3 CRIMINAL LAW, CRIMINAL PROCESS
ҚЫЛМЫСТЫҚ ҚҰҚЫҚ, ҚЫЛМЫСТЫҚ ҮРДІС
УГОЛОВНОЕ ПРАВО, УГОЛОВНЫЙ ПРОЦЕСС

IRSTI 10.77.91
UDC 343.985.3
JEL K4, K14

https://doi.org/10.46914/2959-4197-2024-1-4-19-29

DAUBASSOVA SH.S.,*[1]
master of law, senior lecture.
*e-mail: daubassova2017@gmail.com
ORCID ID: 0000-0003-4543-7866
ALAEVA G.T.,[1]
c.l.s., professor.
e-mail: alaevagulnaz@mail.ru
ORCID ID: 0000-0003-1672-2238
DZHUMABAYEVA K.A.,[1]
PhD, associate professor.
e-mail: k.jumabaeva@turan-edu.kz
ORCID ID: 0000-0002-5483-3783
[1]Turan University,
Almaty, Kazakhstan

AI AND CRIMINAL SURVEILLANCE IN KAZAKHSTAN

Abstract

In this study, both application and implications for artificial intelligence are explored within the context of Kazakhstan, a nation that is increasingly adopting artificial intelligence technologies in criminal surveillance to enhance public security. Although AI-driven techniques like facial recognition, predictive policing, and smart city infrastructures present intriguing opportunities for crime prevention and surveillance, they also introduce complex legal and ethical dilemmas. This study seeks to assess the degree of AI integration into Kazakhstan's law enforcement procedures, focusing on the alignment of these technologies with international human rights norms and state legislative safeguards. Following a critical analysis of Kazakhstan's legal framework, significant gaps are uncovered in regulating artificial intelligence surveillance, particularly relating to privacy and transparency. This study utilises global precedents and ethical frameworks to solve existing gaps and provides practical policy recommendations specific to Kazakhstan's unique socio-political context. The findings of this study highlight the need for robust legal safeguards, such as independent oversight bodies and data protection laws, to balance security with civil liberties. By situating Kazakhstan's approach within the broader discourse on AI ethics and surveillance, this study contributes valuable insights into developing AI policies that support both technological advancement and the protection of human rights. The practical significance of this work extends to policymakers, scholars, and human rights advocates aiming to navigate the delicate equilibrium between public safety and personal freedoms in the era of AI-enhanced policing.

Key words: artificial intelligence, surveillance, smart policing, smart cities, facial recognition, human rights, ethics.

Introduction

Artificial Intelligence (AI) is utilised in criminal surveillance. Supporters of the use of AI in criminal investigations claim that it can enhance the efficiency and efficacy of criminal investigations. However, despite the plethora of advantages that AI can bring to criminal investigations, it should not be seen as a panacea. There exists a myriad of legal and ethical considerations surrounding the increasing use of AI in criminal investigation, including bias and discrimination, human rights, and data security and privacy.

In the context of Kazakhstan, the integration of AI in criminal surveillance and criminal investigations holds profound implications for the security, privacy, and civil liberties of citizens. The timeliness of this research is underscored by Kazakhstan's growing application of AI in criminal surveillance. Despite an increase in AI applications for law enforcement in Kazakhstan, research particularly examining the ethical, operational, and societal ramifications of AI-driven criminal monitoring in Kazakhstan is scarce. This article aims to explore the existence of criminal surveillance within Kazakhstan, as well as the legal regulations of it. The article aims to answer the following research questions:

1) To what extent is AI present in criminal investigations in Kazakhstan?

2) What are the legal regulations governing AI in criminal investigations?

It is important to note that no studies have been conducted specifically within the Kazakhstani context. Consequently, this research draws upon studies and findings from other regions, adapting insights where possible to address the unique considerations and potential applications within Kazakhstan.

Materials and methods

A large and growing body of literature has investigated the application of AI in criminal surveillance in other countries. Fontes et al. [1] analysed the ethical and sociological aspects of AI-driven surveillance, underscoring advantages including improved security while stressing substantial privacy issues, biases, and threats to social autonomy. The authors promote rigorous regulatory frameworks, openness, and accountability to reconcile security requirements with ethical considerations in AI surveillance systems.

Huang et al. [2] offer an examination of interdisciplinary strategies for tackling ethical issues in AI, encompassing ethical, technical, and legal perspectives, as well as a review of the methods for analysing AI ethics. The authors declare that the success of AI within society is contingent on the efficacy of ethical AI systems to uphold privacy, freedom and autonomy, and fairness and justice. In another study Pagallo, Quattrocolo [3] explore how AI is reshaping criminal law. The authors contend that AI is revolutionising both substantive criminal law (e.g., definitions of criminality) and procedural law (e.g., case handling), necessitating new frameworks to guarantee that AI-enhanced systems preserve justice and human rights.

The impact of big data, AI, and networking on enhancing urban operations such as transportation, energy, and healthcare are examined by Yin et al. [4]. Their work also addresses obstacles like data security, privacy issues, the digital divide, and the necessity for collaborative governance to effectively implement smart city programs. According to Singh et al. [5], in smart cities, surveillance technologies and AI have connected functions and consequences. However, surveillance technologies are being used to improve public safety and monitor metropolitan areas, raising privacy and civil rights issues. The authors stress the need for transparent surveillance technology rules and ethical frameworks to protect citizens' rights and increase security. AI also analyses massive volumes of data from surveillance systems and other smart city applications to improve urban planning services and predictive analytics. The authors emphasise the need for ethical AI systems that prioritise justice, accountability, and transparency to avoid biases in AI algorithms that might unfairly treat particular populations.

Recent high-profile police brutality instances have raised public scepticism of law enforcement and require a rethinking of policing practices. Maliphol, Hamilton [6] advocate for the allocation of funds towards smart policing initiatives, in hope that they may reduce racial prejudice and increase law enforcement openness and accountability. Ekaabi et al. [7] promote smart policing by emphasising its benefits and the need to monitor and improve service quality. The authors believe technology and data analytics may improve policing efficiency, responsiveness, and community participation.

Conversely, Moon et al. [8] found that members of the public in South Korea believed that privacy infringement was the primary consequence associated with the implementation of smart policing technologies. The authors contend that because of the differing perspectives of the public and police officers on the impact of smart policing technologies, it is essential to evaluate the viewpoints of various stakeholders prior to formulating a research and development plan on policing.

This paper employs a qualitative methodology. More specifically, this paper conducts a critical analysis and policy recommendations based on the landscape, instances, and examples, of international case studies pertaining to the use of facial recognition technologies, Smart Cities, and Smart Policing in Kazakhstan.

Results and discussion

Landscape of Criminal Surveillance in Kazakhstan

Despite concerns regarding the ethical implications of government surveillance and the apprehensions surrounding potential human rights violations, in 2017, Safe City initiatives commenced in Astana. This occurred after the ratification of an agreement between domestic IT businesses and the Kazakh government, with the aim of constructing video surveillance systems capable of utilising facial recognition technologies [9].

Moreover, according to Feldstein [10], facial recognition systems in Kazakhstan are not just employed in Smart Cities but have been further adopted in Smart Policing. This truly highlights the prevalence of AI surveillance technologies within the country. According to Feldstein and the AI and Big Global Surveillance Index, Kazakhstan's three main manifestations of surveillance technologies are facial recognition systems, Smart Cities, and Smart Policing. These technologies are outlined below:

Smart Cities A city that employs information and communications technology to enhance its essential infrastructure and services. These services include energy distribution, education, health, social care, emergencies, and security. Considering the implications for surveillance these cities may be equipped with sensors that communicate up-to-the-minute data to enhance service delivery, municipal management, and public safety. Facial recognition cameras, sensors, and police body cameras are integrated into intelligent command centres to prevent crime, maintain public safety, and promptly address emergencies.

Facial Recognition Systems – Biometric technology that uses cameras to compare recorded or real-time video of persons with photos from databases.

Smart Policing Data-driven analytical technology that makes it easier for law enforcement to conduct investigations and respond to complaints; other systems employ algorithmic analysis to forecast potential crimes.

An advanced AI technology platform, Sergek, plans to install more than 13,000 cutting-edge surveillance cameras throughout the capital, Astana, which will be incorporated into a cohesive surveillance system. The Astana Police Department reported that Sergek discovered 831 thousand instances of traffic infractions from January to November 2018. This technology has the capability to oversee a complete metropolis from a solitary operational centre. Sergek has extended its activities to Almaty and Shymkent, although Astana remains the central hub for the development of Kazakhstan's facial recognition technology. Sergek was utilised to prevent unnecessary trips during the COVID-19 epidemic by determining drivers' residential and workplace locations to assess if they had deviated from their usual routes without valid justification. In addition to Sergek, another Kazakh endeavour to construct a Safe City was initiated in 2018 in the city of Akqol, known as "Smart Akqol." This pilot programme aimed to assess the efficacy of Safe City projects on a smaller scale.

Further plans for expanding surveillance in Kazakhstan can be viewed in the G4 city project, in conjunction with Singapore. Developing initially in the Almaty region, this project will comprise four 'smart' urban areas, with a combined population of 2,200,000 residents and an estimated 1 million plus employment opportunities, anticipated by the year 2050 [11].

The further spread of surveillance technologies in Kazakhstan can be seen with the partnering with the Israeli division of US-based company Verint systems, and NICE systems, located in Israel. These companies have provided Kazakhstan with monitoring centres capable of mass surveillance. These facilities have the capability to intercept large amounts of telephone, mobile, and IP network data. These technologies can enable security and law enforcement carte blanche access to the private communications of any citizen [12].

Furthermore, Kazakhstan has transitioned to e-governance (the digital management of government services and information. Despite supporters for e-governance, and its role in the promotion of transparency, democratisation, and 'good' governance, e-governance in Kazakhstan has also enabled the state to college large volumes of personal data and engage in digital surveillance of Kazakhstani citizens.

According to Kassenova, Duprey [13], concerns regarding digital surveillance, data protection, and privacy within Kazakhstan have been present even prior to the coronavirus outbreak. Human rights advocates have been invested in the situation from the country's increased collaboration with China in 2018 when the Kazakh government initiated its national plan for "Digital Kazakhstan" and other Smart City projects aimed to transform urban environments by using information technology.

Since that time, facial recognition, biometrics, AI, and video surveillance technologies have advanced rapidly within the country, in partnership with firms from the EAEU region, including Russian and Belarusian companies, alongside several Chinese enterprises such as Hikvision and Dahua Technology, which have been sanctioned by the United States for their participation in human rights abuses against Muslim minorities in China. Korkem Telecom is the primary collaborator in enhancing video surveillance systems in five major cities in Kazakhstan, known as Sergek, aimed at diminishing traffic accidents and criminal activities.

National rollout of these surveillance technologies would demand the installation of thousands of surveillance cameras by the year 2022, as outlined in the Ministry of Interior's crime prevention strategy. Furthermore, there are intentions to establish a countrywide biometric identification system and gather fingerprints in 2021. This will result in the most extensive digitisation of the nation's personal data, which must be collected, processed, and securely kept on local servers with adequate protections against unauthorised access and data breaches.

With regard to data protection, there remains uncertainty regarding the individuals or entities authorised to access and oversee the security of the collection, processing, and retention of personal data. The situation deteriorates due to ambiguity surrounding the extent to which state agencies, particularly security services, will respect citizens' rights to protect their personal data. In the context of implementing the National Video Monitoring System, the critical issue is how the government can effectively navigate the delicate balance between preserving individuals' right to privacy and intervening to maintain public order and ensure national security.

Legal Regulation of Criminal Surveillance in Kazakhstan

Kazakhstan, along with 167 other states, has ratified the International Covenant on Civil and Political Rights. This treaty covers various commitments to human rights, and particularly those that are directly linked to communication surveillance. Specifically, the entitlement to privacy (Article 17), as well as the rights that depend on privacy for their fulfilment, such as freedom of expression (Article 19) and freedom of association (Article 22) [14].

As mandated by international law, the constitution of Kazakhstan stipulates that any infringements on rights must be carried out only under authorised authority and under restricted circumstances. The constitutional safeguards are strengthened by domestic criminal laws that prohibit unauthorised monitoring and intervention in certain private communications. According to the Law of the Republic of Kazakhstan, surveillance activities are permitted to safeguard the lives, well-being, possessions, legal entitlements, and interests of individuals involved in the criminal procedure [15].

Article 16 of the Kazakhstan Code of Criminal Procedure entitled 'Privacy of correspondence, telephone conversations, postal, telegraph and other communications' mandates the rights of privacy for Kazakhstani citizens, and that the 'Limitation of this right shall be permitted only in cases and manner directly established by law.' Article 231 'Undercover investigative actions' states that undercover audio and (or) video surveillance of the person or place; and secret surveillance of a person or place may be performed as part of undercover investigative actions. The right withheld by the government of Kazakhstan to use surveillance as part of criminal proceedings is further highlighted in Article 242. Undercover audio and (or) video surveillance of the person or place and Article 248. Secret surveillance of a person or place [16].

Ostensibly, Kazakhstan and its citizens have sufficient human rights protections regarding criminal surveillance and privacy infringements, as ratified unilaterally by international and domestic law. However, despite these purported legal protections that citizens of Kazakhstan benefit from, and the interferences with the right to individual privacy purportedly only occurring within authorised lawful authority, the reality is very different. According to Privacy International (2014), there are inadequacies in Kazakhstan's legislations regarding its obligations to human rights laws. The laws of Kazakhstan do not limit surveillance capabilities beyond what is essential to prevent their arbitrary use. Ex-post warrant procedure monitoring or inspection is not included in the applicable statute, and warrants may be renewed periodically or indefinitely without restrictions on length. The use or disposal of intercepted material or personal data once monitoring has ended is not regulated. No statute defines how to handle secret or privileged information, and no restrictions exist regarding the custody, storage, or access to intercepted content.

Furthermore, there exists no legislation in Kazakhstan that allows or regulates bulk data collection for internet or digital communications, internet filtering or monitoring, or communications data collection, beyond criminal investigation powers. There are also no laws in Kazakhstan that allow or regulate the use of Trojans or hacking tactics. Thus, surveillance by state security or law enforcement authorities outside of targeted criminal investigations is unregulated and violates domestic constitutions and international human rights law. Privacy International found no oversight regime for security services and law enforcement agencies, either within or outside of legislation, based on available materials. This implies that the security services in Kazakhstan may be operating without legal constraints or independent channels for accountability, which is a topic of serious concern.

According to the United States Embassy & Consulate in Kazakhstan [17], both international and local human rights organisations have documented instances of the government monitoring the work of non-governmental organisations on sensitive subjects. This monitoring included harassment tactics such as police visits to NGO offices, surveillance of NGO staff, and even surveillance of their family members.

Furthermore, anonymous communication is subject to government-imposed restrictions. Starting from December 2017, individuals are obligated to authenticate their identity on domestic websites by utilising government-issued digital signature authentication before being able to comment. This lack of anonymity restricts citizens from dissent and criticisms of government policy without anonymity [18].

Case Studies of Implications of Artificial Intelligence in Criminal Surveillance

An increasing number of nations are using sophisticated AI surveillance technologies to observe, trace, and monitor their populations in order to achieve various policy goals. While some of these purposes are legal, some infringe upon human rights, and many fall into a morally ambiguous area. A total of 75 nations out of the 176 countries worldwide are now using AI technology for the specific aim of surveillance. This encompasses Smart City and Safe City initiatives in fifty-six nations, facial recognition systems in sixty-four countries, and Smart Policing in fifty-two countries.

Considering these instances of expanding surveillance, data storage, and the digitalisation of Kazakh governance, it is important to focus on instances of AI proliferation in criminal surveillance in other nations. Below is an overview of international case studies of the three prevalent AI technologies used in Kazakhstan; FRT, Smart Cities, and Smart Policing.

Facial Recognition Technologies

In the United States, the implementation of real-time facial recognition technology has aided the NYPD in achieving its goals by reducing apprehension, improving flexibility, and offering an extra layer of security for underground passengers in New York City [19].

In August 2019, New York law enforcement utilised facial recognition technology to rapidly identify a suspected rapist within twenty-four hours of the alleged incident. The Facial Identification Section employed technology to analyse CCTV video from a nearby grocery shop in conjunction with previous mugshots of the suspect [20].

Real-time facial recognition technology was initially implemented in the United States at the 2001 Super Bowl, screening 100,000 individuals. Nineteen individuals were apprehended due to active arrest warrants. In 2017, the Metropolitan Police in London employed real-time facial recognition technology to monitor attendees at a memorial gathering. The database comprised 50 individuals exhibiting obsessive conduct towards notable figures. While none of the individuals were pursued for previous offences, it was a precautionary move to guarantee safety at significant, high-profile events.

In Australia, authorities have instituted FRTs to address distracted driving. Cameras capture photographs of all passing cars and evaluate these images to detect drivers using mobile phones while operating their vehicles. Should it be established that the motorist is employing a mobile device, categorising them as a "distracted driver," the system will encrypt the image and relay it to the relevant authorities. If the inattentive driver is not recognised, the image will be deleted [20].

Despite these advantages of the application of AI-assisted facial recognition technologies globally, facial recognition technologies present several challenges with privacy, result accuracy, intentional circumvention of real-time facial recognition systems, public confidence, and potential abuse by law enforcement agencies. It also underscores issues related to the acquisition, dissemination, and distribution of personal data obtained by face recognition technology.

In China, there is growing concern over the possible threats to privacy, data security, and social equality posed by the misuse of Facial Recognition Technology. FRT is vulnerable to data security threats because of its dependence on machine-readable information storage systems. The stored face data is appealing to hackers because of its considerable economic value. In 2019, Shenzhen Deepnet Vision Technology Co Ltd suffered a massive data breach, jeopardising the personal information of over 2.5 million persons. The hack led to the exposure of 6.8 million data records, encompassing identity card information and face recognition images. The revelation of such information subjects impacted individuals to several risks, including identity theft and online fraud [21].

Despite significant advancements in facial data analysis, the elevated mistake rate of facial recognition technologies remains a critical concern. This mostly results from the inherent structural limitations of deep learning algorithms, which render them susceptible to spoofing assaults. In 2019, Kneron, a US AI business, tricked Alipay's facial recognition system using a mask produced by 3D printing. The advancement of these cracking techniques by grey market participants may lead to risks such as theft and privacy violations.

In the United Kingdom, numerous regional police forces have encountered significant issues with the accuracy of facial recognition technology. The Metropolitan Police exhibits the lowest accuracy rate, achieving less than 2% in its automatic facial recognition 'matches', with over 98% of these matches erroneously identifying innocent individuals. South Wales Police's accuracy rate is a mere 9%, with an alarming 91% of matches leading to the wrongful identification of innocent individuals [22].

Although there have been advancements in AI and machine learning for facial recognition technologies, algorithms developed in China, Japan, and South Korea exhibit superior competency in identifying East Asian faces relative to Caucasian ones. In contrast, algorithms developed in France, Germany, and the United States have shown enhanced efficacy in recognising Caucasian face characteristics. This suggests that the conditions surrounding an algorithm's creation, particularly the racial diversity of its development team and the datasets of test images utilised, may influence the accuracy of its results [23].

Smart Cities

The potential of Smart City technology to improve government services and foster openness has garnered extensive praise. Sensor technology can provide congestion pricing, hence improving the efficiency of government services. Policymakers may leverage access to big data to improve infrastructure services [24].

Extensive control centres are essential for safeguarding individuals in Smart Cities. These centres aggregate and evaluate data concerning traffic trends, human behaviour, and sensor metrics, including water levels in flood-prone regions. Security is approached from multiple perspectives, encompassing preparedness for emergency responses, traffic management during peak periods, and resource coordination in the event of a disaster or pandemic.

Nonetheless, advancements in Smart Cities present considerable risks, particularly the expansion of surveillance systems. The deployment of Smart City technologies by law enforcement agencies poses the greatest threats to residents' civil liberties and privacy. Smart Cities facilitate a marked increase in surveillance capabilities. The IBM Intelligent Operations Centre in Rio de Janeiro, Brazil, exemplifies the sophisticated technology that enables city officials to observe residents through surveillance cameras and collect behavioural data via sensors. This technology raises profound concerns regarding civil rights and privacy. The primary objective of the IBM Centre is to improve traffic conditions and efficiently manage emergency situations by monitoring a network of sensors and cameras.

Smart Policing

Smart Policing prioritises data and analytics to improve analysis, performance measurement, and research assessment. It is closely related to Smart Cities. Both use technology and data to improve residents' safety, efficiency, and quality of life. Automation surveillance, an element of Smart Policing, uses AI data mining and visual analytics to analyse automated and crowdsourced data for law enforcement purposes, including real-time monitoring.

According to Afzal, Panagiotopoulos [25], there are four key approaches to automated surveillance: sensor alerting, automated pattern recognition, radio-cell analysis, and social mapping.

Sensor alerting utilises video analytics, optical character recognition, and acoustic correlations to provide alerts from CCTV, environmental sensors, automated number plate identification systems, and ShotSpotter systems. The deployment of sensor alerting allowed the Camden Police in New Jersey, USA, to realise a 50% reduction in response times and an overall crime reduction of 40% from 2013 to 2014. From 2015 to 2017, the deployment of sophisticated CCTV systems for traffic enforcement in Shanghai resulted in a significant increase in seat belt compliance, rising from 60.8% to 84.9%.

Automated pattern recognition produces temporal, locational, and route patterns that aid in predicting the future locations of vehicles that are suspected or under observation. The New York police have employed this technology to locate persons who have absconded from court, thwart kidnappings, and capture repeat offenders in the act.

Radio-cell analysis is a technique that employs mobile phone connection data to discover and identify dubious links associated with riots and grave offences such as homicide and abduction. Detectives examine these alleged ties to ascertain parallels with criminal conduct. In the 2011 Dresden riots, German police employed radio-cell analysis to identify and prosecute 379 individuals classified as suspects from a total of 153,622 connections.

Social mapping is the collection and analysis of social media data related to a suspected individual, group, or event within criminal investigations. Data is acquired by human searches, automated searches using web crawlers, legal interception using deep packet inspection, and targeted interception through the installation of a Trojan on a specific device. The data are analysed with various methodologies. An instance is the partnership between the Vancouver Police Department and the Insurance Corporation of British Columbia utilising face recognition technology to identify suspects involved in the 2011 riots.

Implementing Smart Policing tactics may effectively address accountability concerns related to alleged acts of brutality and other abuses by law enforcement. The deployment of body cameras can act as a disincentive for police personnel, dissuading them from participating in actions that may result in allegations of brutality [26].

Although these instances of effective criminal AI monitoring using smart policing exist, they pose substantial concerns regarding privacy rights, anonymity, and civil liberties. Given the extensive revelation of personal and intimate information on social media, alongside the increasing utilisation of this data by law enforcement and intelligence agencies to profile and target individuals, it is crucial to scrutinise the validity of this assumption, both presently and historically. Can the collection and use of personal data without consent or awareness infringe upon an individual's privacy? [27].

The principal challenge in executing such a system is the protection of citizen privacy, given that it necessitates the collecting and processing of citizen data [28]. Moreover, data integrity may be compromised during the processes of data capture and storage, while the variety of ad hoc systems and the necessity to protect citizens' privacy could pose significant obstacles to information sharing at regional, national, and global levels.

Observers and commentators increasingly fear that improvements in information and communication technology may facilitate the emergence of a surveillance state, wherein all aspects of citizens' lives may be meticulously observed and examined. Significant evidence indicates that both state security services and large corporations may extensively employ information and communication technology to gather data on the activities, social connections, and personal habits of ordinary persons. Under the dominion of a totalitarian regime, emerging technologies have considerable potential to facilitate heightened monitoring and oppressive methods.

Members of particular social or ethnic groups may be more likely to be selectively targeted by these systems, especially when their deployment aims at anti-terrorism or de-radicalisation efforts [29]. A high incidence of false positives increases the probability that certain individuals and groups are repeatedly and disproportionately identified as potential criminals, leading to stigmatisation. The deployment of the CAS system in the Netherlands has demonstrated that ethnic profiling by law enforcement is a significant concern, as evidenced by research.

Policy Recommendations

Kazakhstan is a nation characterised by authoritarian policies and remains with the greatest levels of state capacity within Central Asia. Furthermore, the state has announced comprehensive plans to establish statewide facial recognition surveillance systems. According to Yelegen [30], the speed of technological advancements in AI for criminal surveillance are being designed and utilised, far surpasses the speed at which Kazakhstan's regulatory framework oversees them. This requires meticulous consideration from policymakers and decision-makers concerning the deployment of AI. Considering this, below is a list of policy recommendations based on the fair and ethical implementation of AI usage in criminal surveillance in Kazakhstan:

1) Algorithmic Fairness and Bias Testing: Mandate routine evaluations of AI models employed in surveillance to detect and address biases against any group, hence assuring equitable and impartial technology. This is especially true considering the multi-racial demographics of Kazakhstan.

2) Citizen Consent and Transparency: Require that individuals be aware of the extent and use of AI surveillance technology in public areas, including the processing and storage of personal data.

3) Establish Relevant Usage: Restrict AI surveillance data acquisition exclusively to instances with probable cause, guaranteeing that every surveillance is warranted, essential, and minimal.

4) Robust Legal Framework: Establish and implement ethical frameworks to regulate the use of AI in surveillance, ensuring the protection of human rights and equality. Furthermore, ensure that the usage of AI in surveillance adheres to both domestic and international law.

5) Strict Data Security: Establish stringent security protocols to safeguard surveillance data against unauthorised access and breaches, accompanied by frequent audits and upgrades. Furthermore, establish clear guidelines for regular automatic deletion of irrelevant surveillance data.

6) Independent Regulation: Formulate an autonomous oversight body to inspect AI surveillance, assessing data accessibility, privacy adherence, and conformity with ethical standards.

Conclusion

AI in criminal investigations is presently at the nascent phase of implementation in Kazakhstan. The implications of the pervasive application of AI in criminal monitoring in Kazakhstan need to be determined. The widespread use of this technology, without adequate considerations, may result in catastrophic effects for the populace of Kazakhstan and its citizen's human rights.

Implementing AI in criminal surveillance in Kazakhstan necessitates a meticulous equilibrium between augmenting security and preserving citizens' rights to privacy and data protection. The suggested regulations prioritise openness, accountability, and stringent privacy protections to guarantee the ethical and responsible use of AI surveillance technologies. By instituting these recommendations, Kazakhstan may develop a framework that honours individual liberties while using AI's capabilities for public safety. This balanced strategy will cultivate public trust, harmonising AI surveillance tactics with national security objectives and societal ethical norms.

REFERENCES

1 Fontes C., Hohma E., Corrigan C.C., Lütge C. AI-powered public surveillance systems: why we (might) need them and how we want them // Technology in Society. 2022. No. 71(102137). P. 1–12.

2 Huang C., Zhang Z., Mao B., Yao X. An overview of artificial intelligence ethics // IEEE Transactions on Artificial Intelligence. 2022. No. 4(4). P. 799–819.

3 Pagallo U., Quattrocolo S. The impact of AI on criminal law, and its two fold procedures // In Research handbook on the law of artificial intelligence. Edward Elgar Publishing. 2018, pp. 385–409

4 Yin C., Xiong Z., Chen H., Wang J., Cooper D., David B. A literature survey on smart cities // Science China. Information Sciences. 2015. No. 58(10). P. 1–18.

5 Singh T., Solanki A., Sharma S.K., Nayyar A., Paul A. A decade review on smart cities: paradigms, challenges and opportunities // IEEE Access. 2022. No. 10. P. 68319–68364.

6 Maliphol S., Hamilton C. Smart Policing: Ethical Issues & Technology Management of Robocops // In 2022 Portland International Conference on Management of Engineering and Technology (PICMET). 2022, pp. 1–15.

7 Ekaabi M.A., Khalid K., Davidson R., Kamarudin A.H., Preece C. Smart policing service quality: conceptualisation, development and validation // Policing: An International Journal. 2020. No. 43(5). P. 707–721.

8 Moon H., Choi H., Lee J., Lee K.S. Attitudes in Korea toward introducing smart policing technologies: Differences between the general public and police officers // Sustainability. 2017. No. 9(10). P. 1–17.

9 Stryker C. Importing Chinese Surveillance Technology: Are Central Asian States on the Path to Digital Authoritarianism? // Doctoral dissertation. 2022.

10 Feldstein S. AI & Big Data Global Surveillance Index // Data.mendeley.com. 2022. Vol. 4.

11 Shayakhmetova Z. Kazakhstan and Singapore Agreed to Develop Smart Cities in Almaty Region. The Astana Times. 2021. URL: https://astanatimes.com/2021/10/kazakhstan-and-singapore-agreed-to-develop-smart-cities-in-almaty-region/

12 Privacy International. Private Interests: Monitoring Central Asia. Special report. 2014, pp. 1–153.

13 Kassenova N., Duprey B. Digital silk road in Central Asia: Present and future. Davis Center for Russian and Eurasian Studies. 2021.

14 United Nations, International Covenant on Civil and Political Rights. 1966. OHCHR URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights accessed 11 September 2024.

15 On State Protection of Persons, Participating in Criminal Procedure. 2000. URL: On state protection of persons, participating in criminal procedure – “Adilet” LIS

16 Criminal Procedure Code of the Republic of Kazakhstan. 2014. URL: Criminal Procedure Code of the Republic of Kazakhstan – “Adilet” LIS

17 US Embassy & Consulate in Kazakhstan. 2023 Country Reports on Human Rights Practices: Kazakhstan. 2024. URL: https://kz.usembassy.gov/2023-country-reports-on-human-rights-practices-kazakhstan/

18 Freedom House, Kazakhstan: Freedom on the Net 2020 Country Report. 2020. URL: https://freedomhouse.org/country/kazakhstan/freedom-net/2020

19 Carter A.M. Facing reality: The benefits and challenges of facial recognition for the NYPD // Homeland Security Affairs. URL: https://www.hsaj.org/articles/14656#:~:text=Facial%20recognition%20technology%20(FRT)%20is,crimes%2C%20locating%20missing%20persons%2C%20providing

20 McClellan E. Facial recognition technology: balancing the benefits and concerns // J. Bus. & Tech. L. 2019. No. 15(363). P. 363–380.

21 Li Z., Guo Y., Yarime M., Wu X. Policy designs for adaptive governance of disruptive technologies: The case of facial recognition technology (FRT) in China // Policy Design and Practice. 2023. No. 6(1). P. 27–40.

22 Krueckeberg J., Ferris G. Face off: The lawless growth of facial recognition in UK policing. Big Brother watch. 2018.

23 Garvie C., Frankle J. Facial-recognition software might have a racial bias problem // The Atlantic. 2016. No. 7(04).

24 Hamilton E. The Benefits and Risks of Policymakers’ Use of Smart City Technology // Mercatus Center Paper. 2016.

25 Afzal M., Panagiotopoulos P. Smart policing: A critical review of the literature // In Electronic Government: 19th IFIP WG 8.5 International Conference EGOV 2020. Linköping, Sweden. 2020. P. 59–70.

26 Bruce D., Tait S. Challenges and opportunities in implementing smarter policing in South Africa // In A ‘Third Umpire’ for Policing in South Africa: Applying Body Cameras in the Western Cape. Igarape Institute. 2015. P. 19–29.

27 Edwards L., Urquhart L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? // International Journal of Law and Information Technology. 2016. No. 24(3). P. 279–310.

28 Yamin M.M., Shalaginov A., Katt B. Smart policing for a smart world opportunities, challenges and way forward // In Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC). Springer International Publishing. 2020. Vol 1. P. 532–549.

29 Van der Sloot B., Broeders D., Schrijvers E. Exploring the boundaries of Big Data. Amsterdam University Press. 2016.

30 Yelegen A.Y. Обеспечение права человека и гражданина на здоровье в Республике Казахстан в эпоху искусственного интеллекта // Вестник КазНУ. Серия Юридическая. 2023. No. 2(106). С. 14–20.

ДАУБАСОВА С.Ш.,*[1]
з.ғ.м., аға оқытушы.
*e-mail: daubassova2017@gmail.com
ORCID ID: 0000-0003-4543-7866
АЛАЕВА Г.Т.,[1]
з.ғ.к., профессор.
e-mail: alaevagulnaz@mail.ru
ORCID ID: 0000-0003-1672-2238
ДЖУМАБАЕВА К.А.,[1]
PhD, қауымдастырылған профессор.
e-mail: k.jumabaeva@turan-edu.kz
ORCID ID: 0000-0002-5483-3783
[1]«Тұран» университеті,
Алматы қ., Қазақстан

ҚАЗАҚСТАНДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ҚЫЛМЫСТЫҚ ҚУДАЛАУ

Аңдатпа

Бұл зерттеуде қылмыстық қудалауда жасанды интеллекттің қолданылуы мен салдары зерттеледі. Аталған мәселе қоғамдық қауіпсіздікті арттыру үшін жасанды интеллект технологияларын қылмыстық қудалауда жиі қолданып жатқан Қазақстан контекстінде қарастырылған. Бет-әлпетті тану, болжамды полиция және ақылды қала инфрақұрылымдары сияқты жасанды интеллект әдістері қылмыстың алдын алу және қудалау үшін кең мүмкіндіктер ұсынғанымен, бұл әдістер күрделі құқықтық және этикалық дилеммаларды тудырады. Бұл жұмыста аталған әдістерді халықаралық адам құқықтары нормаларымен және мемлекеттік заңнамалық кепілдіктермен сәйкестендіруге баса назар аудара отырып, Қазақстанның құқық қорғау процедураларына жасанды интеллект интеграциясының дәрежесін бағалауға бағытталған. Қазақстанның заңнамалық базасын сыни талдау нәтижесінде жасанды интеллект бақылауын реттеуде, әсіресе құпиялылық пен ашықтыққа қатысты елеулі олқылықтар анықталды. Бұл зерттеуде олқылықтарды шешу үшін жаһандық прецеденттер және этикалық негіздемелер пайдаланады және Қазақстанның бірегей әлеуметтік-саяси контекстіне тән практикалық бағдар бойынша ұсыныстар беріледі. Бұл зерттеудің нәтижелері қауіпсіздікті азаматтық бостандықтармен теңестіру үшін тәуелсіз қадағалау органдары мен деректерді қорғау туралы заңдар сияқты сенімді құқықтық кепілдіктердің қажеттілігін көрсетеді. Қазақстандық көзқарасты жасанды интеллект этикасы мен қадағалауы туралы кеңірек пікірталас аясында орналастыра отырып, бұл зерттеу технологиялық прогресті және адам құқықтарын қорғауды қолдайтын жасанды интеллект саясатын әзірлеуге құнды түсініктер береді. Бұл жұмыстың практикалық маңыздылығы жасанды интеллектпен күшейтілген полиция қызметі дәуірінде қоғамдық қауіпсіздік пен жеке бостандықтар арасындағы нәзік тепе-теңдікті басқаруға ұмтылатын саясаткерлерге, ғалымдарға және адам құқықтарын қорғаушыларға таралады.

Тірек сөздер: жасанды интеллект, қудалау, ақылды полиция, ақылды қалалар, бет-әлпетті тану, адам құқығы, этика.

ДАУБАСОВА С.Ш.,*[1]
м.ю.н., старший преподаватель.
*e-mail: daubassova2017@gmail.com
ORCID ID: 0000-0003-4543-7866
АЛАЕВА Г.Т.,[1]
к.ю.н., профессор.
e-mail: alaevagulnaz@mail.ru
ORCID ID: 0000-0003-1672-2238
ДЖУМАБАЕВА К.А.,[1]
PhD, ассоциированный профессор.
e-mail: k.jumabaeva@turan-edu.kz
ORCID ID: 0000-0002-5483-3783
[1]Университет «Туран»,
г. Алматы, Казахстан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И УГОЛОВНОЕ ПРЕСЛЕДОВАНИЕ В КАЗАХСТАНЕ

Аннотация

В этом исследовании изучаются применение и последствия искусственного интеллекта в контексте Казахстана, страны, которая все чаще внедряет технологии искусственного интеллекта в уголовном преследовании для повышения общественной безопасности. Хотя такие методы на основе ИИ, как распознавание лиц, предиктивная полиция и инфраструктуры умных городов предоставляют широкие возможности для профилактики преступности и при преследовании, они также представляют сложные правовые и этические дилеммы. Данная работа стремится оценить степень интеграции ИИ в процедуры правоохранительных органов Казахстана, уделяя особое внимание согласованию этих технологий с международными нормами в области прав человека и государственными законодательными гарантиями. После критического анализа правовой базы Казахстана были обнаружены значительные пробелы в регулировании уголовного преследования с помощью искусственного интеллекта, особенно в отношении конфиденциальности и прозрачности. В данной работе также рассматриваются мировые прецеденты и этические рамки для устранения существующих пробелов и даны практические рекомендации по данной политике, характерные для уникального социально-политического контекста Казахстана. Результаты этого исследования подчеркивают необходимость надежных правовых гарантий, таких как создание независимых надзорных органов и законов о защите данных, для балансирования безопасности и гражданских свобод. Рассматривая подход Казахстана в рамках более широкого дискурса этики и наблюдения ИИ, это исследование вносит ценные идеи в разработку политики ИИ, которая поддерживает как технологический прогресс, так и защиту прав человека. Практическое значение этой работы распространяется на политиков, ученых и защитников прав человека, стремящихся найти тонкое равновесие между общественной безопасностью и личными свободами в эпоху усиленной ИИ полиции.

Ключевые слова: искусственный интеллект, преследование, умная полиция, умные города, распознавание лиц, права человека, этика.