ABSTRACT
of the dissertation
by APSIMET NURDAULET MUKHAMEDIYARULY
titled "Pre-trial investigation of crimes in the field of online fraud: modern problems" submitted for the degree of Doctor of Philosophy (PhD)
within the educational program "8D04203 - Jurisprudence"

Relevance of the research topic. The global digitalization of society and the rapid development of the fintech industry have shifted property crimes into the virtual environment, giving rise to new and transformed forms of criminal activity. The share of online fraud increased from 1.8% in 2018 to 60.5% in 2025, while the number of registered offences grew several times over. At the same time, the high latency of such crimes and the low rate of damage recovery significantly increase their social danger. The President of the Republic of Kazakhstan, Kassym-Jomart Tokayev, noted that only one out of every five cases of online fraud is successfully solved, highlighting the need for new approaches to combating cybercrime. The legal dimension of the problem is associated with the inability of criminal procedural legislation to keep pace with digital realities. The Criminal Procedure Code of the Republic of Kazakhstan does not contain the concept of “electronic (digital) evidence”; digital traces are artificially incorporated into the category of traditional evidence, while legal provisions restricting the registration of complaints in the presence of indications of a civil-law dispute create additional obstacles to the investigation of digital fraud. Furthermore, mechanisms of international legal assistance have not been adapted to the operational nature of cross-border cyber-enabled theft. Academic scholarship has yet to develop a unified approach to understanding the legal nature of digital theft and the essence of digital traces. This necessitates a transition from the traditional investigative paradigm to an approach that regards digital data as the primary object of cognition and evidentiary analysis. In practice, only a small proportion of registered cyber-enabled theft cases reach the courts; most proceedings are terminated due to the failure to identify suspects, while investigative authorities face a shortage of specialized competencies and technical capabilities for handling digital evidence. These circumstances necessitate the prompt preservation of digital traces, the algorithmization of investigative activities, and the integration of banking anti-fraud systems into criminal proceedings.

The purpose of the dissertation research is to conduct a comprehensive theoretical, legal, forensic, and praxeological analysis of the mechanism of pre-trial investigation of online fraud in the context of global digitalization, with a view to developing a scientifically substantiated set of proposals for improving the legislation of the Republic of Kazakhstan and establishing an innovative artifact-oriented model of criminal justice.

To achieve the stated objective, the following research tasks were identified:

– to reveal the theoretical foundations and historical-legal genesis of online fraud;

– to develop a multifactor classification model of online fraud;

– to conduct a comparative legal analysis of traditional and digital models of fraud;

– to analyze the regulatory and law enforcement framework governing the initiation stage of pre-trial investigations in order to identify the causes of online fraud latency and the determinants of institutional paralysis;

– to assess the conceptual, procedural, and cognitive barriers hindering the effective collection, procedural authentication, and evaluation of hypervolatile electronic (digital) evidence;

– to examine the impact of the cross-border (extraterritorial) nature of cyber-enabled theft on national jurisdiction and to study advanced international practices in combating online fraud;

– to determine the directions for improving the legislation of the Republic of Kazakhstan under conditions of contemporary digitalization.

Object of the research: a complex of social relations regulated by legal norms and arising within criminal proceedings during the pre-trial investigation of criminal offences related to online fraud in the context of the global digitalization of the financial and telecommunications environment.

Subject of the research: the norms of criminal, criminal procedural, and related legislation of the Republic of Kazakhstan governing electronic (digital) evidence and pre-trial proceedings, as well as international legal instruments in the field of combating cybercrime.

Scientific novelty of the research. The scientific novelty of the dissertation lies in the development of a comprehensive theoretical, methodological, and practical framework for countering cyber-enabled theft, aimed at bridging the conceptual gap between the highly dynamic digital environment and the traditionally conservative structure of criminal proceedings. Within the framework of this research, the concept of “digital deception” is introduced into the scientific discourse of the Republic of Kazakhstan for the first time. An evolutionary model of online fraud is substantiated, and an original definition of “electronic (digital) evidence” is proposed, eliminating the requirement to associate virtual data with a physical storage medium. The study formulates the phenomena of “digital nihilism” and “technological elusiveness” in law enforcement practice and substantiates the concept of the “dual-object nature” of microcredit-related theft. The dissertation proposes an original artifact-oriented cyber-procedural model and a five-level integrative system encompassing preventive, initiation, artifact, attribution, and suppression levels. In addition, a multifactor classification of cyber-enabled theft and a tactical “72-hour algorithm” based on the prompt cryptographic preservation of digital traces have been developed. The research provides a scientific justification for the nature of virtual traces and the concept of “accelerated degradation”, while also proposing a platform-based model of legal convergence aimed at integrating banking anti-fraud systems with the activities of investigative authorities. The approaches developed in this study contribute to eliminating legal uncertainty regarding the status of digital evidence, reducing

artificial latency at the stage of complaint registration, and enhancing the effectiveness of investigations into transnational cybercrimes.

Methodological framework of the research. The methodological framework of the study is based on the dialectical method of scientific cognition, which makes it possible to examine the phenomenon of online fraud in its evolutionary development and interconnection with global digitalization processes. The reliability of the findings is ensured through the comprehensive application of general scientific and specialized legal research methods. Methods of analysis and synthesis, together with the system-structural approach, were employed to develop a multifactor classification of cyber-enabled theft and an artifact-oriented paradigm of pre-trial investigation. The historical-legal method was used to examine the genesis and transformation of virtual deception as a criminal phenomenon. The comparative legal method facilitated the analysis of international practices, the identification of distinctions between traditional and digital forms of fraud, the comparison of approaches adopted by the civil law and common law legal traditions to the qualification of cybercrime, and the assessment of the effectiveness of foreign technological investigation models and public-private partnership mechanisms. The formal legal method was applied to the interpretation of the provisions of the criminal and criminal procedure legislation of the Republic of Kazakhstan, the identification of institutional conflicts and inconsistencies, and the development of proposals aimed at modernizing the regulatory framework. Statistical and criminological methods were employed to assess crime dynamics, the level of procedural latency, and regional characteristics of online fraud on the basis of empirical data.

Key provisions submitted for defense:

1. It has been demonstrated that the introduction of digital technologies has resulted not merely in a quantitative increase in property-related offences but in a fundamental qualitative transformation of their operational mechanism. This conclusion is substantiated through the author's three-stage evolutionary model encompassing the phases of emergence, development, and institutionalization. To accurately reflect this phenomenon at the doctrinal level, the concept of “digital deception” is introduced, denoting the transition from direct distortion of objective reality to a remotely mediated virtual mechanism of fraud;

2. A unified definition of online fraud has been formulated as a hybrid criminal phenomenon. In order to ensure appropriate criminal procedural differentiation, a multifactor classification has been developed, integrating technological, object-related, structural, and traceological criteria. For the first time, the classification incorporates the criterion of “procedural complexity of investigation” (low, medium, and high), which determines the selection of tactical and organizational algorithms for pre-trial proceedings;

3. It has been substantiated that online fraud in the microcredit sector is characterized by a dual-object structure: direct pecuniary damage is inflicted upon the financial institution, while additional informational harm is caused to the individual whose personal data have been compromised. It is argued that the financial institution should be recognized as the primary victim. In this regard, it is

proposed to supplement Part 2 of Article 190 of the Criminal Code of the Republic of Kazakhstan with a special qualifying element: *“misappropriation through the insertion of knowingly false computer data into the information system of a financial institution”*.

Furthermore, the necessity of formally recognizing the staged nature of cyber-enabled theft at the level of official judicial interpretation has been substantiated. The unlawful acquisition of confidential authentication information (CVV codes, SMS verification passwords, and similar credentials) through deception should be classified as an attempt to commit fraud. To this end, it is proposed to amend Regulatory Resolution No. 6 of the Supreme Court of the Republic of Kazakhstan dated 29 June 2017;

4. For the purpose of implementing the procedural concept of recognizing a financial institution as the primary victim, a mechanism for the pre-trial restoration of the rights of individuals whose personal data have been unlawfully used has been developed. In this regard, it is proposed to supplement Part 19-1 of Article 193 of the Criminal Procedure Code of the Republic of Kazakhstan with the following provision: *"at the stage of pre-trial investigation, submits to the investigating judge a motion for recognizing the lending institution as the victim in criminal proceedings and for cancelling the credit obligations of persons in whose name the loan was issued"*.

In addition, it is proposed to supplement Paragraph 5-1 of Part 2 of Article 55 of the Criminal Procedure Code of the Republic of Kazakhstan with the following provision: *"Upon the prosecutor’s submission, considers the issue of recognizing the lending institution as the victim in criminal proceedings and cancelling the credit obligations of persons in whose name the loan was issued";*

5. The objective necessity of a paradigmatic transition from the traditional subject-oriented logic of criminal proceedings to an innovative artifact-oriented model has been substantiated. This concept establishes the absolute procedural priority of the immediate cryptographic preservation and fixation of highly volatile electronic traces over attempts to promptly identify the offender, treating the digital artifact as the primary and indispensable source of information for subsequent de-anonymization;

6. An authorial definition of “electronic (digital) evidence” has been formulated, ensuring a definitive departure from the archaic procedural linkage of virtual data to a physical medium. A forensic concept of the “accelerated degradation of digital traces” has been substantiated, explaining the asymmetry between the lifespan of digital data and the inertia of investigative processes. In addition, the destructive law-enforcement phenomenon of “digital nihilism” has been conceptualized as the systematic disregard by investigative authorities for the technological specificity of virtual artifacts. For the institutionalization of the proposed concept, a package of amendments and additions to the Criminal Procedure Code of the Republic of Kazakhstan has been developed:

– to supplement Article 7 of the Criminal Procedure Code with Paragraph 59 as follows: *"Electronic (digital) evidence means data (information) created, stored, processed, or transmitted in digital form within information systems, network*

resources, and electronic devices, used for establishing and verifying circumstances relevant to a criminal case";

– to supplement Part 2 of Article 112 of the Criminal Procedure Code with the following provision: *"Factual data relevant to the proper resolution of a criminal case shall be established by the testimony of the suspect, accused, victim, witness, witness entitled to defense, expert, and specialist; expert and specialist opinions; physical and electronic (digital) evidence; records of procedural actions; and other documents";*

– to supplement Part 1 of Article 118 of the Criminal Procedure Code with Paragraph 6 as follows: *"Data (information) created, stored, processed, or transmitted in digital form within information systems, network resources, and electronic devices, used for establishing and verifying circumstances relevant to a criminal case";*

7. An original five-level integrative architecture of investigation has been proposed, combining preventive, initiation, artifact, attribution, and suppression levels into a unified system. To implement this architecture, the introduction of the urgent “72-hour” algorithm has been substantiated as a mandatory chronological filter for evidence preservation. It is also proposed to supplement Part 4 of Article 131 of the Criminal Procedure Code of the Republic of Kazakhstan with a new ground for detention: *"where there is suspicion of serial online fraud committed through the use of distributed information systems, due to the necessity of urgent cryptographic preservation of traces located on remote servers"*.

Approbation of the dissertation results. The dissertation was completed at the Department of criminal law, criminal procedure and criminalistics of the Faculty of Law of the Al-Farabi Kazakh National University. The results of the research have been reflected in 15 scientific publications, including 8 articles published in scientific journals recommended by the Science and Higher Education Quality Assurance Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan, 5 articles published in proceedings of international scientific conferences, and 2 articles published in journals indexed in international scientometric databases (Scopus and Web of Science).

Structure of the dissertation. The structure of the dissertation corresponds to the stated aims and objectives of the research. The dissertation consists of an introduction, three chapters comprising ten sections, a conclusion, and a list of references. The volume of the dissertation complies with the established requirements for doctoral dissertations.