IRSTI 10.79.35; 10.79.91 https://doi.org/10.26577/JAPJ2025116411

A. Tolybayeva[1*], A. Issayeva[2], Sh. Zhumagulova, E. Ashimova[3], D.U. Baitukayeva[4]

[1]M. Yesbulatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Almaty, Kazakhstan
[2]Korkyt Ata Kyzylorda University, Kyzylorda, Kazakhstan
[3] L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[4]Al-Farabi Kazakh National University, Almaty, Kazakhstan
*e-mail: a.tolybaeva95@mail.ru

PROBLEMS OF ELECTRONIC CRIMINAL PROCEDURE IN KAZAKHSTAN AND COMPARATIVE ANALYSIS OF FOREIGN DIGITAL INVESTIGATION MODELS

The digitalization of criminal procedure has become a key vector in the modernization of law enforcement systems. The use of ICT accelerates pre-trial investigations and enhances data-processing accuracy. In the Republic of Kazakhstan, the basic infrastructure for electronic criminal procedure, including online services, has already been established; however, existing regulations and the practical functioning of electronic systems reveal systemic limitations that impede the development of a fully integrated digital investigation model. The purpose of this study is to provide a comprehensive assessment of the current state and prospects for the development of electronic criminal procedure in Kazakhstan. The research includes identifying regulatory and practical challenges, analysing conflicts between the Criminal Procedure Code of the Republic of Kazakhstan and subordinate acts, conducting a comparative review of foreign models (CMS, e-File, eDiscovery), and formulating proposals for adapting effective international practices.

The methodological framework relies on legislative analysis, an assessment of digital infrastructure, and the study of international experience. Systematization and comparative legal methods were applied, enabling the identification of seven key issues affecting the effectiveness of electronic investigations.

The analysis revealed the absence of clear ICT procedural regulations, inconsistencies between the CPC and the Prosecutor General's Order No. 2, weak integration of the "E-QI" and "Qamqor" systems with the databases of the Committee on Legal Statistics, and the lack of a defined liability mechanism for breaches of confidentiality in the "Jaria Sector." Additional gaps were identified in the regulation of remote investigative actions, the handling of physical evidence, and the determination of criteria limiting the use of electronic formats. The scholarly value lies in formulating a systemic conceptual framework based on the identification of seven structural barriers. This integrated approach, combining legal, technological, and organizational dimensions, fills a methodological gap in national academic discourse.

The practical significance is reflected in the proposed solutions designed for implementation in regulatory and technological environments: unifying the regulatory framework (a supplementary CPC chapter), establishing an integration bus and Data Hub, introducing a QR-based evidence management module, and creating a liability mechanism for confidentiality breaches within the "Jaria Sector." These measures are expected to enhance investigative efficiency and support the development of a full-fledged electronic ecosystem for criminal procedure in Kazakhstan.

Keywords: electronic criminal procedure, digital pre-trial investigation, chain of custody, information system integration.

А.А. Толыбаева*[1], А.Ж.Исаева[2], Ш.Р. Жумагулова[2],
Э. Ашимова[3], Д.У. Байтукаева[4]

[1]Қазақстан Республикасы Ішкі Істер Министрлігінің М. Есболатов атындағы Алматы академиясы, Алматы, Қазақстан
[2]Қорқыт Ата атындағы Қызылорда университеті, Қызылорда, Қазақстан
[3]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
[4]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
*e-mail: a.tolybaeva95@mail.ru

Қазақстан Республикасындағы электрондық қылмыстық іс жүргізудің проблемалары және шетелдік цифрлық сотқа дейінгі тергеп-тексеру модельдеріне салыстырмалы талдау

Қылмыстық сот ісін цифрландыру құқық қорғау жүйелерін жаңғыртудың негізгі бағыттарының біріне айналуда. АКТ қолдану досудебный тергеудің жеделдігін арттырып, деректерді өңдеу дәлдігін күшейтеді. Қазақстан Республикасында электрондық форматтың базалық инфрақұрылымы, оның ішінде онлайн-сервистер қалыптасқанымен, қолданыстағы нормативтік актілер мен электрондық жүйелерді пайдалану практикасы толыққанды цифрлық тергеу моделін қалыптастыруға кедергі келтіретін жүйелік шектеулерді көрсетеді. Зерттеудің мақсаты – Қазақстандағы электрондық қылмыстық сот ісін жүргізудің қазіргі жағдайы мен даму перспективаларын кешенді бағалау. Жұмыс құқықтық реттеудегі және практикалық іске асырудағы проблемаларды анықтауды, ҚР ҚПК мен ведомстволық актілер арасындағы коллизияларды талдауды, шетелдік үлгілерге (CMS, e-File, eDiscovery) салыстырмалы шолуды және халықаралық тәжірибені бейімдеу жөніндегі ұсыныстарды әзірлеуді қамтиды. Методология заңнаманы талдауға, цифрлық инфрақұрылымды бағалауға және халықаралық тәжірибені зерттеуге негізделген. Жүйелеу және салыстырмалы-құқықтық талдау әдістері қолданылып, электрондық тергеудің тиімділігіне әсер ететін жеті негізгі проблема айқындалды.

Анализ ИКТ қолдану тәртібінің нақты регламенттелмегенін, ҚР ҚПК мен Бас прокурордың № 2 Бұйрығы арасындағы қайшылықтарды, «E-Қİ» мен «Qamqor» жүйелерінің Құқықтық статистика комитетінің деректер базаларымен жеткіліксіз интеграциясын, сондай-ақ «Жария секторда» құпиялылық бұзылғаны үшін жауапкершіліктің реттелмегенін көрсетті. Қашықтан тергеу әрекеттерін жүргізу, заттай дәлелдемелерді айналымға енгізу және электрондық форматты шектеу критерийлерін айқындауда да нормативтік олқылықтар байқалды. Зерттеудің құндылығы жеті құрылымдық кедергіні анықтауға негізделген электрондық қылмыстық сот ісін жүргізуді талдаудың жүйелі тұжырымдамасын қалыптастыруында. Құқықтық, технологиялық және ұйымдастырушылық аспектілерді біріктіретін кешенді тәсіл ұлттық ғылыми әдебиеттегі әдіснамалық олқылықты толтырады.

Практикалық маңызы нормативтік және технологиялық ортаға енгізуге бағытталған шешімдер ұсынумен көрінеді: реттеу базасын унификациялау (ҚПК-ке толықтыру), интеграциялық шина мен Data Hub құру, QR-белгілеуі бар заттай дәлелдемелерді есепке алу модулін енгізу және «Жария секторда» құпиялылық бұзылғаны үшін жауапкершілік механизмін қалыптастыру. Бұл шаралар тергеу тиімділігін арттыруға және қылмыстық сот ісін жүргізудің толыққанды электрондық экожүйесін дамытуға мүмкіндік береді.

Түйін сөздер: электрондық қылмыстық сот ісін жүргізу, цифрлық досудебный тергеу, дәлелдемелерді сақтау тізбегі, ақпараттық жүйелер интеграциясы.

А.А. Толыбаева[1*], А.Ж. Исаева[2], Ш.Р. Жумагулова[2],
Э. Ашимова[3], Д.У. Байтукаева[4]

[1]Алматинская академия Министерства внутренних дел Республики Казахстан имени М. Есбулатова, Алматы, Казахстан
[2]Кызылординский университет имени Коркыт Ата, Кызылорда, Казахстан
[3]Евразийский национальный университет имени Л.Н. Гумилева, Астана, Қазахстан
[4]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
*e-mail: a.tolybaeva95@mail.ru

Проблемы электронного уголовного судопроизводства в Республике Казахстан и сравнительный анализ зарубежных моделей цифрового досудебного расследования

Цифровизация уголовного судопроизводства становится ключевым направлением модернизации правоохранительных систем. Использование ИКТ ускоряет досудебное расследование и повышает точность обработки данных. В Республике Казахстан уже создана базовая инфраструктура электронного формата, включая онлайн-сервисы, однако действующие нормативные

акты и практика применения электронных систем показывают наличие системных ограничений, препятствующих становлению полноценной цифровой модели расследования. Цель исследования заключается в комплексной оценке текущего состояния и перспектив развития электронного уголовного судопроизводства в Казахстане. Работа охватывает выявление проблем правового регулирования и практической реализации, анализ коллизий между УПК РК и подзаконными актами, сравнительный обзор зарубежных моделей (CMS, e-File, eDiscovery), а также разработку предложений по адаптации эффективных международных подходов. Методология исследования основана на анализе законодательства, оценке цифровой инфраструктуры и изучении международного опыта. Применены методы систематизации и сравнительно-правового анализа, что позволило выделить семь ключевых проблем, влияющих на эффективность электронного расследования.

Анализ показал отсутствие четких процедур использования ИКТ, наличие противоречий между УПК РК и Приказом Генерального прокурора № 2, слабую интеграцию систем «E-Қİ» и «Qamqor» с базами данных Комитета по правовой статистике, а также отсутствие регламентации ответственности за нарушение конфиденциальности в «Жария сектор». Отмечены пробелы в регулировании дистанционных следственных действий, обращении с вещественными доказательствами и установлении критериев применения электронного формата. Ценность работы заключается в создании системной концепции анализа электронного уголовного судопроизводства на основе идентификации семи структурных барьеров. Комплексный подход, объединяющий правовые, технологические и организационные аспекты, восполняет методологический пробел в национальной научной литературе.

Практическая значимость выражается в предложении решений, ориентированных на внедрение в нормативную и технологическую среду: унификация базы регулирования (дополнение к УПК), создание интеграционной шины и Data Hub, внедрение модуля учета вещественных доказательств с QR-маркировкой и формирование механизма ответственности за нарушение конфиденциальности в «Жария сектор». Эти меры способны повысить эффективность расследований и обеспечить развитие полноценной электронной экосистемы уголовного судопроизводства в РК.

Ключевые слова: электронное уголовное судопроизводство, цифровое досудебное расследование, цепочка хранения, интеграция информационных систем.

Introduction

Digital transformation of criminal justice has become one of the key trends in the development of contemporary law enforcement systems. The application of information and communication technologies in criminal investigations contributes to reducing the duration of pre-trial proceedings, increasing the accuracy of data processing, and expanding the possibilities for analytical processing of large-scale datasets (see, for example, the U.S. study: "National Institute of Justice – 'Digital Evidence and the U.S. Criminal Justice System'") (https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf). International practice demonstrates the high effectiveness of electronic case-management systems, digital evidence repositories, and automated analytical platforms implemented in the United States, EU member states, Singapore, Canada, and other jurisdictions. In the EU, the "Digital Criminal Justice Programme" includes a case management system (CMS) and the JUDEX information-exchange platform (https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice-programme). In Singapore, the ICMS (Integrated Case Management System) (https://www.judiciary.gov.sg/services/icms) enables the conduct of criminal proceedings in an electronic format.

In the Republic of Kazakhstan, recent years have seen the development of an infrastructure aimed at transitioning to an electronic model of pre-trial investigation. For instance, the online complaint-submission service (e.g., via the Qamqor portal) allows citizens to file police reports electronically (https://egov.kz/cms/en/articles/legal_relations/zayavlenie_v_policiuy). In addition, there are academic publications devoted to the digitalization of Kazakhstan's criminal procedure and judicial system (for example, an overview of the digital transformation of Kazakhstan's judiciary) (https://bulletin-law.kaznu.kz/index.php/journal/article/view/2066).

The Prosecutor General's Office and the Ministry of Internal Affairs articulate a consistent course toward further modernization of procedural mechanisms, taking into account the need to adapt international practices and enhance the transparency of criminal justice (https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1514369324&utm).

Despite the progress achieved, an analysis of current regulatory acts and the operational practice of electronic systems reveals several systemic constraints that hinder the establishment of a fully integrated digital model of pre-trial investigation. One of the key challenges is the absence of clearly formulated mechanisms and technical procedures for the use of information and communication technologies in criminal investigations (a study of the legal and technical aspects of criminal procedure digitalization) (https://bullaw.enu.kz/index.php/main/article/view/304).

The regulatory framework contains internal inconsistencies arising between the provisions of the Criminal Procedure Code of the Republic of Kazakhstan and subordinate acts governing the conduct of criminal proceedings in electronic form (https://cis-legislation.com/document.fwx?rgn=69097). In addition, the integration of the "E-QI" and "Qamqor" systems with the databases of the Committee for Legal Statistics and Special Records remains insufficient, which limits the ability of participants in the process to access necessary information promptly (analysts note the need for further integration of information systems).

A significant issue concerns the absence of regulations governing the liability of participants in criminal proceedings when accessing case materials through the "Zhariya sektor" platform, which creates risks of violating confidentiality rules and misusing the information obtained (https://academy-rep.kz/uploads/4905e565bb7092d73b2159aec9d9f303.pdf). Mechanisms for conducting certain investigative actions remotely are not sufficiently developed, although current conditions and international practice confirm the necessity of such procedures to ensure the efficiency of investigations and the involvement of remote experts (the international trend toward the use of electronic evidence) (https://www.osce.org/secretariat/530833).

The issue of digital recording and integration of physical evidence into an electronic criminal case remains unresolved, complicating the maintenance of an unbroken chain of custody (as noted in academic analyses of criminal procedure digitalization). The absence of criteria for determining categories of criminal cases for which the electronic format of investigation is only partially applicable also creates uncertainty in law enforcement practice (researchers highlight gaps in the regulatory framework) (https://vestnik.zqai.kz/index.php/vestnik/article/view/781).

The issues identified indicate the need for a comprehensive scholarly study that includes an analysis of national regulation, an assessment of the effectiveness of the existing digital infrastructure, and an examination of international models of electronic criminal justice. This approach enables the identification of directions for further modernization and the development of systemic solutions aimed at enhancing the efficiency, transparency, and technological resilience of pre-trial investigations in the Republic of Kazakhstan.

The purpose of the study is to conduct an in-depth examination of the current state and prospects for the development of electronic criminal justice in the Republic of Kazakhstan, based on an analysis of the regulatory framework, an evaluation of the functioning of existing information systems, and a comparison of the national model with international enforcement practices.

To achieve this objective, a set of tasks has been formulated, covering the key areas of modernization of digital pre-trial investigation:

- Identification of systemic problems in the legal regulation and practical implementation of the electronic format of investigation, including the absence of effective procedures for the use of information and communication technologies, insufficient integration mechanisms between information systems, and the lack of regulation of certain aspects of procedural liability;
- Analysis of the current legislation of the Republic of Kazakhstan governing electronic criminal proceedings, with a view to identifying internal inconsistencies as well as contradictions between the Criminal Procedure Code and subordinate acts that determine the procedure for conducting criminal cases in digital form;
- Comparative study of foreign models of electronic pre-trial investigation, including the examination of technologies for electronic document management, automated case-management systems, electronic registration of physical evidence, and remote investigative actions used in advanced legal systems;
- Development of proposals for the implementation of effective foreign approaches into the national law enforcement and regulatory environment, taking into account the specific features of Kazakhstan's law enforcement system, the architecture of information platforms, and the requirements of criminal procedure.

The novelty of the study lies in the formation of a holistic scholarly approach to the analysis of electronic criminal justice in Kazakhstan, based on the systematization of seven key problems affect-

ing the effectiveness of pre-trial investigation in the digital environment. The proposed systematization covers issues of legal regulation, technological support, interagency integration, liability of participants in the proceedings, remote conduct of investigative actions, digital recording of physical evidence, and the determination of the limits of application of the electronic format.

The scientific significance of the work is reflected in the possibility of applying the results obtained to improve the regulatory acts governing the electronic format of criminal procedure, as well as to develop practical solutions aimed at enhancing the transparency, technological sophistication, and manageability of pre-trial proceedings. The proposals justified in the study regarding the adaptation of foreign models may serve as a reference point for the formation of a modern digital ecosystem of criminal justice that strengthens the guarantees of the rights of participants in the proceedings and improves the quality of criminal investigations.

Materials and methods

The research materials encompassed national regulatory acts of the Republic of Kazakhstan, the operational practice of the information systems "E-QI", "Qamqor", the Unified Register of Pre-Trial Investigations (ЕРДР), and the Criminal Procedure Statistics and Case Management System (КПСиСУ), as well as foreign models of digitalization in criminal proceedings represented by the CJIS and eDiscovery systems (USA), e-Justice and e-File (Estonia), ICMS (Singapore), and the Digital Case File (United Kingdom). The methodological framework relied on comparative legal analysis, systemic and formal-logical methods, which enabled the identification of key regulatory and technological inconsistencies that hinder the full-scale digital transformation of pre-trial proceedings.

The study was aimed at assessing the current state of electronic criminal procedure in Kazakhstan, identifying systemic challenges, and comparing national practices with international solutions. The scientific contribution lies in the systematization of seven problem domains and the development of proposals for modernizing the digital architecture, including the creation of an integration bus, a platform for remote investigative actions, a unified module for the registration of physical evidence, and a special regulatory appendix to the Criminal Procedure Code of the Republic of Kazakhstan. Collectively, these measures provide the foundation for constructing a coherent model of electronic pre-trial investigation.

Literature review

Research focused on the digitalization of criminal proceedings occupies a significant place in the international academic literature and provides a substantial theoretical and practical foundation for developing modern models of electronic pretrial investigation. A considerable body of foreign scholarship addresses the handling of digital evidence, the development of electronic case-management systems, and the establishment of digital platforms for prosecutorial and police activities. International studies emphasize the need to ensure the continuity of the digital chain of custody, the standardization of metadata, and the use of automated analytical tools to improve the quality of investigations (https://www.ijrte.org/wp-content/uploads/papers/v10i3/C64490910321.pdf). A substantial contribution to this field has been made by research conducted within the framework of the digital evidence concept, which focuses on rules for handling, authenticity, integrity, and admissibility of electronic data in criminal proceedings (https://www.researchgate.net/publication/395027730_Digital_Evidence_in_Criminal_Proceedings_Legal_Standards_Chain_of_Custody_and_Evidentiary_Reliability_in_The_Digital_Era).

An important part of the global scientific discourse is represented by studies examining the functioning of electronic case-management systems and the automation of investigative bodies. Researchers pay particular attention to solutions implemented in the United States through the Criminal Justice Information Services Division (CJIS), which enables data integration across federal and local law-enforcement agencies (https://www.fbi.gov/services/cjis). In the European Union, especially in Estonia, the development of the e-Justice platform has become one of the most successful examples of building a digital justice infrastructure, incorporating electronic criminal case processing, automated data verification, and interagency information exchange (https://e-estonia.com/solutions/e-governance/justice-public-safety/). With respect to Singapore, research highlights the active use of digital and automated investigative tools, including platforms for case submission and management, although the iFAMS/ICMS system is less comprehensively presented in relation to criminal investigations (https://www.judiciary.gov.sg/services/e-platforms).

In Kazakhstani academic literature, the digitalization of the criminal process is gradually attracting greater attention; however, the degree of elaboration of certain aspects remains limited. Existing publications primarily address general directions for modernizing law-enforcement activities, transforming procedural mechanisms, and incorporating information technologies (https://cyberleninka.ru/article/n/tsifrovizatsiya-ugolovnogo-protsessa-v-respublike-kazahstan-stanovlenie-i-praktika-primeneniya). Despite the availability of studies on the operation of the "E-QI" and "Qamqor" systems, academic works rarely analyze the full-scale integration of information systems, which creates a methodological gap in examining interagency coordination.

The issue of conducting investigative actions remotely has likewise not received adequate scholarly attention. Publications in Kazakhstan primarily limit themselves to theoretical considerations and do not address the technological and legal mechanisms enabling remote participation by investigators, experts, and other participants in criminal proceedings. For instance, the use of videoconferencing for remote consideration of criminal cases is noted as insufficiently regulated at the normative level (https://online.zakon.kz/Document/?doc_id=38147903). Moreover, procedural liability arising from the use of electronic platforms remains insufficiently examined, including the process of familiarizing parties with case materials in the "Zharyia Sector," where no comprehensive studies have assessed the risks of breaches of confidentiality or the adequacy of legal data protection. Academic literature also identifies certain inconsistencies between the Criminal Procedure Code of the Republic of Kazakhstan and subordinate regulatory acts (for example, the Instruction on Maintaining a Criminal Case in Electronic Format). However, the analysis of these discrepancies lacks a systematic character and is not accompanied by proposals for remedying the identified gaps.

The results of the review of domestic and foreign literature demonstrate notable differences in both the direction and depth of scientific elaboration on the topic. International research offers integrated models of electronic criminal procedure, providing detailed organizational, legal, and technological solutions (https://online.zakon.kz/Document/?doc_id=35690135). In the Kazakhstani academic tradition, the focus is largely on identifying isolated challenges associated with digitalization, yet studies that synthesize the key elements of electronic pre-trial proceedings into a unified conceptual framework remain absent. Meanwhile, a comprehensive approach that encompasses legislative regulation, interagency integration, digital evidence capture, remote procedural mechanisms, and the limits of applicability of the electronic format holds the greatest scientific and practical value (https://law-vestnik.buketov.edu.kz/index.php/law/article/download/338/304/602).

Results and discussion

The study of the state of digital transformation of pre-trial investigation in the Republic of Kazakhstan demonstrates the absence of a coherent system of regulatory, methodological, and technological mechanisms necessary for the effective application of information and communication technologies in investigative practice. Existing legal acts lack detailed regulations that would define the algorithms for using electronic resources during specific investigative actions, the procedures for recording digital traces of crime, and the rules governing the use of automated data-analysis tools. This gap is repeatedly noted both in scholarly literature and in analytical reports concerning the implementation of the electronic criminal case and the Unified Register of Pre-Trial Investigations (URPI) (https://zakon.uchet.kz/rus/history/V14W0009744/23.12.2014). Underdeveloped guidelines for handling digital materials impede the formation of uniform requirements for the procedural documentation of results obtained through ICT and hinder the establishment of standardized procedures that would ensure the reliability of digital information.

One of the most significant limitations is the absence of uniform standards for storing digital evidence, including requirements for data structure and formats, verification procedures, maintenance of the chain of custody, and protection against unauthorized access. These shortcomings are highlighted both in Kazakhstani and comparative legal studies (https://lawinfo.ru/articles/8453/perspektivy-ispolzovaniya-informacionnyx-texnologii-v-ugolovnom-sudoproizvodstve-v-kontekste-realizacii-prokurorskix-polnomocii). Fragmented regulation results in digital media and electronic files being recorded, transferred, and stored without appropriate standardization, which creates risks to the integrity and authenticity of evidentiary information; similar issues are reported in relation to the functioning of the URPI and the electronic criminal case module (https://www.agka.kz/cms/wp-content/uploads/2021/09/%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D0%B8%

D1%8F.pdf). As a consequence, law-enforcement bodies encounter difficulties in ensuring the procedural admissibility of digital evidence, particularly in cases requiring confirmation of data immutability during processing, a concern reflected in reviews of practice and departmental publications on the digitalization of criminal procedure (https://avestnik.kz/o-czifrovizaczii-ugolovnogo-proczessa/).

Foreign practice demonstrates the existence of well-established mechanisms that provide a significantly higher level of technological support for criminal investigations. In the United States, the eDiscovery framework is highly developed, enabling systematic digital processing of evidence, automated classification, indexing, and the use of analytical tools to identify significant correlations; the legal foundations of this institution are reflected in several provisions of the Federal Rules of Civil Procedure and in specialized guidelines issued by governmental authorities (https://www.justice.gov/sites/default/files/usao/legacy/2011/07/08/usab5903.pdf). The Estonian model of centralized electronic criminal case management provides for storing all information in unified electronic files, with access regulated by strict protocols and automated logging of all user actions; the e-File system functions as the central information platform for the police, prosecution service, courts, correctional institutions, and other actors, ensuring end-to-end electronic document circulation in criminal, civil, and administrative proceedings (https://www.kohus.ee/sites/default/files/tekstidokumendid/central_database_for_justice_e-file.pdf). In the United Kingdom, the digital case file (Digital Case File, DCF) format is widely used; it establishes unified standards for the preparation and transmission of criminal case materials between the police, the Crown Prosecution Service, and the courts. Its development is documented in CPS prosecution guidelines, inspection reports, and interagency agreements on the exchange of digital evidence (https://www.cps.gov.uk/prosecution-guidance/directors-guidance-charging-sixth-edition-december-2020-incorporating-national). These examples illustrate the demand for comprehensive solutions that ensure the structured organization of digital data, timely access, and transparency of all information-processing procedures, which makes it possible to compare them with the current state of digital transformation in Kazakhstan's pre-trial investigation system and to identify pathways for improving the national model.

A comparison of national and foreign approaches indicates the need to develop specialized automation modules in Kazakhstan aimed at analytical data processing, the creation of electronic investigative files, and enhanced support for documenting digital evidence (https://www.gov.kz/memleket/entities/aqmola-esil/press/article/details/124877). Another important modernisation priority is the standardisation of metadata, including the definition of mandatory parameters recorded during the collection, transfer, and storage of digital traces (https://portal.ejtn.eu/PageFiles/20609/Guidelines%20on%20electronic%20evidence.pdf). The unification of data formats and structures will ensure the comparability of materials originating from different sources and strengthen the reliability of the evidentiary foundation, which aligns with international recommendations on the handling and preservation of digital evidence (https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html).

An additional contribution comes from the adaptation of effective foreign models that provide for comprehensive regulatory and technological support for digital investigation, including the legal framework governing cross-border access to electronic evidence and procedures for obtaining data from private service providers (https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI%282021%29690522_EN.pdf). The implementation of such approaches presupposes the development of a system of electronic procedures integrated with existing information platforms and aligned with the specific features of the national criminal process, which is confirmed by Kazakhstan's experience in developing the e-UD modules and integrating the Unified Register of Pre-Trial Investigations, "Zandylyk", and "Torelyk" systems (https://online.zakon.kz/Document/?doc_id=34878697). The introduction of these measures will ensure the formation of a structured and technologically robust environment for the use of ICT in criminal investigations, which is already reflected in strategic documents and programmes for the phased transition of criminal proceedings to an electronic format in the Republic of Kazakhstan (https://cyberleninka.ru/article/n/elektronnyy-format-dosudebnogo-rassledovaniya-v-deyatelnosti-pravoohranitelnyh-organov-respubliki-kazahstan-problemnye-aspekty).

An examination of the regulatory framework governing electronic criminal proceedings in the Republic of Kazakhstan reveals significant inconsistencies between the provisions of the Criminal Procedure Code of the Republic of Kazakhstan and the

norms established by Order No. 2 of the Prosecutor General of the Republic of Kazakhstan (https://online.zakon.kz/Document/?doc_id=34195283). These divergences are systemic in nature and directly affect the guarantees available to participants in pre-trial proceedings, the legal certainty of procedural steps, and the uniformity of law-enforcement practice.

One of the key contradictions concerns the definition of an electronic criminal case. The CPC of Kazakhstan does not contain a clearly formulated concept of an "electronic criminal case," whereas Order No. 2 and its accompanying Instruction provide that criminal proceedings in electronic form are carried out through the creation and storage of case materials within the relevant information system. The absence of conceptual alignment results in a lack of a uniform approach to the structure of the electronic case file, the scope of materials included, and the procedures for their procedural documentation.

Discrepancies are also evident in the regulation of access by participants in criminal proceedings to materials in electronic format. Order No. 2 provides for expanded possibilities for electronic familiarisation and remote access, while the CPC of Kazakhstan remains oriented predominantly toward the traditional paper format, despite the introduction of Article 42-1, which allows criminal proceedings to be conducted electronically (https://kodeksy-kz.com/ka/ugolovno-protsessualnyj_kodeks/42-1.htm). As a result, investigative bodies are compelled to apply varying algorithms depending on how the norms are interpreted, leading to errors and ambiguity in ensuring the parties' rights to defence and access to information.

Significant inconsistencies concern the procedures for recording investigative actions. The Criminal Procedure Code of the Republic of Kazakhstan (CPC RK) sets out classical requirements for drafting procedural records without providing for the specificities of digital documentation, including electronic metadata, video recording, automated activity logs, and other technical elements that are indispensable in a digital environment (https://cyberleninka.ru/article/n/problemy-vnedreniya-elektronnogo-formata-ugolovnogo-rassledovaniya-v-respublike-kazahstan). Order No. 2 partially compensates for this gap; however, it does so at the level of a subordinate act, which limits the legal force of the relevant provisions and reduces their obligatory nature for practitioners (https://online.zakon.kz/Document/?doc_id=34126206). Moreover, discrepancies were identified in the regulation of timelines and procedures for uploading materials into the electronic case file. The subordinate act establishes more flexible procedures for uploading and updating information in the system, whereas the CPC RK relies on traditional procedural time limits that do not reflect the specifics of digital data processing. These divergences create risks of non-compliance with procedural requirements, the emergence of disputes concerning the timeliness of uploading materials, and inconsistent practices across investigative bodies.

The consequences of the identified conflicts manifest in legal uncertainty that complicates the consistent and predictable application of norms governing electronic criminal proceedings. The lack of coherence in the regulatory framework leads to divergent interpretations of procedures, a higher probability of procedural errors, and risks of violating the rights of participants in the criminal process, including the right of access to case materials, the right to defence, and the right to a fair trial.

Addressing these contradictions requires the harmonization of regulatory provisions and a structured approach to the legal framework governing electronic pre-trial proceedings. It appears necessary to incorporate the key provisions of the subordinate act into the text of the CPC RK, ensuring the statutory regulation of the specificities of electronic document management, digital recording of investigative actions, procedures for accessing materials, and timelines for their submission. An additional avenue for improvement may include the development of a special normative supplement to the CPC RK in the form of an "Electronic Criminal Procedure Code Supplement," which would systematize technical and procedural requirements applicable exclusively to electronic criminal case files. The creation of such a comprehensive regulatory instrument would support uniform law-enforcement practice and enhance the stability of the digital model of pre-trial investigation.

One of the key factors limiting the development of electronic pre-trial investigation in the Republic of Kazakhstan remains the insufficient integration of the information systems "E-ҚІ" and "Qamqor" with the infrastructure of the Committee for Legal Statistics and Special Records. These systems operate in fragmented architectural environments, resulting in technical and organizational gaps in data exchange. For example, the study notes that "the electronic criminal case project has not yet covered the entire cycle of the criminal process in

a unified digital format" (https://online.zakon.kz/Document/?doc_id=34878697). Incompatibility of individual modules, differences in data formats, and the absence of a unified digital platform for synchronizing procedural information hinder the creation of end-to-end digital processes encompassing the full cycle of pre-trial investigation.

A serious problem concerns the absence of a unified metadata base that would ensure standardized recording of parameters of digital documents, investigative actions, and procedural decisions. Metadata in different systems are generated using divergent algorithms, which impedes automated data comparison and leads to the need to duplicate information or perform manual verification of its accuracy. Such inconsistencies reduce the transparency of the criminal process, complicate interagency cooperation, and restrict the use of analytical tools based on processing large data sets. More broadly, in the context of digitalization of criminal procedure in Kazakhstan, issues of standardization and interoperability of IT systems are consistently noted (https://cyberleninka.ru/article/n/vnedrenie-informatsionnyh-tehnologiy-v-ugolovnoe-sudoproizvodstvo).

Insufficient integration of information systems directly affects the ability of participants in criminal proceedings to access materials of electronic case management. In the absence of coordinated interaction protocols between the systems, users frequently encounter delays in obtaining access to documents necessary for preparing procedural decisions, filing motions, or exercising the right to review case materials. Such delays pose a risk of violating the rights of participants in criminal proceedings and may lead to disputes related to compliance with procedural time limits. For example, the report indicates that the transition to electronic criminal case management in Kazakhstan is proceeding with a number of temporal and technical constraints (https://cyberleninka.ru/article/n/proizvodstvo-po-ugolovnomu-delu-v-elektronnom-formate-po-zakonodatelstvu-respubliki-kazahstan).

To address the identified issues, it is necessary to establish a technologically unified environment for electronic criminal proceedings. One of the most promising solutions is the development of an integration bus (middleware) that enables standardized data exchange between "E-QI", "Qamqor", and the systems of the Committee for Legal Statistics. The use of an integration bus would make it possible to unify data formats, ensure automated information routing, and reduce functional duplication across different systems.

An important conceptual direction in the development of digital infrastructure is the implementation of the principle of information equilibrium, which presupposes guaranteed and equal access to procedural information for all parties to the criminal process (https://vestnik.kosgos.ru/attachments/article/1440/kuzmina-ov-skotnikova-mm-vestnik-ksu-2024-4.pdf). The practical application of this principle requires not only technological interoperability of information systems but also the normative consolidation of procedures that ensure transparency and equality in accessing case materials (https://www.lawjournal.digital/jour/article/view/155).

The creation of a centralized data repository (Data Hub) functioning as a single access point to digital materials of the criminal process may serve as an effective tool for ensuring the continuity of information flows. A unified Data Hub would make it possible to structure procedural information, ensure its real-time availability, and support all elements of electronic pre-trial investigation within an integrated digital environment (https://journal.unnes.ac.id/journals/lslr/article/download/14341/4345/83130).

Collectively, the proposed measures can shape a coherent architecture for electronic criminal procedure, aligned with international standards and ensuring a higher level of technological interoperability and legal certainty (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).

The operation of the "Zharya Sektor" platform has significantly expanded the possibilities for electronic access to case materials for participants in criminal proceedings (see the report of the Ministry of Justice of the Republic of Kazakhstan on the digitalization of criminal justice). However, the expansion of access to digital documents is accompanied by heightened risks related to information security and confidentiality. One of the most significant threats is the potential leakage of personal data, including information about victims, witnesses, and other participants in the process. Similar risks arise when case materials are published unlawfully in open sources, which may harm the interests of the parties, exert pressure on witnesses, and affect the objectivity of judicial proceedings. For example, the OECD report emphasizes that timely and adequate access to case materials must be balanced with the protection of confidential information (https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/10/access-to-the-case-file-and-protection-of-confidential-information_cf558708/91c55a68-en.pdf).

Despite the importance of ensuring information security, the current regulatory framework does not establish specific procedural sanctions for violating the rules governing the use of materials obtained through the "Zharya Sector" platform. The lack of legally defined liability reduces the disciplining effect of procedural norms and creates conditions in which improper conduct by participants remains without consequences. The absence of regulation generates uncertainty in law enforcement practice and complicates the protection of the interests of individuals affected by the unauthorized dissemination of data. In Kazakhstan, it is noted that the transition to a digital format of the criminal process has been officially declared, yet concrete measures regarding liability for improper access to and publication of materials remain vague (https://www.gov.kz/memleket/entities/pravstat/press/news/details/797150).

A comparative analysis of foreign models demonstrates a higher level of regulation concerning access to criminal case materials and liability for violations of related requirements. Germany and France maintain a strict control regime over the dissemination of information related to criminal prosecution: access is granted only to a narrowly defined group of authorized persons, with mandatory compliance with established procedures (for example, personal data protection norms and judicial practice related to the oversight of information processing) (https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0). In the United States, courts apply protective orders that prohibit the transfer of materials to third parties and establish liability for violations, including procedural fines and restrictions on participation in certain stages of the proceedings (https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf). These mechanisms ensure a balance between the need for access to case materials and the protection of information from unlawful dissemination.

Given the identified characteristics of national regulation and international experience, it appears advisable to establish a specialized section on liability governing the conduct of participants in criminal proceedings when using materials posted in the "Zharya Sector" system. Such a section should define clear procedural duties, prohibitions, and sanctions for violating confidentiality requirements (https://www.researchgate.net/publication/395331612_Electronic_evidence_in_criminal_proceedings_experience_of_foreign_countries_and_Russian_prospects). An important element of the proposed system is the introduction of a mechanism for electronic acknowledgment by participants of the rules governing the handling of criminal case materials. Electronic confirmation of consent to the established conditions would make it possible to determine the scope of obligations imposed on the individual and would serve as a legal basis for applying liability measures (in the Russian Federation, electronic signatures are regulated by Federal Law "On Electronic Signatures" No. 63-FZ of 06.04.2011) (https://cis-legislation.com/document.fwx?rgn=32989).

Within the proposed model, it is appropriate to establish a multi-tier system of sanctions that includes administrative measures, restrictions or temporary suspension of access to electronic materials, as well as additional procedural consequences in cases of systematic violations. The development of such a legal framework would strengthen the information security regime, enhance the predictability of law-enforcement practice, and ensure the protection of the rights and legitimate interests of participants in criminal proceedings during electronic access to case materials (which aligns with research on the specifics of digitalization of criminal justice and the use of information technologies in the procedural sphere) (https://ijeba.com/journal/611/download/Information%2BTechnologies%2Bin%2BCriminal%2BProceedings%2Bof%2BRussia%3A%2BControversial%2BIssues%2Bof%2BProof.pdf).

The evolution of digital technologies and the changing organizational conditions of law-enforcement activity have necessitated the introduction of mechanisms for conducting certain investigative actions remotely. Given the geographical expanse of the Republic of Kazakhstan, the remoteness of certain settlements, and the limited resources of investigative units, the remote format is capable of improving the efficiency of investigations and ensuring access to justice for all participants in criminal proceedings (https://law-vestnik.buketov.edu.kz/index.php/law/article/view/338). An important factor is also the need to involve foreign experts and specialists, whose participation is often hindered by territorial and organizational constraints.

Despite the practical significance of remote procedures, the current procedural regulation does not contain structured provisions defining the procedure for their implementation within electronic pre-trial investigation. The absence of corresponding mechanisms prevents the use of video interrogations, remote inspections of locations and objects, or the remote participation of experts and specialists in investigative actions. In the absence of normative grounds, such actions are carried out in a limited

manner or are excluded from practice altogether, which reduces the flexibility of investigative bodies and constrains their ability to collect evidence effectively.

International practice demonstrates that remote investigative actions can become a full-fledged and stable component of criminal procedure. During the COVID-19 pandemic, many legal systems, including the United States and the member states of the European Union, expanded the use of videoconferencing, remote evidence-recording procedures, and distance participation of experts. As a result, models were developed that ensure the procedural legitimacy of such actions, technical transparency, and an adequate level of control over the protection of participants' rights (https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/09/access-to-justice-and-the-covid-19-pandemic_0ea1b2a3/09a621ad-en.pdf). These approaches have proved effective and continue to be applied after the lifting of restrictions, which indicates the long-term relevance of the remote format within justice and law-enforcement digitalization.

Given the identified gaps in national regulation, it appears appropriate to develop a specialized digital platform "Offline-SDTB" designed for conducting remote investigative actions in an electronic environment. The platform should provide full participant identification, secure data transmission, and integration with the information systems "E-ҚІ" and "Qamqor." A key element of the proposed platform may be a module for simultaneous recording and automatic registration of procedural information, incorporating metadata generation, user-action logging, cryptographic data protection, and automated integrity control of digital materials.

The technical implementation of such solutions will ensure preservation of evidentiary information, procedural transparency, and the possibility of subsequent verification of the legitimacy of actions taken by investigators and other participants. The introduction of these mechanisms would represent a significant step toward modernizing electronic pre-trial investigation, enabling the conduct of investigative actions regardless of territorial or organizational constraints and reinforcing guarantees of the rights of individuals involved in criminal proceedings.

One of the substantial limitations in forming a fully digital model of pre-trial investigation in the Republic of Kazakhstan is the absence of effectively functioning mechanisms for accounting, identifying, and integrating physical evidence into the "E-ҚІ" information system. Physical evidence occupies a central position in evidentiary procedure, yet its procedural movement in Kazakhstan is predominantly recorded in traditional paper form, which complicates maintenance of an unbroken chain of custody and reduces transparency in handling such objects. The transfer of physical evidence between investigative units, forensic institutions, and prosecutorial bodies is often accompanied by the lack of a unified, standardized electronic control mechanism, which increases the likelihood of technical errors, data loss, or inconsistencies between records and actual object movements (https://pmc.ncbi.nlm.nih.gov/articles/PMC10000967/).

A significant challenge arises from the disconnect between electronic criminal case materials and physical evidence. Information on material objects is recorded in electronic protocols; however, the actual movement of these objects and changes in their status are not automatically reflected in the digital environment. This approach creates a risk of discrepancies between the content of the electronic case file and the actual condition of the evidence. The absence of unified digital tracking prevents prompt verification of an object's ownership, transfer time, storage conditions, and movement path, which reduces the reliability of the evidentiary base and may adversely affect the court's procedural assessment of the evidence (https://media.neliti.com/media/publications/296457-the-management-of-physical-evidence-and-6c1fe85d.pdf).

In foreign practice, the storage and chain-of-custody control of physical evidence are regulated through specialized evidence management systems. These systems include modules for automated registration, scanning, and labeling of objects, as well as electronic real-time tracking of all actions performed with them. In several jurisdictions, including the United States, Canada, and Australia, such systems are integrated with forensic laboratories and enable full traceability of evidence movement, covering its receipt, transfer, analysis, storage, and disposal. The use of such solutions has proven effective in ensuring procedural transparency and establishing a reliable evidentiary infrastructure (https://policinginsight.com/feature/advertisement/nice-investigate-digital-investigation-and-evidence-management/).

Taking into account international experience and the identified gaps in national regulation, it is advisable to develop a unified module for physical evidence management integrated into the "E-ҚІ" platform. This module should provide automated

identification, registration, and tracking of all actions related to material objects, with mandatory metadata and timestamp recording (https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf). An important component of this mechanism may include a generator of unique QR codes that enables labeling of each piece of evidence, followed by electronic scanning and automatic upload of information into the digital system. This will maintain the continuity of the chain of custody, eliminate data duplication, and prevent inconsistencies between paper and electronic records (a need widely recognized in practice for both digital and physical evidence https://sefcom.asu.edu/publications/CoC-SoK-tps2024.pdf).

Another area for improvement relates to integrating the evidence-management module with forensic laboratories. Linking digital platforms will enable automatic transmission of information regarding the submission of objects for examination, registration of expert conclusions, recording of receipt and transfer times, and monitoring of storage conditions. Such integration will significantly enhance the reliability of evidence handling, reduce interagency processing time, and ensure full control over the procedural movement of objects (this conclusion aligns with recommendations on unified evidence-management and audit systems in digital environments). Implementing the proposed mechanisms will create a technologically coherent system that supports uninterrupted digital recording of physical evidence, improves storage quality and accessibility, and strengthens procedural safeguards within the electronic criminal case process.

Despite the considerable potential of digital technologies to enhance the efficiency of pre-trial investigations, their use cannot be universal. Law-enforcement practice demonstrates that certain categories of criminal cases possess characteristics that impede the full-scale application of an electronic format. When electronic case management is viewed as a strategic direction for the development of the law-enforcement system, the absence of legally established criteria defining the limits of applicability of the digital investigation model creates additional risks for ensuring legality and safeguarding the rights of the parties involved (studies underscore the need for transparent and clearly defined processes for the chain of custody and digital evidence).

One of the key categories of cases that require exclusion from the electronic format comprises cases containing information classified as state secrets or otherwise restricted. Processing such materials in electronic systems not adapted to heightened security standards creates risks of unauthorized access, data leakage, and violations of secrecy requirements. Technical limitations of existing platforms, including the absence of specialized high-grade cryptographic protection modules, make it impossible to use them for electronic investigations of cases marked “құпия” (classified).

Particular attention should be given to criminal cases in which investigative actions necessitate physical interaction with objects that are critical to the investigation. In such situations, the recording, transportation, and examination of physical evidence cannot be fully transferred to an electronic format without risking loss of evidentiary information or violating chain of custody requirements. For example, a forensic review notes that “the chain of custody is the most important and simultaneously the most critical process of documenting evidence: … it is necessary to ensure that the evidence is the same item that was seized at the crime scene”. The importance of the investigator’s direct contact with objects and the need for their physical assessment limit the potential for digitalization in these categories of cases.

An additional limitation arises in situations where the risks of information leakage outweigh the advantages of electronic document management. This may concern cases involving high-tech crimes, organized crime, or corruption offenses, where maintaining confidentiality and protecting personal data are of paramount importance. Research indicates that, with digital evidence, risks of mishandling, volatility, and data alteration on cloud platforms are especially significant (https://www.scitepress.org/Papers/2024/127028/127028.pdf). In the absence of specialized technical and legal mechanisms to ensure information security, transferring such cases to an electronic format jeopardizes the interests of the state and of participants in criminal proceedings.

International practice demonstrates the necessity of establishing clearly defined exceptions. In several European states and in the United States, specific categories of cases are either completely excluded from electronic document management or are permitted for digital processing only within specialized secure systems. For example, within the EU’s EVIDENCE Project, the “Common European Framework for the correct and harmonised handling of electronic evidence during its entire lifecycle …” was developed to ensure the exchange of electronic evidence and compliance with requirements of reliability and integrity (https://cordis.europa.eu/project/id/608185/reporting). This approach is based on the principle of proportionality between the level

of technological protection and the risks associated with data leaks or violations of procedural integrity.

Given the absence of comparable regulatory standards in the Republic of Kazakhstan, it appears necessary to develop a system of criteria enabling the classification of criminal cases according to their suitability for electronic proceedings. Such a system should take into account the level of confidentiality of case materials, the nature of investigative actions, requirements concerning the handling of physical evidence, and the degree of risk to information security. The legislative establishment of these criteria would ensure predictability in law enforcement and define the boundaries for the application of electronic pre-trial investigation.

An important area for further improvement is the development of a classification methodology incorporating algorithms for assessing risks, technological constraints, and procedural characteristics. The use of such a methodology would allow investigative authorities to make well-grounded decisions regarding the appropriate form of case management, improve the quality of procedural operations, and secure the compliance of digital mechanisms with the requirements of legality and evidentiary reliability. Scholarship in the field of digital forensics emphasizes that without an assured chain of custody and proper documentation of data transfer, the credibility of digital evidence becomes questionable (https://www.sciencedirect.com/science/article/pii/S266628172300063X).

Conclusion

The study was aimed at a comprehensive analysis of the current state and development prospects of electronic criminal procedure in the Republic of Kazakhstan. Examining the digital infrastructure, regulatory framework, and foreign models made it possible to identify key modernization vectors and determine systemic barriers hindering effective digital transformation. The scholarly approach included an analysis of the CPC of the Republic of Kazakhstan and subordinate legislation, an assessment of the functioning of information systems, and a comparison of the national model with foreign law-enforcement solutions.

It was established that digital criminal procedure is evolving yet remains characterized by significant structural problems. A holistic analytical model was developed, within which seven core obstacles-previously examined only fragmentarily-were systematized: regulatory conflicts between the CPC of the Republic of Kazakhstan and subordinate acts; insufficient integration of the “E-ҚІ”, “Qamqor”, and CPSiSU databases; lack of regulated liability for handling digital materials; gaps in the legal framework governing remote investigative actions; underdevelopment of mechanisms for managing physical evidence; uncertainty in technical regulations for the application of ICT; and the absence of criteria for cases only partially suitable for the electronic format. This systematization helped fill a methodological gap in the domestic scholarly tradition.

The synthesis of results confirms the need for a comprehensive modernization of electronic criminal procedure with the adaptation of proven international practices. It was proposed to unify the regulatory framework by incorporating key digital provisions into the CPC of the Republic of Kazakhstan; to create an integration bus and a centralized data repository for standardized interagency exchange; to establish liability rules for work within the “Zharyia sektor” platform; to develop a digital platform for remote investigative actions; to implement a unified module for managing physical evidence using QR-marking; and to define criteria governing the application of the electronic format in specific categories of cases.

Implementing these measures will eliminate systemic constraints, establish a technologically resilient architecture for electronic criminal proceedings, enhance the effectiveness of investigations, and strengthen procedural safeguards for all participants. This will form the foundation for a fully developed modern digital ecosystem of criminal justice in the Republic of Kazakhstan. The electronic format may be compared to a high-speed highway: key segments have already been built, yet bottlenecks, discontinuities, and the absence of unified navigation solutions remain. The proposed measures serve as infrastructural linkages and common operating rules that ensure coherence, security, and the accelerated functioning of the entire system.

References

Sean E. Goodison, Robert C. Davis, and Brian A. Jackson. Digital Evidence and the U.S. Criminal Justice System https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

Digital Criminal Justice Programme https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice-programme

Integrated Case Management System (ICMS) https://www.judiciary.gov.sg/services/icms

How to lodge a complaint with the police online. Qamqor service functionality https://egov.kz/cms/en/articles/legal_relations/zayavlenie_v_policiuy

Ondashuly E. Digitalization of legal system of Kazakhstan on the example of judicial system // Journal of Actual Problems of Jurisprudence. №4 (88). 2018 48-52

Electronic criminal case https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1514369324&utm

Tolybayeva A., Daurembekov Y., Nessipbaeva I. Legal and theoretical foundations of the digitalisation of crime investigation // BULLETIN of L.N. Gumilyov Eurasian National University. Law Series, 145(4), 2023. pp. 73–82. https://doi.org/10.32523/2616-6844-2023-145-4-73-82

Code of Penal Procedure of the Republic of Kazakhstan https://cis-legislation.com/document.fwx?rgn=69097&

D.P. Utepov. Digital information as proof in criminal proceedings https://academy-rep.kz/uploads/4905e565bb7092d73b2159aec9d9f303.pdf

Enhancing Kazakhstan's capacities to effectively address crime by requesting electronic evidence across borders https://www.osce.org/secretariat/530833

Финк Д.А. Доступ к уголовно-процессуальным средствам восстановления прав потерпевшего в начале досудебного расследования // Вестник Института законодательства и правовой информации Республики Казахстан, № 4(71), 2022. pp. 117–123. https://doi.org/10.52026/2788-5291_2022_71_4_117

Devesh Banwani, Yatin Kalra. Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody // International Journal of Recent Technology and Engineering (IJRTE), Volume 10, Issue 3, September 2021. pp. 90–96. https://www.ijrte.org/wp-content/uploads/papers/v10i3/C64490910321.pdf

Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era https://www.researchgate.net/publication/395027730_Digital_Evidence_in_Criminal_Proceedings_Legal_Standards_Chain_of_Custody_and_Evidentiary_Reliability_in_The_Digital_Era

Information Services Division (CJIS) https://www.fbi.gov/services/cjis

e-Governance in Estonia: 100% Digital, 100% Trusted https://e-estonia.com/solutions/e-governance/justice-public-safety/

Тлеубаев Д.К., Иманбаев С.М., Карымсаков Р.Ш. Цифровизация уголовного процесса в Республике Казахстан: становление и практика применения // Colloquium-journal, № 11 (98), 2021. pp. 31–37. https://doi.org/10.24412/2520-6990-2021-1198-31-37

Рассмотрение судом уголовных дел посредством видеосвязи: процессуальное регулирование и реалии https://online.zakon.kz/Document/?doc_id=38147903

Влияние цифровизации и искусственного интеллекта на уголовное право: краткий обзор современных зарубежных исследований https://online.zakon.kz/Document/?doc_id=35690135

Приказ Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89. Зарегистрирован в Министерстве юстиции Республики Казахстан 23 сентября 2014 года № 9744 Об утверждении Правил приема и регистрации заявлений и сообщений об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований https://zakon.uchet.kz/rus/history/V14W0009744/23.12.2014

Перспективы использования информационных технологий в уголовном судопроизводстве в контексте реализации прокурорских полномочий https://lawinfo.ru/articles/8453/perspektivy-ispolzovaniya-informacionnyx-texnologii-v-ugolovnom-sudoproizvodstve-v-kontekste-realizacii-prokurorskix-polnomocii

Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан г. Астана, 2017 Информационная система «Единый реестр досудебных расследований» Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан Подсистема «Публичный сектор» https://www.agka.kz/cms/wp-content/uploads/2021/09/инструкция.pdf

О цифровизации уголовного процесса https://avestnik.kz/o-czifrovizaczii-ugolovnogo-proczessa/

SUMMARY OF THE INITIATIVE https://www.kohus.ee/sites/default/files/tekstidokumendid/central_database_for_justice_e-file.pdf

Director's Guidance on Charging, sixth edition, December 2020, incorporating the National File Standard https://www.cps.gov.uk/prosecution-guidance/directors-guidance-charging-sixth-edition-december-2020-incorporating-national

Akimat of the Yesil district https://www.gov.kz/memleket/entities/aqmola-esil/press/article/details/124877

Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings https://portal.ejtn.eu/PageFiles/20609/Guidelines%20on%20electronic%20evidence.pdf

E4J University Module Series: Cybercrime Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

Electronic evidence in criminal matters https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI%282021%29690522_EN.pdf

Электронное уголовное судопроизводство в Республике Казахстан https://online.zakon.kz/Document/?doc_id=34878697

Шульгин Е.П. Электронный формат досудебного расследования в деятельности правоохранительных органов Республики Казахстан: проблемные аспекты правовой регламентации // Труды Академии управления МВД России, № 4 (52), 2019. pp. 108–116.

Приказ Генерального прокурора Республики Казахстан от 3 января 2018 года № 2 Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате https://online.zakon.kz/Document/?doc_id=34195283

Уголовно-процессуальный кодекс РК https://kodeksy-kz.com/ka/ugolovno-protsessualnyj_kodeks/42-1.htm#google_vignette

Беляева И.М., Кусаинова А.К., Нургалиев Б.М. Проблемы внедрения электронного формата уголовного расследования в Республике Казахстан // Вестник Южно-Уральского государственного университета. Серия: Право, т. 18, № 2, 2018. pp. 7–12.

Утверждена Инструкция о ведении уголовного судопроизводства в электронном формате https://online.zakon.kz/Document/?doc_id=34126206

Комарова Е.А., Гундерич Г.А. Внедрение информационных технологий в уголовное судопроизводство // Право и государство: теория и практика, № 10 (190), 2020. pp. 152–154.

Задорожная В.А. Производство по уголовному делу в электронном формате по законодательству Республики Казахстан // Правопорядок: история, теория, практика, № 4 (19), 2018. pp. 70–75.

Кузьмина О.В., Скотникова М.М. Электронное уголовное дело: зарубежный опыт и перспективы внедрения в российский уголовный процесс // Вестник Костромского государственного университета, т. 30, № 4, 2024. с. 173–177. https://doi.org/10.34216/1998-0817-2024-30-4-173-177

Concept of Electronic Evidence in Criminal Legal Procedure https://www.lawjournal.digital/jour/article/view/155

Aristo Evandy A.Barlian a , Atip Latipulhayatb , Elis Rusmiatic , Widati Wulandarid , Ahmad Novindri Aji Sukma. The Digital Transformation of Criminal Justice: A Comparative Examination of Indonesia's E-Court System and Global Best Practices https://journal.unnes.ac.id/journals/lslr/article/download/14341/4345/83130

Governing with Artificial Intelligence 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

Working Party No. 3 on Co-operation and Enforcement https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/10/access-to-the-case-file-and-protection-of-confidential-information_cf558708/91c55a68-en.pdf

Guide to the Case-Law of the of the European Court of Human Rights https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0

Cross-border data access in criminal proceedings and the future of digital justice https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf

Electronic evidence in criminal proceedings: experience of foreign countries and Russian prospects. https://www.researchgate.net/publication/395331612_Electronic_evidence_in_criminal_proceedings_experience_of_foreign_countries_and_Russian_prospects

Federal law of the Russian Federation of April 6, 2011 No. 63-FZ https://cis-legislation.com/document.fwx?rgn=32989

Information Technologies in Criminal Proceedings of Russia: Controversial Issues of Proof https://ijeba.com/journal/611/download/Information%2BTechnologies%2Bin%2BCriminal%2BProceedings%2Bof%2BRussia%3A%2BControversial%2BIssues%2Bof%2BProof.pdf

Access to justice and the COVID-19 pandemic https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/09/access-to-justice-and-the-covid-19-pandemic_0ea1b2a3/09a621ad-en.pdf

The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data https://pmc.ncbi.nlm.nih.gov/articles/PMC10000967/

The Management of Physical Evidence and Chain of Custody (CoC) in Digital Forensic Laboratory Storage https://media.neliti.com/media/publications/296457-the-management-of-physical-evidence-and-6c1fe85d.pdf

NICE Investigate: Digital Investigation and Evidence Management https://policinginsight.com/feature/advertisement/nice-investigate-digital-investigation-and-evidence-management/

Digital Evidence Preservation Considerations for Evidence Handlers https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf

Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics https://sefcom.asu.edu/publications/CoC-SoK-tps2024.pdf

Challenges of Trustworthy of Digital Evidence and Its Chain of Custody on Cloud Computing Environment: A Systematic Review https://www.scitepress.org/Papers/2024/127028/127028.pdf

European Informatics Data Exchange Framework for Courts and Evidence https://cordis.europa.eu/project/id/608185/reporting

Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations https://www.sciencedirect.com/science/article/pii/S266628172300063X

Information about the authors:

Tolybayeva Aiman Asankyzy – PhD student, police captain, M. Yesbulatov Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan (Kazakhstan, Almaty, e-mail: a.tolybaeva95@mail.ru)

Issayeva Ainur Zhenisovna – Doctor of PhD, Acting Associate Professor of the Departament of «Jurisprudence» of the Korkyt Ata Kyzylorda University, (Kyzylorda, Kazakhstan, e-mail: ayim_09@mail.ru)

Zhumagulova Sholpan Rustemovna – Candidate of Law, Senior lecturer of the educational program «Jurisprudence» of the Korkyt Ata Kyzylorda University (Kazakhstan, Kyzylorda, e-mail: jumagulova_sholpan@mail.ru)

Ashimova Elnara Ashimovna – Candidate of Law, Senior Lecturer at the Department of Criminal Law Disciplines of the L.N. Gumilyov Eurasian National University (Astana, Kazakhstan, e-mail: ashimova.e@mail.ru)

Baitukaeva Dana Umirbekovna – PhD, acting. Associate Professor of the Kazakh National University named after Al-Farabi (Almaty, Kazakhstan, e-mail: baitukaeva_dana@mail.ru).

Авторлар туралы мәлімет:

Толыбаева Айман Асанқызы – полиция капитаны, докторант, Қазақстан Республикасы Ішкі Істер Министрлігінің М. Есболатов атындағы Алматы академиясы (Қазақстан, Алматы, e-mail: a.tolybaeva95@mail.ru)

Исаева Айнур Женисовна – PhD докторы, Қорқыт Ата атындағы Қызылорда университетінің «Құқықтану» кафедрасының қауымдастырылған профессоры м.а. (Қызылорда, Қазақстан, e-mail: ayim_09@mail.ru)

Жумагулова Шолпан Рустемовна – заң ғылымдарының кандидаты, Қорқыт Ата атындағы Қызылорда университетінің «Құқықтану» Білім беру бағдарламасының аға оқытушысы (Қазақстан, Қызылорда, e-mail: jumagulova_sholpan@mail.ru)

Ашимова Эльнара Ашимовна – кандидат юридических наук, старший преподаватель кафедры уголовно-правовых дисциплин Евразийского национального университета им. Л.Н. Гумилева (Казахстан, Астана, e-mail: ashimova.e@mail.ru)

Байтукаева Дана Өмірбекқызы – PhD, әл-Фараби атындағы Қазақ ұлттық университетінің доцент м.а. (Алматы, Қазақстан, Астана, e-mail: baitukaeva_dana@mail.ru)

Информация об авторах:

Толыбаева Айман Асанқызы – капитан полиции, докторант, Алматинская академия Министерства внутренних дел Республики Казахстан имени М. Есбулатова (Алматы, Казахстан, e-mail: a.tolybaeva95@mail.ru)

Исаева Айнур Женисовна – доктор PhD, и. о. ассоциированного профессора кафедры правоведения Кызылординского университета имени Коркыт Ата (Кызылорда, Казахстан, e-mail: ayim_09@mail.ru)

Жумагулова Шолпан Рустемовна – кандидат юридических наук, старший преподаватель образовательной программы «Юриспруденция» Кызылординского университета имени Коркыт Ата (Кызылорда, Казахстан, e-mail: jumagulova_sholpan@mail.ru)

Ашимова Эльнара Ашимовна – кандидат юридических наук, Евразийский национальный университет имени Л.Н. Гумилева (Қазақстан, Астана, e-mail: ashimova.e@mail.ru)

Байтукаева Дана Умирбековна – PhD, и. о. доцента Казахского национального университета имени аль-Фараби (Алматы, Казахстан, e-mail: baitukaeva_dana@mail.ru).

Registered: June 20, 2025.
Accepted: December 20, 2025.