suspicious cryptocurrency transactions, 49% more than in 2022, while the number of recorded serious incidents potentially linked to money laundering, market manipulation or drug trafficking using cryptocurrencies rose by 90% (Financial Services Commission of Korea, 2024a). Enforcement effectiveness indicators show an increase in the proportion of reports that led to criminal proceedings, from 12% in 2022 to 23% in 2023. Concrete results of activity include the arrest of around one thousand suspects in cryptocurrency-related crimes in the first half of 2024, more than double the figure for the same period of the previous year, with the most high-profile case being the arrest of 215 individuals in November 2024 in connection with a cryptocurrency investment scam worth 320 billion won, equivalent to approximately 228 million US dollars (South Korean police arrest…, 2024).

The methodological basis of Korean digital forensics demonstrates a comprehensive approach to investigating cryptocurrency-related crime through the integration of technical and traditional investigative methods, including the analysis of blockchain data using specialised software, open-source intelligence to de-anonymise users by correlating cryptocurrency wallet addresses with activity on social networks, and monitoring of internet forums and messengers to detect the sale of stolen assets or the recruitment of investors. The judicial system of the Republic of Korea has accumulated practice in accepting electronic evidence collected in the blockchain as admissible and reliable in criminal cases concerning money laundering via cryptocurrencies. The practical application of these methods was demonstrated in the 320-billion-won case, in which an organised criminal group sold 28 types of virtual tokens via front investment companies without any real activity, artificially inflating their price through pyramid methods and market manipulation; in the course of the investigation, 22 bitcoins were confiscated and other assets of the group worth approximately 34 million US dollars were seised (South Korean police arrest…, 2024). The case illustrates the maturity of Korea's digital forensic system and its capacity to combine technical methods of blockchain analysis with traditional investigative measures effectively in order to achieve concrete law enforcement outcomes.

Comparative analysis and international cooperation in cryptocurrency crime investigations. The comparative analysis of national approaches to combating cryptocurrency crime in the Republic of Kazakhstan and the Republic of Korea reveals fundamentally different strategies, reflecting disparities in the development levels of national cryptocurrency markets, institutional capabilities, and regulatory priorities. Systematic comparison of practices allows for identifying the peculiarities of national models and assessing the prospects of bilateral cooperation in this field. The regulatory-institutional differences are fundamental and define the nature of law enforcement activity in the field of virtual assets. In the Republic of Korea, the regulatory regime is characterised by strictness and proximity to traditional financial supervision, with direct involvement of financial regulators in monitoring and investigating abuses in the virtual asset market (Financial Services Commission of Korea, 2024a). The Act of the Republic of Korea No. 19563 (2024) imposes direct obligations on service providers to counter fraud through monitoring trading activities and allows sanctions for non-compliance.

In contrast, the Kazakh model shows greater liberalisation concerning licensed market participants: the state focuses on legalising activities in mining and exchange operations, and on identifying blatantly illegal entities, including unlicensed exchangers and financial pyramids (Ministry of Artificial Intelligence…, 2022). The Law of the Republic of Kazakhstan No. 193-VII ZRK (2023) differs in that it does not contain detailed provisions on market manipulation or consumer protection but integrates general requirements for anti-money laundering and combating the financing of terrorism, extending financial monitoring provisions to the digital asset sphere. Institutionally, the fight against cryptocurrency crime in Kazakhstan is carried out by the Agency of the Republic of Kazakhstan for Financial Monitoring and the National Security Committee in cooperation with law enforcement agencies, while in the Republic of Korea, an integrated coordination system exists between the police, prosecutors, and financial regulators. This difference in approaches reflects different levels of maturity in the cryptocurrency markets and different state policy priorities in the sphere of financial innovation.

Analysis of quantitative performance indicators reveals a significant asymmetry in the scale of the problem and corresponding institutional response between the two countries, which is determined by the differing levels of development of national cryptocurrency ecosystems. In Kazakhstan, initial results have been achieved in seising crypto-assets worth millions of dollars, blocking thousands of illegal online resources, charging several individuals, and securing judicial convictions for cryptocurrency crimes, demonstrating the formation of basic capabilities in this area. Specific achievements include the liquidation of 36 illegal crypto exchanges with a total turnover of over 110 million USD, freesing assets worth 4.8 million USDT,

and returning approximately 545,000 USDT to victims (Agency of the Republic of Kazakhstan for Financial Monitoring, 2025a).

South Korea demonstrates much larger-scale law enforcement activity, reflecting the maturity of its institutional system in combating cryptocurrency crimes. In the first half of 2024, nearly a thousand suspects in cryptocurrency crimes were arrested, and hundreds of millions of dollars in both cryptocurrency and fiat were frozen and seized. The international INTERPOL (2024a) operation HAECHI-V, with active participation from the Republic of Korea in 2024, covered 40 countries, resulting in the arrest of 5,500 people and the confiscation of over 400 million USD in cryptocurrency and fiat assets. During this operation, Korean police, in cooperation with Chinese counterparts, dismantled a large-scale phone fraud network that caused 1.5 trillion won in losses and used cryptocurrency for money laundering, underscoring Korea's leading role in global efforts to combat cryptocurrency crime.

Common challenges and gaps in national systems are linked to the adaptability of criminal schemes to regulatory measures, requiring continuous improvement of digital forensics methods and international coordination of efforts. Criminals are increasingly using decentralised tools, including decentralised exchanges and mixing services, to circumvent regulatory requirements and complicate the tracing of funds. South Korean law enforcement agencies are recording cases of stolen funds being converted into private cryptocurrencies with increased anonymity, using decentralised finance protocols to hide traces, or multi-stage exchanges between stablecoins to obscure the source of asset origins. Kazakhstan faces the problem of transferring illegally obtained cryptocurrency assets abroad, especially through offshore platforms, complicating national law enforcement efforts and requiring international coordination to freeze such assets.

The technical complexity of evidence collection remains a shared challenge for both countries, as in order to bring a case to court, it is necessary not only to trace the transaction on the blockchain but also to prove that a particular cryptocurrency wallet belongs to a specific individual, which requires the combination of technical and traditional investigative methods. The legal foundation for bilateral cooperation between Kazakhstan and the Republic of Korea in combating cryptocurrency crime is based on a series of international agreements and multilateral mechanisms, creating the necessary institutional foundation for effective cooperation in cross-border crime investigations. The basic legal foundation was established on 13 November 2003 with the signing of the Extradition Treaty and the Mutual Legal Assistance Treaty (MLAT) in criminal matters (Ministry of Foreign Affairs of the Republic of Korea, 2003), which, after ratification in both countries, created a formal mechanism for the extradition of offenders and the exchange of evidential information in criminal cases. The MLAT obliges the parties to provide assistance in conducting investigative actions, including obtaining testimonies, documents, and physical evidence for use in criminal prosecution.

At the operational level, INTERPOL (2023) channels function through the I-24/7 system and global financial operations HAECHI under the coordination of the Republic of Korea, aimed at countering online fraud and cryptocurrency scams. The Republic of Korea is one of the main sponsors and coordinators of INTERPOL's HAECHI series operations, aimed at combating financial cybercrime, including cryptocurrency investment frauds, romantic scams involving cryptocurrency, and online gambling fraud. During HAECHI-IV, the Republic of Korea not only provided funding but also sent experts to joint headquarters in INTERPOL's Global Complex in Singapore, and initiated the publication of special notifications to inform other countries about new fraud schemes. Practical mechanisms of information exchange demonstrate the effectiveness of a multilateral approach to combating cross-border cryptocurrency crime through timely identification of new schemes and methods of their implementation, including the Republic of Korea's initiative to spread warnings about NFT rug pulls and the USDT Token Approval Scam through INTERPOL (2023).

The results of multilateral cooperation involving both countries confirm the effectiveness of coordinated international efforts in combating cryptocurrency crime. Operation First Light 2024, conducted under INTERPOL's aegis from March to May 2024 with the participation of 61 countries, including Kazakhstan, resulted in the arrest of 3,950 suspects and the freesing of assets totalling 257 million USD, of which 135 million USD were fiat funds and 2 million USD in cryptocurrency (INTERPOL, 2024b). The operation demonstrated the effectiveness of the Global Rapid Intervention of Payments mechanism in tracking and intercepting illicit income in both fiat currencies and cryptocurrencies through coordination between law enforcement and financial institutions across jurisdictions. The subsequent HAECHI VI operation, conducted from April to August 2025 with the participation of 40 countries and territories, including both Kazakhstan and South Korea, achieved significant results with the recovery of 439 million USD, including 342 million USD in fiat money and 97 million USD in physical and virtual assets (INTERPOL, 2025). During this operation, law enforcement agencies blocked over 68,000 bank accounts and froze about 400 cryptocurrency wallets, with approximately 16 million USD of illicit funds recovered from cryptocurrency wallets. A notable example of effective bilateral coordination was the successful recovery of 6.6 billion won (equivalent to 3.91 million USD), which the Korean steel company had transferred to an illegitimate bank account in Dubai after the detection of forged transport documents, with rapid communication between the two countries through the Global Rapid Intervention of Payments mechanism allowing the intercepted stolen funds to be fully returned (INTERPOL, 2025).

Kazakhstan is actively developing international cooperation in cryptocurrency forensics through participation

in regional initiatives under the Eurasian Group on Money Laundering and INTERPOL's working groups on Darknet and cryptocurrencies. The Agency of the Republic of Kazakhstan for Financial Monitoring is establishing working contacts with leading financial intelligence units globally, including the Korea Financial Intelligence Unit (n.d.), for the rapid exchange of intelligence on suspicious transactions and coordination of joint activities. From 2023 to 2025, within the framework of the Organisation for Security and Co-operation in Europe (2023; 2025) project on enhancing cybercrime capabilities, specialised training in blockchain forensics was conducted for Kazakhstani law enforcement officers with the participation of international experts, aligning standards for evidence collection and tracing. The structure of international cooperation mechanisms between Kazakhstan and the Republic of Korea in combating cryptocurrency crime is detailed in Table 2.

Table 2. Mechanisms of international cooperation and capacity building

Mechanism	Parties / Organiser	What it contributes to digital forensics	Current Status / Latest Activity
Bilateral Treaties: Extradition and Mutual Legal Assistance (MLAT)	Kazakhstan and the Republic of Korea (government agreements signed on 13.11.2003 in Seoul)	Legal basis for the execution of procedural requests, obtaining evidence (logs, exchange/bank records), temporary asset freezes, and extradition of suspects in cryptocurrency-related cases	Treaties in force; used as the basic channel for MLAT/extradition in cross-border investigations
INTERPOL's HAECHI Operations Series	INTERPOL with the support of the Republic of Korea; participation of dozens of countries	Operational headquarters, exchange of intelligence on fraudulent crypto schemes; flash alerts (typologies); rapid "cold" freesing of stolen digital assets via exchange-law enforcement coordination	Active programme; 2024 – record results (HAECHI-V, Jul-Nov 2024); large-scale multinational coordination
Joint Training on Cryptocurrencies and Darknet	OSCE and UNODC in cooperation with Kazakhstan (law enforcement agencies)	Standardisation of methodologies: address clustering, transaction chain tracing, crypto-asset seizure, OSINT in Darknet; training officers capable of working with evidence under Korean and international standards	23.06.2023 – course in Astana; 12-13.06.2025 – workshop with new competency framework in cybercrime (update to 2025 approach)
Banking-Crypto Interaction at the AIFC	AFSA (AIFC), banks of the Republic of Kazakhstan, and digital asset market participants	Regulated channel for linking on-chain data with banking logs (fiat on/off-ramps), accelerating request processing, wallet/account reconciliation	Rules in force; used during compliance checks and requests by law enforcement and supervisory agencies

Note: OSINT – Open Source Intelligence

Source: compiled by the authors based on INTERPOL (n.d.; 2024a), Ministry of Foreign Affairs of the Republic of Korea (2003), Astana International Financial Centre (2023), Organisation for Security and Co-operation in Europe (2023; 2025)

Table 2 illustrates the multi-layered architecture of international cooperation between Kazakhstan and the Republic of Korea in combating cryptocurrency crime, demonstrating a combination of bilateral legal instruments and multilateral operational mechanisms. The bilateral treaties of 2003 establish a stable legal foundation for formalised mutual legal assistance procedures, while participation in INTERPOL's global initiatives provides access to operational information and coordinated actions against transnational cryptocurrency networks. Capacity-building programmes under the aegis of the OSCE and other international organisations play a role in standardising methodological approaches and aligning technical competences, which are prerequisites for effective evidence exchange and joint investigations. Banking-cryptocurrency interaction within the AIFC provides an additional channel for obtaining financial information that may be relevant for international requests when cryptocurrency operations intersect with traditional banking systems. The asymmetry in the level of activity of different mechanisms reflects the current state of bilateral relations and the potential for deepening cooperation through intensified Kazakhstan's participation in global Korean-led initiatives.

The practical roadmap for bilateral cooperation between Kazakhstan and the Republic of Korea can rely on existing institutional mechanisms and foresee the gradual deepening of cooperation through specific operational measures and technical solutions. Recommended measures include updating operational protocols between financial intelligence units by creating contact points for urgent asset freezes and standardising data formats, which will ensure the speed and effectiveness of information exchange in critical situations. Integrating Kazakhstan into HAECHI operations with a focus on cross-border investment schemes and arbitrage operations will enable the country to contribute to global efforts to combat cryptocurrency crime and gain access to advanced methodologies and technical solutions. The use of the institutional architecture of the 2003 treaties to form expedited request procedures in virtual asset cases through standard lists of requested artifacts, agreed response times, and standardised procedures for data preservation and transmission will increase the efficiency of bilateral cooperation. Digital forensics has become an integral part of law enforcement tools in both countries, with varying levels of integration and technological maturity, while cooperation between the two countries

and integration into global initiatives is a strategic resource for enhancing the effectiveness of national systems in countering cryptocurrency crime.

Discussion

The research results revealed fundamental differences between the regulatory philosophies of Kazakhstan and the Republic of Korea, where the Kazakh model focuses on the legalisation of the crypto industry through licensing and special legal regimes within the AIFC, while the Korean approach is characterised by strict financial oversight and preventive monitoring with the integration of consumer protection requirements. This conclusion is fully supported by the detailed analysis of J. Lee (2024), who traced the evolution of Korean legislation from the initial ban on ICO in 2017 through the Terra/Luna crisis to the adoption of the VAUPA in 2023, highlighting the phased nature of regulatory changes. W. Jon & W. Yang (2025) further specified the mechanisms of the dual regulatory structure, where tokenised assets, defined as securities, are regulated by the Capital Markets Act, while other virtual assets fall under VAUPA, which fully correlates with the comprehensive oversight strategy identified in the study. The study by A. Sapa (2025) empirically demonstrated the positive impact of blockchain technologies on the financial security of 200 Kazakh enterprises between 2017 and 2023, using quantile regression and revealing coefficients ranging from 0.062 to 0.124 for blockchain and from 0.054 to 0.098 for tokenisation, depending on the level of financial vulnerability. This supports the study's conclusion about the legalisation strategy through the creation of a favorable business environment. A.B. Zhanabilova (2024) analysed the legal mechanisms of digital asset inheritance in Kazakhstan and confirmed the creation of a comprehensive institutional foundation through the distinction between secured and unsecured assets, which aligns with the identified feature of the Kazakh approach to categorising virtual assets.

The study also identified significant asymmetry in the practical results of applying digital forensics, where Kazakhstan achieved initial successes with the liquidation of 36 illegal exchanges and the confiscation of over 110 million USD in assets, while the Republic of Korea demonstrated large-scale results with the arrest of about a thousand suspects within six months and participation in global operations confiscating hundreds of millions of dollars. This confirms the findings of E. Ove *et al.* (2025) and C. Leuprecht *et al.* (2023). E. Ove *et al.* conducted a comprehensive analysis of the effectiveness of blockchain forensics in detecting illegal financial flows and confirmed that Korean tools from Chainalysis, CipherTrace, and Elliptic, through the use of machine learning algorithms and data visualisation, allowed law enforcement to identify suspicious activities in decentralised ecosystems, explaining the high success rates of operations. The authors detailed significant confiscation cases and law enforcement operations, confirming the growing role of blockchain forensics in dismantling criminal networks through darknet markets and unregulated exchanges. C. Leuprecht *et al.* conducted a cross-case analysis of 12 cases of transnational money laundering through cryptocurrencies and found that Bitcoin remains popular among money launderers alongside altcoins, with the use of third-party exchanges being a common method for creating and hiding illicit funds, which fully correlates with the trend of diversifying criminal schemes and justifies different national approaches to regulating exchanges.

The multi-level architecture of international cooperation identified in the study, from the 2003 bilateral treaties to participation in INTERPOL's HAECHI operations and capacity-building programs through the Organisation for Security and Co-operation in Europe, is fully supported by the research of Y. Ma (2025), who independently concluded the critical importance of coordinated international operations in combating transnational cryptocurrency networks.

The authors also conducted a detailed analysis of tracing techniques, including graph analysis, heuristic clustering algorithms, and probabilistic deanonymisation, and evaluated the evolution of the regulatory landscape, particularly the role of the Office of Foreign Assets Control and their legal challenges, which aligns with the recommendations of the study regarding the standardisation of methodological approaches. Y. Ma conducted a detailed study of the challenges in identifying VASP in cross-chain bridges through the analysis of the money laundering case from the 2022 Harmony hack and highlighted significant deficiencies and ambiguities in the current Financial Action Task Force regulatory frameworks, particularly regarding the distinction between owners/operators and other influential parties in decentralised financial arrangements, fully confirming the findings of the study about the need for specialised methodologies for international evidence exchange in cases involving decentralised tools.

C. Volten *et al.* (2025) used a mixed approach to study the impact of the Dutch implementation of the Fifth Anti-Money Laundering Directive on cryptocurrency exchanges, analysing over 335,000 transactions and conducting seven qualitative interviews with exchanges and supervisory authorities, revealing that regulatory measures created a high administrative burden and significant fees for relatively small exchanges, which provided additional insights into the implementation of international standards and emphasised the need for a proportional approach to regulating different types of market participants.

The conceptualisation of two trajectories of development for national digital forensics systems – the evolutionary model of gradual regulatory infrastructure building and the model of simultaneous market legalisation and law enforcement capability development – is fully supported by methodological research that developed the technical foundations of blockchain forensics. Y. Gong *et al.* (2025) focused on Bitcoin blockchain analysis and improved address clustering, presenting an enhanced simulation model for accurately modeling real Bitcoin transactions and

proposing a new heuristic algorithm for identifying one-time change addresses with experimental results demonstrating more accurate clustering results compared to existing heuristic methods, supporting the study's conclusion about the importance of technical competences for the evolutionary model of development and the need for standardised platforms to evaluate clustering algorithms.

H. Atlam *et al.* (2024) conducted a systematic literature review of 46 articles from an initial pool of 672 publications and systematically analysed the challenges of blockchain forensics, emphasising the difficulties in identifying and tracking illegal activity due to the decentralisation of technology and issues with preserving the integrity of evidence due to blockchain immutability, which fully correlates with the study's identified technical limitations regarding proving the ownership of cryptocurrency wallets by specific individuals. A. Choudhary (2023) highlighted the transformative potential of blockchain technology for forensic investigations and computer forensics, noting the possibilities of using hash values for verifying the authenticity of digital data and emphasised the need for specialised knowledge and tools for the successful investigation of crimes involving blockchain, supporting the conclusion about the dependence of effectiveness on institutional maturity and the importance of developing technical competences in law enforcement agencies. R. Shevchuk *et al.* (2025) and S.A. Al Naqbi *et al.* (2025) conducted bibliometric analyses and demonstrated the rapid growth of publications on anomaly detection in blockchain networks from 2017 to 2024 and the increasing interest in machine learning in blockchain security, identifying key scientific clusters, including unsupervised learning, Bitcoin security, and lightweight federated learning, which supports the study's findings about the technologisation of law enforcement and the evolution from basic protection mechanisms to complex artificial intelligence approaches.

The conclusion of the study regarding the critical role of the legal framework in creating an effective evidence trail and ensuring transparency in cryptocurrency operations is fully supported by legal and social studies. C. Ahn & N. Obermeier (2023) conducted a nationally representative survey experiment in South Korea and empirically demonstrated that exposure to information about cryptocurrency volatility increases trust in the government, while positive information about cryptocurrencies does not undermine trust in the government or support for state regulation, confirming the effectiveness of the comprehensive regulatory approach and the importance of public perception of legal measures for their legitimacy and effectiveness. A. Popik-Mazur (2025) analysed 1,249 articles from Scopus and Web of Science databases and applied a thematic synthesis of 1,135 articles to present the current state of the literature on illegal financial flows and money laundering, finding that 38% of the literature focuses on knowledge systematisation, while advanced machine learning techniques make up 26%, and modified gravitational models make up 3.33%, supporting the study's conclusion about the need for integration of technical and legal competences and an interdisciplinary approach to combating cryptocurrency crime.

The analysis of international scientific research demonstrates significant convergence of findings on key aspects of the development of digital forensics in the field of cryptocurrencies and confirms the theoretical and practical foundations established in the study. Most of the analysed works confirm the importance of adaptive regulatory approaches, the need for technological modernisation of law enforcement systems, and the critical importance of international coordination in combating transnational cryptocurrency crimes. The scientific community is increasingly focusing on developing standardised methodologies and technical solutions, applying machine learning algorithms to automate suspicious transaction detection processes, and creating integrated systems for monitoring cryptocurrency flows, indicating the formation of a consensus on the directions for the development of digital forensics and confirming the relevance of the comparative approach to analysing national models.

Conclusions

The study revealed fundamental differences between national approaches to the application of digital forensics in combating cryptocurrency crimes, systematised regulatory mechanisms, and assessed the effectiveness of law enforcement activities in two jurisdictions with different levels of cryptocurrency market development. The comprehensive analysis allowed for the identification of patterns in the formation of national models for combating cryptocurrency crime and identified key factors for their success. The analysis established that the legal systems of Kazakhstan and the Republic of Korea demonstrate different regulatory philosophies: the Kazakh model is oriented towards the legalisation of the crypto industry through licensing and tax incentives, with an emphasis on creating special legal regimes within the AIFC, while the Korean approach is characterised by stringent financial oversight and preventive monitoring with integrated consumer protection requirements. The study confirmed the significant asymmetry in the practical results of digital forensics application: Kazakhstan achieved initial successes with the confiscation of crypto-assets worth over 110 million USD and the liquidation of 36 illegal exchanges, demonstrating the formation of basic institutional capabilities, while the Republic of Korea demonstrated large-scale results with the arrest of around a thousand suspects within six months and participation in global operations confiscating hundreds of millions of dollars, confirming the maturity of the national system. The systematisation of international cooperation mechanisms revealed the operation of a multi-level architecture from the bilateral treaties of 2003 to participation in INTERPOL's HAECHI operations, while capacity-building programs through OSCE ensure the standardisation of methodological approaches and alignment of technical competences.

The results conceptualise two trajectories for the development of national digital forensics systems: the evolutionary model of gradual regulatory infrastructure building and the model of simultaneous market legalisation and law enforcement capacity building. The study confirms the critical role of the legal framework for creating an effective evidence trail and demonstrates the potential for international cooperation through a combination of formal treaty mechanisms and operational multilateral initiatives. The methodological contribution of the work lies in the development of a comparative analytical framework for assessing the effectiveness of national digital forensics systems. The practical significance of the results lies in identifying the preconditions for the successful functioning of digital forensics, including the need for integrating technical and legal competences, creating specialised institutional structures, ensuring inter-agency coordination, and the potential for mutual learning between jurisdictions with different experiences in regulating cryptocurrency markets.

The limitation of the study was its focus on two jurisdictions and limited access to detailed statistical information on specific aspects of operational investigative activities and international requests in cryptocurrency cases. A promising direction for future research is the expansion of the comparative analysis to other jurisdictions, the study of the impact of technological innovations on the effectiveness of digital forensics, and the development of standardised methodologies for international evidence exchange in cases involving decentralised financial instruments.

Acknowledgements
None.

Funding
None.

Author Contributions
A. Vilks conceived and supervised the study, and drafted the manuscript. A. Kipane contributed to data analysis and the development of methodology. A. Krivins revised the manuscript and provided significant input to the interpretation of results. All authors reviewed and approved the final manuscript.

Conflict of Interest
None.

References
[1] Abuova, A., Bakirova, N., Begaliyev, Y., Begaliyev, B., & Kaliyev, A. (2025). Prosecutorial effectiveness in Kazakhstan's criminal justice: The role of digital forensics and online trial broadcasting. *Mitteilungen Klosterneuburg*. doi: 10.61586/fg5bE.

[2] Act of the Republic of Korea No. 14839 "On Reporting and Using Specified Financial Transaction Information". (2017, October). Retrieved from https://law.go.kr/LSW/lsInfoP.do?lsiSeq=195313&urlMode=engLsInfoR&viewCls=engLsInfoR.

[3] Act of the Republic of Korea No. 19563 "On the Protection of Virtual Asset Users". (2024, July). Retrieved from https://law.go.kr/engLsSc.do?menuId=1&subMenuId=21&tabMenuId=117#.

[4] Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2023). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*, 34(2), article number e2255. doi: 10.1002/nem.2255.

[5] Agency of the Republic of Kazakhstan for Financial Monitoring. (2025a). *Liquidation of cryptocurrency money laundering structures*. Retrieved from https://www.gov.kz/memleket/entities/afm/press/news/details/913888.

[6] Agency of the Republic of Kazakhstan for Financial Monitoring. (2025b). *In Almaty, a verdict was issued in the case of a crypto exchanger: Digital assets and a car were confiscated*. Retrieved from https://www.gov.kz/memleket/entities/afm/press/news/details/955747?lang=en.

[7] Ahn, C., & Obermeier, N. (2023). Cryptocurrency and the state: Evidence from South Korea. *Open Science Framework*. doi: 10.31219/osf.io/r4ayu.

[8] Al Naqbi, S.A., Nobanee, H., & Ellili, N.O.D. (2025). Global trends and insights into cryptocurrency-related financial crime. *Research in International Business and Finance*, 75, article number 102756. doi: 10.1016/j.ribaf.2025.102756.

[9] Alimkulov, Y., Sharipova, A., Zhanibekov, A., Mukhamadiyeva, G., & Aryn, A. (2023). Private detective activity of the law enforcement system of Kazakhstan on the experience of foreign countries. *International Journal of Electronic Security and Digital Forensics*, 15(6), 644-654. doi: 10.1504/IJESDF.2023.133964.

[10] Apsimet, N.M., Alimkulov, Y.T., & Duisenbayeva, G.Z. (2024). The collection of digital traces in the investigation of online crimes. *Law Series*, 7(4), 170-185.

[11] Astana International Financial Centre. (2023). Rules and mechanisms of cooperation of unbacked digital asset exchanges and/or centre participants authorised to carry out digital assets-related activities with second-tier bank of the Republic of Kazakhstan. In *AIFC Rules* (No. FR00063). Astana: AIFC.

[12] Atlam, H.F., Ekuri, N., Azad, M.A., & Lallie, H.S. (2024). Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions. *Electronics*, 13(17), article number 3568. doi: 10.3390/electronics13173568.

[13] Chainalysis. (2024). *The 2024 crypto crime report: The latest trends in ransomware, scams, hacking, and more*. Retrieved from https://www.pensamientopenal.com.ar/system/files/Documento_Editado1686.pdf.

[14] Chainalysis. (2025). *2025 crypto crime trends: Illicit volumes portend record year as on-chain crime becomes increasingly diverse and professionalized*. Retrieved from https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/.
[15] Choi, S.W., Lee, J., & Lee, S. (2024). Cryptocurrency Ponzi schemes and their modus operandi in South Korea. *Security Journal*, 37, 1285-1300. doi: 10.1057/s41284-024-00417-5.
[16] Choudhary, A. (2023). Forensic investigations and computer forensics in the age of blockchain. *ISACA Journal*, 5.
[17] Crypto license in Kazakhstan. (n.d.). *GoFaizen & Sherle*. Retrieved from https://gofaizen-sherle.com/crypto-license/kazakhstan.
[18] Dudani, S., Baggili, I., Raymond, D., & Marchany, R. (2023). The current state of cryptocurrency forensics. *Forensic Science International: Digital Investigation*, 46, article number 301576. doi: 10.1016/j.fsidi.2023.301576.
[19] Financial Action Task Force. (2021). Virtual assets and virtual asset service providers. In *Updated guidance for a risk-based approach*. Paris: FATF/OECD.
[20] Financial Action Task Force. (2025). International standards on combating money laundering and the financing of terrorism & proliferation. In *The FATF recommendations*. Paris: FATF/OECD.
[21] Financial Services Commission of Korea. (2023). *FSC proposes rules on the protection of virtual asset users*. Retrieved from https://fsc.go.kr/eng/pr010101/81217.
[22] Financial Services Commission of Korea. (2024a). *The act on the protection of virtual asset users to take effect from July 19*. Retrieved from https://fsc.go.kr/eng/pr010101/82683.
[23] Financial Services Commission of Korea. (2024b). *Strengthening responses to money laundering related to virtual assets and illegal private financing: Current status and plans*. Retrieved from https://www.fsc.go.kr/no010101/81712.
[24] Gong, Y., Chow, K.P., & Yiu, S.M. (2025). Improved Bitcoin simulation model and address heuristic method. *Forensic Science International: Digital Investigation*, 53, article number 301935. doi: 10.1016/j.fsidi.2025.301935.
[25] Greshnikov, K. (2025). New in the regulation of digital assets in Kazakhstan. *Chambers and Partners*.
[26] Hassan, B. (2025). *South Korean Island targets crypto tax evaders*. Retrieved from https://livebitcoinnews.com/south-korean-island-targets-crypto-tax-evaders.
[27] INTERPOL. (2023). *USD 300 million seised and 3,500 suspects arrested in international financial crime operation*. Retrieved from https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation.
[28] INTERPOL. (2024a). *INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million*. Retrieved from https://www.interpol.int/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million.
[29] INTERPOL. (2024b). *USD 257 million seised in global police crackdown against online scams*. Retrieved from https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams.
[30] INTERPOL. (2025). *USD 439 million recovered in global financial crime operation*. Retrieved from https://www.interpol.int/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation.
[31] INTERPOL. (n.d.). *Financial crime initiatives*. Retrieved from https://www.interpol.int/Crimes/Financial-crime/Financial-crime-initiatives.
[32] Jon, W., & Yang, W. (2025). Mapping South Korea's digital asset regulatory landscape: From criminal code to the recently implemented virtual asset user protection act. *Computer Law & Security Review*, 57, article number 106140. doi: 10.1016/j.clsr.2025.106140.
[33] Kaliyev, A. (2024). Selected aspects of investigating Internet fraud. *Newsletter of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 80(2), 294-301.
[34] Korea Financial Intelligence Unit. (n.d.). *What we do: Our efforts to prevent money laundering*. Retrieved from https://kofiu.go.kr/eng/policy/guide04.do.
[35] Kubanova, N., Nessipbayeva, I., Dyussebaliyeva, S., & Halibati, H. (2025). Countering cyber attacks in the Republic of Kazakhstan: Interdisciplinary issues and legal frameworks in the context of social security and economic stability. *Social & Legal Studies*, 8(1), 179-194. doi: 10.32518/sals1.2025.179.
[36] Law of the Republic of Kazakhstan No. 193-VII ZRK "On Digital Assets in the Republic of Kazakhstan". (2023, February). Retrieved from https://adilet.zan.kz/eng/docs/Z2300000193.
[37] Lee, J. (2024). An introductory review of virtual asset regulations in Korea. *Journal of Korean Law*, 23, 391-412.
[38] Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime*, 30(4), 1036-1054. doi: 10.1108/JFC-07-2022-0161.
[39] Ma, Y. (2025). Who constitute the VASPs in DeFi? A case study on money laundering via cross-chain bridge from the 2022 harmony hack. *Journal of Economic Criminology*, 7, article number 100131. doi: 10.1016/j.jeconc.2025.100131.
[40] Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan. (2022). *Digital assets industry*. Retrieved from https://www.gov.kz/memleket/entities/maidd/press/article/details/84078.

[41] Ministry of Foreign Affairs of the Republic of Korea. (2003). *Signing of the Korea-Kazakhstan treaty on extradition and treaty on mutual assistance in criminal matters*. Retrieved from https://mofa.go.kr/eng/brd/m_5676/view.do.
[42] Organisation for Security and Co-operation in Europe. (2023). *Joint OSCE-UNODC training course on cryptocurrencies and Darknet investigations held in Kazakhstan*. Retrieved from https://osce.org/secretariat/546977.
[43] Organisation for Security and Co-operation in Europe. (2025). *OSCE workshop in Kazakhstan advances national training strategy on cybercrime and electronic evidence*. Retrieved from https://osce.org/secretariat/593071.
[44] Ove, E., Williams, S., & Anderson, G. (2025). *The effectiveness of blockchain analytics in detecting illicit financial flows*. Retrieved from https://www.researchgate.net/publication/394929590_The_Effectiveness_of_Blockchain_Analytics_in_Detecting_Illicit_Financial_Flows.
[45] Park, A., Ryu, H., Park, W., & Jeong, D. (2023). Forensic investigation framework for cryptocurrency wallet in the end device. *Computers & Security*, 133, article number 103392. doi: 10.1016/j.cose.2023.103392.
[46] Popik-Mazur, A. (2025). A systematic literature review of illicit financial flows and money laundering: Current state of research and estimation methods. *Journal of Economics and Management*, 47, 257-298. doi: 10.22367/jem.2025.47.11.
[47] Prosecutor's Office of Astana. (2024). *Cryptocurrency as an object and means of committing crimes*. Retrieved from https://www.gov.kz/memleket/entities/prokuror-astana/press/news.
[48] Recent trends in virtual asset regulation. (2024). *Kim & Chang*. Retrieved from https://kimchang.com/en/insights/detail.kc?sch_section=4&idx=29294.
[49] Saniyazova, Y., Mediyev, R., Saitova, E., Utegenova, G., & Kzylkhojayeva, A. (2024). Advancing forensic science in Kazakhstan: The emergence and impact of digital forensics in cybercrime investigation. *Law, State and Telecommunications Review*, 16(2), 48-68. doi: 10.26512/lstr.v16i2.49190.
[50] Sapa, A. (2025). The impact of blockchain adoption and tokenisation on the financial security of Kazakhstani enterprises. *Futurity Economics & Law*, 5(3) 4-31. doi: 10.57125/FEL.2025.09.25.01.
[51] Seoul Southern District Prosecutors' Office. (2024). *One year of achievements and determination of the "virtual asset crime joint investigation team"*. Retrieved from https://www.spo.go.kr/site/spo/ex/board/View.do?bcIdx=1057718&cbIdx=1403.
[52] Shevchuk, R., Martsenyuk, V., Adamyk, B., Benson, V., & Melnyk, A. (2025). Anomaly detection in blockchain: A systematic review of trends, challenges, and future directions. *Applied Sciences*, 15(15), article number 8330. doi: 10.3390/app15158330.
[53] South Korean police arrest 215 people in suspected $228m crypto scam. (2024). *The Guardian*. Retrieved from https://theguardian.com/world/2024/nov/13/south-korea-crypto-scam-arrests.
[54] State Revenue Committee of the Ministry of Finance of the Republic of Kazakhstan. (2025). *Cryptocurrencies under control: How Kazakhstan regulates digital mining*. Retrieved from https://www.gov.kz/memleket/entities/kgd/press/news/details/963148.
[55] Volten, C., van Eeten, M., & van Wegberg, R. (2025). Money for nothing, supervision for a fee: Investigating the effects of the 5th anti-money laundering directive on cryptocurrency exchanges in the Netherlands. *European Journal on Criminal Policy and Research*. doi: 10.1007/s10610-025-09640-1.
[56] Zhanabilova, A.B. (2024). Legal regulation of the turnover of digital assets in the Republic of Kazakhstan and the possibility of their inheritance. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 3(78), 124-133. doi: 10.52026/2788-5291_2024_78_3_124.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.7

Article's History:
Received: 04.08.2025; Revised: 11.11.2025; Accepted: 16.12.2025

Legal and social consequences of the use of death penalty in China and Iran: A comparative analysis

Yerzhan Bimoldanov*
Deputy Head
Almaty Academy of MIA of the RK named after M. Yesbulatov
050060, 29 Utepova Str., Almaty, Kazakhstan
https://orcid.org/0009-0005-5247-1087

Abstract. The aim of this article was to conduct a comparative assessment of the impact of the use of death penalty in China and Iran on the legal system and social sphere. The study used a special legal method to analyse the normative consolidation of the death penalty, a comparative legal analysis to compare the institutional models of China and Iran, and a case study method to identify social selectivity and its impact on public perception of criminal justice. It has been established that in China, the death penalty was legally enshrined as a type of criminal punishment and was applied exclusively for "extremely serious crimes," the list of which was specified in the Special Part, in particular, intentional crimes against life, crimes against state security, generally dangerous acts, and certain corruption crimes on an especially large scale. It has been found that the Chinese model was specific in that it has two forms of death penalty (immediate execution and a two-year reprieve), as well as mandatory centralised review of all death sentences by the Supreme People's Court of the People's Republic of China, which limits the discretion of lower courts. It has been established that in Iran, the criterion of the seriousness of the crime was not formulated through a single category, but was determined by the offence's classification under the qisas, hadd or tazir regimes, which results in different legal grounds and mechanisms for the implementation of the death penalty. An analysis of judicial review materials for 2022-2023 showed a systematic change of death sentences to death with a two-year reprieve or life imprisonment, which indicates the real impact of centralised control on the restriction of judicial discretion. In Iran, on the contrary, a decentralised and regime-fragmented institutional model has been identified, in which final decisions on the execution of the death penalty were made by different courts depending on the regime of responsibility (qisas, hadd, tazir) without a single national review mechanism. It has been found that the centralised review of death sentences in China increases the legitimacy of justice, but does not eliminate the social selectivity of the application of this sanction. It was concluded that in both states, the death penalty was being transformed from an instrument of justice to a mechanism of social control. The results obtained can be used to develop more transparent standards of judicial control and to formulate criminal policy aimed at reducing social selectivity

Keywords: criminal punishment; extremely serious crimes; life imprisonment; regime of responsibility; trust in justice

Introduction

The use of the death penalty continues to remain a component of criminal law policy in a number of states, including China and Iran, which necessitates scholarly analysis of its legal and social consequences. The relevance of this study was determined by the combination of two circumstances: the retention of the death penalty as an instrument of state coercion and the active development of international human rights standards aimed at restricting or abolishing this form of punishment. In such conditions, there arises a need to determine how the death penalty affects the legal system, judicial practice, and social processes in states with different legal traditions and models of governance.

In academic discourse, the issue of the death penalty was mainly considered through the prism of normative

Suggest Citation:
Bimoldanov, Ye. (2025). Legal and social consequences of the use of death penalty in China and Iran: A comparative analysis. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 90-100.

*Corresponding author

admissibility, comparative criminal law and social justice, but the social consequences of its application remain fragmentarily understood. A study by M.F. Anwar (2024), devoted to a comparative analysis of the preservation of the death penalty in China and Pakistan, showed that the legal arguments in favour of this sanction were based on political and ideological factors rather than empirically proven effectiveness. The author concluded that the death penalty in these legal systems functions as an instrument of state sovereignty, while its impact on trust in justice and perceptions of social equality was ignored. The moral and legal dimensions of the death penalty were explored in the work of D. Choong En Jie *et al*. (2023), which finds that even in legal systems where the death penalty was formally recognised as permissible, its legitimacy remains conditional and dependent on the perception of procedural fairness. The authors show that public acceptance of the death penalty declines when there were doubts about the equality of the parties and the transparency of the judicial process. The problem of selectivity in the application of the death penalty was explored in a systematic review by A.T. Cobb *et al.* (2024), which found a correlation between the racial, age and gender characteristics of defendants and the likelihood of receiving a death sentence. The researchers concluded that the death penalty reproduces structural social inequalities, undermining the principle of equality before the law. The Iranian model of criminal justice was analysed in a study by D. Dyke & H. Enayat (2025), which shows that the use of the death penalty was closely linked to the ideological nature of the judiciary and personalised decision-making practices. The authors prove that death sentences were used not only as a legal remedy but also as an instrument of political security. The political dimension of the use of the death penalty in Iran was revealed in the work of B. Egan (2023), which found that foreign citizens were disproportionately often the subject of death sentences in cases related to security narratives. The author showed that the death penalty in such cases performs a symbolic function of state control.

A separate area of research was devoted to the influence of the individual characteristics of defendants on the imposition of the death penalty. S.J. Fogel *et al*. (2024) found that taking into account adverse childhood experiences reduces the likelihood of imposing the death penalty on young offenders. The results indicate that humanising factors may mitigate the severity of the sanction; however, their influence was fragmentary and depends on the court's willingness to integrate socio-psychological arguments into legal evaluation. A subsequent study by M.D. Smith *et al*. (2025) showed that, in practice, judicial decisions in death penalty cases were formed not only with regard to formally recognised mitigating or aggravating circumstances. The authors proved that even factors that were not enshrined in law or were officially rejected during the trial actually influence the final choice of punishment. This result highlights the structural unpredictability and selectivity of the application of the death penalty, which directly affects its perception as an instrument of fair justice.

The social perception of capital punishment in China has been analysed by J.Z. Liu (2021), who demonstrated that support for this sanction was higher among political and administrative elites than among the general population. This indicates a persistent gap between official criminal policy discourse and public sentiment. Research by T. Smith & D. Pascoe (2022) has shown that the institution of suspended death penalty transforms it into a form of conditional social control. The authors found that postponing the execution of a sentence reduces the level of international criticism while maintaining the disciplinary effect of the sanction.

An analysis of contemporary studies on the death penalty reveals several underdeveloped topics, including the impact of this sanction on social structures, institutional processes, and mechanisms for building public trust in justice. The field of research was limited in its comparative scope, as the interaction between democratic and authoritarian regimes has been studied unevenly, and empirical data was mainly focused on Western countries. Individual and contextual factors influencing the imposition of the death penalty were also insufficiently researched. The problem lies in the limited comparative assessment of death penalty practices in China and Iran, especially with regard to their impact on the principles of legality, legal certainty, trust in the judicial system, and social stability. The aim of this article was to assess the legal and social consequences of the use of the death penalty in China and Iran based on a comparative analysis of the legal framework, judicial practice and social effects. To achieve this aim, the article addresses the following objectives: analyse the legal foundations of the death penalty in China and Iran; to examine the practices of imposing and carrying out death sentences; and to evaluate the social consequences of the death penalty and conduct their comparative analysis.

Materials and Methods

The study of the legal and social consequences of the use of the death penalty in China and Iran covered the period from 2007 to 2025, due to key institutional changes in the mechanisms for imposing and reviewing death sentences. The choice of the initial time frame was related to the fact that in 2007, the Supreme Peoples Court of the People's Republic of China (SPC PRC) (n.d.) restored its exclusive jurisdiction to confirm or overturn death sentences, which fundamentally transformed the model of judicial control and the practice of applying this sanction. The geographical boundaries of the study were defined as the People's Republic of China and the Islamic Republic of Iran, which was justified by the preservation of the death penalty in both states, combined with fundamentally different institutional models for its imposition and review. The choice of these countries was determined by the possibility of conducting a comparative analysis of centralised (China) and fragmented (Iran) systems of judicial review, as well as identifying

differences in the social consequences of the application of the death penalty.

A special legal method was used to analyse the normative consolidation of the death penalty in the criminal legislation of China and Iran, as well as to identify the legal constructs that determine the grounds, conditions and limits of its application. The materials used to implement this method were the Criminal Law of the People's Republic of China (2020) and the Islamic Penal Code (2013), the provisions of which were analysed in conjunction with the relevant norms of criminal procedure law and official judicial interpretations.

Comparative legal analysis was used to systematically compare the key elements of the legal regulation of the death penalty in China and Iran. Within the first analytical block, the comparison was made on the basis of substantive parameters that determine the grounds for the application of the death penalty, including methods of legal specification of the category of seriousness of offences, the scope and nature of social relations protected by the possibility of imposing the death penalty, as well as techniques for the normative formalisation of its exceptionality. The second block was devoted to comparing institutional and procedural mechanisms and covered models of control over the imposition of death sentences, the competence of courts of various instances, the role of the highest judicial authorities, and the nature of appellate review. The norms of the analytical materials from The Dui Hua Foundation (2023; 2024) on the correction of death sentences in 2022-2023 served as materials for analysing China's institutional model. To assess the scale and conditions of the use of the death penalty in China, summary data and human rights assessments by Amnesty International (2024) were also used.

The comparative analysis of Iran's institutional architecture was based on the provisions of the Islamic Penal Code (2013), which define the composition of criminal offences and the limits of the application of the death penalty. Certain aspects of the practice of imposing and carrying out death sentences were clarified on the basis of materials from the annual reports of Iran Human Rights & ECPM (2023; 2024). General conclusions regarding the fragmentary and variable application of this sanction were specified taking into account the special reports of the United Nations Human Rights Council (2024).

The case study method was used to analyse individual court decisions illustrating the practice of applying the death penalty to socially and politically vulnerable groups of the population, as well as to identify the mechanisms of social selectivity of this sanction. Cases were selected based on the following criteria: the availability of confirmed information regarding the imposition or execution of the death penalty; the availability of official or independently verified materials regarding the course of the case, the trial and the subsequent review of the sentence; the representativeness of the case for identifying characteristic features of judicial practice, rather than isolated exceptional events. The application of this method was aimed at clarifying how specific judicial practices influence public perceptions of the fairness of criminal justice and transform the death penalty from a formally neutral sanction into an instrument of social control.

The results of the study were limited by the availability of open statistical data on the use of the death penalty in China and Iran, which made it impossible to fully quantify the extent of its use. In addition, the comparative analysis covered only two countries, which allowed for an in-depth study of their institutional and social differences, but did not envisage the universalisation of the conclusions for all legal systems in which the death penalty was retained.

Results

Legal basis for the application of the death penalty in China and Iran

The normative regulation of the death penalty in China and Iran operates within different models of criminal law, which leads to distinct approaches to defining its legal status and mechanisms of application. In China, the death penalty was directly established in the Criminal Law of the People's Republic of China (2020) as one of the forms of criminal punishment. The legislator includes it in the general list of sanctions alongside life imprisonment and fixed-term imprisonment, which indicates its institutional integration into the system of criminal penalties rather than its existence outside it. A distinctive feature of the Chinese model was the existence of two forms of death sentence: immediate execution and the death penalty with a two-year reprieve. The suspended death sentence has independent normative regulation and provides for the possibility of automatic commutation to life imprisonment or fixed-term imprisonment if no new serious offences were committed during the reprieve period. This structure creates an intermediate level of sanctions between the death penalty and life imprisonment and at the same time performs the function of reducing the number of actual executions. In the academic literature, this mechanism was regarded as a way of combining the severity of criminal repression with the manageability of its application (Xiong *et al*., 2022; Bessler, 2022). At the same time, the Special Part of the Criminal Law of the People's Republic of China (2020) provides that the death penalty was applied only for "extremely serious crimes," thereby normatively limiting the scope of its admissibility. The concept of "extremely serious crimes" was not defined through a universal definition but was specified through a list of offences whose sanctions allow for the death penalty. This category includes intentional crimes against life and physical integrity, such as intentional homicide, causing death under aggravating circumstances, and certain forms of violent offences if they result in death or mass casualties. In such cases, the criterion of "extreme seriousness" was linked to the irreversibility of the consequences and the level of harm caused. A separate group consists of crimes against state security and the constitutional order, including acts against sovereignty, territorial integrity, and state authority. In these offences, "extreme

seriousness" was determined not by individual harm to specific persons but by the potential or actual impact on the stability of the state system and the functioning of the political order. The category of extremely serious crimes also includes certain offences of general danger, such as terrorist acts, explosions, arson, or other actions that create a mass threat to life and public safety. In this context, the decisive factor was not only the actual result but also the scale of potential harm, which corresponds to the preventive logic of criminal legislation. Within the category of extremely serious crimes, economic offences were also singled out, for which Chinese criminal law formally provides the possibility of the death penalty while limiting its application through special conditions. This primarily concerns corruption offences committed on an especially large scale or under legally defined aggravating circumstances. In such cases, the criterion of "extreme seriousness" was linked to the scale of harm to state interests and the functioning of the public administration system, rather than to the presence of physical violence against a person.

An additional structural element of the legal status of the death penalty in China was centralised judicial review over its application. All death sentences were subject to mandatory review by the Supreme People's Court of the People's Republic of China, which creates a separate institutional level for verifying the legality and justification of this form of punishment. This mechanism unifies the practice of applying the death penalty at the national level and reduces the variability of decisions by lower courts, limiting their discretion in matters of legal qualification and sentencing. As a result, the death penalty in the Chinese legal system retains the status of a primary form of criminal punishment; however, its application was simultaneously constrained by a combination of substantive criteria concerning the severity of the offence and procedural mechanisms of multi-level judicial review. It was precisely this combination of normative narrowing of the range of eligible offences and centralised institutional oversight that forms the specific model of the "managed exceptionalism" of the death penalty in China, distinguishing it from approaches established in other legal systems.

In contrast to the Chinese model, where the criterion of "extreme seriousness" was formed through a normatively defined set of offences, in Iran the legal assessment of the seriousness of an act that allows for the death penalty was based on the classification of the offence within one of the basic regimes of criminal liability established in the Islamic Penal Code (2013). The Code does not employ a single universal category of "especially" or "extremely" serious crimes; instead, it differentiates legal consequences through the systems of qisas, hadd, and ta'zir, each of which establishes its own grounds, conditions, and limits for the application of the death penalty. Within the qisas regime, the criterion of seriousness was linked to an intentional encroachment on life, which was regarded as a legally sufficient basis for the most severe legal consequence. In this case, the death penalty functions not as a sanction within a general scale of punishments, but as a normatively defined outcome of intentional homicide. At the same time, the implementation mechanism of qisas was structurally combined with legal possibilities for suspending the execution of the death sentence, particularly through forgiveness by the victim's family or substitution with financial compensation (diya). This alters the procedural trajectory of the case but does not eliminate the initial legal assessment of the act as reaching the highest level of seriousness. The hadd regime constructs the criterion of seriousness differently, as it provides fixed punishments directly prescribed in the Code for a defined range of offences. In this context, the death penalty was applied to acts that the legislator classifies as having heightened normative significance for the protection of religious-legal and public order. Seriousness here was determined not by an individualised assessment of harm, but by the very fact that the act belongs to the hudud category, for which the Code prescribes a death outcome if the evidentiary requirements were met. Within the ta'zir regime, the criterion of seriousness takes on a criminal-policy character, as it concerns acts for which punishment was determined by the legislator within the scope of state discretion. It was precisely in this category that a significant proportion of death sentences was concentrated, particularly for drug-related offences and other acts defined by the legislator as posing a threat to public security or social order. In such cases, severity was linked neither to an attack on a specific life nor to a fixed religious-legal sanction, but was justified by the scale of the threat as defined at the level of criminal policy. A synthesis of these differences makes it possible to systematically compare the approaches of China and Iran to defining the "seriousness" of offences for which the death penalty was permitted, according to key parameters (Table 1).

Table 1. Comparison of the criteria for determining the "seriousness" of crimes permitting the application of the death penalty in China and Iran

Comparison parameter	China	Iran
Method of legal specification of seriousness	"Extreme seriousness" was specified through the list of offence types in the Special Part of the Criminal Law, the sanctions of which expressly permit the imposition of the death penalty. The criterion of seriousness was materialised at the level of the legislative qualification of specific offence types.	"Seriousness" was primarily encoded through the classification of the offence under one of the regimes of criminal liability (qisas, hadd, ta'zir). Specific offence types have a derivative significance within the relevant regime.

Continued Table 1

Comparison parameter	China	Iran
Protected legal interest determining the applicability of the death penalty	The criterion of seriousness was formed through the combination of several blocks: intentional offences against life; generally dangerous acts threatening public safety; crimes against state security; and certain economic offences, where they cause significant harm to state interests or public administration.	The threshold of seriousness was differentiated by regimes: qisas – intentional deprivation of life; hadd – acts with fixed consequences defined by the code; ta'zir – acts recognised by the legislator as creating a substantial threat to public order or security, including drug offences.
Model of the "exceptional" nature of the death penalty as a legal technique	The exceptional nature was structured through the normative formula "only for extremely serious crimes", combined with the institution of a two-year reprieve from execution and the mandatory centralised review of death sentences by the Supreme People's Court of the People's Republic of China, which reduces variability in practice.	There was no single universal formula of exceptionalism. Different regimes (qisas, hadd, ta'zir) have autonomous grounds for the application of the death penalty, distinct procedural trajectories, and different mechanisms influencing the execution of the sentence, which complicates the unification of the substantive criterion of seriousness.
Offence types whose sanctions permit the death penalty	Intentional murder; terrorist activity; arson, explosion, or other generally dangerous acts causing grave consequences; rape under aggravating circumstances; large-scale drug trafficking; corruption offences involving "especially serious consequences"; treason.	Intentional murder; rape; armed robbery; spreading corruption; repeated alcohol consumption; large-scale drug trafficking.

Source: compiled by the author based on Islamic Penal Code (2013), Criminal Law of the People's Republic of China (2020)

The comparative analysis demonstrated that the criteria for determining the "seriousness" of crimes permitting the application of the death penalty in China and Iran were formed on different normative and institutional foundations. In the Chinese model, the seriousness of the offence was determined by a legally defined range of offence types, with the subsequent restriction of the death penalty by substantive and procedural filters, including centralised judicial control. In the Iranian model, seriousness was differentiated depending on the legal regime of liability, which results in multiple grounds, procedural trajectories, and mechanisms for implementing the death sentence. These differences were not only doctrinal but also practical in significance, as they directly affect the scale, selectivity, and public perception of the application of the death penalty. This necessitates further analysis of the social consequences and actual practices of applying the death penalty in both states, which will make it possible to assess how different legal constructions were transformed into specific social effects.

Practices of imposing and carrying out the death penalty: institutional and procedural aspects

The institutional architecture of the bodies involved in imposing the death penalty in China was structured according to the principle of strict centralised judicial control, which structurally distinguishes it from most legal systems in which the death penalty was retained. Criminal cases in which the death penalty may potentially be imposed were heard by intermediate people's courts or higher people's courts, but their competence was limited to issuing the initial sentence without a final decision on the execution of the death penalty. Thus, courts of first instance effectively perform the function of primary case selection but were not the final authority in sanctioning a death sentence. The key element of the institutional model was the mandatory review of all death sentences by the Supreme People's Court of the People's Republic of China (n.d.), which, after 2007, restored its exclusive competence to confirm or overturn such sentences. This review was not merely formal and includes a repeated assessment of the evidentiary basis, the correctness of the legal qualification of the act, compliance of the sentence with the criterion of "extreme seriousness", and the proportionality of applying the death penalty.

Empirical data confirm the practical significance of this centralised level of control. In particular, an analysis of judicial review materials published in 2022-2023 indicates systematic correction of death sentences at the level of the SPC PRC, including the commutation of the death penalty to death with a two-year reprieve or life imprisonment. Such decisions were recorded in independent analytical studies, including reports by the non-governmental organisation The Dui Hua Foundation (2024), which monitors the activity of the SPC PRC as the sole institutional centre for sanctioning death sentences. Additionally, according to Amnesty International (2024), China continues to remain the state with the largest number of executions in the world, although official statistics were not disclosed and the actual number of executions was only estimated. It was in this context that the institutional role of the SPC PRC becomes crucial, as centralised review was regarded as the primary mechanism for restraining and unifying the practice of applying the death penalty under conditions of limited transparency.

Centralised review transforms the boundaries of judicial discretion. Lower-level judges formally retain the authority to establish the factual circumstances and choose the type of punishment, but their decisions are, a priori, oriented towards the expected position of the SPC PRC. As a result, discretion acquires an indirect character and operates within established standards formed at the level of the higher judicial instance, which reduces regional variability and contributes to the formation of a unified practice of applying the death penalty. The participation of other state bodies, in particular the prosecution, in the Chinese model has an auxiliary and supervisory character and does not influence the final decision on the execution of the death

sentence. Thus, China's institutional model concentrates decisive competence within the judicial system itself, minimising extrajudicial channels of influence on the outcome.

The institutional architecture of death penalty in Iran has a different logic and was characterised by the fragmentation of judicial powers. Criminal cases in which the death penalty may be imposed were heard by different courts depending on the nature of the offence and the legal regime of liability enshrined in the Islamic Penal Code (2013). Revolutionary courts, general criminal courts and specialised judicial bodies have autonomous jurisdiction to impose death sentences within their respective categories of cases, which creates a multiplicity of institutional trajectories for the imposition of this type of punishment. Unlike the Chinese model, Iran does not have a single centralised judicial body that would carry out mandatory review of all death sentences according to uniform standards. Appeals and cassation reviews were carried out depending on the legal regime of the case (qisas, hadd or ta'zir), which results in varying degrees of control and different procedural routes. This institutional heterogeneity was confirmed by the materials of special reports by Iran Human Rights & ECPM (2023; 2024), which note that death sentences in Iran can become final at different levels of the judiciary without a single mechanism for centralised unification of practice.

Empirical court cases analysed in the reports of the United Nations (UN) Special Rapporteur on Human Rights in Iran (United Nations Human Rights Council, 2024) show that under the ta'zir regime, particularly in cases involving drug-related crimes, the final decision to carry out the death penalty was made by the courts without further automatic review at the national level. This means that institutional control was limited to the procedural framework of a particular regime, and the limits of judicial discretion depend on the type of court and category of case, rather than on a centralised standard. Thus, the institutional practice of imposing and carrying out the death penalty in Iran confirms the absence of a single centre for the final authorisation of death sentences. Unlike China's centralised model, the Iranian system was characterised by a multiplicity of judicial and extrajudicial channels for final decision-making, which leads to increased variability in practice and varying degrees of actual judicial discretion depending on the legal regime of the case. Combined with the previously analysed features of China's centralised model, this provides grounds for a systematic comparison of the institutional and procedural parameters of the imposition of the death penalty in both countries (Table 2).

Table 2. Institutional and procedural architecture of the imposition of the death penalty in China and Iran

Comparison criterion	China	Iran
General model of institutional control	A strictly centralised model with the concentration of the final decision at the level of the SPC PRC.	A decentralised, regime-fragmented model without a single centre for final sanctioning.
Courts of first instance	Intermediate or higher people's courts deliver the initial sentence without authority over the final execution of the death penalty.	Revolutionary, general criminal, and specialised courts impose death sentences within their autonomous competences.
Role of the higher court	The SPC PRC conducts a mandatory review of all death sentences and holds exclusive competence to confirm or alter them.	There was no single body for mandatory centralised review; appellate and cassation control depends on the regime of the case.
Nature of the review of the death sentence	Reassessment of evidence, legal classification, compliance with the criterion of "extreme seriousness", and proportionality of the punishment.	The scope of review varies according to the regime (qisas, hadd, ta'zir) and was not governed by a unified standard.

Source: compiled by the author based on Islamic Penal Code (2013), Criminal Law of the People's Republic of China (2020)

The summary presented in Table 2 demonstrates a fundamental difference in the institutional logic of imposing the death penalty in China and Iran. In the Chinese model, the final sanctioning of a death sentence was concentrated at the level of a single supreme judicial instance, combining the functions of legal control, unification of practice, and correction of judicial discretion. By contrast, the Iranian model was characterised by the distribution of powers among different courts and legal regimes, as well as the involvement of extrajudicial actors, which prevents the formation of a single institutional standard for the final decision. Thus, the difference between centralised and decentralised architectures determines not only the process of imposing the death penalty but also the degree of predictability and consistency in judicial practice.

The identified institutional and procedural differences were significant not only at the level of the formal organisation of the judiciary, but also for understanding the broader social consequences of the death penalty. It was precisely the nature of judicial control, the limits of discretion, and the presence or absence of a centralised review mechanism that shape public perceptions of the death penalty, the level of trust in criminal justice, and the actual practices of carrying out sentences. This necessitates further analysis of the social effects of the death penalty and the particularities of its practical implementation in China and Iran.

Social consequences of the use of the death penalty and their comparative assessment

The death penalty, in its social dimension, was not a neutral criminal sanction. Its retention in legislation shapes the perception of the state as an actor that reserves for itself the right to the most extreme and irreversible form of coercion. In public consciousness, such a sanction reinforces the image of criminal justice as a maximally punitive mechanism intended to respond to actions regarded as threats to the

basic social order. The very existence of the death penalty strengthens the association of state authority with coercive force, even in conditions of limited or closed statistics regarding its application (Cheeseman, 2017; May *et al*., 2025).

In public consciousness, the death penalty combines several normative ideas that were not internally consistent. It was simultaneously associated with justice as retribution, with the provision of collective security, and with the demonstration of the sovereign power of the state. This combination forms a particular model of legitimising criminal justice, in which the severity of the sanction was perceived as an indicator of the determination and effectiveness of state control. Comparative criminal policy studies show that in states where the death penalty was retained, public support for the justice system was based not on trust in procedures, but on expectations of a harsh response to deviant behaviour (Condon, 2020). The absence of statistical transparency does not reduce the social impact of the death penalty. On the contrary, limited access to official data, characteristic of China and Iran, reinforces its symbolic role, as the sanction functions as an abstract threat rather than an accountable instrument of criminal policy. According to Amnesty International (2024), the uncertainty surrounding the scale of the application of the death penalty contributes to the perception of its pervasive presence within the system of social control.

The death penalty affects trust in the judicial system because it shifts questions of the quality of justice into the sphere of irreversible consequences. Under such conditions, any judicial error, procedural defect, or lack of transparency in decision-making acquires not only legal but also social resonance. Academic research emphasises that in states retaining the death penalty, the level of public sensitivity to standards of proof and reasoning in judgments was higher than in jurisdictions where alternative sanctions were applied (Bullock, 2021). The model of reviewing death sentences plays a decisive role in shaping perceptions of the legitimacy of justice. A centralised mechanism for final sanctioning, as in China, enables the state institutionally to limit arbitrariness and to project the image of controlled application of the ultimate sanction. Analytical studies of judicial practice confirm that such a model contributes to the perception of the death penalty as an exceptional measure subject to especially strict control (The Dui Hua Foundation, 2024). By contrast, the fragmented system of final decision-making characteristic of Iran produces a different social perception. The absence of a single centre for final review reinforces perceptions of selectivity and unpredictability in law enforcement. This reduces trust in the judiciary and transforms the death penalty from an instrument of justice into a means of repressive control. Such conclusions were consistently recorded in the reports of the United Nations Human Rights Council (2024) and Iran Human Rights & ECPM (2023; 2024).

In the system of social control, the death penalty serves to establish a normative hierarchy of prohibitions rather than as an instrumental means of deterring crime. Its presence in criminal law structures the legal space according to the principle of extremity, highlighting a range of acts that the state considers incompatible with the foundations of social order. In this sense, the death penalty serves not as a means of responding to individual criminal behaviour, but as a mechanism for establishing a symbolic boundary of what was permissible, which has a preventive effect on society as a whole. Unlike traditional sanctions, its disciplinary potential was realised beyond the scope of specific law enforcement. The death penalty influences behavioural expectations by forming an idea of the extreme form of state intervention, which remains permanently possible, even if it was applied selectively or irregularly. It was this potential, rather than the frequency of executions, that ensures its role as an instrument of social control based on the preventive symbolisation of threat (Stetler *et al*., 2022). At the same time, in conditions of limited transparency of criminal statistics, social control associated with the death penalty was intensified. Uncertainty about the scope and criteria for its application transforms the sanction from a specific punitive measure into an abstract instrument of discipline, the limits of which remain blurred for society. This effect was characteristic of legal systems in which the death penalty functions in conjunction with a high level of state discretion and limited access to official information (Amnesty International, 2024).

The social selectivity of the application of the death penalty was evident from an analysis of specific court decisions in which the extreme sanction was in fact concentrated on socially and politically vulnerable groups. It was precisely such cases that allow to trace how the death penalty loses its universal character as a legal response and acquires the characteristics of an instrument of structural control. A case analysed by The Dui Hua Foundation (2023) was illustrative in this context. It concerned the sentencing to death (later commuted to death with a two-year reprieve) of a rural migrant accused of murder during a domestic dispute. The case was characterised by the absence of premeditation and the presence of mitigating circumstances, but the court of first instance imposed the death penalty, citing the "serious public danger" of the act. Only at the review stage did the Supreme People's Court of the People's Republic of China (n.d.) commute the sentence. The analytical value of this case lies in the fact that crimes of similar severity committed by persons with higher social status or in complex economic contexts were much less likely to result in the death penalty at the first instance. In public perception, this practice reinforces the idea that the ultimate sanction was applied primarily to socially marginalised individuals, while centralised review performs a compensatory function of selectivity.

Social selectivity can also be seen in Iranian practice, particularly in drug-related cases. The report of the United Nations Human Rights Council (2024) analyses the case of a young man from the Baloch ethnic minority who was sentenced to death for transporting narcotic substances under the tazir regime. The facts of the case indicated a low

level of procedural guarantees, limited access to a lawyer, and the absence of automatic review of the sentence at the national level. The sentence became final after a formal appeal hearing, without the application of a unified standard for assessing the proportionality of the punishment. According to Iran Human Rights & ECPM (2023; 2024), such cases account for a significant proportion of death sentences carried out in Iran, disproportionately affecting poor and ethnically marginalised groups.

Thus, the social consequences of the use of the death penalty in China and Iran go beyond purely criminal law regulation and were determined by a combination of symbolic, institutional and socio-selective dimensions. From a comparative perspective, the death penalty appears not as a universal instrument of justice, but as an element of social control, the effectiveness and perception of which depend on the model of judicial review, the level of transparency and the structure of social inequality. Centralised control in China partially mitigates the social risks associated with extreme punishment, but does not eliminate its selective nature, while the fragmentation of the Iranian system exacerbates the repressive effect and undermines confidence in the principle of equality before the law. As a result, the death penalty in both legal systems functions primarily as an indicator of the nature of the relationship between the state and society, reflecting not only criminal policy but also the underlying mechanisms of legitimising power and maintaining social order.

Discussion

The conclusions obtained in the study partially correlate with the results presented by S.S. Silvee & X. Wu (2021), who, in a comparative analysis of India and Bangladesh, showed that the key factor in the application of the death penalty was not the abstract "seriousness" of the crime, but the way it was normatively specified within the national legal system. The authors concluded that the formal existence of the death penalty in legislation does not mean that it has the same legal status, as institutional mechanisms and procedural restrictions were of decisive importance. A similar approach can be seen in the results of this study on China, where the death penalty was normatively integrated into the system of punishments, but its application was limited by a legally defined range of offences and centralised judicial control. At the same time, unlike the conclusions of S.S. Silvee & X. Wu, where colonial legal heritage plays a key role, in the case of China and Iran, the decisive factor was the difference between the codified state model and the regime-differentiated system of criminal responsibility.

The results of the analysis of the Chinese model of capital punishment were consistent with the conclusions of T. Smith *et al.* (2022), who analysed institutional changes in the field of capital punishment during Xi Jinpings reign. The authors found that the reduction in the actual use of the death penalty was not achieved through a formal review of sanctions, but through tighter procedural controls and restrictions on public discourse on this institution. This study also found that the key limiting factor in China was not a change in the normative status of the death penalty, but a combination of criteria of "extreme seriousness" with mandatory review of death sentences by the Supreme People's Court. However, unlike T. Smith *et al.*, who focused primarily on political and discursive dimensions, this study emphasises the structural and legal mechanisms that shape the model of institutionally controlled exceptionality of the death penalty.

The conclusions regarding Iran partially overlap with the results obtained by I. Wahyudi (2024), who studied the death penalty from the perspective of its criminological effectiveness and impact on crime rates. The author concluded that the severity of sanctions alone does not reduce crime, and that its impact depends on the context of legal regulation and social perception. This study found that in Iran, the criterion of the severity of a crime was not formed as a single material standard, but was determined by the act's belonging to the qisas, hadd or ta'zir regimes. Unlike I. Wahyudi, who focused on criminological indicators, this study shows that it was the normative differentiation of criminal liability regimes that determines the variability of the practice of applying the death penalty, regardless of the declared preventive goals.

The results obtained regarding the institutional and procedural organisation of the imposition of the death penalty were partly consistent with the conclusions of K.M. Barry (2019), who analysed the death penalty through the prism of the fundamental right to life. His study emphasised that the key risk from a human rights perspective was not only the very fact of maintaining the death penalty, but also the institutional structure of the final decision-making process, in particular the concentration or dispersion of powers. The results of this study confirmed this thesis, showing that China's centralised model provides a higher level of unification and procedural control compared to Iran's decentralised model. At the same time, unlike K.M. Barry's norm-oriented analysis, this study demonstrated that even under conditions of limited transparency, centralised judicial control serves as an effective deterrent to the use of the death penalty.

The findings of this study were also conceptually related to the work of M. Matić Bošković & I.L. Gal (2021), which analysed the relationship between the right to life, the prohibition of the death penalty, and standards for the enforcement of life imprisonment. The authors concluded that institutional guarantees and procedural mechanisms determine the actual level of protection of the right to life, even in states where the death penalty was not formally applied. The results of this study expanded on this approach, showing that in legal systems where the death penalty was retained, the nature of the institutional architecture for reviewing sentences, or its absence, was of decisive importance. Thus, it was established that the formal presence or absence of the death penalty was less indicative than the mechanisms for controlling its imposition.

Some of the study's findings were consistent with the conclusions of R.M.S. Naseem *et al.* (2025), who examined the reform of the death penalty from a constitutional and political-legal perspective. In their work, the authors emphasised that a key indicator of a state's readiness for reform was not only a reduction in the number of death sentences, but also a transformation of the procedures for their imposition and review. The results of the current study confirmed this position, establishing that in China, the institutional concentration of powers in the SPC PRC reduces the variability of judicial practice, while in Iran, the absence of a single mechanism for final review complicates the implementation of systemic reforms. At the same time, unlike the general theoretical models proposed by these authors, this study specified how these processes were implemented at the level of individual judicial regimes and practical cases.

The results obtained were consistent with the conclusions of A. Arifullah (2024), who conducted a legal analysis of the death penalty from a human rights perspective and emphasised its systemic impact on public perception of state power. His study showed that the death penalty shapes the perception of the state as an entity legitimised to use extreme coercion, regardless of the frequency of actual executions. The results of the current study confirm this approach, demonstrating that even in conditions of limited statistical transparency, the death penalty retains its high symbolic and disciplinary potential. At the same time, unlike the predominantly normative analysis of A. Arifullah, this study specifies this influence through institutional models of judicial control and their connection with the social selectivity of the application of extreme sanctions.

The conclusions of this section were also conceptually consistent with the arguments of B. Jones (2023), who considered the death penalty through the prism of the right to life and the principle of necessity. The author concluded that the preservation of the death penalty undermines the legitimacy of criminal justice because it shifts the emphasis from procedural justice to the demonstrative severity of the sanction. The results of the current study confirm this thesis, showing that in countries with the death penalty, public support for justice was based on the expectation of a harsh response rather than on trust in procedural standards. At the same time, the comparative analysis complements B. Jones approach, demonstrating that centralised judicial control (as in China) can partially mitigate this effect, while fragmented models (as in Iran) reinforce the repressive perception of justice.

The findings of this study partly correlate with the results of P. Obiri-Korang (2022), who analysed the socio-legal consequences of retaining the death penalty in the context of national legislation reform. His work argued that the death penalty disproportionately affects socially vulnerable groups and reproduces structural inequality in the criminal justice system. The results obtained in the current study confirm this thesis based on data from China and Iran, where there was a concentration of death sentences for people with low socio-economic status and representatives of marginalised communities. However, unlike P. Obiri-Korang's focus on legislative and constitutional changes, this study shows that even without the formal abolition of the death penalty, institutional mechanisms for reviewing sentences influence social perceptions of justice and equality before the law. Thus, the results of this study not only confirmed certain provisions of contemporary doctrine regarding the role of institutional mechanisms in the field of capital punishment, but also clarified them through a comparative analysis of practices in China and Iran.

Conclusions

The study found that the legal basis for the application of the death penalty in China and Iran was based on fundamentally different models of criminal law regulation, which leads to differences in the definition of criteria for the seriousness of crimes and the mechanisms for implementing this type of punishment. In China, the death penalty was normatively integrated into the system of basic criminal penalties and was applied exclusively to a legally defined range of "extremely serious crimes," which includes crimes against life, state and public security, as well as certain economic crimes, with an additional restriction in the form of a two-year deferral of execution and mandatory centralised review of death sentences by the SPC PRC. In Iran, on the contrary, there was no single substantive criterion of seriousness, since the possibility of applying the death penalty was determined by the classification of the offence under the qisas, hadd or tazir regimes, which creates multiple legal grounds and procedural trajectories for the implementation of the death penalty. A comparative analysis has led to the conclusion that the Chinese model was characterised by a unified and institutionally controlled structure of "managed exceptionalism" of the death penalty, while the Iranian model was marked by normative differentiation of seriousness criteria depending on the legal regime of responsibility, which has a direct impact on the practice of its application.

It has been established that the death penalty in China and Iran performs not only a punitive but also a socio-symbolic function, shaping the perception of the state as an entity that reserves the right to extreme and irreversible coercion. Its presence in criminal law influences public perception of criminal justice, reinforcing the image of the state's most severe response to acts that were classified as a threat to the basic social order. It has been proven that even in conditions of limited or closed statistics, the death penalty retains a high social impact, as it functions as an abstract threat rather than an accountable instrument of criminal policy.

It has been determined that in the system of social control, the death penalty performs the function of normative hierarchisation of prohibitions, rather than instrumental deterrence of crime. Its disciplinary potential was realised primarily through the symbolisation of the ultimate limit of what was permissible, rather than through the actual

frequency of executions. It has been noted that in conditions of limited transparency of criminal statistics, the social effect of the death penalty was amplified, since the uncertainty of the scale of its application broadens the perception of its potential omnipresence in the system of state control.

A separate result of the study was the identification of social selectivity in the application of the death penalty. Analysis of court cases and reports from international organisations has shown that the ultimate sanction disproportionately affects socially and politically vulnerable groups, in particular people with low socio-economic status and representatives of ethnic minorities. In comparative terms, centralised review in China partially compensates for such selectivity, while in Iran the absence of a single mechanism of final control reinforces the repressive nature of the death penalty. As a result, the death penalty in both legal systems was an indicator of the nature of the relationship between the state and society, reflecting not only the peculiarities of criminal policy, but also the underlying mechanisms of legitimising power and maintaining social order. Prospects for further research related to the analysis of the relationship between institutional models of judicial control, the level of social trust in criminal justice, and long-term transformations of legal consciousness in states where the death penalty was retained.

Acknowledgements
None.

Funding
None.

Author Contributions
Y. Bimoldanov independently developed the research concept, conducted a literature review, and collected and analysed the data. The author carried out a comparative legal analysis of the institutional models of China and Iran, and prepared both the initial draft and the final version of the manuscript.

Conflict of Interest
None.

References
[1] Amnesty International. (2024). *Death sentences and executions in 2024*. Retrieved from https://www.amnesty.org/en/documents/act50/8976/2025/en/.
[2] Anwar, M.F. (2024). Retention of death penalty: A comparative analysis of China and Pakistan. *The Critical Review of Social Sciences Studies*, 2(2), 1657-1670. doi: 10.59075/rr4ex018.
[3] Arifullah, A. (2024). A juridical study of the death penalty from a human rights perspective. *Golden Ratio of Law and Social Policy Review*, 4(1), 1-11. doi: 10.52970/grlspr.v4i1.940.
[4] Barry, K.M. (2019). The death penalty & the fundamental right to life. *Boston College Law Review*, 60, article number 1545. doi: 10.2139/ssrn.3287213.
[5] Bessler, J. (2022). *The death penalty's denial of fundamental human rights: International law, state practice, and the emerging abolitionist norm*. Cambridge: Cambridge University Press. doi: 10.1017/9781108980159.
[6] Bullock, A. (2021). *The scope of the death penalty*. (Master's thesis, Concordia University, St. Paul).
[7] Cheeseman, C. (2017). The death penalty as addressed by regional and international human rights bodies: Exploring jurisprudential cross-fertilisation and harmonisation. In C. Buckley, A. Donald & P. Leach (Eds.), *Towards convergence in international human rights law: Approaches of regional and international systems* (pp. 68-102). Leiden: Brill Nijhoff. doi: 10.1163/9789004284258_004.
[8] Choong En Jie, D., Ngu Choung Chii, A., & Althabhawi, N.M. (2022). The moral and legal permissibility of the death penalty. *Current Law Journal: Legal Network Series (A)*, 1.
[9] Cobb, T.A., Stinson, J.D., & Sanders, C.L. (2024). Race, sex, and age disparities in death penalty sentencing: A systematic review. *Journal of Ethnicity in Criminal Justice*, 22(1), 45-65. doi: 10.1080/15377938.2024.2322931.
[10] Condon, J.-B. (2020). Denialism and the death penalty. *Washington University Law Review*, 97(5), 1397-1445.
[11] Criminal Law of the People's Republic of China. (2020, December). Retrieved from https://en.spp.gov.cn/2020-12/26/c_948417_2.htm.
[12] Dyke, D., & Enayat, H. (2025). The administration of criminal justice in Iran: Ideology, judicial personalism, and the cynical manipulation of security. In H. Enayat & M. Künkler (Eds.), *The rule of law in the Islamic Republic of Iran: Power, institutions, and the limits of reform* (pp. 66-103). Cambridge: Cambridge University Press. doi: 10.1017/9781108630603.003.
[13] Egan, B. (2023). *The politics of capital punishment for foreign nationals in Iran*. Oxford: Death Penalty Research Unit, University of Oxford.
[14] Fogel, S.J., Bjerregaard, B., Cochran, J.K., & Smith, M.D. (2024). Capital punishment trials of youthful offenders: The impact of ACEs mitigation. *Youth & Society*, 56(2), 300-326. doi: 10.1177/0044118X231165817.
[15] Iran Human Rights, & ECPM. (2024). *Annual report on the death penalty in Iran 2023*. Retrieved from https://iranhr.net/media/files/Iran_Human_Rights-Annual_Report_2023.pdf.
[16] Iran Human Rights, & ECPM. (2025). *Annual report on the death penalty in Iran 2024*. Retrieved from https://www.iranhr.net/media/files/Rapport_iran_2024-WEB.pdf.

[17] Islamic Penal Code. (2013, April). Retrieved from https://www.unodc.org/cld/uploads/res/islamic-penal-code_html/Islamic_Penal_Code.pdf.
[18] Jones, B. (2023). Death penalty abolition, the right to life, and necessity. *Human Rights Review*, 24(1), 77-95. doi: 10.1007/s12142-022-00677-x.
[19] Liu, J.Z. (2021). Public support for the death penalty in China: Less from the populace but more from elites. *The China Quarterly*, 246, 527-544. doi: 10.1017/S0305741020000739.
[20] Matić Bošković, M., & Gál, I.L. (2021). The right to life: Prohibition of death penalty and right to life in prison. In Z. Pavlović (Ed.), *Yearbook human rights protection: Right to life, No. 4* (pp. 165-178). Novi Sad; Belgrade: Provincial Protector of Citizens – Ombudsman; Institute of Criminological and Sociological Research.
[21] May, L.C., Ripper, B., & Johnson, R. (2025). The constitutionality of life under the credible threat of death by execution: The view from death row. *N.Y.U. Review of Law & Social Change*, 48(3), 353-392.
[22] Naseem, R.M.S., Sethi, A., & Hashmi, M.A.I. (2025). Reforming the death penalty: Constitutional, human rights, and policy dimensions. *Advance Social Science Archive Journal*, 4(2), 277-293. doi: 10.5281/zenodo.17284884.
[23] Obiri-Korang, P. (2022). Reconsidering the abolition of capital punishment in Ghana: The need for legislative and constitutional amendments. *Bratislava Law Review*, 6(1), 107-124. doi: 10.46282/blr.2022.6.1.284.
[24] Silvee, S.S., & Wu, X. (2021). Death penalty in South Asia: A comparative study between India and Bangladesh. *Journal of Asian and African Studies*, 56(3), 415-433. doi: 10.1177/0021909620926539.
[25] Smith, M.D., Murdock, A.M., Bjerregaard, B., & Fogel, S.J. (2025). Do changes of venue impact capital punishment sentencing? An empirical analysis. *Journal of Crime and Justice*, 1-18. doi: 10.1080/0735648X.2025.2581982.
[26] Smith, T., & Pascoe, D. (2022). Suspended execution beyond China's borders. *Asian Journal of Law and Society*, 9(1), 133-167. doi: 10.1017/als.2021.19.
[27] Smith, T., Robertson, M., & Trevaskes, S. (2022). (Not) talking about capital punishment in the Xi Jinping era. *International Journal for Crime, Justice and Social Democracy*, 11(3), 79-91. doi: 10.5204/ijcjsd.2478.
[28] Stetler, R., McLaughlin, M., & Cook, D. (2022). Mitigation works: Empirical evidence of highly aggravated cases where the death penalty was rejected at sentencing. *Hofstra Law Review*, 51(1), 89-141.
[29] Supreme People's Court of the People's Republic of China. (n.d.). Retrieved from https://english.court.gov.cn/.
[30] The Dui Hua Foundation. (2023). *2023 annual report: 25 years of advancing rights through dialogue*. Retrieved from https://duihua.org/wp-content/uploads/2024/11/duihua-annualreport2023.pdf.
[31] The Dui Hua Foundation. (2024). *Curious timing: SPC death penalty reviews posted after Universal Periodic Review (Part I)*. Retrieved from https://www.duihuahrjournal.org/2024/07/curious-timing-spc-death-penalty.html.
[32] United Nations Human Rights Council. (2024). *Situation of human rights in the Islamic Republic of Iran: Report of the special rapporteur on the situation of human rights in the Islamic Republic of Iran* (A/HRC/55/62). Retrieved from https://documents.un.org/doc/undoc/gen/g24/012/59/pdf/g2401259.pdf.
[33] Wahyudi, I. (2024). The impact of the application of the death penalty on reducing crime rates: Legal and criminological perspectives. *Golden Ratio of Data in Summary*, 4(2), 205-215. doi: 10.52970/grdis.v4i2.535.
[34] Xiong, M., Liu, S., & Liang, B. (2022). Death sentence review by the Supreme People's Court in China: Decision patterns and variations. *China Review*, 22(3), 137-166.

Asian Journal of Criminal Justice and Forensic Studies

Vol. 1, No. 1. 2025

Journal homepage: https://asianjustice.kz/

UDC 343.326:340.5

Article's History:
Received: 10.07.2025; Revised: 05.11.2025; Accepted: 16.12.2025

The concept of "Global Terrorism" and its implementation in the criminal legislation of Indonesia, the Philippines, and Malaysia

Nurlan Apakhaev*
PhD in Law, Professor
Q University
050026, 125 Bayzakov Str., Almaty, Kazakhstan
https://orcid.org/0000-0001-7795-2518

Abstract. The aim of the article was to determine the peculiarities and level of adaptation of international counter-terrorism standards in the criminal legislation of Indonesia, the Philippines, and Malaysia. The study was conducted within a qualitative-comparative legal design, employing the special-legal method, comparative legal analysis, and the case study method. The research established that the examined countries implement international counter-terrorism standards through different criminal law models: functional (Indonesia), hybrid (the Philippines), and preventive (Malaysia). It was found that in all three legal systems, criminal liability extends not only to completed terrorist acts but also to financing, recruitment, training, preparation, and participation in terrorist organisations without the need to prove a specific act of violence. Significant differences were identified in sanctioning policies: Indonesia provides for the death penalty, life imprisonment, or imprisonment from 20 years for the most serious terrorist acts, whereas in the Philippines and Malaysia, the maximum penalty is life imprisonment with an emphasis on preventive measures. It was determined that international counter-terrorism standards form not a unified definition but a "minimum core" of terrorism, which includes a violent act or the threat of its use, a special purpose of intimidation or coercion, and heightened public danger. The comparative analysis showed that Indonesia, the Philippines, and Malaysia formally implement this core; however, they utilise different legislative models: functional (Indonesia), hybrid with a link to underlying offences (the Philippines), and preventive with an emphasis on potential threat (Malaysia). It was revealed that the level of legal certainty is highest in the Philippine model and lowest in the Malaysian model, where the expansion of the definition through categories of national security creates tension with the principle of *nullum crimen sine lege certa*. The obtained results can be used by legislators and courts to adjust national anti-terrorism definitions and their application practices, with the aim of clearly delineating the boundaries of criminalisation, selecting adequate standards of proof, and preventing the excessive expansion of preventive powers

Keywords: international obligations; regional security mechanisms; violent act; public danger; preventive measures

Introduction

In the 21st century, terrorism has evolved into a transnational phenomenon that transcends the borders of individual states, acquires a networked character, and utilises global financial, informational, and migratory flows. In scientific and political-legal discourse, this has led to the formation of the concept of "global terrorism", which emphasises the supranational nature of the threats and the unification of approaches to the criminalisation of terrorist activities. At the same time, the implementation of this concept into national criminal law systems remains fragmented and dependent on the historical, religious, and security peculiarities of specific states. The countries of Southeast Asia, particularly Indonesia, the Philippines, and Malaysia, are in a zone of heightened risk of terrorist activity, which combines local separatist conflicts with the influence of global extremist ideologies. Their criminal legislations have undergone significant transformations under the influence of international obligations, regional security mechanisms, and the practice of counter-terrorism operations.

Suggest Citation:
Apakhaev, N. (2025). The concept of "Global Terrorism" and its implementation in the criminal legislation of Indonesia, the Philippines, and Malaysia. *Asian Journal of Criminal Justice and Forensic Studies*, 1(1), 101-112.

*Corresponding author

In academic discourse, the issue of the relationship between counter-terrorism legislation and human rights is increasingly being understood through the prism of the structural consequences of preventive approaches. Thus, R.A. Ahmad & S. Dhillon (2022) concluded that in the Malaysian context, the prevention of terrorism is institutionally accompanied by a systematic expansion of the discretionary powers of the state, leading to a lowering of legal certainty standards and a weakening of judicial control. They established that human rights violations are not a side effect of law enforcement but logically follow from the legislative construction of anti-terrorism norms, which are oriented towards risk assessment rather than proving actual violence. However, the study did not conduct a comparative analysis with alternative model approaches, which limits the possibility of generalising the obtained results beyond the Malaysian legal order. Further development of this issue can be traced in the study by N.M. bin Idris & Y.H. Khoo (2025), which shows that Malaysian anti-terrorism legislation creates a persistent imbalance between security objectives and international human rights protection standards. The authors established that preventive detention mechanisms, restrictions on freedom of movement, and the broad interpretation of threats to national security have a cumulative effect that weakens procedural guarantees. However, the research focuses primarily on the human rights dimension and does not analyse how the legislative technique of defining terrorism influences the boundaries of criminalisation as such, leaving the question of the model-based conditionality of the identified violations open.

A different analytical perspective is offered by J. Jupp (2022), who, using the example of the United Kingdom, demonstrated the transformation of anti-terrorism legislation from dynamic response to a state of regulatory "stagnation". The researcher established that the expansion of definitions of terrorism, particularly in the area of countering far-right extremism, has led to a blurring of the boundaries between ideological threat and criminally punishable conduct. At the same time, the author showed that even in a legal order with a developed judicial tradition, such evolution creates tension with the principle of legality. However, the question of whether these tendencies are universal for other legal systems with a different model architecture of anti-terrorism norms remains overlooked. In the Philippine context, R.U. Mendoza *et al.* (2021) established that the effectiveness of counter-terrorism measures largely depends on the clarity of the normative distinction between terrorism and ordinary criminal offences. The authors showed that linking terrorist acts to underlying offences, combined with a special purpose, increases the predictability of law enforcement. At the same time, they noted the limited adaptability of such an approach to new forms of violent activity. The study did not conduct a systematic comparison of this hybrid approach with functional or preventive models, which complicates the assessment of its relative advantages and risks.

A separate strand of literature is devoted to the financial aspects of terrorism, particularly in the work of F. Muslim *et al.* (2025), where it was established that strengthening state control over crowdfunding reduces the risks of financing terrorist activities but simultaneously negatively affects legitimate charitable practices. The authors concluded that preventive regulatory mechanisms can have a disproportionate effect if they are not embedded within a clearly defined legal framework. However, the study analyses financial instruments in isolation from the general definitional logic of terrorism, which does not allow for tracing their relationship with the boundaries of criminal liability. A critical analysis of Indonesian anti-terrorism legislation is presented in the work of I.M. Riduan (2024), which shows that the legitimacy of counter-terrorism norms largely depends on their perception by society and their compliance with the principles of legal certainty. The author established that expanding the object of the offence to abstract categories of social stability creates a risk of overcriminalisation. At the same time, the study focuses on political-legal legitimacy, leaving the comparative dimension and the relationship with the international "minimum core" outside detailed analysis.

The issue of the interaction between science and practice in the field of counter-terrorism is explored by Z.A. Sukabdi (2021), who established that integrating academic approaches into the formulation of state policy contributes to a more balanced equilibrium between security and human rights. The author concluded that it is precisely conceptual clarity in defining terrorism that enhances the effectiveness of law enforcement. However, the study does not detail which specific model constructs of the definition are most compatible with such a balance, leaving room for further comparative research. Finally, I.E. Okoye & P. Adejoh (2025), analysing the experience of Nigeria, found that victims of counter-terrorism operations most frequently encounter human rights violations in the context of preventive measures and the broad discretionary powers of security forces. The authors demonstrated that the absence of clear boundaries for criminalisation exacerbates the vulnerability of the civilian population. At the same time, the African context is examined without comparison with Asian or European models, which precludes the identification of universal patterns. Thus, the literature review attests to the existence of a substantial body of research devoted to the human rights implications of anti-terrorism legislation. However, the problem lies in the absence of a comprehensive comparative analysis of how the concept of "global terrorism" is translated into the criminal law norms of the aforementioned states, which elements of this concept are fully integrated, and which are modified or ignored. Addressing these gaps is necessary to enhance the effectiveness of counter-terrorism policy, ensure legal certainty, and formulate coherent approaches to countering global terrorist threats in regional and international dimensions. The aim of the article was a comparative assessment of the degree and forms of implementation of

international counter-terrorism standards in the criminal legislation of Indonesia, the Philippines, and Malaysia. To achieve this aim, the following tasks were set: to analyse the norms of the criminal legislation of Indonesia, the Philippines, and Malaysia that regulate liability for terrorist crimes; to determine the compliance of national definitions and elements of crimes with international standards.

Materials and Methods

The methodological foundation of the study was a qualitative-comparative legal design, focused on identifying the substantive characteristics of the concept of "global terrorism" and analysing the mechanisms of its implementation in the criminal legislation of Indonesia, the Philippines, and Malaysia. The methodological logic of the research was based on a combination of normative analysis, the study of judicial practice, and the comparative interpretation of law enforcement models. The chronological scope of the study covered the period from 2001 to 2024. The lower boundary was determined by the formation of the modern concept of global terrorism following the events of September 11, 2001, and the subsequent adoption of key UN – United Nations Security Council (n.d.), which established the normative framework for international counter-terrorism. The upper boundary of the study allowed for the consideration of the latest transformations in anti-terrorism legislation and judicial practice, associated with the strengthening of preventive approaches, the expansion of the state's security powers, and the actualisation of the problem of legal certainty. The chosen period ensured the possibility of analysing not the static state of legal regulation, but its evolution in response to changing security challenges.

The selection of Indonesia, the Philippines, and Malaysia as subjects of comparative analysis was determined by a combination of normative and empirical factors. All three states belong to the same region, have experienced real terrorist threats, and have simultaneously implemented international counter-terrorism standards through different models of criminalisation. Indonesia represents a functional model, within which key importance is attached to actual violence and its social effect; the Philippines – a hybrid model, combining formalised offences with the requirement to prove a special purpose; Malaysia – a preventive model, focused on early intervention and the assessment of security risk. This sample allowed for the identification of structural differences in the implementation of the concept of global terrorism under conditions of a shared international normative core.

Within the study, the special-legal method was applied, the purpose of which was to identify the peculiarities of the normative implementation of the concept of "global terrorism" and to analyse the legal technique of criminalising terrorist acts in the national legislation of Indonesia, the Philippines, and Malaysia. The material basis for the special-legal analysis comprised international counter-terrorism instruments that form the normative "minimum core" of the concept of terrorism, including the International Convention… (1999) and Resolution of the United Nations Security Council No. 1373 (2001), and Resolution of the United Nations Security Council No. 1566 (2004). The national dimension of the special-legal method encompassed the analysis of legislative acts of Indonesia, the Philippines, and Malaysia that directly regulate liability for terrorism. Specifically, the provisions of the Law of the Republic of Indonesia No. 5 (2018), which define the functional model for qualifying terrorist acts, were analysed. For the Philippine legal order, the Criminal Code of the Philippines (2014) was examined in order to trace the logic of criminalising terrorism through the combination of predicate offences and a special purpose. In the context of the Malaysian legal system, the special-legal method was applied to the analysis of the Penal Code No. 574 (1997), the Act of Malaysia No. 769 (2015), and the Act of Malaysia No. 747 (2015). Additionally, within the framework of the special-legal method, a structural-dogmatic analysis of the elements of terrorist offences was carried out, aimed at identifying how the key elements of terrorism are normatively constructed and the boundaries of criminal liability are delineated in the legislation of Indonesia, the Philippines, and Malaysia. The analytical procedure involved examining the object of the offence, the actus reus (the violent nature or threat thereof), the specific terrorist purpose (mens rea), and the subject of the crime.

One of the research methods employed was comparative legal analysis, applied to identify common features and differences in the implementation of the concept of global terrorism across the three legal orders. This method was used not for the formal juxtaposition of norms, but for analysing the model logic of criminalisation and its impact on the boundaries of law enforcement. The study also utilised the case study method, the purpose of which was to identify the peculiarities of the practical application of anti-terrorism legislation and to analyse how the chosen criminal law model influences judicial reasoning in qualification, the structure of evidence, and the limits of criminalisation of terrorist acts. The materials for the case studies were typical court cases representing the functional, hybrid, and preventive models of terrorism criminalisation. To analyse the functional model, court proceedings related to the Bali bombings of October 12, 2002, were used, particularly the decision of the Constitutional Court of the Republic of Indonesia Case No. 013/PUU-I/2003 (2003), which examined the issue of the retroactive application of anti-terrorism legislation. To study the hybrid model of applying anti-terrorism legislation, the decision of the Supreme Court of the Philippines in the consolidated cases Supreme Court of the Philippines G.R. No. 252578 (2021), concerning the constitutionality of the Act of the Republic of the Philippines No. 11479 (2020), was analysed. Within the analysis of the preventive model, materials from Malaysian judicial practice were used, specifically the decision of the Court of Appeal in the case of Court of Criminal Appeal of Malaysia No. W-05-141-05 (2014), which illustrates

the application of anti-terrorism norms in the context of assessing security risk and preparatory acts. This case was used to examine how courts shift the focus of proof from demonstrating a completed violent act to analysing a potential threat to national security while simultaneously attempting to establish normative limits on the application of preventive measures.

Results and Discussion

Criminal law regulation of liability for terrorist crimes in Indonesia, the Philippines, and Malaysia

In international law, the concept of "global terrorism" is formed not through a single universal definition, but by establishing functional minimum standards in United Nations Security Council (n.d.) resolutions and sectoral anti-terrorism conventions, which regard terrorism as a transnational threat to international peace and security. The starting point for the criminalisation of terrorist crimes are the provisions of Resolution of the United Nations Security Council No. 1373 (2001) and Resolution of the United Nations Security Council No. 1566 (2004), in which terrorism is delineated through a combination of a violent act or the threat of its commission, the specific purpose of intimidating a population, compelling a government or an international organisation, and heightened public danger, irrespective of the territorial boundaries of the act's commission. Further normative specification of this model is contained in the International Convention… (1999), which establishes a universal purposive criterion ("by its nature or context intended to intimidate a population or compel a government or an international organisation"), thereby forming a generally accepted international understanding of a terrorist act for the purposes of domestic criminalisation. Collectively, these instruments lay the conceptual foundation for "global terrorism" as a phenomenon characterised by transnationality, ideological or political conditionality, and an aim to undermine public security through psychological and institutional impact. It is within this international legal framework that the structure of the constituent elements of terrorist crimes in the criminal legislation of Indonesia, the Philippines, and Malaysia is constructed, albeit with varying degrees of abstraction and different legislative techniques.

The criminalisation of terrorism in Indonesia, the Philippines, and Malaysia is based on different legislative models; however, in all three states, an aspiration to adapt national criminal law to the contemporary understanding of terrorism as a complex and potentially transnational phenomenon can be observed. An analysis of the structure of the constituent elements of terrorist crimes has revealed how each legal system defines the key elements of terrorism and delineates the boundaries of criminal liability. In Indonesia, the definition of terrorist crimes is enshrined in the Law of the Republic of Indonesia No. 5 (2018). Indonesian legislation employs a broad functional model of criminalisation, whereby terrorism is defined through the purpose and consequences of the act, rather than through an exhaustive list of specific offences. Terrorist crimes are characterised by the use or threat of violence with the aim of creating an atmosphere of mass fear, causing significant loss of life, or inflicting damage on strategically important objects, infrastructure facilities, or international institutions. The Law explicitly considers the political, ideological, and security-related motivation of such acts and acknowledges their potential connection to activities carried out both within and outside the territory of Indonesia, indicating the incorporation of a transnational element.

In the Philippines, the criminalisation of terrorism is effected pursuant to the Act of the Republic of the Philippines No. 11479 (2020). Philippine law applies a hybrid model, which combines a general definition of terrorism with reference to specific offences already provided for in the Criminal Code of the Philippines (2014). Terrorism is qualified as the commission of such acts in the presence of a specific purpose – intimidating the population, spreading fear, destabilising public order, or compelling the government or international organisations. This approach allows for the preservation of the list of basic criminal offences while simultaneously expanding their criminal law assessment by considering the functional criterion of purpose and societal effect. The Act also explicitly covers cross-border aspects, including participation in the activities of foreign terrorist organisations and the commission of acts outside the state, if they produce consequences within the territory of the Philippines.

In Malaysia, the criminalisation of terrorist crimes is carried out primarily on the basis of the Penal Code No. 574 (1997), the Act of Malaysia No. 747 (2015), and the Act of Malaysia No. 769 (2015). The Malaysian model is characterised by a broad preventive approach, whereby terrorist crimes encompass not only direct violent acts but also conduct related to supporting, organising, or facilitating terrorist activity. Criminal legislation establishes liability for actions aimed at achieving political, religious, or ideological goals through violence or threats intended to influence the government or intimidate the population. Particular attention is paid to the criminalisation of preparatory acts, participation in terrorist organisations, and the financing of terrorism, reflecting an orientation towards proactive threat response. Overall, the national definitions of terrorist crimes in Indonesia, the Philippines, and Malaysia encompass the key elements inherent in the concept of "global terrorism", specifically ideological or political motivation, the aim of intimidating the population or exerting pressure on state institutions, and the recognition of the transnational character of such acts. At the same time, differences in legislative technique give rise to varying approaches to defining the boundaries of criminal liability: Indonesia and Malaysia favour broad functional formulations, whereas the Philippines combines functional criteria with reference to specific criminal offences. It is precisely these differences that condition the further expansion of criminalisation through various forms of participation in terrorist activity.

Consequently, the criminal law regulation of terrorism in Indonesia, the Philippines, and Malaysia is characterised by an expansion of the boundaries of criminal liability by encompassing not only completed terrorist acts but also various forms of participation in terrorist activity. This approach is dictated by the international legal understanding of terrorism as an enduring and networked threat realised through financing, organisational support, and preparatory actions. Accordingly, national legislation aims to criminalise conduct that creates the conditions for the commission of terrorist acts, irrespective of the fact of their direct perpetration. In Indonesia, the Law of the Republic of Indonesia No. 5 (2018) provides for separate offences for the financing of terrorism, as well as for the provision or collection of funds, property, or other resources with the knowledge that they are to be used for terrorist purposes. Criminal liability also extends to preparatory and ancillary actions, including recruiting, training, and preparing individuals for the commission of terrorist crimes. Participation in terrorist organisations is separately criminalised, with proof of a specific terrorist act not being a mandatory condition for liability. This structure is aimed at preventing the formation and functioning of terrorist networks. In the Philippines, the Act of the Republic of the Philippines No. 11479 (2020) establishes criminal liability for a wide range of forms of participation in terrorist activity, supplementing the basic offences provided for in the Criminal Code of the Philippines (2014). The Act directly criminalises the financing of terrorism, planning, preparation, and training for the purpose of committing terrorist acts, as well as the provision of material, technical, or organisational support to terrorist structures. Membership or another form of participation in terrorist organisations, regardless of the individual's involvement in a specific act of violence, is recognised as a separate offence. This allows for the coverage of activity aimed at maintaining the institutional capacity of terrorism. In Malaysia, the expansion of criminal liability is implemented through a combination of norms from the Penal Code No. 574 (1997), the Act of Malaysia No. 747 (2015), and the Act of Malaysia No. 769 (2015). The legislation establishes liability for the financing of terrorist activity, participation in terrorist organisations, and also for preparatory and ancillary actions that create the conditions for the commission of terrorist acts. A characteristic feature is the preventive orientation, whereby conduct associated with a potential threat to national security is deemed criminally punishable, even without proof of a specific act of violence. This approach is aimed at the early detection and neutralisation of terrorist activity.

Thus, within the legal orders of Indonesia, the Philippines, and Malaysia, terrorism is regarded not merely as an isolated violent act, but as a complex of interconnected actions that ensure the functioning of terrorist networks. It is precisely the criminalisation of such forms of participation that allows national legislations to reflect the concept of "global terrorism" as an enduring transnational threat and to justify the application of proactive criminal law mechanisms. At the same time, this model of expanded criminalisation directly influences the formation of sentencing policy, as punishment is directed not only towards a repressive response to a completed terrorist act but also towards neutralising the potential risks associated with the support, organisation, and perpetuation of terrorist activity. In this context, sanctions acquire a systemic and preventive character, which conditions their heightened severity and a departure from traditional notions of proportionality of punishment.

The sanction policy in the field of counter-terrorism in the countries under study is characterised by a high level of repressiveness and a focus on neutralising security risks, rather than merely on retribution for an already committed crime. In the criminal legislation of these states, sanctions for terrorist offences exceed the punishments for general criminal violent acts and are applied both to completed acts of terrorism and to preparatory and ancillary forms of activity. In Indonesia, Law of the Republic of Indonesia No. 5 (2018) provides for a multi-level system of sanctions depending on the nature and consequences of the terrorist crime. For the commission of terrorist acts that result in loss of life or mass destruction, the penalties established are the death penalty, life imprisonment, or imprisonment for a term of 20 years. For the financing of terrorism, participation in terrorist organisations, recruitment, and training, imprisonment terms ranging from 5 to 20 years are provided, along with additional sanctions in the form of confiscation of property. This gradation of sanctions indicates the use of criminal law as a deterrent instrument at all stages of terrorist activity. In the Philippines, the Act of the Republic of the Philippines No. 11479 (2020) establishes the penalty of life imprisonment without the possibility of parole for the commission of terrorist acts, as well as for participation in terrorist organisations. For the financing of terrorism, planning, preparation, and training for terrorist purposes, imprisonment up to life imprisonment is prescribed, along with the mandatory confiscation of funds and assets related to the crime. The death penalty is not applied in the Philippine legal system; however, the severity of sanctions is compensated for by life sentences and an expanded scope of criminally punishable forms of participation, ensuring a preventive effect. In Malaysia, terrorist offences and participation in terrorist organisations are punishable by long terms of imprisonment, including life imprisonment, as well as special preventive measures against individuals who pose a threat to national security. Criminal liability applies regardless of proof of a specific act of violence if an individual's conduct poses a real terrorist threat. In summary, the sanction models of Indonesia, the Philippines, and Malaysia demonstrate a departure from the classical principle of strict proportionality between harm and punishment. Severe prison terms, life sentences, and, in the case of Indonesia, the death penalty are employed as prevention tools aimed at neutralising potential terrorist risks.

Thus, an analysis of the criminalisation of terrorism in Indonesia, the Philippines, and Malaysia indicates that all three states have implemented key international approaches to counter-terrorism; however, they have realised them within different legal models (Table 1). International counter-terrorism standards in these legal orders function as a normative framework that defines minimum requirements for criminalisation but does not form a unified legislative matrix. The presented systematisation demonstrates that the implementation of international counter-terrorism standards in the studied states occurs within different criminal law models, determined by national security priorities and legislative traditions. This necessitates further comparative analysis of the compliance of national definitions and elements of terrorist crimes with international standards. The obtained results regarding the international legal nature of "global terrorism" are consistent with the conclusions of T. Pék (2022), who showed that international criminal law has not developed a single universal definition of terrorism and instead operates with a set of functional features and target criteria. This author's work emphasises that it is precisely the fragmentation of international definitions that leads to different national techniques of criminalisation, where states construct the actus reus and specific intent differently. This coincides with the fact established in this study of the existence of three different legislative models in Southeast Asia: functional (Indonesia), hybrid (Philippines), and preventive (Malaysia). At the same time, the results of this analysis elaborated on T. Pék's thesis using normative material: the minimum standards reflected in Resolution of the United Nations Security Council No. 1373 (2001) and Resolution of the United Nations Security Council No. 1566 (2004) effectively function as a "framework", but not as a unified template; therefore, national definitions retain different levels of abstraction and different constructions of the offence.

Table 1. Implementation of international approaches to the criminalisation of terrorism in Indonesia, the Philippines, and Malaysia

Analysis Criterion	Indonesia	Philippines	Malaysia
Model of Criminalisation of Terrorism	Functional Model	Hybrid Model	Preventive Model
Method of Defining a Terrorist Offence	A violent act or threat of its commission, specific purpose (intimidating the population, creating mass fear, or influencing state institutions), heightened public danger	Commission of crimes already provided for in criminal legislation, in the presence of a specific terrorist purpose (intimidating the population, coercing the government or an international organisation)	Acts involving the use of violence or a threat to national security, committed with a political, religious, or ideological purpose
Criminalisation of Forms of Participation	Financing, recruitment, training, participation in terrorist organisations	Financing, planning, training, membership and other participation	Financing, preparatory acts, participation, facilitation
Maximum Sanctions	Death penalty, life imprisonment	Life imprisonment	Life imprisonment, preventive restrictive measures

Source: compiled by the author based on Penal Code No. 574 (1997), Act of Malaysia No. 747 (2015), Act of Malaysia No. 769 (2015), Law of the Republic of Indonesia No. 5 (2018), Act of the Republic of the Philippines No. 11479 (2020)

The conclusions regarding the trend towards expanding criminal liability by encompassing preparatory and ancillary forms of activity correlate with the arguments of A. Sagara (2024), who, within the framework of international criminal law analysis, emphasised the need to cover not only the completed act of violence but also the infrastructure of terrorist activity. His work underscores that the criminalisation of financing, participation in organisations, and other "network" forms of involvement is critical for countering transnational threats, as these elements ensure the reproduction of terrorism as a phenomenon. This aligns with the results of this study, which show that in all three legal orders, liability arises not only for a terrorist act but also for financing, recruitment, training, preparation, and participation in terrorist organisations without the mandatory proof of a specific act of violence. At the same time, this study recorded that the national systems of Indonesia, the Philippines, and Malaysia have already implemented "pre-emptive" criminalisation through domestic laws, whereas A. Sagara primarily considered the issue in the realm of international criminal jurisdiction and its possible expansion, i.e., at a different level of normative regulation.

The obtained results regarding sanction logic and its preventive nature partially coincide with the conclusions of R.S. Ogbe (2023), who analysed the dynamics of the criminalisation of terrorism in international criminal law and pointed to a trend towards "security-oriented" justification of punishment. The author emphasised that in countering terrorism, criminal justice systems use harsh sanctions not merely as a reaction to consequences but as a mechanism for deterrence and risk neutralisation. This aligns with the fact established in this study of the increased severity of sanctions in the three states, including maximum repressiveness for the most serious forms of terrorism. At the same time, the results of this analysis refined R.S. Ogbe's thesis using the example of specific legal orders: in Indonesia, the sanction model provides for the death penalty and, alternatively, life imprisonment or imprisonment from 20 years for terrorist acts with grave

consequences, whereas in the Philippines and Malaysia, the upper limit focuses on life imprisonment, demonstrating different national trajectories of the "security-oriented" approach under a formally shared preventive goal.

International counter-terrorism standards and their reflection in national definitions of terrorism

In international law, the concept of terrorism is not codified within a single universal definition. However, this does not imply the absence of normative standards for its criminal law definition. On the contrary, the international community has developed a model minimum core, formed through the recurrence of key elements in resolutions such as Resolution of the United Nations Security Council No. 1373 (2001) and Resolution of the United Nations Security Council No. 1566 (2004), as well as in law enforcement practice. Analysis of these sources confirms that this core includes: a violent act or the threat thereof; the presence of a specific purpose in the form of intimidating a population or compelling a government or an international organisation; an enhanced public danger of the act directed against public security; and a transnational context justifying the need for international cooperation and expanded jurisdictional mechanisms. Scholarly research confirms that it is precisely this "framework" model that is definitive for international criminal law. Specifically, A.P. Schmid (2023) argued that international standards in the field of terrorism function as structural constraints that guide the national legislator but leave room for diverse legislative techniques and varying degrees of abstraction in definitions. A similar position was articulated by A.M. Salinas de Frías *et al.* (2012), noting that the key requirement is not the unification of wording, but the preservation of the mandatory elements of violence, specific purpose, and public danger, without which criminalisation loses its connection to international standards. Research by the United Nations Office on Drugs and Crime (2021) also emphasises that transnationality in the contemporary understanding of terrorism is not always an element of the actus reus of the crime but serves as a normative justification for expanding cooperation and the mutual recognition of jurisdiction.

The transition from the international "minimum core" to the assessment of national definitions necessitates the application of qualitative criteria that go beyond the mere formal reproduction of individual terms. In the international legal doctrine of counter-terrorism, it is emphasised that compliance with international standards, shaped notably by Resolution of the United Nations Security Council No. 1373 (2001) and Resolution of the United Nations Security Council No. 1566 (2004), is primarily manifested in legislative technique: the ability to clearly delineate terrorism from related ordinary criminal or political offences; the prevention of substituting the violent element with vague categories such as "threat to national security"; sufficient specificity of the special purpose; and the presence of safeguards against the criminalisation of legitimate political activity (Walker, 2021). Particular attention in research is devoted to adherence to the principle of *nullum crimen sine lege certa*, which, in the context of counter-terrorism legislation, acts as an indicator of the balance between the state's security interests and the requirements of legal certainty (Bantekas & Oette, 2013). Thus, international counter-terrorism standards for the definition of terrorism should be understood not as a rigid, unified formula, but as a set of mandatory elements and methodological requirements that constrain the national legislator. It is precisely through the lens of these criteria that national definitions of terrorism in Indonesia, the Philippines, and Malaysia should be assessed, focusing not only on their content but also on the consequences for the scope of criminal liability and legal certainty.

In Indonesian legislation, the definition of terrorism (Law of the Republic of Indonesia No. 5, 2018) is constructed according to a functional logic that broadly corresponds to international standards (European Convention on Human Rights, 1950). At the core of the definition lies a violent act or a credible threat thereof, aimed at creating an atmosphere of fear among the population or compelling state authorities, which directly reproduces the key elements of the international minimum core. At the same time, Indonesia's normative regulation expands the object of the offence, including not only public security but also the stability of state institutions and the public order in general. The legal consequence of this is an increased flexibility of criminalisation, which, however, requires enhanced oversight by judicial practice to prevent the blurring of boundaries between terrorism and related violent crimes.

A different logic is observable in the definition of terrorism enshrined in the legislation of the Philippines, which represents a hybrid model of implementing the international core. Here, the international elements – violence or the threat thereof, the specific purpose of intimidating the population or compelling the state – are combined with a technique of "anchoring" terrorism to a list of predicate criminal offences (Act of the Republic of the Philippines No. 11479, 2020). This approach allows for a clearer distinction of terrorism from ordinary crime, since an act acquires a terrorist character only when accompanied by an additional specific purpose. However, the hybridity of the definition leads to a certain fragmentation: the boundaries of terrorism depend on a pre-determined list of offences, which may limit the law's ability to respond to new forms of violent activity. From the perspective of the international minimum core, this model generally meets the requirements of certainty and foreseeability but shifts the emphasis from public danger as an independent characteristic to the formal classification of acts.

A structural deviation from the "classic" international minimum core is evident in the preventive definition of terrorism enshrined in the legislation of Malaysia. Although the violent component and specific purpose are formally retained, the legislative technique emphasises not so much actual harm as the creation or likelihood of

creating a serious security risk. Consequently, the object of the offence is expanded to "national security" in a broad sense, and a terrorist character may be attributed to acts at early, preparatory stages. This approach enhances the preventive potential of criminal law and aligns with the logic of international cooperation in counter-terrorism, yet it weakens the requirement of legal certainty. Comparison with the international minimum core reveals that it is precisely at the definitional level that tension arises between security expediency and the principle of *nullum crimen sine lege certa*, as the boundaries of criminal liability become less foreseeable (Table 2).

Table 2. Compliance of national definitions of terrorism with the international minimum core: A comparative legal analysis

Element of the International Minimum Core	International Standard (General Framework)	Indonesia (Functional Model)	Philippines (Hybrid Model)	Malaysia (Preventive Model)
Violent Act or Threat	Mandatory presence of actual violence or a credible threat of its use as a key characteristic of terrorism	Directly enshrined as a central element; encompasses both completed violence and the threat thereof	Derived through a list of predicate serious offences (murder, kidnapping, bombing, etc.), which acquire a terrorist character	Formally retained but may be "diffused" within the broader category of acts creating a security risk
Specific Purpose	Intimidating a population or compelling a government/international organisation	Clearly formulated; functions as a key criterion for distinguishing from ordinary criminal violence	A mandatory additional characteristic "superimposed" upon the predicate offence	Broadly formulated; combined with goals of protecting national security and social stability
Object of the Offence / Public Danger	Public safety, public order, international peace and security	Public safety specified through the harm caused by the predicate offence	Public safety specified through the harm caused by the predicate offence	Public safety in a broad sense, including potential threats
Delineation from Related Offences	Terrorism must be clearly distinguishable from ordinary criminal and political offences	Delineation achieved through the combination of violence and specific purpose	Delineation formalised through the list of predicate offences and the additional purpose	Boundaries blurred due to the inclusion of a wide range of preventive actions
Transnational Context	Not necessarily an element of the corpus delicti, but a basis for cooperation and jurisdiction	Present as a justification for enhanced powers and international cooperation	Indirectly enshrined through mechanisms of mutual legal assistance and extradition	Actively used to justify preventive measures
Level of Legal Certainty	Requirement of adherence to the principle of *nullum crimen sine lege certa*	High, provided that the courts interpret it narrowly	High, conditional upon narrow interpretation by judicial practice	Reduced due to the breadth of wording and emphasis on potential danger

Source: compiled by the author based on European Convention on Human Rights (1950), Penal Code No. 574 (1997), Resolution of the United Nations Security Council No. 1373 (2001), Resolution of the United Nations Security Council No. 1566 (2004), Act of Malaysia No. 747 (2015), Act of Malaysia No. 769 (2015), Law of the Republic of Indonesia No. 5 (2018), Act of the Republic of the Philippines No. 11479 (2020)

The comparative table demonstrates that the national definitions of terrorism in Indonesia, the Philippines, and Malaysia are formally based on the international minimum core established in Resolution of the United Nations Security Council No. 1373 (2001) and Resolution of the United Nations Security Council No. 1566 (2004), as well as related law enforcement practices. However, they differ significantly in legislative technique and regulatory logic. All three legal systems reproduce the basic elements of violent action or threat and special intent, indicating a maintained connection with international standards at the conceptual level. At the same time, the method of integrating these elements directly impacts the scope of criminalisation and the level of legal certainty. The functional model, implemented in Indonesian legislation, provides relatively flexible coverage of terrorist activities but requires a heightened role for judicial interpretation to prevent expansive application. The Philippines' hybrid model, which combines international features of terrorism with a list of predicate offences, is characterised by a higher level of predictability and clearer boundaries of criminal liability, yet it potentially limits the law's adaptability to new forms of terrorist activity. Malaysia's preventive model, while maximising the state's security potential, simultaneously deviates most significantly from the requirement of legal certainty, as it expands the definition of terrorism through the categories of potential threat and national security.

These findings align with the conclusions of F. Ní Aoláin (2024), whose research demonstrated that contemporary counter-terrorism regimes shift the balance in favour of security expediency to the detriment of legal certainty and human rights protection. The conducted analysis confirmed this thesis at the level of terrorism definitions, particularly in Malaysia's preventive model, where the expansion of the concept through national security and potential threat categories weakens the

requirement of *nullum crimen sine lege certa*. At the same time, the obtained results refine F. Ní Aoláin's approach, demonstrating that the source of risk to human rights is not only the practice of applying anti-terrorism measures but the very architecture of the legislative definition itself.

The study's conclusions also correlate with the analytical propositions of I. Sobol *et al.* (2023), who emphasised the absence of a direct link between the expansion of counter-terrorism powers and increased effectiveness in combating terrorism. The comparative analysis of national definitions confirmed that the preventive expansion of the corpus delicti is not accompanied by an automatic increase in the quality of law enforcement; instead, it reduces the level of predictability of criminal liability. However, the research findings refine the approach of I. Sobol *et al.*, demonstrating that effectiveness and the human rights balance depend significantly on the definitional model logic (functional, hybrid, or preventive), not merely on the intensity of state intervention. This allows the hybrid model to be viewed as a compromise between security and legal certainty.

The obtained results partially coincide with the conclusions of L. Ginsborg (2021) regarding the trend towards criminalising so-called "pre-crime" as a result of the UN Security Council's normative activities. The analysis confirmed that international standards create preconditions for the preventive expansion of criminal liability, particularly through an emphasis on risk and preparatory stages. However, the study revealed a certain divergence from L. Ginsborg's generalised approach, as it showed that not all national implementations of the international "minimum core" equally gravitate towards the "pre-crime" logic. The functional and hybrid models (Indonesia, the Philippines) maintain a closer connection with actual violence and special intent, which limits the encroachment of preventive criminalisation and confirms the significance of national legislative technique as a constraining factor.

Overall, the research findings are consistent with the contemporary doctrine of international counter-terrorism law, but they also expand it by demonstrating that the key variable is not the mere absence of a universal definition of terrorism, but rather the method of normative construction of national definitions within the international minimum core. This allows for a reassessment of the role of international standards – not as a source of unification, but as a framework space within which national legal systems shape different balances between security and the principle of legality.

The practice of applying anti-terrorism legislation through the prism of functional, hybrid, and preventive models

The practice of applying anti-terrorism legislation confirms that it is the chosen model – functional, hybrid, or preventive – that determines the logic of judicial analysis, the structure of evidence, and the actual boundaries of criminalisation. Typical court cases in Indonesia, the Philippines, and Malaysia demonstrate that, despite the formal commonality of the international minimum core, different models allocate emphasis differently among actual violence, special intent, and the assessment of security risk.

Within the functional model, characteristic of the Indonesian approach, judicial practice focuses primarily on the factual role of violence and its social effect. The adjudication of cases related to the Bali bombings of October 12, 2002, which resulted in the deaths of over 200 people, illustrates the specific judicial approach to qualifying terrorist acts (Hassan, 2007). The courts proceeded from the necessity to prove not only the fact of extreme violence itself but also its purposiveness. Decisive importance was attached to establishing that the violent acts were aimed at creating an atmosphere of mass fear and undermining public safety. It was the combination of actual violence, large-scale consequences, and the established special intent to intimidate the civilian population that served as the basis for qualifying the acts as terrorist and for upholding this qualification at the stages of appellate and cassation review.

At the same time, Indonesian judicial practice demonstrates that the flexibility of the functional model is not unlimited and is subject to constitutional constraints. Illustrative in this context is the case of Masykur Abdul Kadir v. State (Constitutional Court of the Republic of Indonesia Case No. 013/PUU-I/2003, 2003), in which the Constitutional Court examined the issue of the retroactive application of anti-terrorism legislation to the events of October 12, 2002. Despite the obvious terrorist nature of the acts in view of the scale of violence, the number of victims, and the established special intent to intimidate the population, the Court concluded that the imposition of criminal liability could not exceed the bounds of the principle nullum crimen sine lege. Thus, the Constitutional Court's decision confirmed that within the functional model, judicial interpretation itself plays a dual role: on the one hand, it ensures the adaptive qualification of terrorist acts, and on the other, it acts as a guarantee against preventing the excessive expansion of criminalisation even in situations of extreme public danger.

The hybrid model, characteristic of Philippine practice, forms a different logic of law enforcement, clearly manifested in the Supreme Court's decisions regarding the application of the Anti-Terrorism Act. Judicial reasoning follows a two-tiered scheme: first, the commission of a predicate criminal offence must be established, and only then – the presence of a special terrorist intent in the form of intimidating the population or coercing the state. The Supreme Court's decision of December 7, 2021, in the consolidated cases concerning the constitutionality of the anti-terrorism legislation explicitly emphasises that without proving such special intent, even serious violence cannot automatically be qualified as terrorism (Supreme Court of the Philippines G.R. No. 252578, 2021). The practical effect of the hybrid model lies in narrowing the discretion of prosecution authorities and increasing

the predictability of the boundaries of criminal liability. However, it simultaneously limits the ability to respond to atypical or new forms of terrorist activity that do not fall within the pre-defined list of predicate offences.

The preventive model discernible in Malaysian practice shifts the focus of judicial analysis from proving a completed act of violence to assessing risk and potential threats to national security. The Court of Appeal's decision in Court of Criminal Appeal of Malaysia No. W-05-141-05 (2014) illustrates that courts operate within a sphere of preventive rationality, relying on security assessments and preparatory acts. Concurrently, even within this model, the judiciary endeavours to establish normative boundaries for the application of anti-terrorism measures, particularly by limiting their territorial scope. This indicates a structural tension between the pursuit of the earliest possible intervention and the requirement of legal certainty, a tension that constitutes a systemic feature of the preventive approach.

The findings of this study concerning the preventive model correlate with the conclusions of E. Janfada *et al.* (2024), who analysed the impact of counter-terrorism measures on the rights of the accused. The authors concluded that the expansion of the state's preventive powers systematically shifts the focus of criminal procedure from proving actual violence to assessing risk and potential threat, thereby complicating the safeguarding of procedural guarantees. Their research demonstrated that courts often attempt to compensate for this shift by strengthening oversight of the proportionality and legality of measures; however, this mechanism is not always sufficient. The results obtained in this article confirmed these observations, as Malaysian practice exhibited structural tension between early intervention and the demand for legal certainty, even in the presence of judicial attempts to delineate the normative limits of preventive measures.

The analysis of the hybrid model also partially aligns with approaches documented in works dedicated to the judicial review of anti-terrorism legislation, yet it also revealed certain discrepancies. Unlike the preventive logic, the hybrid model, as the research findings indicated, has institutionalised a specific terrorist purpose as the key filter for criminalisation, thereby narrowing the discretion of prosecuting authorities and enhancing the predictability of law enforcement. In this aspect, the results are consistent with the conclusions of S. Melander (2023), who established that modern criminal law has undergone a so-called "preventive turn"; however, the intensity of this turn varies significantly depending on the model's construction. S. Melander demonstrated that where a specific purpose remained a central element of the actus reus, courts retained greater scope for upholding the principle of legality. The conducted research confirmed this finding using the example of Philippine practice, while simultaneously revealing the hybrid model's limited capacity to respond to new or atypical forms of terrorist activity. The comparative analysis of application practice confirmed that the actual limits of the criminalisation of terrorism are shaped not only at the level of the legislative text but also at the intersection of the chosen model and judicial interpretation. The functional model places upon the courts the decisive role in determining the social meaning of violence; the hybrid model institutionalises a specific purpose as a filter for criminalisation; whereas the preventive model reorients the burden of proof towards the categories of risk and threat. It is precisely this difference in law enforcement practices that explains why, despite a shared international minimum core, anti-terrorism law in different jurisdictions produces different standards of proof, different intensities of intervention, and a different balance between the effectiveness of security and the principle of legality.

Conclusions

As a result of the study, it has been established that the concept of "global terrorism" in international law is implemented not through a unified definition, but through a system of minimum functional standards enshrined in United Nations Security Council resolutions and sectoral anti-terrorism conventions. These encompass the violent nature of the act, the specific purpose of intimidation or coercion, and the transnational dimension of the threat. A comparative analysis of the criminal legislation of Indonesia, the Philippines, and Malaysia demonstrated the implementation of these standards within different criminal law models: the functional-preventive model (Indonesia, Malaysia) and the combined functional-listing model (the Philippines). International standards serve as a normative framework that directs national criminalisation but does not form a unified legislative matrix.

The study established that the criminal legislation of Indonesia, the Philippines, and Malaysia is aimed at covering not only completed terrorist acts but also behaviour that precedes or accompanies their commission. Such behaviour includes the financing of terrorist activities, the recruitment and training of individuals, preparation for the commission of terrorist offences, and participation in terrorist organisations regardless of proof of a specific act of violence. This implies that criminal liability arises already at the stage of forming or supporting terrorist activity. Consequently, the criminal law response shifts from reacting to the consequences of a terrorist act to preventing its potential commission.

Based on the results of analysing the application practice of anti-terrorism legislation, it has been established that the functional, hybrid, and preventive models shape qualitatively different standards of judicial analysis, proof, and the actual limits of the criminalisation of terrorism, even in the presence of a shared international minimum core. The examination of judicial cases from Indonesia, the Philippines, and Malaysia showed that in the functional model, proving actual violence, its social effect, and the specific purpose of intimidation is of decisive importance. This is confirmed by the practice of qualifying the 2002

Bali bombings, which resulted in over 200 fatalities, while simultaneously being constrained by the constitutional prohibition of retroactive criminalisation.

Within the hybrid model, the specific terrorist purpose is institutionalised as a key filter for criminal liability, ensuring a higher level of legal certainty but limiting the adaptability of law enforcement. In contrast, the preventive model shifts judicial analysis from proving violence to assessing risk and preparatory acts, enhancing early state intervention while simultaneously exacerbating tension with the principle of *nullum crimen sine lege certa* and necessitating heightened scrutiny of proportionality. Prospects for further research lie in an in-depth empirical analysis of the judicial practice of other regional legal systems, with the aim of identifying the long-term impact of functional, hybrid, and preventive models on standards of proof, procedural guarantees, and the transformation of the principle of legality in the context of increasing security-driven prevention.

Acknowledgements
None.

Funding
None.

Author Contributions
Nurlan Apakhaev carried out a full research cycle, ranging from the development of a comparative legal methodology to an analysis of the counter-terrorism legislation of Indonesia, the Philippines and Malaysia. The author independently systematised the functional, hybrid and preventive models of implementing international standards and conducted a critical analysis of key court cases in the region. The entire article is the result of individual work at every stage of its preparation.

Conflict of Interest
None.

References
[1] Act of Malaysia No. 747 "Security Offences (Special Measures) Act 2012". (2015, August). Retrieved from https://andyreiter.com/wp-content/uploads/military-justice/my/Laws%20and%20Decrees/Malaysia%20-%202012%20-%20Security%20Offences%20(Special%20Measures)%20Act.pdf.

[2] Act of Malaysia No. 769 "Prevention of Terrorism Act 2015". (2015, May). Retrieved from https://www.icnl.org/wp-content/uploads/Malaysia_terrormalay.pdf.

[3] Act of the Republic of the Philippines No. 11479 "An Act to Prevent, Prohibit and Penalize Terrorism, Thereby Repealing Republic Act No. 9372, Otherwise Known as the 'Human Security Act of 2007'". (2020, July). Retrieved from https://www.officialgazette.gov.ph/2020/07/03/republic-act-no-11479/.

[4] Ahmad, R.A., & Dhillon, S. (2022). Must the prevention of terrorism entail the violation of human rights? A view from Malaysia. *UUM Journal of Legal Studies*, 13(2), 243-266. doi: 10.32890/uumjls2022.13.2.10.

[5] Bantekas, I., & Oette, L. (Eds.). (2013). Human rights and counter-terrorism. In *International human rights law and practice* (pp. 613-655). Cambridge: Cambridge University Press. doi: 10.1017/CBO9781139048088.016.

[6] bin Idris, N.M., & Khoo, Y.H. (2025). Counterterrorism legislation and its impacts on human rights in Malaysia. *Indonesia Law Review*, 15(2), article number 6. doi: 10.15742/ilrev.v15n2.2.

[7] Constitutional Court of the Republic of Indonesia Case No. 013/PUU-I/2003. (2003, October). Retrieved from https://en.mkri.id/download/decision/putusan_sidang_eng_ConstitutionalCourtDecisionTerroristAct.pdf.

[8] Court of Criminal Appeal of Malaysia No. W-05-141-05 "Public Prosecutor v. Yazid bin Sufaat & Ors". (2014, January). Retrieved from https://surl.lu/ycseyc.

[9] Criminal Code of the Philippines. (2014, September). Retrieved from https://www.doj.gov.ph/files/ccc/Criminal_Code_September-2014(draft).pdf.

[10] European Convention on Human Rights. (1950, November). Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf.

[11] Ginsborg, L. (2021). Moving toward the criminalization of "pre-crime": The UN Security Council's recent legislative action on counterterrorism. In A. Vedaschi & K.L. Scheppele (Eds.), *9/11 and the rise of global anti-terrorism law: How the UN Security Council rules the world* (pp. 133-154). Cambridge: Cambridge University Press. doi: 10.1017/9781009023146.008.

[12] Hassan, M.H.B. (2007). Imam Samudra's justification for Bali bombing. *Studies in Conflict & Terrorism*, 30(12), 1033-1056. doi: 10.1080/10576100701670896.

[13] International Convention for the Suppression of the Financing of Terrorism. (1999). Retrieved from https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf.

[14] Janfada, E., Taheri Bojd, M.A., & Hashemi, S.H. (2024). Safeguarding human rights of the accused in counter-terrorism measures: Reconciling national security with civil liberties. *International Law Review*, 41(75), 251-272. doi: 10.22066/cilamag.2024.2010011.2437.

[15] Jupp, J. (2022). From spiral to stasis? United Kingdom counter-terrorism legislation and extreme right-wing terrorism. *Studies in Conflict & Terrorism*, 48(7), 763-783. doi: 10.1080/1057610X.2022.2122271.

[16] Law of the Republic of Indonesia No. 5 "On the Eradication of Criminal Acts of Terrorism into Law". (2018). Retrieved from https://peraturan.bpk.go.id/Details/82689/uu-no-5-tahun-2018.
[17] Melander, S. (2023). Preventive turn in criminal law. *Peking University Law Journal*, 11(1), 11-23. doi: 10.1080/20517483.2023.2223843.
[18] Mendoza, R.U., Ong, R.J.G., Romano, D.L.L., & Torno, B.C.P. (2021). Counterterrorism in the Philippines: Review of key issues. *Perspectives on Terrorism*, 15(1), 246-261.
[19] Muslim, F., Zulfa, E.A., & Syauqillah, M. (2025). Managing crowdfunding risks in terrorism financing: A mediated analysis of government intervention and donation intentions. *Indonesia Law Review*, 15(2), article number 5. doi: 10.15742/ilrev.v15n2.4.
[20] Ní Aoláin, F. (2024). The rise of counter-terrorism and the demise of human rights. *Emory International Law Review*, 39(1).
[21] Ogbe, R.S. (2023). The dynamics of terrorism and international criminal law. *ABUAD Law Journal*, 11(1), 179-193. doi: 10.53982//alj.2023.1101.08-j.
[22] Okoye, I.E., & Adejoh, P. (2025) Human rights violations in counter-terrorism efforts: A qualitative study of victims experiences in Nigeria. *African Journal of Criminology and Justice Studies*, 14(2), article number 3.
[23] Pék, T. (2022). Overview of the definitions of terrorism in international criminal law. *Hungarian Law Enforcement*, 22(1), 65-78. doi: 10.32577/mr.2022.1.4.
[24] Penal Code No. 574. (1997). Retrieved from https://www.refworld.org/legal/legislation/natlegbod/1997/en/40022.
[25] Resolution of the United Nations Security Council No. 1373. (2001, September). Retrieved from https://undocs.org/S/RES/1373(2001).
[26] Resolution of the United Nations Security Council No. 1566. (2004, October). Retrieved from https://undocs.org/S/RES/1566(2004).
[27] Riduan, I.M. (2024). Unraveling legitimacy: A critical examination of anti-terror legislation in Indonesia. *Religió: Journal of Religious Studies*, 14(1), 22-43. doi: 10.15642/religio.v14i1.2580.
[28] Sagara, A. (2024). *Terrorism: Criminalization, definition of the crime and extension of the ICC's jurisdiction ratione materiae*. Retrieved from https://hal.science/hal-04861606v1/file/Terrorism%20%28F%29.pdf.
[29] Salinas de Frías, A.M., Samuel, K.L.H., & White, N.D. (Eds.). (2012). *Counter-terrorism: International law and practice*. Oxford: Oxford University Press. doi: 10.1093/acprof:oso/9780199608928.001.0001.
[30] Schmid, A.P. (2023). *Defining terrorism*. Retrieved from https://icct.nl/sites/default/files/2023-03/Schmidt%20-%20Defining%20Terrorism_1.pdf.
[31] Sobol, I., Moncrieff, M., & Gaggioli, G. (2023). *Exploring counterterrorism effectiveness and human rights law*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4584358.
[32] Sukabdi, Z.A. (2021). Bridging the gap: Contributions of academics and national security practitioners to counterterrorism in Indonesia. *International Journal of Law, Crime and Justice*, 65, article number 100467. doi: 10.1016/j.ijlcj.2021.100467.
[33] Supreme Court of the Philippines G.R. No. 252578. (2021, December). Retrieved from https://elibrary.judiciary.gov.ph/assets/pdf/philrep/2021/G.R.%20No.%20252578.pdf.
[34] United Nations Office on Drugs and Crime. (2021). *Counter-terrorism legal training curriculum: Module 1 – counter-terrorism in the international law context*. Retrieved from https://www.unodc.org/pdf/terrorism/CTLTC_CT_in_the_Intl_Law_Context_1_Advance_copy.pdf.
[35] United Nations Security Council. (n.d.). Retrieved from https://main.un.org/securitycouncil/en.
[36] Walker, C. (2021). Counterterrorism within the rule of law? Rhetoric and reality with special reference to the United Kingdom. *Terrorism and Political Violence*, 33, 338-352.

ASIAN JOURNAL
of Criminal Justice and Forensic Studies

Volume 1, No. 1
2025

E-mail: info@asianjustice.kz
https://asianjustice.kz/