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.