Kazakhstan Institute
for Strategic Studies
under the President of
the Republic of Kazakhstan

ARTIFICIAL INTELLIGENCE AND DIGITAL TRANSFORMATION OF THE LAW ENFORCEMENT SYSTEM: THE CASE OF THE PROSECUTOR GENERAL'S OFFICE OF KAZAKHSTAN

insightscentral.asia

Kazakhstan Institute
for Strategic Studies
under the President of
the Republic of Kazakhstan

ANALYTICAL REVIEW

ARTIFICIAL INTELLIGENCE AND DIGITAL TRANSFORMATION OF THE LAW ENFORCEMENT SYSTEM: THE CASE OF THE PROSECUTOR GENERAL'S OFFICE OF KAZAKHSTAN

Astana – 2026

UDC 351.74/.75:004.8
LBC 67.71:32.973
A12

Recommended for publication by the Academic Council of Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan

Reviewers:

Zholdybalina A. *– Deputy Director for Domestic Policy at Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan, Doctor of Philosophy (PhD), Associate Professor.*

Dzhunusbekova G. *– Director of the Institute of Applied Research in Public Administration, Digitalization and AI of the Academy of Public Administration under the President of the Republic of Kazakhstan, Candidate of Economic Sciences, Professor.*

Authors:

Abdrashitova A., Zatilla N.

Artificial Intelligence and Digital Transformation of the Law Enforcement System: The Case of the Prosecutor General's Office of Kazakhstan. Artificial Intelligence and Digital Transformation of the Law Enforcement System: The Case of the Prosecutor General's Office of Kazakhstan, 2026. – 48 pp.

ISBN 978-601-12-8513-1

This analytical review is dedicated to analyzing the implementation of digital technologies and AI within the operations of Kazakhstan's law enforcement agencies, with a specific focus on the Prosecutor General's Office.

The work examines the history of integrating IT into the procedural activities of law enforcement. It reviews key digital solutions developed by the Prosecutor General's Office, including Big Data processing technologies for crime forecasting, monitoring citizen appeals, and recidivism prevention. The report explores the potential and practical implementation of predictive analytics and integrated information systems aimed at increasing operational efficiency. Furthermore, it outlines the possibilities of applying specific prosecutorial tools to administrative offenses and within the framework of collaborative efforts with other national law enforcement agencies.

A separate analysis is provided on international practices regarding the digitalization of prosecution services and the broader law enforcement system (e.g., OECD, EU, USA). Challenges and prospects for the digital development of law enforcement agencies are also identified.

The review was prepared using data and official materials from the Kazakh Prosecutor General's Office, as well as international research on digitalization and the application of AI in law enforcement systems. Additionally, state programs and strategic documents were analyzed.

UDC 351.74/.75:004.8
LBC 67.71:32.973

CONTENT

ABBREVIATIONS

AI	Artificial Intelligence
AWS	Automated Workstation
BNS ASPR RK	of National Statistics of Agency for Strategic Planning and Reforms of the Republic of Kazakhstan
CDB	Centralized Data Bank
CLSSA	Committee on Legal Statistics and Special Accounts of the Prosecutor General's Office of the Republic of Kazakhstan
CPC RK	Criminal Procedure Code of the Republic of Kazakhstan
DEMS	Digital Evidence Management Systems
EBSR	Electronic Book of Statement Registration
ECC	Electronic Criminal Case
e-CODEX	Electronic Communication via Online Data Exchange
EDS	Electronic Digital Signature
e-justice	European Electronic Justice Portal
e-Otinish	System for submitting requests and statements to government agencies
EPPO	European Public Prosecutor's Office
EU	European Union
GDPR	General Data Protection Regulation
IS	Information System
IT	Information Technologies
LLM	Large Language Models
MIA RK	Ministry of Internal Affairs of the Republic of Kazakhstan
NLP	Natural Language Processing
OECD	Organisation for Economic Co-operation and Development
PGO RK	Prosecutor General's Office of the Republic of Kazakhstan
RK	Republic of Kazakhstan
UN	United Nations
URAP	Unified Register of Administrative Proceedings
URPI	Unified Register of Pre-trial Investigations
URSOI	Unified Register of Subjects and Objects of Inspections
USA	United States of America
URAP	Unified Register of Administrative Proceedings
URPI	Unified Register of Pre-trial Investigations
URSOI	Unified Register of Subjects and Objects of Inspections

INTRODUCTION

The rapid development of information and communication technologies has fundamentally transformed approaches to the collection, processing, and analysis of Big Data. The mass transition from analog systems to digital data collection has opened new opportunities for deep insight and process optimization across all spheres of human activity.

Digitalization and the subsequent processing of large volumes of data allow for not only the study of current events but also the effective execution of predictive modeling. The integration of AI technologies significantly simplifies these processes, providing precise, data-driven recommendations aimed at improving the quality of life for citizens.

In this regard, the Prosecutor General's Office of the Republic of Kazakhstan (PGO RK) stands as one of the key institutions defining the vector of digital transformation and the implementation of new technologies within the law enforcement sector. Specifically, the Committee on Legal Statistics and Special Accounts of the PGO RK (CLSSA) is undergoing a strategic transformation, guided by the principle: "from the generation of statistics toward the forecasting of threats to public safety."

Over more than a decade, the CLSSA has accumulated a significant body of data in the criminal, civil, and administrative domains, which serves as the fundamental basis for this work. Experience in this field demonstrates that the advancement of AI technologies creates new horizons for the preventive fight against crime.

This analytical review was prepared by Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan. In studying the data, methods and approaches such as comparative and retrospective analysis, periodization, and classification were applied. The primary objective of the review is to present best practices for the application of digital technologies in the law enforcement system of Kazakhstan for their further implementation and adaptation in other sectors.

The findings and recommendations presented in this review are addressed to policymakers, researchers, and stakeholders both within Central Asia and beyond. We hope that this review will serve as a valuable analytical source and provide a foundation for making well-informed decisions regarding digital development and ensuring public safety.

KEY FINDINGS

Chapter 1

- A retrospective view of the digitalization process within Kazakhstan's prosecution authorities reveals a consistent transition from simple document automation to the creation of comprehensive data management ecosystems.
- A pivotal milestone in this transformation was the implementation of the Unified Register of Pre-trial Investigations (URPI). This system facilitated the shift of the criminal process into a digital format, ensuring transparency and eliminating the possibility of reporting manipulation.
- Efficiency assessments indicate that digitalization has not only reduced bureaucratic overhead and shortened investigation timelines but has also transformed the nature of interaction between law enforcement agencies by establishing a unified information space.
- Furthermore, a retrospective analysis confirms that the successful implementation of these technologies was directly dependent on political will and the readiness of the legal and regulatory framework to adapt to technological shifts.
- Ultimately, the initial stage of digitalization laid the foundation for the transition toward utilizing big data analytics and AI components in contemporary supervisory activities.

Chapter 2

- The modern stage of digitalization marks a fundamental transition from the mere recording of offenses to proactive public safety management.
- The implementation of intelligent forecasting models has enabled individualized prevention strategies, achieving a predictive accuracy of 83% for street crime and risks of repeat offenses within pilot regions.
- The use of Natural Language Processing (NLP) in analyzing the e-Otinish system has transformed the handling of citizen appeals, acting as a vital tool for identifying latent social threats and monitoring the social tension map in real-time.
- Digital tools, such as the Digital Assistant and the Prosecutor's Filter, have drastically optimized labor costs—reducing operation times tenfold—while establishing an automated barrier that minimizes operational errors and corruption risks.
- The integration of predictive analytics with scientific-educational environments and IT hubs creates a foundation for scaling AI solutions into adjacent sectors (such as healthcare and land relations), forming a comprehensive framework for preventing systemic risks in public administration.

Chapter 3

- Analysis of international experience indicates that the digitalization of law enforcement systems in OECD, EU, USA and other countries is not merely a standalone IT project, but a comprehensive reform, which encompasses data infrastructure, inter-agency cooperation, procedural frameworks, and analytical tools, including AI.
- The European model is characterized by deepening integration and the formation of supra-national digital infrastructure, which accelerates cross-border cooperation and establishes unified standards for digital interaction across different jurisdictions.
- In the USA, the surging volume of digital evidence (video footage, device data, and cloud services) increases the risk of IT infrastructure overload and procedural failures, such as delays and rising costs, that underscores the critical need for standardized formats, scalable storage solutions, and robust technological support for prosecutorial offices.
- The experience of non-EU countries demonstrates the adoption of proven practices (e-justice, DEMS, partial analytics), though the pace and depth of these reforms remain contingent upon national context, funding, and human resource capabilities.
- Comparative analysis shows that Kazakhstan has developed a highly centralized digital law enforcement ecosystem based on unified registers and integrated platforms. This has ensured end-to-end digitalization of processes, strengthened the supervisory function, and enhanced the overall controllability of the system.
- In a comparative dimension, the Kazakh model is distinguished by a more proactive implementation of AI tools and predictive analytics than most OECD countries and several EU states, that signifies a strategic shift from a reactive response to a proactive model of ensuring legality.
- The further evolution of Kazakhstan's digital model will depend on the ability to balance the efficiency of algorithmic management with institutional resilience and the protection of citizens' rights as the use of intelligent systems continues to expand.

Chapter 4

- The risks associated with digitalization and AI implementation are systemic in nature. These include evidence overload and infrastructural limitations, threats of data breaches and privacy violations, and complexities regarding the admissibility of digital and algorithmically generated evidence. Furthermore, the system faces a deficit of digital competencies, talent attrition ("brain drain"), algorithmic bias, and the dilution of accountability when applying AI.
- The utilization of algorithmic and analytical tools currently outpaces the development of regulatory frameworks, creating an urgent need for the standardization of their application.
- However, these challenges do not constitute grounds for restraining digital transformation. On the contrary, they define a roadmap for institutional, personnel, and regulatory support for digitalization. This roadmap includes the development of a unified justice ecosystem, enhancing the quality of evidence management, accelerating international data exchange, and establishing new roles and standards for AI regulation.

CHAPTER 1. DIGITALIZATION OF THE LAW ENFORCEMENT SYSTEM IN RETROSPECTIVE FOCUS: ASSESSMENT OF EFFECTIVENESS

The integration of digital solutions into Kazakhstan's law enforcement system, encompassing the automation of key processes and the integration of AI tools, transcends standard technical modernization. This process represents a fundamental transformation of the entire public administration architecture within the realm of public order.

The transition to innovative work methods within the PGO RK through digital solutions has shifted the institutional paradigm. Specifically, there is a move from a reactive mode (responding to offenses after they occur) toward a proactive strategy for managing public safety. The PGO RK digital ecosystem covers all critical aspects—from the operational collection and verification of primary data to the automation of investigative stages—thereby ensuring transparency and the optimization of state resources.

The establishment of the PGO RK's modern IS was not a singular event. It has been a multi-year journey of development, achieved through sequential testing and the adaptation of technologies to the realities of the legal landscape. The evolution of departmental platforms is characterized by a transition from the basic digitization of paper archives and reports to the creation of high-tech intelligent IS. These systems are capable of not only accumulating massive datasets but also qualitatively accelerating case review and decision-making processes.

A retrospective focus identifies two primary stages in the establishment of IS within the law enforcement system:

1) 2004-2014 – Building the foundation for digital development;

2) 2015-2025 – Ecosystem-based development of digital solutions.

This chapter analyzes and evaluates the key projects implemented as part of the PGO RK's digital transformation. The study aims to cover the integration of modern IT solutions, ranging from document workflow automation to the implementation of comprehensive analytical platforms.

1.1 Building the Foundation for the Digital Development of the Law Enforcement System (2004–2014)

During the ten-year period from 2004 to 2014, the law enforcement system of the RK evolved from the fragmented automation of individual functions to the creation of a comprehensive digital accounting ecosystem. The primary achievement of this period was a qualitative shift in the paradigm of offense monitoring—specifically, the transition from retrospective data recording on paper media to operational digital control in real-time.

Key results of this stage include the formation of a unified legal and regulatory framework that legitimized the priority of electronic databases over paper registers. The implementation of end-to-end digital accounting significantly reduced the level of latent crime, as the automation of primary registration processes minimized opportunities for statistical manipulation and the concealment of offenses.

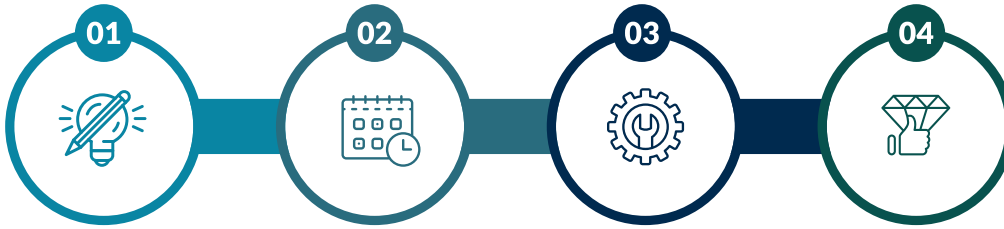
Thus, by 2014, legal statistics had transformed from a passive reporting document into an active tool for prosecutorial oversight and strategic planning.

Institutional Framework and the Initial Steps in Automation

The systematic digital transformation began with the adoption of Government Decree of the Republic of Kazakhstan No. 1374, dated December 24, 2004 [1] . This act approved the "Program for the Development of State Legal Statistics and Special Accounts in the Republic of Kazakhstan for 2005–2007," which officially laid the legal and technological foundation for unifying disparate departmental archives. During that period, law enforcement agencies were in urgent need of eliminating manual data management practices, which created conditions for a lack of transparency in the workflow process.

In 2005, the Criminal Statistics Automated Workstation (AWS) was commissioned. Initially, the solution was hybrid in nature, as databases were populated exclusively based on paper statistical cards filled out manually by investigators. Despite the continued dependence on physical media, the implementation of the AWS allowed for the formation of an ordered data structure available for centralized departmental analysis. However, the system recorded information post-facto, which did not allow for operational control over the progress of investigations.

Figure 1. Criminal Statistics AWS



SOLUTION	LAUNCHED	MAIN FUNCTION	RESULT
Criminal Statistics AWS	2005	Systematization of data based on paper cards.	A centralized data structure has been formed. The dependence on manual input has been retained.

Transition to the Operational Control Model: The EBSR Project

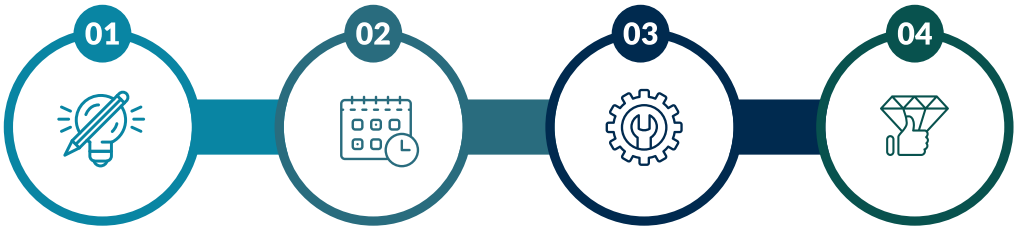
The logical continuation of digital evolution was the launch of the Electronic Book of Statement Registration (EBSR) pilot project in early 2010. This initiative, implemented by the CLSSA in collaboration with the MIA RK, was designed to transition crime registration into the sphere of direct digital monitoring [2].

The fundamental difference of EBSR lay in providing prosecutors and law enforcement leadership with the ability to track the dynamics of appeals daily through automated interfaces [3]. The system reflected critical parameters, including compliance with legally established deadlines, the validity of procedural decisions made, and facts regarding the transfer of cases based on investigative jurisdiction.

The results of implementation in pilot regions (Astana and Pavlodar region) demonstrated the advantage of the digital method. Specifically, during the first 15 days of February 2010, compared to the same period in 2009, 41.2% more decisions to initiate criminal cases were made based on applications registered during those days, including a 67.7% increase in decisions made within 3 days. Overall, under EBSR, more than half of the procedural decisions were made within 3 days, and compared to the same period last year, the number of such decisions increased 2.5 times. As a result, the number of applications for which decisions had not been made decreased by almost half compared to the same period in 2009 [4].

This experience proved the effectiveness of the service model of legal statistics and paved the way for the subsequent implementation of more advanced digital solutions.

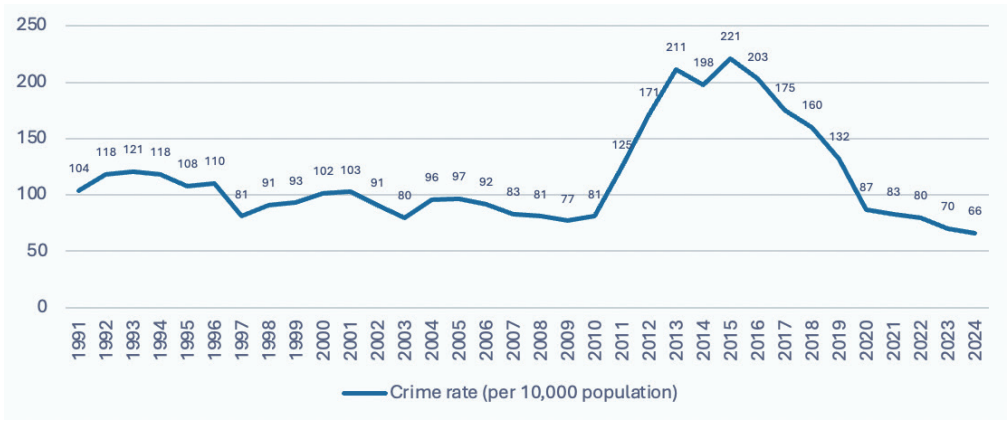
Figure 2. Electronic Book of Statement Registration



SOLUTION	LAUNCHED	MAIN FUNCTION	RESULT
Electronic Book of Statement Registration (EBSR)	2010	Transfer of statement registration to digital format.	Reduced decision-making time. Transparent accounting. Prosecutor's oversight.

The implementation of digital tools in law enforcement provided an immediate effect, manifested in a qualitative change in statistical indicators. The study of statistical data collected through aggregation methods revealed a growth trend in official crime registrations from 2011 to 2015 (Figure 3) [5] . It can be inferred that this phenomenon is not necessarily caused by an actual worsening of the crime situation, but rather by a decrease in latency due to the transparency of electronic record-keeping—specifically, EBSR.

Figure 3. Dynamics of registered crimes per 10,000 population, 1991–2024, based on data from the BNS ASPR RK, 2025



The statistical analysis confirms that the level of registered crime per 10,000 population showed a sharp spike in 2011, increasing more than 1.5 times (from 81 to 125 units) compared to the previous period. Such significant dynamics may attest to the effectiveness of digital solutions, which limited the opportunities for concealing offenses and ensured more comprehensive coverage of criminal acts for the purpose of further planning crime prevention strategies.

Thus, the first stage of digital development established the necessary technological and methodological foundation, proving the effectiveness of transparent digital accounting. This allowed the law enforcement system to transition from simple document digitization to a qualitative transformation of the criminal process, which was most fully realized in the next stage of development. The regulatory consolidation of these processes in 2011–2014 (PGO RK Orders No. 26, No. 83, and No. 80) definitively established the priority of digital data. This allowed for the completion of the foundational stage and the transition to a qualitative transformation of the criminal process based on modern analytical platforms.

1.2 Ecosystem-based development of digital solutions (2015-2025)

The period from 2015 to 2025 was marked by a transition from fragmented automation to the creation of a comprehensive digital ecosystem for the law enforcement sphere—spanning from the registration of an offense to the enforcement of a decision. The primary outcome of this stage was not only a significant reduction in bureaucratic procedures and administrative costs but also the formation of a transparent environment that minimizes corruption risks. The key results of this stage are as follows:

- **Building the digital foundation of the criminal process.** The implementation of the URPI IS and the Electronic Criminal Case module allowed for the complete abandonment of paper registration logs. This ensured transparency in how crimes enter the orbit of justice and eliminated the possibility of unjustified refusals to initiate cases.
- **Ecosystem integration and interdisciplinary coverage.** Within the Digital Kazakhstan program, digitalization expanded beyond the criminal field, encompassing administrative proceedings (URAP), and state control (URSOI). This ensured the consolidation of data based on 33 IS of various state bodies.
- **Reduction of corruption risks through Big Data centralization.** The transition to storing data on CLSSA servers eliminated the risk of local manipulations and the deletion of records regarding fines or inspections, which were characteristic of fragmented infrastructure.
- **Digital protection of public and business interests.** The launch of the URSOI system, the implementation of QR coding for inspection acts, and the introduction of the Qamqor mobile application and the Prosecutor's Filter for entrepreneurs and investors established a reliable mechanism for curbing illegal state interference in entrepreneurial activity.
- **Improvement of executive discipline.** The automation of procedures through e-Otinish led to a 57% decrease in the number of requests and statements processed past their deadlines, achieved through the implementation of transparent monitoring mechanisms.

Unification of Investigations: The Unified Register of Pre-trial Investigations

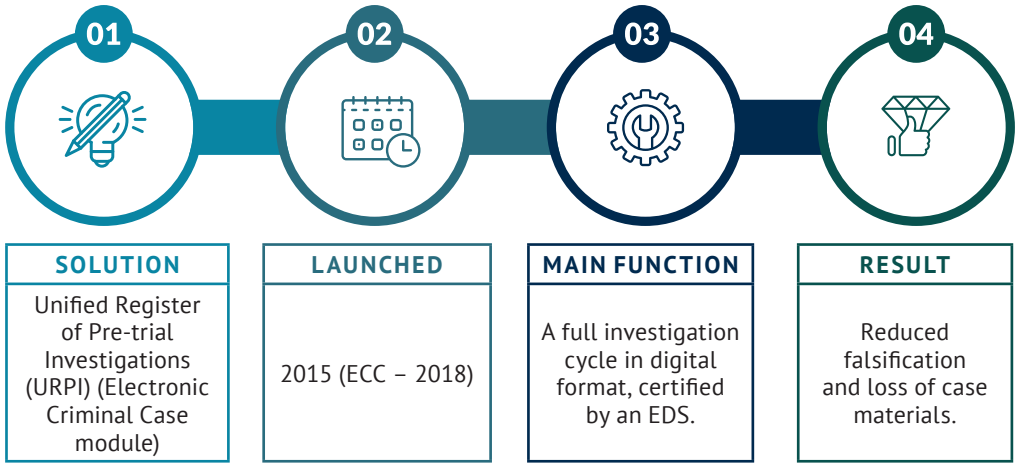
Between 2015 and 2020, digitalization in the law enforcement system evolved beyond mere data recording to become an integral part of criminal, administrative, and civil proceedings. During this period, Kazakhstan transitioned from a strategy of building digital archives to creating comprehensive systems that encompass the full case lifecycle—from the moment an offense is recorded to the final enforcement of the sentence.

The adoption of the new edition of the Criminal Procedure Code of the Republic of Kazakhstan (CPC RK) in 2014 (which came into effect in 2015) served as a pivotal turning point in the digitalization of criminal justice [6] . A key innovation of the code was the legislative consolidation of the ability to conduct proceedings in digital format. Specifically, under Article 42-1 of the CPC RK, criminal justice was transitioned into a hybrid format,

permitting the parallel or exclusive use of electronic forms alongside traditional paper documentation.

A cornerstone of this process was the implementation of the Unified Register of Pre-trial Investigations (URPI) information system. Launched on January 1, 2015, pursuant to PGO Order No. 89 dated September 19, 2014 ("On approval of the Rules for receiving and registering statements, messages, or reports of criminal offenses, as well as maintaining the Unified Register of Pre-trial Investigations") [7], the URPI was introduced simultaneously with the new CPC RK [8]. It became the technological foundation of the new criminal process model.

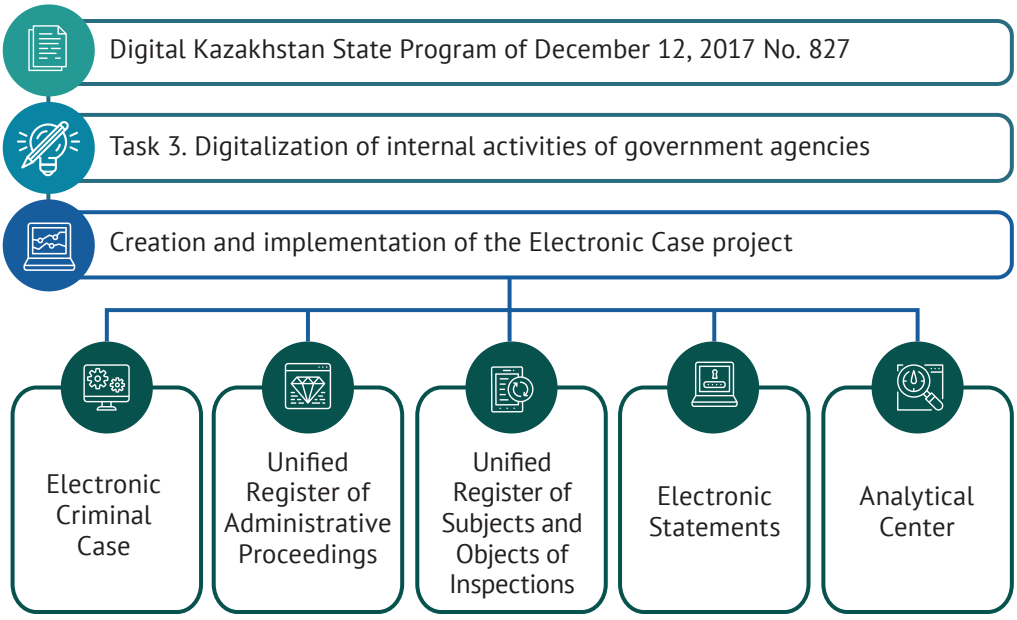
Figure 4. Unified Register of Pre-trial Investigations



In terms of its functionality, this system has completely replaced paper registration logs; that is, from the moment information is entered into the URPI, the case is officially considered initiated. This eliminates the possibility of improper inspections, unjustified refusals to initiate cases, as well as unlawful data manipulation during the investigative stages. Consequently, through the application of digital solutions, transparency has been achieved at the point where crimes "enter" the orbit of justice.

The Digital Kazakhstan State Program, approved in 2017, served as the systemic driver for further changes. The program stated that "to ensure a reliable legal environment and the strict protection of the rights and freedoms of citizens, the interests of legal entities, and the state, a cohesive, global digitalization of this sector is required" [9] . In this regard, the national budget provided for the creation of an operational system for legal statistical information. Specifically, the Electronic Case project was launched, which included the creation and implementation of tools such as the Electronic Criminal Case (ECC), Unified Register of Administrative Proceedings (URAP), Unified Register of Subjects and Objects of Inspections (URSOI), Electronic Statements, and Analytical Center (Figure 5).

Figure 5. The Electronic Case project within the framework of the Digital Kazakhstan State Program



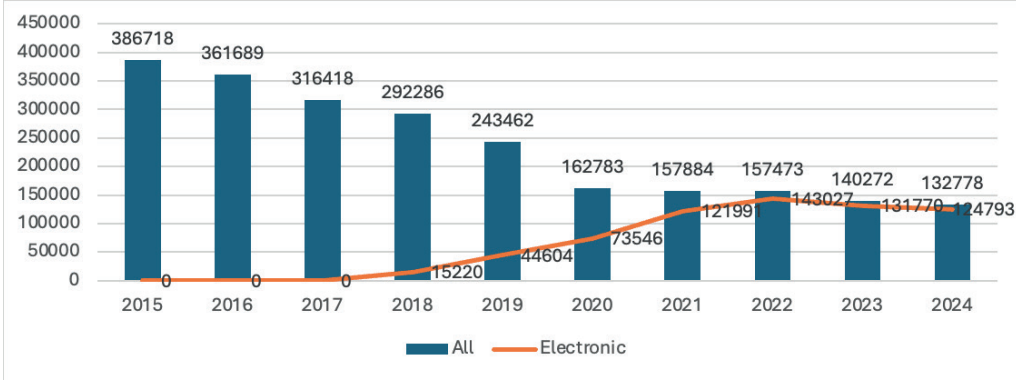
The state program elevated the PGO RK's departmental initiatives to the status of priority national projects, providing the necessary regulatory framework, funding from the national budget, and inter-agency integration.

Specifically, as part of the Digital Kazakhstan State Program in 2017–2018, the ECC module was implemented on the basis of the existing URPI, transitioning the entire investigative process into a digital format.

A defining feature of this system is that the entire body of evidence, protocols, and decrees is generated electronically and verified by an EDS. This comprehensive system was also integrated with government databases, enabling investigators to retrieve information regarding an individual's identity, property, or criminal record within minutes.

Furthermore, a major achievement in the implementation of the ECC was its direct integration with the Torelik Judicial IS, launched in 2016. This ensured the seamless transfer of cases to the court system, eliminating the risk of lost materials or document falsification during physical transit.

Figure 6. Share of criminal investigations in electronic format, 2015–2024, based on data from the CLSSA, 2025.



From Centralized Data Collection to Full Automation: The Unified Register of Administrative Proceedings

The history of the formation and development of the administrative offense accounting system in the RK has followed a path from basic data registration to a full-featured digital ecosystem. The foundation for the creation of the Centralized Data Bank (CDB) on administrative offenses and the persons who committed them was a protocol decision dated September 10, 2003.

At the initial stage, the functionality of the CDB was limited solely to recording the fact of the offense and identifying the subject. However, the objective need for in-depth analysis and systematization of accumulated information led to the introduction of statistical reporting form No. 1-AD in 2010, titled "On the results of the consideration of administrative offense cases by authorized bodies" [10] . This enabled the accumulation of data for the effective monitoring of the entire law enforcement chain.

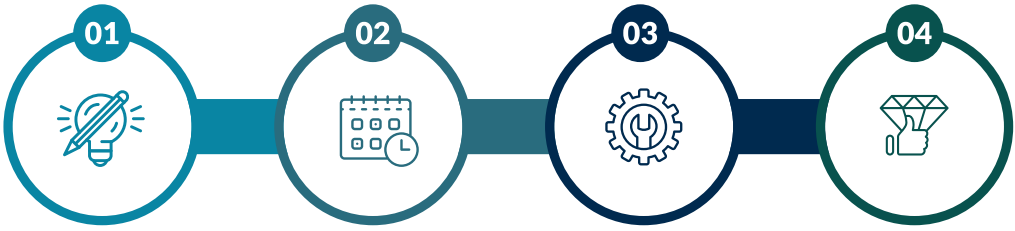
As part of the formation of a unified information space, a branched network infrastructure was built, integrating the CLSSA, its territorial divisions, and nearly all subjects of administrative practice into a shared digital environment. Today, the CDB serves as a fundamental source of verified data, allowing for the tracking of reliable law enforcement dynamics and the formation of an objective picture of the state of legality across the republic.

Thus, the process evolved toward full automation based on the Unified Register of Administrative Proceedings (URAP) IS part of the Digital Kazakhstan State Program. This system provides end-to-end control and tracking of cases at all stages: from the moment of initiation and the drafting of an electronic protocol to the final enforcement of the administrative sanction. Such centralization eliminates data fragmentation and guarantees the transparency of official actions at every stage of the proceedings. Furthermore, integration with photo and video monitoring cameras has made the enforcement process automatic and more transparent.

The technological architecture of the URAP system is represented by three specialized modules:

- Stationary web interface for local workstations;
- Mobile application for tablet devices;
- Centralized Processing Center designed for the automated processing of photo and video monitoring materials.

Figure 7. Unified Register of Administrative Proceedings



SOLUTION	LAUNCHED	MAIN FUNCTION	RESULT
Unified Register of Administrative Proceedings (URAP)	2017	Automation of administrative proceedings from protocol to collection.	Automatic recording of violations. Elimination of localized fine deletion.

The implementation of mobile access to URAP has optimized the process of documenting offenses, providing law enforcement and inspection authorities with the capability for efficient field operations. Currently, the URAP digital ecosystem unites approximately 45,000 verified users from 67 state and local executive bodies, who administer cases in strict accordance with the Kazakh Code of Administrative Offenses.

In its current configuration, URAP provides deep integration with 33 state IS, guaranteeing the instantaneous verification of data regarding vehicles and their owners.

Furthermore, the system's extensive reach is confirmed by the integration of over 6,000 control and measuring instruments and technical devices, the data from which is directly accumulated in the Processing Center. The highest concentration of such devices is recorded in Almaty (1,641), the Atyrau region (1,264), and Astana (750). Statistics attest to the high efficiency of this automation: in 2025, the share of offenses recorded by video monitoring systems accounted

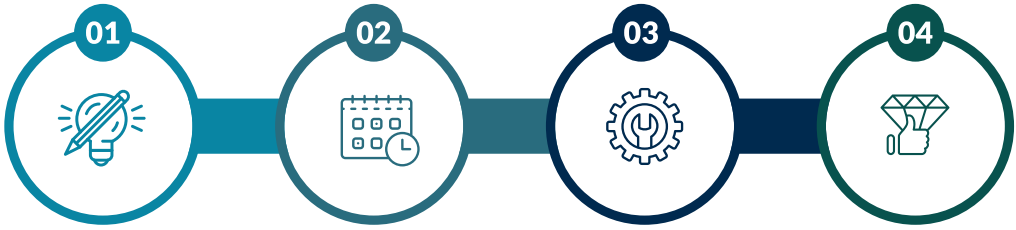
for 63% of the total volume, reaching 11 million proceedings.

The transition to a centralized data storage model based on CLSSA resources has eliminated the systemic flaws of the former fragmented infrastructure. Previously, local server management in the regions created high corruption risks and the possibility of unauthorized deletion of records regarding administrative sanctions, including fines.

Proactive Protection of Entrepreneurs' Rights Against Illegal Inspections: The Unified Register of Subjects and Objects of Inspections

In 2018, as part of the implementation of the Digital Kazakhstan State Program, a qualitatively new technological solution was introduced—the Unified Register of Subjects and Objects of Inspections (URSOI) IS. The implementation of this system for scheduling inspections has become one of the primary tools for protecting business from unjustified interference by regulatory authorities. This has ensured the transparency of state control and oversight, as well as the protection of entrepreneurs' rights [11].

Figure 8. Unified Register of Subjects and Objects of Inspections



SOLUTION	LAUNCHED	MAIN FUNCTION	RESULT
Unified Register of Subjects and Objects of Inspections (URSOI)	2018	Accounting for control and supervisory activities and protection of entrepreneurs' rights.	Reduced number of illegal inspections.

Currently, in the country a complex institutional structure operates comprising 94 types of state control and 17 types of oversight, implemented by 68 state bodies and 20 local executive bodies. The implementation of URSOI has made it possible to systematize this activity by automating the sectoral requirements of circa 600 checklists and 25,000 subjective risk assessment criteria, transforming the system from a simple accounting tool into an analytical platform for detailed legality monitoring.

The system architecture consists of three key components:

- Stationary workstation for administrators;
- Tekseru mobile application for government employees;
- Qamqor application for interacting with businesses.

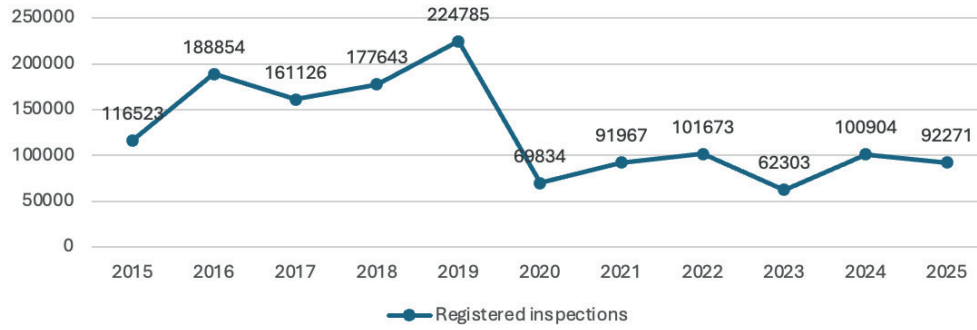
The system's functionality enables the electronic registration of inspection appointment acts, supplementary acts for deadline extensions, and final results. URSOI's intelligent algorithms and built-in Format-Logic Controls (FLC) minimize the possibility of scheduling illegal inspections. The system automatically matches the entrepreneur's category with the control duration and verifies the grounds for the inspection against the agency's competence. A significant technological innovation has been the introduction of the QR coding: acts featuring an electronic seal are generated automatically, relieving inspectors of the need to personally visit CLSSA offices to register documents.

A particular attention in the system's functionality is given to protecting investor rights within the framework of the Prosecutor's Filter mechanism. In accordance with the requirements of the Kazakh Entrepreneurial Code, an integration with the national digital investment platform has been implemented, allowing prosecutors to mandatorily coordinate inspections regarding persons included in the register of investors [12].

Meanwhile, for a wide range of entrepreneurs, the Qamqor application has become a feedback tool, with over 120,000 business entities currently registered as users. The application provides online notifications about upcoming inspector visits, the grounds, and the duration of the control. The presence of a QR code on the act allows for instantaneous verification of the document's authenticity, eliminating corrupt practices.

The results of URSOI's operation demonstrate a significant socio-economic effect and the streamlining of the state control sphere. While 545,000 inspections were registered in 2010, by 2025 this figure had decreased ninefold, totaling 92,000.

Figure 9. Number of registered inspections in 2015–2024, based on CLSSA data, 2025 .



Since the launch of the system, more than 5,000 illegal inspections have been prevented at the registration stage. The current regulatory framework, specifically PGO RK Order No. 162, empowers CLSSA staff to return materials for revision if incompleteness or low-quality graphic copies of the grounds for the inspection are identified [13] .

Thus, URSOI has become the foundation of a digital ecosystem, providing the state with resource savings, businesses with transparent requirements, and society with a guarantee of service quality through publicly open data.

Overall, in conclusion, a retrospective analysis of the digitalization process within the prosecutor's office and law enforcement agencies confirms a profound evolution of the system—from the creation of the first databases in the early 2000s to full-scale digital transformation and the application of state-of-the-art technologies. The performance evaluation of the implemented solutions demonstrates qualitative changes in public administration: a ninefold reduction in the number of unjustified business inspections, and the automation of over 60% of administrative proceedings.

The transition to unified registers has made it possible to eliminate the fragmentation of departmental systems and ensure the reliability of legal statistics. The results achieved confirm that digital transformation has become not merely a technical update, but a strategic tool for protecting the rights of citizens and the interests of business.

This foundation allows for the transition to the next stage of technological development—the integration of AI and predictive analytics. This is not just a technical update, but a fundamental strategic instrument for ensuring legality, transparency, and the protection of the constitutional rights of citizens and businesses in the context of a digital state.

CHAPTER 2.
THE ROLE OF ARTIFICIAL INTELLIGENCE IN CRIME FORECASTING AND ENSURING LAW AND ORDER

Since 2025, the digital paradigm of law enforcement in the RK has undergone a fundamental transformation, shifting its focus from the passive accumulation and recording of statistical data to its intelligent processing for predictive purposes. This stage is characterized by a transition from a reactive mode of responding to already committed offenses to a strategy of proactive public safety management based on AI and Big Data analysis.

In a speech by the President of the RK, K.K. Tokayev, at an expanded meeting of the board of law enforcement agencies on June 23, 2025, it was noted that a key systemic change should be the transformation of the CLSSA into an intelligent think tank [14].

An important element of this architecture is the System for Forecasting Criminal Threats and Public Safety Risks which is being developed. The platform integrates resources from systems such as the URPI, URAP, URSOI, as well as data from external digital platforms.

Today, a specialized Center for Forecasting Criminal Threats and Public Safety Risks is already operational on the basis of the CLSSA, serving as a platform for testing scientific models in real-world practice [15].

Meanwhile, according to global research, the effectiveness of predictive law enforcement directly depends on the ability of algorithms to identify hidden patterns in big data, which is confirmed by systematic reviews of international policing activities [16].

Applied Forecasting Models and Their Effectiveness

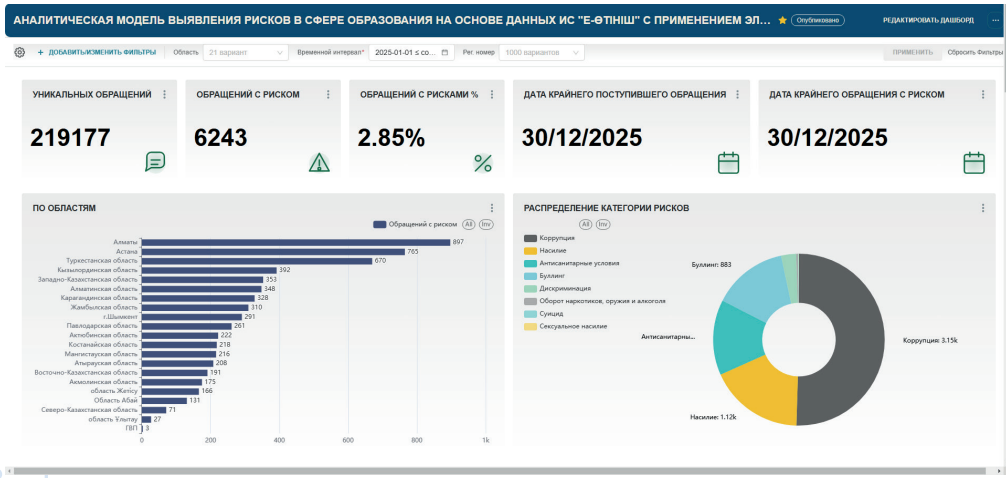
The theoretical basis for risk forecasting in the activities of the prosecutor's office relies on the RNR (Risk-Need-Responsivity) model. This concept involves the individualization of prevention measures based on a deep analysis of risk levels and the specific needs of the offender. The AI algorithms analyze a combination of factors, including administrative history, social status, and discipline in fulfilling financial obligations, which allows for the identification of chains of escalating criminal behavior at early stages. Recent scientific works confirm that intervention based on RNR principles is associated with a significant reduction in recidivism rates, while traditional methods of punishment that do not account for dynamic risk factors prove to be less effective [17].

In the practice of the CLSSA, this analytics functions similarly to preventive medicine: the model does not issue charges but signals the need for timely intervention through social support and education tools. The Kazakh experience demonstrates high effectiveness in the use of comprehensive predictive models. For instance, during the implementation of pilot projects in Astana, Shymkent, and other regions, the accuracy of forecasting street crime and repeat offense risks reached 83%.

The use of Natural Language Processing (NLP) technologies for analyzing citizen requests and statements through the e-Otinish platform holds particular significance in the social well-being monitoring system. Modern models are capable of processing millions of requests within 48 hours—a task that would previously have required colossal human resources over the course of decades. **This approach allows for the identification of hidden social anomalies, such as:**

- Latent bullying in schools;
- Distortion of the essence of systemic problems in the housing and utilities sector;
- Local hotspots of social tension.

Figure 10. Analytical Model for Risk Identification Based on e-Otinish Data



Optimization of Procedural Activities and Oversight Functions

The Digital Assistant intelligent toolkit is radically optimizing the workload of personnel. The automation of audio and video transcription has reduced the time required to draft interrogation protocols from one hour to just three minutes. Minimizing the likelihood of investigative errors is achieved through the autonomous cross-referencing of case materials with current judicial practice. Global reports indicate that the use of AI not only increases productivity by 78% in various government organizations but also helps bridge gaps in personnel competencies [18].

Simultaneously, the Qadagalau IS has been integrated into oversight activities. In this system, the AI autonomously classifies incoming correspondence, determines the nature of the oversight required, and suggests optimal response templates, thereby increasing the speed of prosecutorial response. In administrative practice, this is reflected in the transition to the automatic detection of offenses through cross-system database comparison (for example, identifying the lack of insurance or technical inspections), which eliminates the human factor as a potential source of corruption risks.

The strategic impact of digital solutions on public safety is also evident in the functioning of the Prosecutor's Filter within the URSOI system. This algorithm blocks the scheduling of illegal business inspections at the very stage of electronic act formation. The predictive analytics are also effectively applied in the Information exchange system for law enforcement, special government and other agencies to detect latent offenses and identify hidden relationships between individuals and objects of criminal interest. According to the OECD, utilizing an AI for anticipatory analysis is becoming critically important for agencies seeking to improve the accuracy of threat detection while simultaneously reducing operational costs [19].

Development Perspectives and Integration

The scientific research emphasizes that the creation of a national platform for digital evidence management using AI and blockchain, combined with the implementation of unified cybersecurity standards, could reduce the duration of criminal cases by 20–25%, increase the accuracy of evidence analysis to 90%, and strengthen public trust in the justice system [20].

To further develop the system, the CLSSA is currently collaborating with leading universities of the country to pilot new machine learning models. There are plans to expand NLP models into various other fields to provide prosecutors with timely information regarding systemic failures in local administration. Research in the field of predictive repeat offenses management highlights that optimizing resource allocation and delivering customized interventions significantly reduces crime rates [21]. The AI integration is becoming the foundation for the transition to the next stage of technological sovereignty for the law enforcement system of the Kazakhstan.

In conclusion, it can be stated that the current stage of the development of Kazakhstan's law enforcement system is characterized by the deep integration of digital technologies into the daily activities of the prosecution and investigative bodies. The transition to a predictive public safety management model has not only increased the accuracy

of offense forecasting but has also fostered a new approach to prevention, based on the analysis of individual risks and social anomalies.

The implementation of tools such as the NLP technologies and automated investigative systems ensure a significant reduction in operational costs while simultaneously increasing the transparency of justice.

The strategic significance of these digital solutions lies in the minimization of the human factor and associated corruption risks, directly contributing to the realization of the Just Kazakhstan and Law and Order principles.

Meanwhile, the synergy of state resources, the processing power of the supercomputer, and advanced scientific methodologies creates a stable foundation for the further technological sovereignty of the country. Thus, the digital transformation of the law enforcement sector serves not merely as a process of automating functions, but as a key factor in ensuring national security and social stability within a modern digital state.

CHAPTER 3. INTERNATIONAL EXPERIENCE IN LAW ENFORCEMENT DIGITALIZATION AND COMPARISON WITH KAZAKHSTAN'S PRACTICE

The analysis of international experience shows that in recent years, digital technologies have become one of the key factors in modernizing the law enforcement system. This process is linked to two parallel developments. On the one hand, crime increasingly leaves a digital footprint in the form of communications, transactions, geolocation, and other data from platforms and devices, which form the basis of the evidence base. On the other hand, states strive to increase the efficiency of investigations and case management through electronic case-management systems, data exchange, Big Data analytics, and AI tools.

The digitalization of law enforcement agencies in developed jurisdictions is evolving not as a single IT project, but as a comprehensive reform affecting the data infrastructure and inter-agency cooperation; procedural actions (e-evidence, digital records management, electronic interaction with courts); analytical and algorithmic decision-support tools (including predictive analytics and biometrics).

The experience of the OECD states, European Union (EU) countries, and the USA is most indicative, as digital solutions are already integrated into the daily work of the police and prosecutor's office, and new standards of regulation and oversight are being formed.

It should be noted that several solutions used abroad have been actively implemented and are operational in Kazakhstan. Nevertheless, there are practices that could be adapted to enhance efficiency while simultaneously strengthening the legal and ethical frameworks of digital law enforcement. The most promising approach is not the mechanical copying of individual technologies, but the targeted adaptation of international practices that address future "bottlenecks" in digital development. **These include:**

- Standardized digital evidence management (unified storage rules, chain of custody, and court presentation formats).
- Secure discovery tools (mechanisms for the electronic disclosure of materials to the defense).
- Automated anonymization (redacting personal data during material exchange and the publication of decisions).

- Specialized secure platforms (for inter-agency and inter-regional exchange of evidence and requests).
- Regulatory and ethical AI oversight (mechanisms to ensure transparency and accountability in algorithmic decisions).

Focusing on these areas allows for simultaneously increasing efficiency and maintaining the balance between technological development and the protection of citizens' rights.

Digital Solutions Used in the Law Enforcement Systems

The key types of digital solutions already in use in EU countries, the USA, and other OECD states, which form the modern "justice infrastructure," are as follows:

Transition of record-keeping and workflow into electronic form

This has become one of the fundamental steps of digital transformation in the EU. Prosecution authorities have moved from paper dossiers to electronic cases, which has accelerated the processing of materials and the exchange of information between participants in the process. For these purposes, for example, the Common Platform was implemented in the UK, serving as a unified digital platform for courts, the police, and the prosecution [22]. Over 2.3 million criminal cases are processed on the platform, providing all authorized participants with instant access to up-to-date case information, automating a range of routine operations, and reducing the use of paper documents. The implementation of such a system required a restructuring of processes and staff training; however, ultimately, the unified digital case file accelerated data exchange, reduced the risk of errors, and ensured operational resilience. For instance, access to a case can be obtained from anywhere in the world, even during remote work, which is increasingly penetrating the labor market today.

A similar system operates in Estonia. The country's digital justice ecosystem is based on the central information system e-File, which integrates the databases of the police, prisons, the prosecutor's office, and the courts [23] . All criminal case data is entered into e-File once and is automatically available to all authorized agencies, eliminating duplication and delays. The exchange of procedural documents, filings to court, minutes of hearings, and judicial decisions is carried out exclusively in electronic form through a secure portal accessible 24/7. Through this system, Estonia has achieved some of the fastest judicial proceedings in Europe. The transparency and convenience of interaction have had a positive impact on citizens' trust in justice.

A comparative analysis between these systems and Kazakhstan's practice shows that regarding the transition to electronic criminal cases, Kazakhstan has implemented a digital record-keeping model that is functionally comparable to European countries. In both systems, a full cycle of case support in electronic format, centralized storage of materials, and the legal validity of digital documents are ensured.

At the same time, the institutional emphases of digitalization differ. In EU countries, priority is given to ensuring the interoperability of information systems and developing mechanisms for cross-border interaction between law enforcement and judicial authorities. In Kazakhstan, the main focus is on centralized data management, strengthening supervisory functions, and ensuring vertical integration of the law enforcement system.

Data exchange at the supranational level

The EU countries are actively implementing digital systems to ensure security and data exchange between law enforcement agencies. As far back as 1995, the Schengen Information System (SIS) was launched, which became the foundation for information exchange between police and border services. This IT system allowed participants to register alerts for wanted persons, ensuring a high level of security and cooperation at the supranational level [24].

Subsequently, the EU developed other shared databases. For example, the Prüm agreements initially allowed for the exchange of fingerprints and DNA, while the updated Prüm II mechanism includes the exchange of facial images for automated recognition. Thus, the creation of new large-scale biometric databases in the EU not only strengthens biometric monitoring but also stimulates the broader use of AI in police cooperation.

However, experts fear that expanded data exchange (e.g., facial images) without robust safeguards could lead to the mass processing of personal data without proper protection. They also note that the digitalization of law enforcement can lead to an increase in social tension. This is due to the fact that digital and algorithmic systems operate based on already collected data. Given that data already contains established control practices, new technologies effectively repeat and reinforce previous approaches. Algorithms allow such practices to be applied massively and automatically, which may result in specific population groups or districts being subjected to checks and surveillance more frequently. At the same

time, the decisions themselves become less understandable to citizens, as it is difficult for an individual to understand exactly why they became an object of law enforcement attention. As a result, a sense of injustice and selective control forms within a part of society, which reduces trust in the law enforcement system and can exacerbate social tension.

Nevertheless, digitalization is recognized as strategically important. Therefore, when developing projects, experts recommend that, alongside accelerating cooperation between agencies, the compatibility of this work with human rights requirements be taken into account.

It should be noted that Kazakhstan is developing directions for international cooperation in the field of criminal justice. For instance, on June 18, 2025, the Committee of Ministers of the Council of Europe approved an application initiated by the Prosecutor General's Office of Kazakhstan to join the Council of Europe Convention on Mutual Assistance in Criminal Matters. Participation in this Convention forms the legal basis for more prompt evidence collection, the return of illegally removed assets, and institutionalized interaction with the law enforcement agencies of 46 European states, as well as Israel and South Korea. It is expected that joining this multilateral mechanism will reduce dependence on bilateral agreements and facilitate a transition to a more unified model of international cooperation.

Cross-border solutions to reduce bureaucratic barriers

Separately, it is worth noting the new EU legislative mechanism called the e-Evidence Regulation, adopted in 2023 [25]. This regulatory framework is closely linked to digital platforms and is aimed at reducing bureaucratic obstacles. Statistics show that more than 50% of investigations in the EU require cross-border access to electronic evidence, yet the legacy system is extremely slow. According to Regulation 2023/1543 on European Production Orders for electronic evidence, a unified procedure is introduced that allows the authorities of one EU country to directly request necessary electronic data stored in another country from providers (for example, IT companies).

Previously, this required lengthy mutual legal assistance procedures. However, starting from 2026, providers will be obliged to provide data in response to a European order within 10 days (or 8 hours in emergency cases), regardless of which EU state its servers are located in. The USA is also joining this project.

Digital infrastructure for prosecutors

Efforts are also being made at the supranational level to create a digital infrastructure for prosecutors. One such body is the European Public Prosecutor's Office (EPPO), which began operations in 2021. It was originally built as a fully electronic organization, as, according to EU regulations, all EPPO activities are carried out in a digital environment. For these purposes, its own Case Management System (CMS) was created, linking the central office in Luxembourg with delegated European prosecutors in 22 countries [26].

Such a solution was recognized as critical for increasing efficiency. Without such an electronic system, interaction between states would have practically paralyzed the work of the new body, as it would have been necessary to ensure the transfer of paper materials across 22 countries.

When developing this system, the varying levels of digitalization of national legal systems had to be taken into account, as the penetration of digital technologies and AI varies. The implementation of the

EPPO became a kind of driver, as lagging states strive to accelerate digitalization to integrate into the common European system.

In addition to the EPPO, the European Union Agency for Criminal Justice Cooperation (Eurojust) is active in the EU, having launched the Digital Criminal Justice (DCJ) Programme, aimed at digitalizing cross-border cooperation between prosecutors [27].

As part of the program, Eurojust is developing an updated case management system for itself and national members, as well as the JUDEX secure communication system, through which prosecutor's offices and courts can exchange information and requests for legal assistance directly in electronic form. A secure JITs Collaboration Platform is being developed for Joint Investigation Teams, where prosecutors from different countries belonging to the same group will be able to exchange evidence and coordinate actions online. This mechanism is expected to significantly speed up workflows. It is anticipated that instead of months of waiting for official letters, data will be transmitted almost instantaneously via secure channels. Full commissioning of the system is planned in stages up to 2026-2027.

Electronic evidence system

In the USA, estimates suggest that up to 90% of criminal cases involve digital evidence, which dictates the need for specialized systems to collect, store, analyze, and exchange such evidence [28]. In the absence of such a system, law enforcement agencies face an overload of scattered information. Consequently, many prosecutor's offices in the USA are implementing Digital Evidence Management Systems (DEMS) and transitioning to electronic disclosure of materials to the defense (e-discovery).

The development of technology has led to a literal "explosion" of digital physical evidence in recent years. The proliferation of police body-worn cameras, surveillance cameras, smartphones, and other sensors has resulted in even minor cases being accompanied by thousands of hours of video and terabytes of data [29]. For example, the Denver District Attorney's Office noted a 600% increase in audio and video materials over five years, with even low-level offense cases accumulating up to 1TB of electronic evidence. Such volumes raise issues of reliable storage, rapid searching across datasets, and timely transfer of materials to the defense. Traditional methods (boxes of papers, discs, flash drives) are no longer sufficient. Prosecutors physically lack the time to review all files, and the defense receives access late or in an inconvenient format [30].

In these conditions, there is a risk of judicial errors, where the defense may fail to discover exculpatory information within a mass of files or lack the time to challenge the correctness of data collection, thereby threatening the right to a fair trial. Therefore, experts continue to call for the standardization of electronic evidence formats and for increasing the digital literacy of lawyers so they understand how data is collected and analyzed and can use it effectively.

In response to these data volume challenges, prosecutor's offices have begun using specialized digital platforms for evidence management and information disclosure. The commercial sector has actively joined the search for solutions, offering products that integrate physical evidence storage, material review tools, and secure portals for sharing with defense attorneys. For instance, a number of counties in the USA have implemented cloud-based systems like NICE Justice

or similar platforms, allowing for the entirely electronic receipt, analysis, and transfer of evidence [31]. These platforms allow police to upload video, photos, and documents directly to the cloud, while prosecutors can review and tag materials to generate an electronic "e-discovery" for the defense [32].

While early systems were sometimes inconvenient and unstable, causing frustration among users, the new generation of software focuses on usability and reliability. For example, functions such as bulk file uploading, intelligent content search, and automatic notifications of the receipt and viewing of materials by the defense are already becoming standard. Thus, prosecutor's offices in developed countries are rapidly moving toward a digital cycle for handling evidence. Electronic evidence management is seen as a key element of an effective 21st-century prosecutor's office, without which it is impossible to successfully maintain a prosecution in a digital society.

Digital transformation as a political choice

The analysis of other countries' experiences also leads to the conclusion that the digital transformation of law enforcement is not merely a technical process, but a political choice involving issues of sovereignty, data security, and public trust. For example, the final report of the major research project CUPP (Critical Understanding of Predictive Policing) established that when implementing crime prediction methods in the police forces of Denmark, Norway, Sweden, Estonia, Latvia, and the UK, one of the most significant issues was the choice between in-house development and technology outsourcing [33].

National governments debated what would be more effective and secure: creating digital tools domestically or involving large IT companies. For instance, the police in Denmark and Norway entered into a partnership with the American company Palantir for big data analysis, which sparked a public discussion regarding the political neutrality of such a choice. In Norway, an attempt was made to partially modify the Palantir system using internal resources, which led to complexities and unnecessary expenses. Sweden, by contrast, decided to keep a significant portion of development within the country, although public debate regarding the digitalization of the police there remained limited for a long time.

Comparison of Law Enforcement Digitalization Models in Foreign Countries and Kazakhstan

Summarizing the international experience and Kazakhstan's practice, it is possible to identify the common trends in the development of digital justice that are emerging and to define the specifics of national strategies (Figure 11).

Figure 11. Comparative analysis of approaches in the EU, USA, and OECD countries to the digitalization of law enforcement

CRITERION	EU	USA	OECD COUNTRIES	KAZAKHSTAN
DIGITALIZATION MODEL	Centralized with a focus on unification and supranational standards	Decentralized, dependent on level (federal/ state/county) and budget	A mixed model where national coordination is maintained while maintaining departmental autonomy	A highly centralized ecosystem model based on the CLSSA and unified registries
INSTITUTIONAL POSITION OF THE PROSECUTOR'S OFFICE	The prosecutor's office as part of a unified justice system, facilitating top-down digital modernization	High autonomy of prosecutor's offices, lack of a unified system	From centralized (Great Britain, Japan) to federal (Canada, Australia)	Strong vertical integration of the Prosecutor General's Office in the public administration system
A KEY DRIVER OF DIGITALIZATION	Integration, cross-border interaction, common EU standards	The practical need to process huge volumes of digital evidence	Adaptation of international practices and improvement of efficiency	The need for transparency, reduction of corruption, oversight and prevention
LEVEL OF UNIFICATION	High at the strategic level, but uneven at the national level	Low, as there is a "stratification" between well-equipped and poorly equipped prosecutor's offices	Average, as it depends on the national context and resources	High due to centralization and unified standards
ESSENTIAL DIGITAL TOOLS	Electronic case registers, CMS, e-CODEX, e-Evidence, JUDEX, statistical accounting systems	Case and digital evidence management systems (DEMS), e-discovery, and analytics platforms	Electronic discovery, DEMS, CMS, partial analytics	URPI, ECC, URAP, URSOI, e-Otinish,

 **USE OF AI AND ANALYTICS**	Limited and targeted, primarily for routine tasks	More active (data sorting, risk assessments, document review)	Cautious, focus on auxiliary functions	Active in the form of predictive analytics, NLP, risk models
 **REGULATORY ENVIRONMENT FOR AI**	Formed at the EU level (AI Act)	Lack of a unified law, reliance on courts and professional advice	National regulation, often borrowing from European approaches	Developed within the framework of the digital state strategy
 **INTERNATIONAL COOPERATION**	Institutionalized, supranational (Eurojust, EPPO, JITs, JUDEX)	Through bilateral and multilateral agreements (CLOUD Act, liaison officers)	Participation in international initiatives and exchange of standards	Integration through conventions and international agreements
 **SUPRANATIONAL LEVEL**	EPPO and Eurojust as unique supranational structures	Absent	Absent	Absent
 **KEY ISSUES**	Uneven implementation, caution in using AI	Fragmentation, resource inequality, data overload	Financing, training, legal restrictions	High load on infrastructure, staff shortage in IT
 **GENERAL DEVELOPMENT TRAJECTORY**	Moving towards a paperless, integrated and supranational ecosystem	Pragmatic, bottom-up development focused on practical tasks	Progressive digitalization with the adoption of best practices	Transition to a centralized intelligent management platform

Overall, the data in the table indicate that distinct models for the digitalization of law enforcement have emerged within the jurisdictions under consideration, reflecting their institutional and managerial characteristics:

- **In the EU,** a model centered on institutional integration and supranational coordination dominates. The primary focus is on ensuring the interoperability of IS, developing cross-border platforms, and establishing unified data processing standards. Consequently, such implementations allow for the effective support of international investigations and the unification of procedures. However, they also lead to inconsistencies in implementation at the national level and slow down the scaling of innovative solutions.
- **In the USA,** the digitalization develops primarily according to a decentralized logic, where individual prosecutor's offices and agencies independently determine their technological development priorities, which can be explained by the specific nature of the country's public administration. The key driver is the practical necessity of managing large volumes of digital evidence, which has led to the active adoption of DEMS, e-discovery, and analytical platforms. At the same time, infrastructure fragmentation and uneven resource allocation create significant disparities in the level of digital maturity between states.
- **In OECD countries as a whole,** a mixed model prevails, combining elements of national coordination and departmental autonomy. Digital solutions are implemented progressively, with a focus on adopting international practices and adapting them to the internal context. At the same time, the development of analytical and intelligent tools is cautious and, as a rule, limited to auxiliary functions.
- **Kazakhstan,** by comparison, is characterized by the formation of a highly centralized digital law enforcement ecosystem based on unified registries, integrated platforms, and a vertical data management system. The implementation of the URPI, ECC, URAP, URSOI, and the e-Otinish platform has enabled end-to-end digitalization of key processes and increased the transparency of supervisory activities. Unlike the European model, which focuses on cross-border interoperability, or the US model, which is directed toward local autonomy, the Kazakh approach emphasizes centralization, the prevention of violations, and strengthening the manageability of the system.

The comparative analysis also shows that Kazakhstan demonstrates a more active implementation of AI tools and predictive analytics compared to the majority of OECD countries and several EU states. The use of NLP and complex analytical platforms signifies a transition to a proactive model of ensuring legality. However, such an intensive transition to new technologies leads to an increased load on infrastructure and exacerbates the challenge of staffing in the field of digital competencies.

Based on the analysis of international experience, it can be said that the further development of Kazakhstan's system will depend on the ability to ensure the sustainability of digital infrastructure; develop human capital; maintain a balance between oversight efficiency and the protection of citizens' rights amidst the expansion of algorithmic governance.

CHAPTER 4. CHALLENGES AND PROSPECTS OF DIGITALIZATION AND AI IMPLEMENTATION IN THE LAW ENFORCEMENT SYSTEM

Despite the obvious advantages, digitalization brings a whole series of challenges that prosecutors and legislators must address.

1. Growth of digital data volumes and infrastructural limitations of the prosecution. As noted, prosecution offices now operate with unprecedented volumes of data—from smartphone video recordings to the contents of devices and cloud accounts. According to prosecution representatives, the system is at times "overwhelmed by evidence," which manifests in IT system failures, rising costs for data storage and transmission, and delays in case processing. For instance, in the USA, the general prosecutorial digital evidence storage system implemented in 2015 already requires multiple budget expansions, as the annual volume of stored information continues to grow [34].

Server capacities and cybersecurity are becoming topics that prosecutors—who were previously far removed from IT issues—must now master. Departments with limited budgets suffer particularly. While some cannot afford sufficient cloud storage, others cannot hire technical specialists to maintain the systems. This resource gap can lead to an uneven quality of justice.

Currently, the solution is seen in centralized approaches, where the state invests in shared platforms for all prosecution offices (as seen in several EU countries and Canada through province-wide "cloud hubs") or partnerships are formed with major technology companies. However, the latter raises concerns regarding dependency on a single provider (vendor lock-in) and data security issues.

2. Risks of data leakage and protection of citizens' rights in digital investigations. The digitalization involves the collection and storage of a massive array of personal information (correspondence, footage from private cameras, geolocation, etc.). While acting within the law, prosecutors gain access to this data and must ensure its protection against unauthorized access and leaks. A breach of confidentiality not only undermines public trust but can also lead to evidence being declared inadmissible.

In such situations, rules are being introduced or their scope expanded in several countries to protect data. For example, in the EU, the strict rules of the GDPR (General Data Protection Regulation) also apply to law enforcement. Consequently, every processed piece of digital evidence must have a legal basis,

a defined purpose, and a minimum storage period. Prosecutors must ensure that during data exchange (e.g., providing video recordings to the defense), unnecessary personal information about witnesses, victims, and third parties is not disclosed.

Automated anonymization technologies are used for this purpose. For instance, in Spain, the Ministry of Justice implemented a tool that removes all personal data (names, addresses, numbers) from documents based on set rules so that court decisions can be safely published or shared. In 2025, Croatia introduced the ANON system, integrated into their electronic files, which automatically anonymizes judicial decisions before they are made publicly available [35] . Although these examples are from the courts, the core principle remains: the prosecution also needs tools to redact unnecessary personal information when exchanging digital information.

Another aspect of privacy is the guarantee of citizens' rights during digital surveillance. The prosecutor supervising an investigation must be certain that the data was obtained legally. For example, in the USA, collecting data from a suspect's phone without a warrant will lead to its exclusion from evidence. In the era of big data, prosecutors must maintain a balance and avoid violating constitutional rights in the pursuit of digital clues.

3. Risk of inadmissibility of algorithmically generated evidence. Digital evidence imposes new requirements on traditional rules of evidence law. First, the issue of tampering or altering an electronic file arises. To address this, prosecutors must ensure a rigorous chain of custody, documenting who, when, and how the data was copied, and who had access to it. Experts note that the chain for digital evidence is far more complex and vulnerable than for physical evidence, as it is too easy to copy data without leaving a trace or to accidentally change metadata. Consequently, prosecutors must prove in court that only authorized individuals had access to electronic clues and that copying and analysis were performed using reliable, generally accepted methodologies. If the defense claims a file has been altered, the prosecutor must present an expert to confirm its integrity; otherwise, the court may exclude the evidence.

Second, the volume and form of digital materials cause difficulties for courts and juries. Judges are not accustomed to reviewing thousands of pages of chats or hours of video. For this reason, a prosecutor must be able to structure electronic evidence for presentation (e.g., creating timelines, selections, and printing key fragments). Sometimes, e-courtroom technology is used, where equipped courtrooms display digital evidence on screens, making the process more visual. However, this requires both parties to have equal access to the equipment; otherwise, the principle of equality of arms is violated.

Another problem lies in the forensic examination of software tools. If a prosecutor relies on the results of an AI, the defense may demand the algorithm be disclosed to prove its reliability. However, AI tool manufacturers are often unwilling to reveal trade secrets. In such cases, the court may refuse to accept the materials. Therefore, prosecutors currently try to avoid becoming dependent on opaque algorithms when presenting evidence. Instead, any AI analytics are double-checked using traditional methods before being included in an indictment. Nevertheless, experts argue that in the future, courts will have to adapt their rules by introducing admissibility standards for algorithmic evidence, similar to the standards previously established for DNA analysis.

4. Risk of digital competency deficit in prosecution staff. The digital transformation is impossible without people capable of using it. Prosecutors are, essentially, lawyers with a humanities background; yet they are now required to understand complex technologies. Consequently, there is a growing demand for digital evidence specialists within the prosecution service. Large jurisdictions are already creating positions such as Digital Evidence Prosecutor or establishing entire high-tech crime departments where expertise in cyber-investigations is concentrated. A 2022 study in the USA indicated that a key factor in the successful use of electronic evidence is having at least one prosecutor in the office specializing in digital issues and maintaining strong interaction with technical investigators [36] .

Currently, the solution to the staffing issue involves training existing employees in digital literacy. Courses on handling electronic evidence, cybersecurity basics, and understanding information collection technologies are becoming a necessity. In surveys, approximately 80% of US prosecutors stated they had received some training on digital evidence; however, the majority noted a lack of in-depth knowledge and difficulty accessing advanced training due to time or resource constraints. Training often lags behind the rapid pace of technological development, creating a constant need for knowledge updates. Limited budgets and heavy staff workloads further complicate this task.

5. Risk of algorithmic bias and loss of human accountability in the use of AI. The expanding use of algorithms raises serious ethical questions. One of the primary concerns is bias. If an algorithm assisting a prosecutor is trained on historical data that may contain racial or gender disparities, it can inherit and even amplify existing prejudices. For example, risk assessment systems for recidivism have been criticized for producing higher risk scores for African Americans based on data correlations rather than individual factors.

If a prosecutor were to follow such AI recommendations blindly, it could lead to systemic injustice. Consequently, there is a strict requirement for transparency and explainability in algorithms. A prosecutor must understand the basis on which an AI makes its recommendations and be prepared to justify a decision independently of the algorithm.

Another risk is the erosion of accountability. When AI is involved in decision-making, it is crucial that prosecutors do not shift responsibility onto the technology. For instance, a case prioritization system might suggest which cases are more "promising" for trial. However, legally, decisions that impact a person's fate must be made by a human. To address this, many prosecutorial agencies now explicitly state that the final decision always rests with the prosecutor, and the algorithm remains merely a tool. This aligns with the principles of "Human-in-the-loop" (human control) and "Human accountability".

The lack of a regulatory framework is also a challenge, as legislation often fails to keep pace with technological advancement. Questions frequently arise, such as: "Is it permissible for a prosecutor to use findings from a private algorithm that has not been government-certified?" or "How should privacy be handled if training an algorithm requires using arrays of real criminal case files?" In some countries, specific restrictions are already being implemented. For example, in France, a law was passed prohibiting the analysis of judicial decisions using AI for the purpose of profiling judges, viewing this as a threat to judicial independence. Indirectly, such restrictions could affect the prosecution by banning the use of

big data to predict how a specific judge might rule and tailoring a legal strategy accordingly.

As a result, the ethical use of AI has become a major topic of discussion within the professional community of prosecutors. In 2025, the American Prosecutors Association (APA) at its National Prosecutorial Data Summit discussed how AI and analytics are transforming case processing and emphasized the vital importance of accountability and maintaining fairness [37].

It should be emphasized that these challenges are not grounds for halting digital transformation but, on the contrary, serve as benchmarks for further institutional and regulatory development.

Prospects for the Digital Development of Law Enforcement Agencies

What specific prospects and digital development trends await the prosecution and related law enforcement structures in the coming years? Based on an analysis of international experience, several key directions can be identified. These trends can be implemented in Kazakhstan, taking into account national characteristics and the opportunities for IT sector development.

Formation of a unified digital justice ecosystem.

It is evident that fragmented information systems must give way to integrated platforms uniting the police, prosecution, courts, and potentially prisons into a single data exchange circuit. By 2030, it can be expected that prosecutorial systems in many developed countries will be maximally integrated. Systems must interact seamlessly, following the Estonian model, where data is entered once and is accessible to all relevant agencies. Integration will require both the unification of data standards and the resolution of access issues—for example, ensuring that police see only the authorized parts of a prosecutorial dossier, rather than the entire file. However, this is technically and organizationally feasible, supported by ongoing regulatory changes.

Improving the quality of work with evidence through technology.

The development of AI-powered analytical platforms that help prosecutors analyze data arrays faster and more deeply is a promising direction. Simultaneously, technologies are being developed to guarantee that a file has not been altered since the moment of seizure. Experiments are already being conducted with recording devices that immediately write a data stream with a digital signature, making any subsequent modification detectable. If such technologies become standard, it will be easier for courts to accept electronic evidence without lengthy disputes over its authenticity.

Acceleration and simplification of international information exchange.

Crime is becoming increasingly transboundary, and prosecutors will need to regularly interact with colleagues from other countries in real-time. Therefore, the creation of global or inter-bloc digital gateways for the exchange of legal information is essential. In 2026, the European e-Evidence mechanism is expected to become operational, with the prospect of other non-EU countries joining in the future. Within the EU, active discussions are underway regarding a "European digital evidence repository" for major investigations, where Eurojust and the EPPO could accumulate materials accessible to all participants in a case.

In this regard, Kazakhstan already possesses a developed legal and treaty framework for international cooperation. According to the PGO RK, 82 international

treaties have been concluded with 37 states to date, including 32 agreements on mutual legal assistance in criminal matters, 24 extradition treaties, and 26 agreements on the transfer of convicted persons [38] (see Appendix 1: Map of Kazakhstan's Bilateral Treaties). Looking ahead, the further development of these mechanisms will significantly reduce case processing times and increase the effectiveness of cross-border investigations.

New competencies and management models in the prosecution.

Digital transformation will also change the work culture of prosecutorial organizations. New roles are expected to emerge within the prosecution staff. Interdisciplinary teams may be formed, where a data analyst or programmer works alongside a prosecutor. Prosecution leaders will need to master the principles of change management and IT project management. The exchange of experience and best practices will become part of new management models. We can already see increased activity from international associations, for example, within the framework of the OECD and UN. They host forums on the digitalization of justice where prosecutors share case studies.

Ethical and legal regulation will also change. It is likely that amendments will be made to regulatory legal acts and codes specifically governing digital evidence, algorithms, etc., in order to eliminate legal uncertainties.

A change in the role of the prosecution is not excluded.

With the development of digital services for citizens (online complaint portals, legal information portals), the prosecution will be able to supervise the protection of rights more effectively and respond to requests and statements online. Already, in some jurisdictions, online platforms have been launched for businesses or citizens to submit complaints to the prosecutor's office, which allows for faster identification of violations. In the future, by integrating this data with analytics, the prosecution can operate more proactively, anticipating problem areas.

CONCLUSION

The digital transformation of Kazakhstan's law enforcement system, initiated and implemented by the Prosecutor General's Office, represents a profound evolution—moving from simple automation of paper-based records to the creation of an intelligent ecosystem for proactive public safety management. A retrospective analysis confirms that this journey, which began in the mid-2000s with initial data systematization via the Criminal Statistics workstation and EBSR, successfully eradicated crime latency and established a transparent foundation for subsequent reforms. A pivotal milestone was the implementation of fundamental systems such as URPI, URAP, and UNSOI. These systems not only ensured full coverage of offenses but also minimized corruption risks by eliminating the possibility of unauthorized data manipulation. These solutions have yielded significant practical results, including a reduction in unjustified business inspections and the automation of most administrative proceedings.

At the current stage, starting from 2025, the development vector has shifted toward the implementation of AI technologies and Big Data analytics. The risk forecasting and early detection system which beig developed and the Center for Criminal Threat Forecasting allow the CLSSO to transform into an intellectual "think tank" capable of identifying hidden patterns and preventing the escalation of criminal behavior at early stages. The use of predictive models based on RNR (Risk-Need-Responsivity) principles has already demonstrated a high predictive accuracy of 83%. This allows the state to operate similarly to "preventive medicine," where timely social support measures are applied instead of relying solely on punitive instruments.

Future prospects for digitalization are linked to scaling intellectual tools—such as Natural Language Processing (NLP) for analyzing appeals in the e-Otinish system and the Digital Assistant—into new areas of public administration. The integration of predictive analytics with the country's scientific and educational potential lays the groundwork for transitioning to the highest stage of technological development. Ultimately, the digital transformation of the country's law enforcement system represents the protection of the interests of citizens and the state in the digital age.

International experience shows that electronic case management systems, digital evidence repositories, secure communication platforms, and the prudent use of AI can significantly enhance the effectiveness of prosecutors. These tools accelerate investigations, improve crime clearance rates, and facilitate cooperation with other agencies and countries. At the same time, the implementation of technology highlights new risks and requirements, such as the need to protect

data and citizens' rights, adapt legislation, develop personnel skills, and maintain rigorous oversight of algorithmic usage.

A comparison of practices in the EU, USA, and OECD shows that, despite their differences, all are united by the pursuit of a balance between innovation and legality. Europe implements digital solutions while simultaneously establishing robust human rights guarantees. The USA rapidly adapts technologies to its needs but faces challenges in scaling and ensuring equal access. Other developed nations adopt best practices while seeking their own optimal models.

Key challenges related to data, privacy, admissibility, human resources, and ethics are already recognized by the prosecutorial community. Today, these issues are being addressed through the development of international guidelines, training programs, technical standards, and legal norms. Political will and resource investment remain critical.

In the future, a high-tech law enforcement system will emerge where national borders are no longer an obstacle to justice, and the routine of investigations and processes will be largely automated. However, the role of the prosecutor as the guarantor of legality and justice must remain steadfast. Technologies should serve to strengthen this role. With the right approach, digitalization can render the work of the prosecution more transparent, efficient, and oriented toward protecting the rights of citizens in the modern digital world.

ACKNOWLEDGEMENT

We extend our sincere gratitude to the Prosecutor General's Office of the Republic of Kazakhstan, and specifically the Committee on Legal Statistics and Special Accounts (CLSSA), for their invaluable contribution to this publication. Their provision of comprehensive data and professional insights was fundamental to the accuracy of this analytical review.

REFERENCES

1. Об утверждении Программы развития государственной правовой статистики и специальных учетов в Республике Казахстан на 2005–2007 годы: постановление Правительства Республики Казахстан от 24 дек. 2004 г. № 1374. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/P040001374_
2. Информация о пилотном проекте электронной книги учета заявлений (КУЗ).[Electronic resource] – Access: https://prg.kz/document/?doc_id=30573550&pos=7;246
3. Правоохранительные органы полностью перешли на электронную регистрацию заявлений граждан. [Electronic resource] – Access: https://prg.kz/document/?doc_id=30838856&pos=5;156
4. Ibid.
5. Правонарушения в Республике Казахстан: динамические таблицы за 1991–2024 гг. / Бюро национальной статистики АСПиР РК. [Electronic resource] – Access: https://stat.gov.kz/ru/industries/social-statistics/stat-crime/dynamic-tables/
6. Уголовно-процессуальный кодекс Республики Казахстан / zakon.uchet.kz. [Electronic resource] – Access: https://zakon.uchet.kz/rus/docs/Z970000206
7. Приказ Генерального Прокурора Республики Казахстан от 19 сентября 2014 г. № 89 «Об утверждении Правил приёма и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» / adilet.zan.kz. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/V14W0009744
8. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V ЗРК / adilet.zan.kz. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/K1400000231
9. Постановление Правительства Республики Казахстан от 12 декабря 2017 г. № 827 «Об утверждении Государственной программы "Цифровой Казахстан"» / adilet.zan.kz. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/P1700000827
10. Приказ Генерального прокурора Республики Казахстан «Об утверждении отчёта формы № 1-АД "О результатах …"» (утратил силу) / adilet.zan.kz. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/V1200008047
11. Показатели правовой статистики (ERSOP) / qamqor.gov.kz. [Electronic resource] – Access: https://qamqor.gov.kz/crimestat/indicators/ersop
12. Предпринимательский кодекс Республики Казахстан от 29 октября 2015 г. № 375-V ЗРК (с изменениями и дополнениями) / adilet.zan.kz. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/K1500000375
13. Приказ и. о. Генерального прокурора Республики Казахстан от 25 декабря 2020 г. № 162 «Об утверждении Правил регистрации актов о назначении, …» / adilet.zan.kz. [Electronic resource] – Access: https://adilet.zan.kz/rus/docs/V2000021964
14. Официальный сайт Президента РК. Выступление Касым-Жомарта Токаева на заседании Расширенной коллегии правоохранительных органов. [Electronic resource] – Access: https://akorda.kz/ru/vystuplenie-prezidenta-kasym-zhomarta-tokaeva-na-zasedanii-rasshirennoy-kollegii-pravoohranitelnyh-organov-235114

15. В Астане запускают Центр прогнозирования преступных угроз. [Electronic resource] – Access: https://dknews.kz/ru/v-strane/368239-v-astane-zapuskayut-centr-prognozirovaniya-prestupnyh

16. Lum C., Koper C.S., Wu X. Big Data and Police Effectiveness: A Systematic Review. // Journal of Experimental Criminology. 2024. [Electronic resource] – Access: https://www.tandfonline.com/doi/full/10.1080/24751979.2024.2371781.

17. Andrews D.A., Bonta J. The Risk-Need-Responsivity (RNR) Model: Does Adding the Good Lives Model Contribute to Effective Crime Prevention? // Criminal Justice and Behavior. [Electronic resource] – Access: https://www.researchgate.net/publication/254082762.

18. Stanford Institute for Human-Centered AI. AI Index 2025 Report. [Electronic resource] – Access: https://hai.stanford.edu/ai-index/2025-ai-index-report.

19. OECD. Governing with Artificial Intelligence: AI in Law Enforcement and Disaster Risk Management. 2024. [Electronic resource] – Access: https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html.

20. Akhmetov A. Prosecutorial Effectiveness in Kazakhstan's Criminal Justice: The Role of Digital Forensics and Online Trial Broadcasting. // ResearchGate. 2024. [Electronic resource] – Access: https://www.researchgate.net/publication/394956118.

21. Rochester Institute of Technology. Predictive Management of Recidivism: Resource Optimization. [Electronic resource] – Access: https://repository.rit.edu/cgi/viewcontent.cgi?article=13293&context=theses.

22. Common Platform: a modern digital case management system for the criminal justice system [Electronic resource] // GOV.UK. – Access: https://www.gov.uk/government/case-studies/common-platform-a-modern-digital-case-management-system-for-the-criminal-justice-system

23. e-Governance in Estonia: 100% Digital, 100% Trusted [Electronic resource] // e-Estonia. – Access: https://e-estonia.com/solutions/e-governance/justice-public-safety/

24. The Future of Digitalisation in EU Law Enforcement: Enhanced Exchanges of Personal Data, Privatisation and Algorithmisation [Electronic resource] // European Papers. – Access: https://www.europeanpapers.eu/e-journal/future-digitalisation-eu-law-enforcement-enhanced-exchanges-personal-data-privatisation-algorithmisation

25. EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations [Electronic resource] // White & Case. – Access https://www.whitecase.com/insight-alert/eu-breaks-down-digital-borders-new-e-evidence-rules-facilitate-cross-border

26. EPPO and Digital Challenges [Electronic resource] // eucrim. – Access: https://eucrim.eu/articles/eppo-and-digital-challenges/

27. Digital Criminal Justice Programme [Electronic resource] // Eurojust. – Access: https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice-programme

28. A survey of prosecutors and investigators using digital evidence: A starting point [Electronic resource] / PMC. – Access: https://pmc.ncbi.nlm.nih.gov/articles/PMC10311201/

29. Way too much body camera footage: police, prosecutors and defense attorneys struggle with loads of digital evidence [Electronic resource] // Colorado Public Radio. – Access: https://www.cpr.org/2026/01/02/overwhelming-digital-evidence-body-cam-footage/

30. Current Volume of Digital Evidence Challenge the Criminal Justice System to Do Better [Electronic resource] // Criminal Legal News. – Access: https://www.criminallegalnews.org/news/2023/aug/1/current-volume-digital-evidence-challenge-criminal-justice-system-do-better/

31. Allegheny County District Attorney's Office to Deploy NICE AI-Powered Digital Evidence Management Solution [Electronic resource] // Allegheny County District Attorney's Office. – Access: https://alleghenycountyda.us/allegheny-county-district-attorneys-office-to-deploy-nice-ai-powered-digital-evidence-management-solution/

32. eDiscovery for Prosecutors and Defense Teams: How CivicDocs Enhances the Discovery Process [Electronic resource] // CivicEye. – Access: https://www.civiceye.com/ediscovery-for-prosecutors-and-defense-teams-how-civicdocs-enhances-the-discovery-process/

33. The digitalisation of the police is not neutral, but political. [Electronic resource] // Access: https://www.nordforsk.org/news/digitalisation-police-not-neutral-political#:~:text=Furthermore%2C%20the%20new%20digital%20technologies,Latvia%2C%20and%20the%20United%20Kingdom

34. Way too much body camera footage: police, prosecutors and defense attorneys struggle with loads of digital evidence [Electronic resource] // Colorado Public Radio (CPR). – Access: https://www.cpr.org/2026/01/02/overwhelming-digital-evidence-body-cam-footage/

35. Governing with Artificial Intelligence. The State of Play and Way Forward in Core Government Functions [Electronic resource] / OECD. – Access: https://www.oecd.org/en/publications/2025/06/governing-with-artificial-intelligence_398fa287/full-report/ai-in-justice-administration-and-access-to-justice_f0cbe651.html

36. A survey of prosecutors and investigators using digital evidence: A starting point [Electronic resource] / PMC (PubMed Central). – Access: https://pmc.ncbi.nlm.nih.gov/articles/PMC10311201/

37. AI and Technology [Electronic resource] // American Prosecutors Association (APA). – Access: https://www.apainc.org/ai-and-technology/

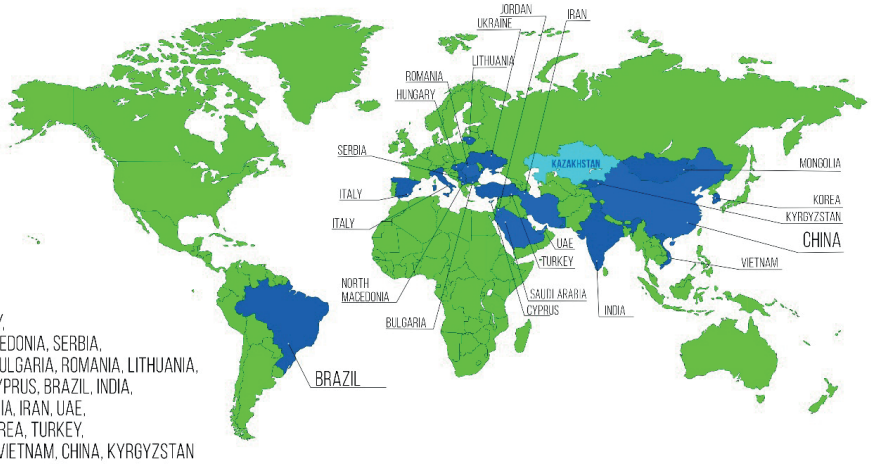
38. Информация о международных договорах в сфере уголовного судопроизводства [Electronic resource] // Официальный интернет-ресурс Генеральной прокуратуры Республики Казахстан. – Access: https://www.gov.kz/memleket/entities/prokuror/documents/details/859154?lang=ru

39. The map of bilateral treaties was developed by the Prosecutor General's Office of the RK: https://www.gov.kz/memleket/entities/prokuror/documents/details/471614?lang=ru

APPENDIX 1.

MAP OF BILATERAL TREATIES OF KAZAKHSTAN [39]

TREATIES ON EXTRADITION (22 COUNTRIES)



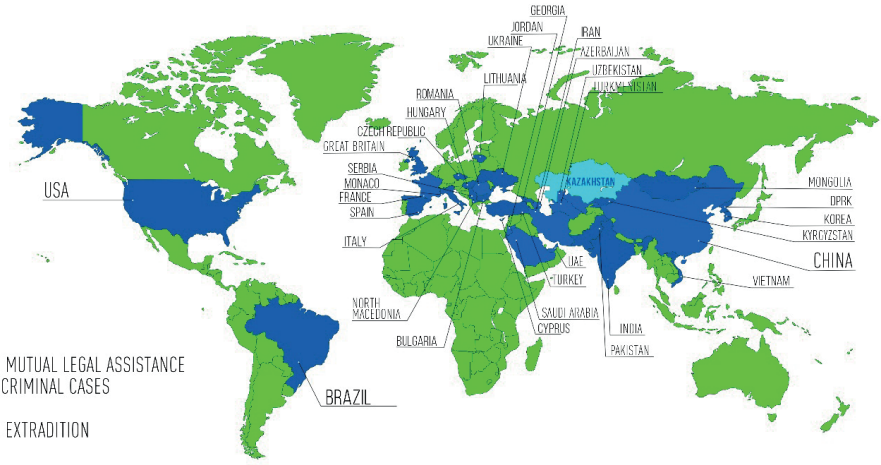
SPAIN, ITALY,
NORTH MACEDONIA, SERBIA,
HUNGARY, BULGARIA, ROMANIA, LITHUANIA,
UKRAINE, CYPRUS, BRAZIL, INDIA,
SAUDI ARABIA, IRAN, UAE,
JORDAN, KOREA, TURKEY,
MONGOLIA, VIETNAM, CHINA, KYRGYZSTAN

TREATMENT ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL CASES (29 COUNTRIES)

MONACO, CZECH REPUBLIC, SPAIN,
ITALY, NORTH MACEDONIA,
SERBIA, GREAT BRITAIN, HUNGARY,
BULGARIA, ROMANIA, LITHUANIA, GEORGIA,
UKRAINE, FRANCE, TURKEY, CYPRUS, USA,
BRAZIL, INDIA, PAKISTAN, UAE,
JORDAN, KOREA, DPRK,
MONGOLIA, VIETNAM, CHINA,
KYRGYZSTAN, UZBEKISTAN

MAP OF CONCLUDING BILATERAL AGREEMENTS WITH COUNTRIES IN THE CRIMINAL LAW SPHERE

KAZAKHSTAN SIGNED 72 TREATIES WITH 34 COUNTRIES

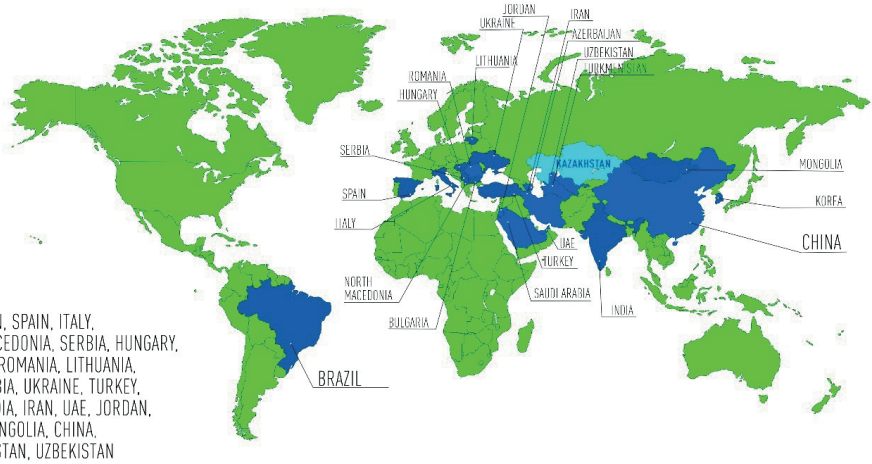


29 ON MUTUAL LEGAL ASSISTANCE IN CRIMINAL CASES

21 ON EXTRADITION

22 ON THE TRANSFER OF SENTENCED PERSONS

TREATIES ON THE TRANSFER OF SENTENCED PERSONS (22 COUNTRIES)



AZERBAIJAN, SPAIN, ITALY, NORTH MACEDONIA, SERBIA, HUNGARY, BULGARIA, ROMANIA, LITHUANIA, SAUDI ARABIA, UKRAINE, TURKEY, BRAZIL, INDIA, IRAN, UAE, JORDAN, KOREA, MONGOLIA, CHINA, TURKMENISTAN, UZBEKISTAN

ANALYTICAL REVIEW

ARTIFICIAL INTELLIGENCE AND DIGITAL TRANSFORMATION OF THE LAW ENFORCEMENT SYSTEM: THE CASE OF THE PROSECUTOR GENERAL'S OFFICE OF KAZAKHSTAN

Design and layout: Subbotina V.

Format 165x238
Digital printing. 25 printed sheets
Circulation: 100 copies

Kazakhstan Institute for Strategic Studies
under the President of the Republic of Kazakhstan
010000, Astana, Beybitshilik Street, 4

Produced by the public association «Development of Entrepreneurship»