

TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 3
SEPTEMBER 2026



JOURNAL DOI: 10.51788/tsul.ir.
ISSUE DOI: 10.51788/tsul.ir.73
E-ISSN: 2181-1024



Founder: Tashkent State University of Law



TSUL LEGAL REPORT
T L R

INTERNATIONAL
ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 3
SEPTEMBER 2026

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.73

«TSUL Legal Report» international electronic scientific journal was registered by the Press and Information Agency of Uzbekistan on April 21, 2020, with certificate number 1342. The journal is included in the list of journals of the Higher Attestation Commission under the Academy of Sciences of the Republic of Uzbekistan. Copyright belongs to Tashkent State University of Law. All rights reserved. Use, distribution and reproduction of materials of the journal are carried out with the permission of the founder.

Publication Officer:
Orifjon Choriev

Editor:
M. Abdullaeva
M. Sharifova

Graphic designer:
Umid Sapaev

Editorial office address:
Tashkent, st. Sayilgoh, 35. Index 100047.
Principal Contact

Tel.: (+998 71) 233-66-36

Fax: (+99871) 233-37-48

Website: legalreport.tsul.uz

E-mail: info@legalreport.tsul.uz

Publishing license
№ 174625, 29.11.2023.

E-ISSN: 2181-1024

© 2026. TSUL – Tashkent State University of Law.

EDITOR-IN-CHIEF

B. Khodjaev – Rector of Tashkent State University of Law, Doctor of Law, Professor

DEPUTY EDITOR

Z. Esanova – Deputy Rector for Scientific Affairs and Innovations of Tashkent State University of Law, Doctor of Law, Professor

EXECUTIVE EDITOR

E. Mustafae – Head of the Periodicals Department of the Editorial and Publishing Center of Tashkent State University of Law

MEMBERS OF THE EDITORIAL BOARD

N. Koutras – Kurtin Law School, PhD (Australia)

H. Yeung – Associate Professor of Leicester Law School, University of Leicester, (UK)

C. Kelley – Associate Professor of Law School of Arkansas University (USA)

A. Younas – Researcher of the Chinese Academy of Sciences, General Director of Ai Mo Innovation Consultants (China)

Sh. Al-Fatih – Lecturer of the University of Muhammadiyah Malang (Indonesia)

A. Jaelani – Lecturer of Sebelas Maret University (Indonesia)

N. Upadhyay – Associate Professor of the Department of Law and Programs of the Symbiosis Law School (India)

Y. Ogurlu – Rector of Balikesir University (Turkey)

K. Molodyko – Chief Expert of the Institute of National and Comparative Law Research at the "School of Higher Economics" of the National Research University of Russia, Associate Professor of the Department of International Law (Russia)

N. AllahRakha – Lecturer of the Department of Law and Technology of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Pakistan)

N. Rakhmonkulova – Professor of the Department of Private International Law of Tashkent State University of Law, Doctor of Law (Uzbekistan)

A. Tadjibaeva – Associate Professor of the Department of Criminal Procedure Law of Tashkent State University of Law, Candidate of Legal Sciences (Uzbekistan)

R. Urinboev – Professor of the Department of Sociology of Law of Lund University, Doctor of Law (Austria)

M. Kudratov – Doctor of Law of the University of Regensburg (Germany)

Kh. Radjapov – Associate Professor of the Department of Entrepreneurship and Corporate Law of Tashkent State University of Law, Doctor of Philosophy (PhD) in Law (Uzbekistan)

O. Narziev – Professor of the Department of Private International Law of Tashkent State University of Law, Doctor of Law (Uzbekistan)

Sh. Rakhmanov – Head of the Department of International Law and Human Rights of Tashkent State University of Law, Doctor of Law, Professor (Uzbekistan)

CONTENTS

12.00.01 – THEORY AND HISTORY OF STATE AND LAW. HISTORY OF LEGAL DOCTRINES

SHOKIROVA-INOMJONOVA MASHKHURAKHON GAYRATJON KIZI

Specific features of the principle of social justice: a legal analysis5

AZIMOV AZIMBEK AZIZBEK UGLI

Participation of non-governmental non-profit organizations in the implementation
of the social function of the state regarding youth 13

12.00.02 – CONSTITUTIONAL LAW. ADMINISTRATIVE LAW. FINANCIAL AND CUSTOMS LAW

ACHILOVA LILIYA ILKHOMOVNA, ROZMETOVA ASAL ANVARZODA

Improving the institution of appeals: time limits, response quality, and monitoring 24

12.00.03 – CIVIL LAW. BUSINESS LAW. FAMILY LAW. INTERNATIONAL PRIVATE LAW

RUZMURODOVA LOBARKHON MIRZABEK KIZI

Defining editorial control without limiting journalists' copyright in the mass media 36

SAMANDAROVA FERUZA BAKHROMJON KIZI

Issues in improving the mechanism for resolving disputes arising from
public procurement contracts 47

ABDURASULOV ABROR AKMAL UGLI

Transplantation of human organs and tissues as a civil law relationship 54

ABDIKHAKIMOV FARKHODJON ZAFAR UGLI

Artificial intelligence: the problem of legal personality in civil law relations 60

12.00.05 – LABOR LAW. SOCIAL SECURITY LAW

RAKHIMBERGANOV KHASANBOY DAVLATNAZAROVICH,

ABDURAKHMANOV ULUGBEK BAKHODUROVICH

Negotiating return: return migration among highly qualified Uzbek migrants
in Japan 67

12.00.06 – THE LAW OF NATURAL RESOURCES. AGRARIAN LAW. ENVIRONMENTAL LAW

NARZULLAEV OLIM KHOLMAMATOVICH, ABANINA ELENA NIKOLAEVNA

Scientific use of biological resources and legal regulation of biosafety 82

12.00.09 – CRIMINAL PROCEEDINGS. FORENSICS, INVESTIGATIVE LAW AND FORENSIC EXPERTISE

KHAMIDOV BAKHTIYOR KHAMIDOVICH, KOZEL VALERY MIKHAILOVICH

Ethical principles of digital investigations: a legal and forensic analysis 90

NOSIROV AMIRKHON BAHODIR UGLI

Forensic aspects of the subject of proof in fraud crimes committed using
information technologies 102

12.00.10 – INTERNATIONAL LAW

SHUKUROVA DIYORA ANVAROVNA

WTO subsidy specificity and article 6.2 of the agreement on agriculture 108

12.00.13 – HUMAN RIGHTS

KALESNYKAS RAIMUNDAS, KAILIUS MARIUS

The architecture of limitation: dogmatic and comparative analysis of human
rights restrictions under the public health imperative 122



TSUL LEGAL REPORT

Journal home page: www.legalreport.tsul.uz



Received: 05.08.2026

Accepted: 11.09.2026

Published: 30.09.2026

DOI: <https://dx.doi.org/10.51788/tsul.lr.73011>

FORENSIC ASPECTS OF THE SUBJECT OF PROOF IN FRAUD CRIMES COMMITTED USING INFORMATION TECHNOLOGIES

Nosirov Amirkhon Bahodir ugli,

Independent Researcher at Tashkent State University of Law

ORCID: <https://orcid.org/0009-0005-3764-5296>

e-mail: a.nosirov.1111tsul@gmail.com

Abstract. *The article analyzes the system of circumstances subject to proof and establishment in the investigation of fraud crimes committed using information technologies. The sharp increase in crime trends and specific forensic challenges arising in investigative practice clearly demonstrate the relevance of research in this area. The article aims to systemize the general circumstances set forth in Articles 82–83 of the Criminal Procedure Code of the Republic of Uzbekistan based on forensic theoretical approaches of foreign experts, as well as international legal instruments (Budapest Convention, FATF Recommendations). The study substantiates the importance of digital identifiers, such as IP addresses, MAC addresses, and device IDs, in identifying the offender's identity, as well as the necessity of ensuring the integrity of digital evidence (digital traces). The article puts forward practical and theoretical recommendations on determining the modus operandi, instruments and means of the crime, as well as the conditions that enabled the commission of the offense. The discussion section addresses the problem of the lack of a distinct qualifying feature for this type of crime in the legislation of Uzbekistan. The paper argues that a comprehensive and interconnected identification of these circumstances is a key prerequisite for improving investigative efficiency, and proposes recommendations for enhancing the legislation.*

Keywords: *information technologies, fraud, criminalistics, subject of proof, digital traces, investigation, cybercrime, criminal procedure legislation, Budapest Convention*

Introduction

Today, statistics on fraud crimes committed using digital technologies are increasing sharply on a global scale. The specific nature of cyberspace, and the transboundary and high technological complexity of criminal actions significantly limit the effectiveness of traditional investigative methods. Therefore, a comprehensive and deep study of the system of circumstances that must be determined in the detection and investigation of this type of crime is the main factor in the effective development of investigative practice and methodology. Within the framework of forensic science, the methodology of the

subject of proof has been conceptually and deeply researched by the well-known scientist R.S. Belkin, who put forward the idea that these two layers must be harmonized when developing an investigative methodology for fraud crimes committed using information technologies. The first layer consists of the general circumstances consolidated in criminal procedural legislation and unified for all criminal acts, while the second is a complex of specific circumstances arising from the forensic characterization of a particular crime type (Belkin, 1997, pp. 344–352). V.A. Obratsov proposed a four-stage classification of the circumstances to be determined within the methodology of crime investigation. According to this system, circumstances related to the crime event, the circle of guilty persons, the consequences resulting from the act, and the conditions that created the opportunity for the commission of the offense are distinguished as objects of proof (Obratsov, 1995, pp. 407–418). In our opinion, these traditional views in the scientific literature are mainly intended for classical crime types. The scientific-theoretical views of R.S. Belkin and V.A. Obratsov serve as a methodological foundation for the development of cybercrime investigation methodology in the modern digital era. Enriching and modernizing these classical theories with digital traces, virtual identification tools, and transboundary cyber-evidence is the primary condition for ensuring the procedural legality and reliability of the process of exposing and proving cyber fraud acts. Furthermore, foreign studies in recent years also confirm the relevance of this problem. In particular, A.A. Khan analyzed methodological approaches in modern digital forensics, problems of maintaining the chain of custody of evidence, and limitations in existing investigative tools (Khan et al., 2022). In the context of the Central Asian region, K.S. Lakbayev studied the concept of high-tech crimes, problems of their classification, and methods of combating them using Kazakhstan as an example (Lakbayev et al., 2020); due to the similarity of regional legal systems, this research is also of methodological interest for Uzbekistan. The transboundary nature inherent in digital crimes requires reliance on international legal factors when determining the system of circumstances to be proven in investigative and practical materials. The section of the 2001 Budapest Convention of the Council of Europe devoted to procedural regulation establishes tactics for preserving computer data, searching for digital objects, and rapidly seizing and securing electronic traces and evidence; it introduces a procedure for the international exchange of digital evidence for serious crimes, which enhances the possibilities of interstate cyber-forensic cooperation in identifying the traces of cross-border cybercrimes.

Methods

The following methods were utilized in the research: normative-legal analysis method—the relevant norms of the Criminal and Criminal Procedural Codes of the Republic of Uzbekistan, as well as international legal documents (Budapest Convention, FATF recommendations), were analyzed; comparative-legal method—national legislative norms were compared with international standards; doctrinal analysis method—the forensic theoretical views of R.S. Belkin, V.A. Obratsov, N.G. Shurukhnov, Yu.V. Gavrilin, and E. Casey were systematically analyzed; through these methods, the circumstances to be determined were divided into five groups, demonstrating their interconnectedness and specific forensic content. The elements of the subject of proof defined in Articles 82–83 of the Criminal Procedural Code of the Republic of Uzbekistan were selected as the object of research, and their forensic characteristics specific to fraud crimes committed using information technologies were chosen as the subject of research. **RESULTS**

Results

According to the analysis, dividing the seven circumstances in Article 82 of the Criminal Procedural Code of the Republic of Uzbekistan into five groups demonstrates

the specificity and practical significance of the proof mechanism, taking into account the characteristics of fraud committed in the digital space. The first group comprises circumstances related to the event of the crime. Within this group, the task of determining the time, place, and method of the act is primarily established. Unlike classical crime types, this offense is committed in a virtual space independent of a specific geographic area and can simultaneously cover the jurisdictions of various states. Therefore, determining the *locus delicti* requires the identification of relevant servers, networks, and digital platforms based on special technical-analytical evaluations. From the perspective of forensic methodology, Yu.V. Gavrilin classifies the mechanism of the *modus operandi* as follows: phishing–stealing digital traces and personal data through fake websites; vishing–deception through voice telephone communication; smishing–misleading through text SMS messages; spoofing–forging network and personal identifiers; and social engineering–influencing the victim via psychological manipulation. Article 8 of the Budapest Convention defines the elements constituting computer fraud, and this international standard serves as a methodological criterion for shaping the content of circumstances to be determined regarding the crime event. According to E. Casey's analytical conclusions, determining the method of committing a cybercrime and its specific mechanism requires a deep, interconnected analysis of information infrastructure elements–transaction data, server log files, and e-mail headers (Casey, 2011, pp. 163–175). The second group consists of circumstances related to the offender's identity. This group differs most significantly from classical investigative cases. According to N.G. Shurukhnov's legal and methodological approach, the lack of special technical knowledge among investigative personnel is a factor that complicates the procedure for identifying cybercriminals. This is because the offender acts while hiding their personal information using software and technical tools that provide multi-stage anonymity (Shurukhnov, 2004, pp. 510–518). In order to establish the offender's identity, the following electronic identifiers are analyzed: IP addresses, MAC addresses, SIM card numbers, user accounts, digital signatures, and device identifiers (IMEI). Analysis shows that, according to Yu.V. Gavrilin's views, none of these identifiers individually possesses the capability to completely expose the subject of the crime. Nevertheless, the synthesized set of this identification information represents a comprehensively reliable and sufficient system of evidence (Gavrilin, 2003, pp. 52–62). Additionally, the technical knowledge level of the criminal or criminal group, the anonymizing tools used by them (VPN, Tor network, proxy servers), group participation and role distribution, as well as the state from which the crime was committed must be determined. As E. Casey pointed out, digital traces are often preserved irreversibly in server logs–this allows evidence to be found even if the criminal attempts to erase their tracks (Casey, 2011, pp. 221–238). The third group involves circumstances related to the victim. Within this group, first and foremost, the amount of material damage caused to the victim is determined. Establishing the amount of damage is carried out through the analysis of operations conducted via electronic payment systems, transaction records in banks, digital wallet history, and cryptocurrency movements. Recommendation 15 of the FATF establishes standards for tracking financial operations carried out through new technologies and determining the amount of damage (Financial Action Task Force, 2020). The victim's level of literacy in the field of information technologies is also determined: according to the legal approach of scholar Yu.V. Gavrilin, the consequences caused by the methods of deception and misleading used by the offender are forensically evaluated and serve as a basis for qualifying the act under a specific *corpus delicti* (Gavrilin, 2003, pp. 63–70). In Article 168 of the Criminal Code of the Republic of Uzbekistan, exploiting the vulnerable state of the victim and

causing a large amount of damage are specifically listed as qualifying features of fraud. B. Nikkel justifies fintech forensics as a distinct branch of digital forensics, emphasizing that instances of criminals using payment systems and other financial technologies for fraud, extortion, and money laundering are increasing, which necessitates a special methodological approach (Nikkel, 2020). The fourth group encompasses circumstances related to crime traces. Digital traces are a special type of invisible trace that can be detected, read, and restored using technical tools. E. Casey distinguishes the following main types of digital traces: connection information in server log files, browser history and cache information, e-mail headers, financial transaction history, mobile device location data, social media activity traces, and digital traces left by malicious programs (Casey, 2011, pp. 238–255). R.S. Belkin singled out the category of crime traces as a distinct, important category, and thoroughly developed the methodological bases regarding their role in the subject of proof, as well as their collection, consolidation, and verification during an investigation (Belkin, 1997, pp. 355–362). Articles 16–17 of the Budapest Convention establish the obligation for the rapid protection and preservation of digital data, and this international standard prioritizes the issue of the integrity and authenticity of digital evidence. In fraud cases committed through cryptocurrency, M.M. Mirza's research is of particular importance: it proved that transaction history, wallet addresses, and other digital artifacts can be recovered from Web wallet applications on mobile devices, which serves as an important source of evidence in fraud cases related to crypto-assets (Mirza et al., 2022). The fifth group contains circumstances related to the causes and conditions that facilitated the commission of the crime (CPC Article 82, paragraph 7). In this group, the following are determined: technical flaws in the security of information systems, i.e., weak passwords, unupdated software, lack of encryption; the public's susceptibility to deception due to low information literacy; inadequate information security systems in organizations; the inefficiency of monitoring mechanisms in financial systems and the banking sector, as well as legislative gaps. Yu.V. Gavrilin divides these factors into technical, organizational, and human factors, emphasizing the need to develop separate preventive measures for each (Gavrilin, 2003, pp. 71–78). Europol's IOCTA 2021 report also specifically notes the lack of preventive measures and low digital literacy in society as factors contributing to the commission of online fraud (Europol, 2021, pp. 18–26).

Discussion

Theoretical analysis of the system of circumstances to be determined shows that these circumstances differ fundamentally from those defined for traditional fraud, not only in content but also in terms of the methods used to determine them. According to R.S. Belkin's theory, the subject of proof is complete only when the general circumstances in the criminal-procedural layer (CPC Article 82) and special circumstances in the forensic layer are harmonized with each other (Belkin, 1997, pp. 344–350). V.A. Obratsov's methodological classification allows for working with these circumstances in groups during the practical investigation process: predetermining the list of circumstances to be established for each group, planning the sequence of investigative actions necessary to determine them, and systematically summarizing the results significantly increases investigative efficiency (Obratsov, 1995, pp. 418–426). Based on Obratsov's grouping method, it is necessary to develop standard investigative action matrices for modern cyber fraud types (e.g., phishing, social engineering, crypto-scams) for investigators. This enables the investigator to correctly separate main and secondary circumstances in the initial stage and secure digital evidence without losing time (fixing through hash codes). In our opinion, the integration of Belkin's and Obratsov's models provides the most optimal methodological basis for transforming the process of collecting, evaluating,

and proving digital evidence into a coherent practical system, rather than merely fulfilling procedural requirements when investigating fraud in the field of information technologies. In Article 83 of the Criminal Procedural Code of the Republic of Uzbekistan, the elements of the subject of proof are determined in detail, and their application in this type of case acquires specific forensic significance: the crime event is determined in a virtual environment; guilt is proven through digital identification; and the damage caused is determined through the analysis of financial transactions. As Yu.V. Gavrilin emphasized, proper criminal-legal qualification is carried out only when all these circumstances are completely proven and mutually corroborating (Gavrilin, 2003, pp. 78–88). From the perspective of international legal frameworks, Articles 2–11 of the Budapest Convention define the elements that constitute cybercrimes, which form the international standard of circumstances to be determined for this type of crime. As N.G. Shurukhnov noted, the need to utilize special technical knowledge in the investigation of this type of crime is an essential condition for completely covering the subject of proof: without technical expertise, determining digital traces, tracing the chain of financial transactions, and digitally identifying the criminal's identity is virtually impossible (Shurukhnov, 2004, pp. 518–526). At the same time, the absence of separate criminalization for this type of crime in the legislation of Uzbekistan creates certain problems in shaping the system of circumstances to be determined. Article 168 of the Criminal Code of the Republic of Uzbekistan provides general liability for fraud, and its commission via information technologies is not indicated as a distinct qualifying feature. This situation makes it difficult for investigators and judges to formulate a list of special circumstances to be determined for this type of crime. The fact that improving legislation in the fight against cybercrime is defined as a priority direction in the Strategy for the Development of the Digital Economy of the Republic of Uzbekistan further confirms the need to introduce a separate norm or qualifying feature in this area.

Conclusion

The circumstances to be established in cases of fraud committed using information technologies—those relating to the crime event, the offender, the victim, digital traces, and the causes and conditions that facilitated the commission of the offense—differ from those encountered in conventional fraud cases and therefore require specific forensic approaches. Their comprehensive and systematic establishment can enhance the effectiveness of investigations and strengthen the evidentiary basis of criminal proceedings.

Based on the findings of the study, the following practical recommendations are proposed. First, uniform methodological guidelines should be developed for law enforcement agencies to identify, collect, analyze, and evaluate evidence relating to the five groups of circumstances identified in this study. Second, national legislation and investigative practice should provide clear procedural and technical safeguards for preserving the integrity, authenticity, and traceability of digital evidence, taking into account the approaches reflected in Articles 16–17 of the Budapest Convention. Third, specialized training programs in digital forensics should be introduced and further developed for investigators and forensic experts, with particular emphasis on the identification, preservation, analysis, and evaluation of digital traces.

The theoretical significance of the study lies in adapting the forensic understanding of the circumstances subject to proof to the specific characteristics of the digital environment and in systematizing these circumstances for technology-enabled fraud. Its practical significance lies in providing a structured framework that may be used to improve investigative methodologies, the handling of digital evidence, and professional training in the investigation of fraud committed using information technologies.

REFERENCES

- Belkin, R. S. (1997). *Kurs kriminalistiki: T. 3. Kriminalisticheskie sredstva, priemy i rekomendatsii* [Criminalistics course: Vol. 3. Criminalistic means, methods, and recommendations]. Yurist.
- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.
- Council of Europe. (2001, November 23). *Convention on cybercrime* (ETS No. 185). <https://rm.coe.int/1680081561>
- Europol. (2021). *Internet organised crime threat assessment (IOCTA) 2021*. Europol Publications Office.
- Financial Action Task Force. (2020). *International standards on combating money laundering: The FATF recommendations*. FATF/OECD.
- Gavrilin, Yu. V. (2003). *Rassledovanie prestupleniy v sfere kompyuternoy informatsii* [Investigation of crimes in the field of computer information]. The Book World.
- Khan, A. A., Shaikh, A. A., Laghari, A. A., Dootio, M. A., Rind, M. M., & Awan, S. A. (2022). Digital forensics and cyber forensics investigation: Security challenges, limitations, open issues, and future direction. *International Journal of Electronic Security and Digital Forensics*, 14(2), 124–150. <https://doi.org/10.1504/IJESDF.2022.121174>
- Lakbayev, K. S., Rysmagambetova, G. M., Umetov, A. U., & Sysoyev, A. K. (2020). The crimes in the field of high technology: Concept, problems and methods of counteraction in Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, 12(4), 412–423.
- Mirza, M. M., Ozer, A., & Karabiyik, U. (2022). Mobile cyber forensic investigations of Web3 wallets on Android and iOS. *Applied Sciences*, 12(21), 11180. <https://doi.org/10.3390/app122111180>
- Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, 33, 200908. <https://doi.org/10.1016/j.fsidi.2020.200908>
- Obratstov, V. A. (Ed.). (1995). *Kriminalistika* [Criminalistics]. Yurist.
- President of the Republic of Uzbekistan. (2020, October 5). *On approval of the “Digital Uzbekistan–2030” Strategy and measures for its effective implementation* (Decree No. PD-6079). LexUZ. <https://lex.uz/docs/5030957>
- Republic of Uzbekistan. (1994a). *Criminal Code of the Republic of Uzbekistan*. LexUZ. <https://lex.uz/docs/111453>
- Republic of Uzbekistan. (1994b). *Criminal Procedure Code of the Republic of Uzbekistan*. LexUZ. <https://lex.uz/docs/111460>
- Shurukhnov, N. G. (2004). *Kriminalistika* [Criminalistics]. Yurist.



TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 3
SEPTEMBER 2026