



Comparative Legal Analysis of the Use of Electronic Format of Criminal Cases and the Procedure under the Code of Criminal Procedure of the Russian Federation*

Dmitriy Ivanov¹, Aleksandr Grinenko², Pavel Fadeev³,
Sergey Ermakov⁴, Svetlana Antimonova⁵

^{1,2}Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University), Russia

^{3,4,5}Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Russia



[10.15408/jch.v12i2.39691](https://doi.org/10.15408/jch.v12i2.39691)

Abstract

The article deals with the foreign experience of digitalisation in the preliminary investigation. Conservative views of law enforcers and legislators on this issue dominate the Russian Federation. There are only small steps towards digitalising preliminary investigations in our country. At the same time, it has been established that the introduction of various information systems and automated workstations into practice, which was supposed to create a unified system and network of broad coverage, has not happened due to the lack of a unified request from the system of investigative bodies and technical capabilities, as well as lack of an urgent need for changes in the working procedure on the part of investigators and interrogators. In conclusion, the authors conclude that there are currently only minor steps towards digitalisation of pre-trial investigations and creating an electronic format for criminal cases in the Russian Federation. However, the rapidly developing information and telecommunication technologies will also do their job in this aspect, which will lead to the creation and successful testing of the topic studied by the authors.

Keywords: Preliminary Investigation; Foreign Experience; Investigator; Interrogator; Crimes

* Received: April 17, 2024; revised: April 20, 2024; accepted: August 15, 2024; published August 30, 2024.

¹ **Dmitriy A. Ivanov**, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University). ORCID: 0000-0002-2023-3771; E-mail: dmitriy.a.ivanov@bk.ru

² **Aleksandr V. Grinenko**, Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University). ORCID: 0000-0002-9996-2714; E-mail: a.v.grinenko@bk.ru

³ **Pavel V. Fadeev**, Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot. ORCID: 0000-0001-5767-0329; E-mail: fadeev.p.v@bk.ru

⁴ **Sergey V. Ermakov**, Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot. ORCID: 0000-0002-5164-6667; E-mail: sergey.v.ermakov@inbox.ru

⁵ **Svetlana I. Antimonova**, Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot. ORCID: 0000-0001-7169-7915; E-mail: svetlana.i.antimonova@mail.ru

**Corresponding author: dmitriy.a.ivanov@bk.ru

A. INTRODUCTION

Digital transformation has significantly influenced various productive and social processes in today's modern society, reshaping how individuals, businesses, and governments operate. The integration of advanced information technology into everyday life has brought about a fundamental shift in the way we communicate, work, and interact with one another. In industries, digital tools such as artificial intelligence, cloud computing, and big data analytics have streamlined operations, enhanced productivity, and allowed organisations to make more informed decisions. In the social sphere, digital transformation has revolutionised communication through social media, instant messaging, and video conferencing, enabling real-time interactions across the globe. The civilized world is now focused on leveraging these technologies to improve the quality of life, increase economic efficiency, and foster innovation. By embracing digital transformation, societies aim to create smarter cities, enhance education, improve healthcare delivery, and achieve sustainable development goals. This transformation has become a key driver of progress and global competitiveness. ([Pushkarev, et.al., 2022](#); [Korotaeva & Kapustina, 2022](#))

Digital technologies are increasingly being introduced into the legal sphere, significantly transforming legal systems. In certain areas, these advancements have proven to be particularly impactful. For instance, the automated system of the Russian Federation, "Justice," streamlines judicial processes, enabling courts to handle cases more efficiently and transparently. This system provides tools for document processing, case management, and online access to court decisions, enhancing accessibility for legal professionals and the public. Similarly, the unified system of information and analytical support of activity (ISOD) of the Ministry of Internal Affairs of Russia offers advanced capabilities for law enforcement agencies. It allows data collection, storage, and analysis to support criminal investigations, improve decision-making, and facilitate coordination among various departments. These systems exemplify how digitalisation reshapes the legal and law enforcement landscape, improving efficiency, accountability, and accessibility. By embracing such technologies, legal institutions can address challenges like case backlogs, lack of transparency, and inefficiency, fostering a more responsive and effective legal environment. The integration of digital tools demonstrates the growing potential of technology to modernise traditional legal frameworks while ensuring better service delivery and public trust. ([Abdullaev, et.al., 2023](#); [Chirkov et.al., 2022](#))

B. METHODS

The primary method employed by the authors in writing this scientific article is the general scientific, systematic method of knowledge. This approach enabled a comprehensive review and detailed analysis of the contentious issues associated with studying foreign experiences and evaluating the prospects for implementing electronic formats of criminal cases within the Russian Federation. By systematically examining these matters, the authors could consider diverse perspectives and highlight key areas of relevance to the topic. This method provided a structured framework to analyse the challenges and opportunities of adopting electronic case formats, ultimately offering valuable insights into their potential application and implications.

The systematic approach allowed for consideration of organisational, procedural, and managerial aspects of foreign experience and prospects for using electronic formats of criminal cases in the Russian Federation. The application of analytical and synthesis methods made it possible to identify existing problems in the context of the introduction of electronic formats of criminal cases in criminal proceedings in Russia. Applying the comparative legal method allowed us to study the domestic legislation and foreign experience of electronic criminal case formats in detail and the possibility of implementing the format in Russian criminal justice. Using this method, we identified existing problems, proposed ways to solve them, and formulated specific proposals.

As a result of the mentioned methodology, the authors have obtained new knowledge about foreign experience and the possibilities of implementing an electronic format of criminal proceedings in the Russian Federation's criminal justice system.

C. RESULTS AND DISCUSSION

Digitalisation in the legal sphere should also affect the activity of preliminary investigation bodies. Personnel problems of bodies of preliminary investigation in the Ministry of Internal Affairs system have become more acute in recent years. An increase in the staff size of the investigative apparatus will not solve all problems. There is a need for state funding and implementation of developments in the computerisation of preliminary investigations, which will intensify the processes of detection and investigation of crimes. Considering the prospects of using electronic criminal case technology in Russia is necessary in this connection.

As part of measures to modernise the Russian Federation's judicial system, based on the federal target program "Development of the judicial system in 2013-2024," the issue of electronic criminal cases and electronic archives is being considered, among other things.

There is a very different understanding of what constitutes an electronic criminal file. In a narrow sense, an electronic criminal file is a document on an electronic medium, a set of electronic documents stored in structured folders. Thus, A. M. Dolgov (2018) suggests that electronic criminal files should be understood as documents on a tangible medium in electronic form that reflect the course of a criminal case investigation.

Globally, the management of pending criminal cases can be streamlined by utilising a unified data platform specifically designed for law enforcement agencies. Such a platform would centralise all relevant information, enabling real-time access and efficient tracking of case progress. By integrating data from various jurisdictions and agencies, this system could enhance coordination, reduce redundancy, and ensure a more transparent workflow in the criminal justice process. Additionally, a single data platform would allow for the implementation of advanced analytical tools, helping to identify patterns, predict outcomes, and improve decision-making. This innovation could significantly modernise law enforcement operations worldwide.

In the Russian Federation, the transition to the electronic format of criminal cases has been very slow, generally relying on the existing experience of foreign countries, such as the USA (PACER - Public Access Court Electronic Records):

- USA (PACER - Public Access to Court Electronic Records) "Electronic Case Management".
- Singapore (ICMS - Integrated Case Management & Filing System) "National Electronic Criminal Justice System".
- Canada, Belgium, Germany, South Korea, Saudi Arabia, etc.

Thus, electronic pre-trial proceedings are provided for in the criminal procedure legislation of many foreign states. However, it is important to note that electronic document flow is adapted to the peculiarities of court proceedings in those states, where a criminal case mainly consists of an electronic dossier of procedural decisions drawn up in the form of digital files and the same digitised evidence. The Russian criminal justice system has its specifics, and no thoughtless copying of such an approach is possible.

In addition, the study of foreign experience in implementing electronic criminal files in various countries has raised concerns among experts regarding the potential risks associated with the security and integrity of such systems. One of the primary issues highlighted is the possibility of unlawful changes or unauthorised alterations to the information contained within a criminal file. As electronic systems rely heavily on digital storage and data transfer mechanisms, there is an inherent risk of hacking, unauthorised access, or internal misconduct, which could compromise the accuracy and authenticity of the case files. Such concerns underscore the need for robust cybersecurity measures, strict access controls, and transparent auditing systems to safeguard sensitive information. Ensuring the integrity of electronic criminal files is essential not only for the justice system's credibility but also for protecting the rights of individuals involved in criminal proceedings. Therefore, addressing these potential risks is crucial when considering the adoption of electronic systems for criminal case management, as they must inspire trust and reliability among all stakeholders, including law enforcement, legal professionals, and the public. By learning from international practices and implementing advanced security protocols, countries can mitigate these risks and maximize the benefits of digitalising criminal justice processes. ([Zuev, 2018](#))

The Republic of Kazakhstan's experience in implementing the "Electronic Criminal File" project as part of the state programme "Digital Kazakhstan" offers valuable insights and is a notable example of the digitalisation of the Russian legal field. This initiative reflects Kazakhstan's commitment to modernising its legal processes by adopting advanced digital technologies. The "Electronic Criminal File" project has enabled the transition from traditional paper-based documentation to electronic systems, ensuring greater efficiency, transparency, and accessibility in criminal investigations and judicial proceedings. This experience highlights the potential benefits of integrating digital tools into legal processes, such as reducing procedural delays, enhancing data security, and improving the overall management of criminal cases. For Russia, which is still in the early stages of digitalising its pre-trial investigations and criminal case formats, Kazakhstan's approach could provide practical solutions and inspiration for overcoming challenges, including developing secure digital platforms and training legal personnel to use such systems effectively. By studying and adapting successful aspects of the "Electronic Criminal File" project, Russia could accelerate its efforts in modernising its legal framework, aligning it with global trends in legal digitalisation and improving the efficiency of its justice system. ([Zadorozhnaya, 2018](#))

The Code of Criminal Procedure of the Republic of Kazakhstan (Parliament of the Republic of Kazakhstan, 2014) provides a procedure for criminal proceedings similar to the one in Russia. The electronic format of criminal cases was established by Order No. 2 of the General Prosecutor's Office of the Republic of Kazakhstan dated 3 January 2018 "On approval of the Instruction on conducting criminal proceedings in electronic format" (General Prosecutor's Office of the Republic of Kazakhstan, 2018) under paragraph 6 of Article 58 of the CPC of the Republic of Kazakhstan. There is an information system, the "Unified Register of Pre-trial Investigations" (IS ERDR), to carry out electronic court proceedings in Kazakhstan. This information system has an additional functionality - the "Electronic criminal case" (e-CID module) module designed to organise electronic criminal cases' preparation, maintenance, dispatch, receipt and storage.

Under Kazakhstan's Criminal Procedure Code, along with the electronic format, the paper-based format of criminal files remains. It is optimistic that the investigator decides on the format of the investigation, notifying the supervising prosecutor. In addition, the procedure for electronic criminal proceedings itself is not regulated in detail in the CPC of the RK; only the possibility of its maintenance and a specific list of procedural documents and types of evidence that may have an electronic format are outlined. During this project, full-fledged electronic criminal cases were successfully investigated according to the developed algorithm. At the beginning of the investigation, an official issued a pre-trial investigation order electronically.

Criminal cases are formed by filling in special sections of the program in electronic forms, starting with the entry of primary information about the criminal offence, which allows for statistical records and the formation of procedural documents with the possibility of printing them. Minutes of interrogation are signed personally using a unique tablet, where the participants confirm with their signature the accuracy of the text typed by the investigator. In addition, the integrity of the content of evidence and other evidence is ensured by the possibility for participants in criminal proceedings to remotely access the electronic criminal case file via the Internet in compliance with information security requirements.

Electronic communication between participants in criminal proceedings optimises the time the investigator (inquirer) spends on formal procedures. For example, notification of the decision to institute criminal proceedings or not to institute criminal proceedings, familiarisation with the decision to commission an expert examination and other materials of the criminal case, and submission

of statements, motions and complaints. The defendant will be able to become acquainted with the indictment, the bill of indictment (ruling) and the defendant with the verdict or other court decisions. It is optimistic that the supervising prosecutor can access criminal cases in real-time. Naturally, the level of access to electronic criminal case files is determined depending on the procedural status of a participant in criminal proceedings ([Van Tien et al., 2021](#)). We believe that in the Russian Federation, it is necessary to organise electronic court proceedings on a similar digital platform.

Some steps have been taken related to introducing the RF of norms in the CPC regarding the procedure for using electronic documents in criminal proceedings and investigative actions to electronic media. Article 474 of the CCrimP of Russia generally allows for the execution of procedural documents electronically ([State Duma of the Federal Assembly of the Russian Federation, 2001](#)). However, in defining the procedure for using electronic documents in criminal proceedings, the legislator in article 474.1 of the CCrimP of RF narrows the possibilities of electronic format of criminal cases to a minimal framework - the interaction of citizens with the court and adjudication.

We believe that transitioning to electronic criminal cases without changing the existing system of criminal-procedural evidence will not fully solve the problem of optimising investigative activities. The written form of evidence dominates criminal procedure. The investigator (inquirer) works according to the principle that "everything I observe and hear, I write in the record." Currently, the investigator (inquirer), even when extracting digital information from various electronic media, fixes it on a traditional sheet of paper to be filed in the criminal case file. The existing procedure of written record-keeping consumes a vast amount of office time.

It is necessary to simplify and, where possible, abandon the written form of fixation of evidence and transfer it to electronic evidence, which is created electronically with minimal human involvement. Suppose electronic evidence is visually perceived by the investigator (the inquirer) on the computer screen. In that case, the judge, the prosecutor, and other participants can perceive it without transforming it into a paper record.

It is quite true what M.P. Polyakov says: Electronic evidence is not a form but a unique technology of forming evidence that allows for a minimal presence of the human factor. Digital fixation of reality fragments through a technical device can be considered objective information. ([Polyakov, 2020, p. 120](#))

Thus, P.S. Pastukhov (2015) proposes the following additions to the CPC RF:

Traces of crime left in the information environment of the Internet in telecommunications channels, if duly copied to confirm their authenticity in court, may be recognised as physical evidence. Only those exhibits whose authenticity is confirmed by documents and interviews with the person who discovered/created them and/or with whom they were kept before submission to the court are admissible during the examination of the case on the merits. ([p. 25](#))

Modern telecommunication means of communication, social networks, messengers and other applications are actively used. Many digital services and applications have appeared, including those tied to various technical devices that record location and other data about the user and his or her preferences. A vast area of social interaction, the information environment, has emerged. The use of computer technologies and the Internet provides vast possibilities for people to use the achievements of contemporary information-telecommunication technologies to commit crimes and realise their selfish ends. ([Ivanov et al., 2022](#); [Pushkarev et al., 2018](#))

The positive aspects of introducing electronic forms for criminal cases are apparent: saving time on forwarding materials (from one unit to another for jurisdiction; from investigator to prosecutor or head of investigative body for verification; from prosecutor to court, etc.), coordinating decisions made with other bodies, and reducing paper expenses.

The introduction of electronic criminal files also involves several challenges that need to be taken into account:

- complexity in ensuring information security (electronic information is susceptible to external influence, i.e. a mechanism for the protection of electronic documents used in a criminal case must be carefully designed);
- inadmissibility of the disclosure of the secrecy of the preliminary investigation;
- inadmissibility of the loss of electronic criminal files;
- high financial costs associated with the purchase of appropriate equipment for users (equipment of an automated workstation of an investigator (the inquirer), (software and hardware complexes, a graphic tablet for creating a digital analogue of the signature, a biometric smart card reader);
- There is a need for substantial server capacity to record and process criminal case information entering the system.

Preservation of the traditional paper format of preliminary investigation, combined with the current need for duplication and copying of materials from the criminal case, for example, in cases of court-ordered restraint, indictment, and other documents, time extensions, approvals, and others, inevitably causes

"technical" workload for investigators (interrogators) in their criminal cases. Transitioning to electronic criminal files will reduce clerical costs and free up time for detecting and investigating crimes.

Experiments with the introduction of electronic criminal files should be carried out only in specific categories of criminal cases that require analysis of a significant amount of evidence, with participants able to use information technology—for example, various economic and tax crimes and IT crimes.

Studying foreign experience using electronic criminal cases in the educational process is also advisable. For the discipline "Preliminary investigation in law-enforcement bodies," the issue of studying foreign experience in forming electronic criminal files in some CIS and non-CIS countries is provided within the theme dedicated to the scientific organisation of the investigator's work. Unfortunately, the topic is devoted to something that does not yet exist in the criminal process in Russia. Furthermore, there is the immutable "paper" criminal process, which is rigidly regulated.

The topic of electronic criminal files itself is not new to us as teachers. In particular, practical investigators have been trained at the Faculty of Advanced Training in using the Investigator's Workstation, the Automated Information System for Investigative Units (AIS SP), and the Automated Information System "Investigation" (AIS "Investigation"). (These systems allowed the investigator, working under his or her user name and password, to create documents, fill out electronic forms for this or that document, and organise criminal case files in a convenient format for the investigator. These systems also contained regulatory documents, guides enabling the formulation of a list of questions for the expert depending on the type of traces and objects to be examined, methodological recommendations for investigating specific types of crime and conducting certain investigative activities. The usefulness of these programmes was obvious ([Tolmachev, et.al., 2022](#)). However, their introduction into practice, which implied the creation of a unified system and broad network coverage, did not take place due to the lack of a unified request from the system of investigating authorities and technical capabilities, as well as a lack of an urgent need to change the working procedures on the part of the investigators and interrogators.

D. CONCLUSIONS

In conclusion, the authors emphasise that, at present, only minor steps have been taken towards digitalising pre-trial investigations and establishing an electronic format for criminal cases in the Russian Federation. The transition to

digital solutions in this sphere is still in its initial stages, and the progress made thus far remains limited in scope and implementation. However, the authors remain optimistic about the transformative potential of rapidly evolving information and telecommunication technologies. These advancements are expected to impact the justice system significantly, fostering the adoption of innovative approaches to handling criminal cases.

As these technologies continue to develop, they will likely contribute to overcoming existing challenges in digitalising legal processes, including issues related to data security, system compatibility, and procedural efficiency. The authors believe that introducing electronic formats for criminal cases will streamline the investigation process and improve transparency, accessibility, and accountability within the legal system. Over time, these technological innovations will pave the way for successful pilot projects and testing, laying the foundation for broader implementation. Thus, the authors highlight the importance of embracing these changes and furthering research into their practical applications to enhance the justice system's overall efficiency and effectiveness.

REFERENCES

- Abdullaev, I., Prodanova, N., Bhaskar, K. A., Lydia, E. L., Kadry, S., Kim, J. (2023). Task offloading and resource allocation in IoT-based mobile edge computing using deep learning. *Computers, Materials & Continua*, No. 76(2), 1463-1477. <https://doi.org/10.32604/cmc.2023.038417>
- Chirkov, D., Plohih, G., Kapustina, D., & Vasyukov, V. (2022). Opportunities for using digital data in evidence for criminal cases. *Revista Juridica*, No. 4(71), 364 - 380. <http://dx.doi.org/10.26668/revistajur.2316-753X.v1i68.5782>
- Dolgov, A. M. (2018). Electronic criminal case in the pre-trial stages of the criminal process in Russia. *Society: Politics, Economics, Law*. No. 9(62), 55-57.
- General Prosecutor's Office of the Republic of Kazakhstan. (2018). Order of the General Prosecutor's Office of the Republic of Kazakhstan of January 3, 2018, No. 2 "On approval of the Instruction on conducting criminal proceedings in electronic format". Retrieved from <https://adilet.zan.kz/rus/docs/V1800016268>
- Ivanov, D. A., Artemova, V. V., & Ermakov, S. V. (2022). Training of specialists for preliminary investigation bodies in the context of combating crimes

committed with the use of information and telecommunication technologies. *Bulletin of Economic Security*. No. 2, 265-270. <https://doi.org/10.24412/2414-3995-2022-2-265-270>

- Korotaeva, I., & Kapustina, D. (2022). Specific Features of the Use of Distance Learning Technologies in Foreign Language Classes with Postgraduate Students. *International Journal of Emerging Technologies in Learning (ijET)*, No. 17(20), 20–33. <https://doi.org/10.3991/ijet.v17i20.30305>
- Parliament of the Republic of Kazakhstan. (2014). The Criminal Procedure Code of the Republic of Kazakhstan of July 4, 2014, No. 231. Retrieved from <https://adilet.zan.kz/rus/docs/K1400000231>
- Pastukhov, P. S. (2015). *Modernization of criminal procedural evidence in the conditions of the information society*: Abstract. diss. ... Doctor of Law. Moscow Academy of Economics and Law, Moscow, 42 p.
- Polyakov, M. P. (2020). "Electronic evidence": A fashionable term or a new phenomenon? In O. V. Khimicheva (Ed.), *Criminal proceedings: Current state and development strategy: Collection of scientific papers of the IX Annual All-Russian Conference* (pp. 115-121). Moscow: Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot.
- Pushkarev, V. V., Poselskaya, L. N., Skachko, A. V., Tarasov, A. V., & Mutaliev, L. S. (2018). Criminal prosecution of persons who have committed crimes in the banking sector. *Cuestiones Políticas*. Vol. 39, No. 69, 395-406. <https://doi.org/10.46398/cuestpol.3969.25>
- Pushkarev, V. V., Skachko, A. V., Gaevoi, A. I., Vasyukov, V. F., & Alimamedov, E. N. (2022). Managing the investigation of cryptocurrency crimes in the Russian Federation. *Revista Electrónica de Investigación en Ciencias Económicas*. Vol. 10, No. 19, 111-125.
- State Duma of the Federal Assembly of the Russian Federation. (2001). The Criminal Procedure Code of the Russian Federation of December 18, 2001 No. 174-FZ. Retrieved from <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102073942&ysclid=lvbdk50qu8745809763>
- Tolmachev M., Korotaeva I., Zharov A., Beloglazova L. (2022). Development of Students' Digital Competence When Using the "Oracle" Electronic Portal. *European Journal of Contemporary Education*, No. 11(4). <https://doi.org/10.13187/ejced.2022.4.1261>

Van Tien, N., Pushkarev, V. V., Tokareva, E. V., Makeev, A. V., & Shepeleva, O. R. (2021). Compensation for damage caused by a crime in the Socialist Republic of Vietnam and the Russian Federation. *Jurnal Cita Hukum*. Vol. 9, No. 2, 211-220. <https://doi.org/10.15408/jch.v9i2.21738>

Zadorozhnaya, V. A. (2018). Proceedings on a criminal case in electronic format under the legislation of the Republic of Kazakhstan. *Law and Order: History, Theory, Practice*. No. 4(19), 70-75.

Zuev, S. V. (2018). Electronic criminal case: Pros and cons. *Law and Order: History, Theory, Practice*. No. 4(19), 6-12.