

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. Mustafaev – 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: 10.07.2026

Accepted: 11.09.2026

Published: 30.09.2026

DOI: <https://dx.doi.org/10.51788/tsul.lr.73010>

ETHICAL PRINCIPLES OF DIGITAL INVESTIGATIONS: A LEGAL AND FORENSIC ANALYSIS

Khamidov Bakhtiyor Khamidovich,

Senior Lecturer of the Department of Criminalistics
and Forensics Examination,
Tashkent State University of Law,
Doctor of Philosophy (PhD) in Law
ORCID: <https://orcid.org/0000-0003-2857-1633>
e-mail: b.hamidov1984bsjm@gmail.com

Kozel Valery Mikhailovich,

Senior Lecturer at the Department of Criminal Law,
Criminal Procedure, and Criminalistics,
Yanka Kupala State University of Grodno
ORCID: <https://orcid.org/0009-0009-6308-599X>
e-mail: valerykozel@yandex.ru

Abstract. *This article examines the significance and application of ethical principles in digital investigations. The rapid development of information technologies and the increasing reliance on digital evidence have created new ethical challenges relating to the collection, analysis, preservation, and use of digital information. Particular concerns include the protection of privacy and personal data, the accuracy and objectivity of information, and the safeguarding of individual rights throughout investigative processes. In Uzbekistan, the ongoing modernisation of investigative practices has been accompanied by the development of legal provisions concerning information security, personal data protection, and the ethical conduct of law-enforcement officials. However, the application of these provisions in digital environments continues to present practical and regulatory challenges. Drawing on international standards and selected foreign practices, the study examines ethical approaches to digital investigations and places particular emphasis on personal data protection. The analysis indicates that the existing codes of ethics applicable to Uzbek law-enforcement agencies and judicial authorities do not fully address the specific characteristics and risks of digital investigations. The article therefore argues for the development of specialised ethical standards governing the collection, preservation, verification, evaluation, and use of digital evidence. Such standards are essential for strengthening legality, transparency, accountability, and the protection of fundamental rights in digital investigations.*

Keywords: *digital investigation, digital ethics, transparency, freedom, accountability*

Introduction

The contemporary phase of digital transformation in Uzbekistan commenced with the adoption of the national development programme “Digital Uzbekistan–2030”, which identified digitalisation as one of the country’s strategic priorities. The implementation of this policy has been accompanied by a substantial expansion of digital infrastructure and connectivity. According to recent statistical data, approximately 32.7 million people were using the Internet in Uzbekistan in early 2025, representing nearly 89% of the country’s population. Moreover, data published by the National Statistics Committee indicate that the share of the population using the Internet increased further to 94.2% during January–August 2025. These indicators demonstrate the unprecedented scale of digital transformation and confirm that digital technologies have become an indispensable component of social, economic, and administrative life in the country.

The rapid expansion of digital technologies is not unique to Uzbekistan and reflects a broader global trend characterised by the increasing reliance on data-driven services and digital platforms (Astunov & Khamidov, 2021, p. 265). The emergence of online labour markets, electronic payment systems, and digital public services has significantly increased the ability of both public authorities and private entities to collect, process, monitor, and utilise information relating to individuals. Consequently, personal data has become a strategic resource with substantial economic, administrative, and social value.

At the same time, the widespread use of digital technologies has generated a number of complex ethical and legal challenges. The digital environment increasingly creates situations in which competing interests must be carefully balanced. On the one hand, constitutional guarantees relating to privacy, personal autonomy, and the protection of personal data require effective legal safeguards. On the other hand, state institutions and private organisations have legitimate interests in the use of digital information for purposes such as public administration, economic activity, and security. The interaction between these competing interests frequently gives rise to conflicts that cannot be resolved solely through traditional legal mechanisms.

In this context, ethics performs an important regulatory function by providing normative principles capable of balancing competing rights and interests. Ethical standards contribute to ensuring fairness, confidentiality, equality, accountability, and transparency in the processing and use of digital information, thereby complementing formal legal regulation and addressing issues that are insufficiently covered by existing legislation.

The influence of digital transformation is particularly evident within the sphere of law enforcement and criminal justice. The growing reliance on digital technologies in investigative activities has fundamentally altered the manner in which information is collected, preserved, analysed, and presented as evidence. These developments have created new forms of legal relationships within digital environments and have raised previously unknown ethical and procedural questions concerning privacy, data protection, and the integrity of digital evidence.

Given the relatively limited practical experience of legislators and practitioners in addressing these challenges, there is an increasing need for comprehensive theoretical research and comparative legal analysis. The examination of international standards and advanced foreign practices may therefore provide valuable methodological guidance for developing an effective regulatory and ethical framework capable of responding to the realities of digital investigations and the broader process of digital transformation.

Methods

This study aimed to identify and systematise the ethical principles applicable to digital investigations and to examine their legal and criminological foundations on the basis of national legislation, international standards, and selected foreign practices.

The study examined key ethical principles governing digital investigations, including respect for privacy, personal data protection, legality, proportionality, transparency, accountability, professional ethics, and impartiality. Particular attention was paid to the theoretical and practical challenges associated with balancing the protection of human rights with legitimate public-security interests in the collection, preservation, examination, and use of digital evidence.

The analysis covered relevant international standards and professional guidelines, including ISO/IEC 29100:2011, Information Technology — Security Techniques — Privacy Framework, the ACPO Good Practice Guide for Digital Evidence, and the PRECEPT framework, as well as selected foreign legal and regulatory approaches to digital forensics and personal data protection. The legislation of the Republic of Uzbekistan concerning personal data protection, informatisation, operational-search activities, and criminal procedure was also systematically examined from the perspective of ethical requirements applicable to digital investigations.

The study employed a combination of general scientific and specialised legal research methods. The dialectical method was used to examine the impact of technological development on investigative practices; the system-structural method was applied to analyse ethical principles as an integrated conceptual framework; and the formal-legal method was used to interpret relevant national and international legal and regulatory instruments. The comparative legal method enabled the comparison of Uzbekistan's legal framework with selected foreign approaches and international standards. In addition, methods of logical analysis and synthesis were used to identify relationships among ethical principles and their conceptual foundations, while content analysis was employed to examine relevant academic literature, international standards, and professional guidelines.

The methodological framework of the study was based on the primacy of human rights, the protection of personal data, legality, proportionality, accountability, and professional ethics. The object of the study comprised the social and legal relations arising in the course of digital investigations, particularly those associated with the identification, collection, preservation, examination, and use of digital evidence. The subject of the study encompassed the ethical principles applicable to digital investigations, their legal and criminological content, and the organisational and legal mechanisms governing their practical implementation.

Results

Ethical Issues in Digital Investigations

The analysis demonstrates that interactions between individuals, institutions, and society are governed not only by legal norms but also by ethical principles and moral standards. Ethical norms are based on values such as mutual respect, trust, fairness, responsibility, integrity, and social solidarity. Unlike legal norms, ethical standards may also apply to areas of social interaction that are not directly or comprehensively regulated by law. At the same time, ethical principles can provide a conceptual and normative foundation for the development and interpretation of legal rules (Khamidov & Askerov, 2023, pp. 917–920).

The findings further indicate that ethical considerations have become increasingly important in digital environments. Digital transformation has affected interpersonal communication, economic activity, public administration, and law-enforcement practices, creating new forms of interaction and generating ethical challenges associated with the collection, processing, storage, and use of digital information.

One of the principal ethical issues identified in the context of digital investigations is the protection of personal data. Investigative authorities may process extensive amounts of

sensitive information, including identification and contact data; financial and employment information; authentication credentials; biometric, genetic, and health data; geolocation and telecommunications data; information concerning criminal records; photographs and video recordings; behavioural and profiling data; and information revealing racial or ethnic origin, religious or philosophical beliefs, trade union membership, gender identity, or sexual orientation. Such information requires enhanced protection because its unauthorised disclosure or misuse may expose individuals to identity theft, financial fraud, extortion, blackmail, discrimination, and other forms of harm.

The analysis of Uzbekistan's legal framework indicates that the adoption of the Law of the Republic of Uzbekistan *On Personal Data* represented an important step towards strengthening the protection of personal information. At the same time, the application of personal-data protection principles in the context of criminal investigations and other law-enforcement activities raises specific legal and ethical questions. These concerns are particularly significant where investigative authorities process sensitive information for purposes related to crime prevention, operational-search activities, criminal proceedings, and other law-enforcement functions.

The findings also demonstrate that the increasing use of digital technologies in crime prevention, criminal investigations, and judicial proceedings has expanded the range of ethical considerations relevant to criminal justice. The digitalisation of investigative bodies and courts, together with the growing use of technologically assisted methods in criminal proceedings (Toshev & Murodkosimov, 2023, pp. 162–175), reinforces the need for ethical standards capable of addressing the specific characteristics of digital evidence and investigative technologies.

Existing general principles of professional ethics remain relevant to digital investigations; however, their application to digital environments requires consideration of the distinctive characteristics of digital information. These include the scale and speed of data collection and processing, the persistence and replicability of digital traces, cross-border information flows, the processing of large volumes of personal data, and the increasing use of automated and algorithmic technologies. Consequently, effective decision-making in digital investigations requires not only compliance with legal rules but also professional competence, ethical judgement, proportionality, and an understanding of the technological processes involved.

Taken together, the analysis identifies several core ethical considerations that should underpin digital investigations: legality, proportionality, privacy and personal-data protection, professional competence, impartiality, transparency, accountability, confidentiality, and the preservation of digital evidence integrity. These principles provide a basis for balancing the legitimate objectives of law enforcement with the protection of fundamental rights and for developing a more coherent ethical framework for digital investigations.

Discussion

The establishment of an effective regulatory framework for digital investigations requires the formulation of clear ethical principles governing the handling of digital evidence. Such principles are essential for reducing the risks associated with the acquisition and use of digital information, enhancing transparency and accountability in investigative activities, and ensuring that decisions are based on scientifically validated methods and reliable technological tools. An appropriate ethical framework also contributes to protecting individual privacy by limiting access to information that has no evidentiary relevance to a criminal investigation.

The findings of the empirical survey conducted as part of this study indicate that a substantial majority of respondents (66%) support the exclusion of personal information

unrelated to the subject matter of an investigation from criminal case materials. This position is consistent with international practices aimed at preventing the unnecessary disclosure of personal data during digital investigations (Dehghantanha & Franke, 2014, pp. 129–138). Some scholars have also advocated the partial automation of investigative procedures as a means of minimising human access to sensitive personal information and thereby strengthening privacy protection.

Privacy and Ethical Handling of Digital Evidence

From an ethical perspective, the handling of digital evidence requires professional standards governing the conduct of experts, investigators, prosecutors, and judicial authorities throughout the collection, preservation, examination, and assessment of such evidence. Unlike traditional evidentiary procedures, digital investigations operate within a technologically complex environment and therefore present distinctive ethical challenges arising from the specific characteristics of digital information and electronic systems.

Digital evidence may contain highly sensitive information. Consequently, law-enforcement authorities face considerable challenges in maintaining objectivity and impartiality during its collection and analysis. The examination of extensive datasets, the use of open-source intelligence, the integration of artificial intelligence tools, and the extraction and preservation of data from digital devices require investigators and forensic specialists to demonstrate not only advanced technical competence but also a high degree of professional responsibility. In many jurisdictions, these issues are addressed through specialised ethical guidelines and professional codes of conduct.

International practice places particular emphasis on the manner in which digital evidence is obtained, preserved, and verified for use in judicial proceedings. Courts may require prosecuting authorities to explain and demonstrate the methods by which digital evidence was collected and preserved (Astanov & Khamidov, 2021, pp. 259–278). The purpose of this approach is to promote procedural fairness, transparency, and the integrity of judicial decision-making. Accordingly, investigators, prosecutors, and forensic experts should be prepared to demonstrate the reliability and authenticity of digital evidence presented before a court and should avoid unsupported or speculative interpretations of digital data.

Effective legal oversight is an important mechanism for ensuring compliance with legal and ethical standards. In the absence of adequate oversight, the risk of unlawful conduct by law-enforcement authorities may increase (Balogun & Zuva, 2017, pp. 55–69). Preventing unethical behaviour and procedural violations in digital investigations therefore requires the clear definition of ethical obligations and professional responsibilities applicable to digital environments (Nikkel, 2014, pp. 249–251).

Another essential element of digital investigations is maintaining trust among participants in criminal proceedings and the wider public. Public confidence in investigative activities depends, among other factors, on the perceived security, reliability, and proportionality of the technological measures employed by law-enforcement agencies. The present study therefore examined international instruments and selected practices developed in the United States, the United Kingdom, and European jurisdictions concerning the protection of personal data during police investigations and judicial proceedings (Khamidov, 2021, pp. 91–97).

International Principles of Digital Investigations

Particular attention should be paid to the work of Ferguson, Renaud, Wilford, and Irons on ethical principles applicable to digital investigations (Ferguson et al., 2020). Drawing on the Core Investigative Doctrine (CENTREX, 2015), the Criminal Procedure and Investigations Act, and the Association of Chief Police Officers (ACPO) *Good Practice

Guide for Digital Evidence*, these scholars formulated principles intended to promote the legality, reliability, and ethical integrity of digital investigative activities. These principles can be grouped into several interconnected dimensions, including privacy protection, procedural transparency, accountability in decision-making, evidentiary reliability, and public trust. Their appropriate adaptation may contribute to the further development of digital investigative practices in Uzbekistan and to the establishment of a coherent ethical framework for the use of digital evidence.

A comparative analysis of international standards governing digital investigations reveals a relatively coherent set of principles developed through legislation, professional guidelines, and investigative practice. Relevant instruments include the Criminal Procedure and Investigations Act (CPIA), the Core Investigative Doctrine (CENTREX), and the ACPO Good Practice Guide for Digital Evidence.

These standards generally require investigators to conduct thorough investigations, identify and examine potentially relevant circumstances, maintain appropriate records of information obtained during the investigative process, and identify persons or entities that may possess information relevant to the case.

International guidance also emphasises the need to distinguish sensitive material from other evidentiary information. Such material should be properly documented and preserved while being clearly identified and handled in accordance with enhanced confidentiality requirements. Investigators may also be required to preserve intangible or volatile information, including digital data that may not exist in a permanent or immediately accessible form.

Another important principle concerns the disclosure and retention of information. Investigators are expected to provide prosecutors with appropriate records of the information collected and to preserve evidentiary materials regardless of whether they support the prosecution or the defence. In accordance with the principle of equality of arms, accused persons should also be afforded an opportunity to inspect information relevant to their defence, subject to lawful restrictions relating to confidentiality and the public interest.

International standards also place considerable emphasis on professional competence. Individuals responsible for digital investigations should possess the technical expertise and professional skills necessary to collect, interpret, and present digital evidence in a reliable and scientifically sound manner. The integrity of information is equally fundamental. Procedures involving digital evidence should therefore preserve the authenticity, completeness, and reliability of information throughout its life cycle.

The principles governing digital investigations provide investigators with a general framework for operating in technologically complex environments. Rather than prescribing rigid procedural rules, they establish standards intended to promote the integrity, reliability, and accountability of investigative processes involving digital information.

Particular attention should also be given to the involvement of third parties in preserving digital evidence. Where potentially relevant information is held by external entities, including communication service providers and other intermediaries, investigators may need to take timely measures to prevent its loss or alteration. Such measures may include notifying data custodians, issuing preservation requests, and initiating appropriate legal procedures to secure access to the information.

Similarly, where relevant information has not yet been recorded in a permanent or readily accessible format, investigators should ensure that it is properly extracted, preserved, and documented. Every action performed on digital evidence should also be documented through an audit trail or comparable mechanism. Such documentation enables independent experts and judicial authorities to verify the procedures employed

and, where appropriate, reproduce the results obtained during the examination of digital evidence (Van Staden, 2013, pp. 19–31).

The protection of human rights in digital investigations is closely associated with safeguarding personal data and informational privacy. Given the substantial amount of sensitive information that may be processed during such investigations, investigators should exercise a high degree of diligence in maintaining confidentiality and preventing unauthorised access to personal information. In this regard, the privacy principles reflected in ISO/IEC 29100 provide a useful methodological framework for balancing legitimate investigative interests with the protection of individual privacy rights.

Comparative analysis also demonstrates that the handling of personal data requires digital forensic specialists to possess not only technical expertise but also a thorough understanding of privacy principles, data protection requirements, and the legal rights and obligations associated with the collection, processing, storage, and disclosure of personal information. Professional competence in digital investigations therefore increasingly encompasses ethical and legal literacy in addition to technical skills.

The literature on digital investigative ethics has been influenced by the work of Ferguson, Renaud, Wilford, and Irons, who proposed a set of core principles for investigative activities in digital environments (Ferguson et al., 2020). These principles provide an ethical framework aimed at promoting the legitimacy, transparency, and accountability of digital investigations. Their practical application, however, necessarily depends on the characteristics of national legal systems and procedural traditions.

This consideration is particularly relevant to civil-law jurisdictions, including the Republic of Uzbekistan. In such legal systems, ethical requirements applicable to investigative activities may be incorporated directly into legislation and regulatory acts rather than being established exclusively through professional guidelines or internal codes of conduct. Consequently, adapting internationally recognised ethical principles to the national context requires careful consideration of existing legislation, procedural guarantees, and institutional practices.

Professional Ethical Standards in Digital Forensics

The regulation of digital investigative ethics is not confined to a single international instrument or professional body. International organisations, law-enforcement agencies, and professional associations have developed various ethical standards and practical guidelines governing the collection, preservation, analysis, and presentation of digital evidence. Although these frameworks differ in their institutional origins, scope, and specific objectives, they share several common elements, including the protection of fundamental rights, preservation of evidential integrity, procedural transparency, professional competence, and accountability.

The experience accumulated by these organisations may be valuable for improving investigative methodologies in cases involving unauthorised access to computer information and other cyber-enabled offences. Their recommendations can provide theoretical and practical guidance for developing national standards for digital investigations and may contribute to improving investigative practices, professional training, and regulatory frameworks in Uzbekistan.

A comparative review of professional organisations involved in digital forensics and cyber investigations indicates differences in the scope and complexity of their ethical and professional standards. Some organisations have adopted relatively concise frameworks establishing fundamental standards of professional conduct, while others have developed more extensive requirements covering professional responsibility, evidence-handling procedures, confidentiality, professional competence, certification, evidence integrity, privacy protection, and accountability.

Despite differences in the structure and scope of these professional standards, a common tendency is the increasing institutionalisation of ethical requirements in digital investigations. Such standards are intended to promote the reliability of digital evidence, maintain public confidence in investigative processes, protect fundamental rights and freedoms, and establish clear professional responsibilities for specialists involved in collecting, examining, and presenting digital evidence.

A fundamental question arising from comparative studies of digital investigative ethics is whether internationally recognised ethical principles can be directly incorporated into national legislation and investigative practice. The findings of this study suggest that the uncritical transplantation of foreign ethical frameworks into domestic legal systems may not always produce the intended outcomes, as their effectiveness depends substantially on the institutional and legal context in which they operate.

In Uzbekistan, the direct incorporation of foreign ethical standards governing digital investigations requires particular caution. In some foreign jurisdictions, investigative and forensic activities are not performed exclusively by public authorities; private forensic experts and commercial entities may also perform relevant functions on the basis of contractual relationships. Under such circumstances, ethical obligations may extend beyond public accountability to include responsibilities towards clients, professional associations, and contractual partners. Principles such as client confidentiality and professional independence may therefore occupy a more prominent position in these frameworks than in systems where investigative functions remain predominantly within the competence of public authorities.

These differences demonstrate that the development of ethical standards for digital investigations in Uzbekistan should not be based solely on the direct reception of foreign models. Instead, it should involve an analysis of existing legislation, the identification of regulatory gaps, and the careful adaptation of relevant international practices to the characteristics of the national legal system and criminal justice framework.

Ethical Governance of Emerging Investigative Technologies

The responsible use of emerging technologies in law enforcement requires a coherent set of ethical principles. These principles may include legality, accuracy, openness and transparency, good governance, fairness, and accountability. Legality requires technological measures and investigative techniques to have an appropriate legal basis and comply with the rule of law. Accuracy requires the reliability, completeness, and correctness of digital information and analytical results. Openness and transparency require appropriate disclosure concerning the methods and technologies employed, subject to legitimate confidentiality and security restrictions. Good governance requires technological systems to be integrated into institutional oversight and risk-management mechanisms. Fairness requires the avoidance of unjustified discriminatory effects and respect for fundamental rights and procedural guarantees. Accountability requires institutions and responsible officials to be able to justify relevant decisions and accept responsibility for the consequences of the technologies they employ.

The detection and investigation of cyber-enabled offences increasingly involve advanced digital technologies. Digital data and electronic information now play an important role in establishing, verifying, and interpreting evidence in criminal proceedings. Technologies such as artificial intelligence, biometric systems, data analytics, cloud computing, the Internet of Things, and other digital tools may enhance the ability of law-enforcement agencies to process and analyse large volumes of information and support evidence-based decision-making.

At the same time, the implementation of such technologies requires clearly defined ethical and operational standards. Ethical principles should be supported by appropriate procedural requirements to promote consistency, accountability, and legal certainty. The principle of accuracy is particularly important in this regard.

From the perspective of ethical governance, accuracy extends beyond the correctness of technological outputs. Investigative authorities should ensure that a technological solution corresponds to a legitimate operational need and is proportionate to its intended purpose. Information systems, algorithms, and datasets should be subject to appropriate evaluation and auditing to assess their accuracy, reliability, continued validity, and potential for biased or discriminatory outcomes. Where algorithmic systems are used, appropriate levels of transparency and technical explainability should also be ensured.

Law-enforcement officials should possess the competence necessary to understand, use, and critically evaluate technological tools in conjunction with their professional expertise. They should also be able to identify and mitigate risks arising from inaccurate predictions, erroneous matches, biased outputs, or technological failures. Effective governance further requires clear criteria for creating and maintaining datasets and watch lists, particularly where information obtained from multiple organisations is integrated into a common system.

Data quality is another essential component of accuracy. Investigative authorities should establish mechanisms to ensure that datasets are sufficiently complete, reliable, collected for legitimate purposes, and regularly reviewed and updated in accordance with applicable data-retention requirements. Similar safeguards should apply to information obtained from third parties, including procedures for assessing the quality and relevance of externally sourced data.

The effective use of digital technologies also depends on the professional training of their users. Training programmes should develop competence in maintaining data integrity and quality, interpreting analytical outputs accurately, understanding the phenomenon of algorithm aversion, and recognising potential injustices arising from inappropriate reliance on technological decisions or outputs.

Ethical Frameworks for Digital Investigations in Uzbekistan

The present study also examined ethical frameworks applicable to law-enforcement agencies and courts in Uzbekistan. The findings indicate that these institutions have adopted various ethical standards and codes of conduct. However, the analysis suggests that existing frameworks primarily establish general ethical principles and do not provide sufficiently detailed guidance concerning the collection, preservation, verification, and evaluation of digital evidence. The absence of clearly defined operational requirements and implementation mechanisms may contribute to inconsistent approaches to digital evidence management and limit the practical effectiveness of ethical regulation in digital investigations.

A comparative analysis of the ethical frameworks applicable to law-enforcement agencies in Uzbekistan demonstrates a considerable degree of consistency among the principles adopted by different institutions. Legality and respect for citizens' rights, freedoms, and legitimate interests occupy an important place in these frameworks, reflecting the requirement that law-enforcement activities comply with constitutional guarantees and fundamental human rights.

Principles relating to fairness, honesty, impartiality, professional responsibility, and commitment to public service also contribute to a common ethical foundation for law-enforcement activities. At the same time, differences among institutional ethical frameworks may remain in relation to specific matters, including personal responsibility, conflicts of interest, transparency, and accountability.

These differences indicate that, despite the existence of common ethical values across law-enforcement institutions, the regulatory framework may lack uniformity in certain areas relevant to digital investigations. Such inconsistencies can complicate the development of a coherent ethical framework, particularly in relation to accountability and the management of conflicts of interest during the collection, preservation, examination, and assessment of digital evidence.

The analysis further indicates that existing ethical frameworks may not define with sufficient precision the scope and mechanisms for implementing ethical principles in digital environments. This limitation becomes particularly important in digital investigations, where the collection, processing, examination, and assessment of digital evidence require clear ethical guidance and well-defined professional responsibilities.

Differences may also arise between the ethical principles applicable to investigative bodies and those governing judicial authorities. Within the judicial system, the administration of justice is guided by principles such as judicial independence, fairness, equality, impartiality, integrity, and professional competence. These principles are intended to protect the integrity of judicial decision-making, maintain public confidence in the courts, and safeguard the rights and legitimate interests of participants in legal proceedings.

The divergence between the ethical frameworks applicable to investigative bodies and courts may create practical and methodological challenges in the handling of digital evidence. Judicial principles place considerable emphasis on independence, equality, impartiality, and professional competence, while ethical standards governing investigative authorities must also adequately address technological accuracy, transparency, accountability, and procedural safeguards associated with the use of digital evidence.

The absence of a harmonised ethical framework may therefore contribute to inconsistent approaches to the collection, preservation, examination, and evaluation of digital evidence at different stages of criminal proceedings. Such inconsistencies may affect the reliability and admissibility of digital evidence and create difficulties in ensuring procedural fairness, transparency, and the effective protection of fundamental rights. Accordingly, there is a need to develop a coherent system of ethical principles specifically adapted to digital investigations and applicable, where appropriate, across the institutions involved in the administration of criminal justice.

Conclusion

Despite the rapid digitalisation of public administration and criminal justice, the existing legal and ethical framework in Uzbekistan does not yet fully address the specific challenges associated with digital investigations. The implementation of the national digital transformation agenda, particularly the *Digital Uzbekistan–2030* Strategy, therefore requires the development of legal and ethical mechanisms capable of responding to the distinctive characteristics of digital evidence and investigative technologies. The expansion of digital investigative practices necessitates not only technological modernisation but also a coherent ethical framework governing the collection, preservation, processing, examination, and use of digital information.

The findings of this study support several conclusions. First, the integration of digital technologies into investigative activities raises interconnected legal, ethical, organisational, and technical challenges that cannot be addressed solely through traditional legal regulation. The handling of digital evidence and the use of technologically assisted investigative methods require specialised expertise and a multidisciplinary approach. Ethical principles should therefore be regarded as an integral component of the regulatory framework governing digital investigations, particularly in relation to legality, proportionality, privacy, accountability, professional competence, and the protection of fundamental rights.

Second, the analysis indicates that existing ethical frameworks do not provide sufficiently detailed guidance for addressing the specific challenges associated with digital evidence. In the absence of clear ethical and procedural standards, investigators and other criminal justice professionals may be required to rely extensively on professional judgement when resolving practical issues concerning the collection, preservation, examination, and evaluation of digital evidence. This may contribute to inconsistent practices and increase the risk of using methods that lack adequate transparency, accountability, or scientific validation.

Third, clearly defined ethical standards are essential for ensuring transparency and accountability in digital investigations. Appropriate procedural and ethical requirements should facilitate the independent verification and review of investigative methods and findings, strengthen the reliability and integrity of digital evidence, and contribute to procedural fairness in criminal proceedings. Particular attention should be paid to the protection of personal data, the preservation of evidential integrity, and the documentation of actions performed on digital evidence.

Fourth, the comparative analysis demonstrates the value of adapting internationally recognised principles and best practices to the specific characteristics of Uzbekistan's legal system and criminal justice framework. Such adaptation should not consist of the direct transplantation of foreign models. Instead, relevant international approaches should be assessed in light of national legislation, institutional structures, procedural guarantees, and investigative practices. Existing codes of ethics applicable to law-enforcement authorities should accordingly be supplemented, where necessary, with principles addressing professional competence, transparency, accountability, data protection, technological accuracy, and the responsible use of digital technologies.

Finally, digital investigations should be governed by ethical requirements specifically adapted to the nature of digital evidence. These requirements should include legality and proportionality in the use of investigative technologies; the comprehensive and objective examination of digital information; the exclusion or appropriate protection of personal data that is irrelevant to the investigation; reliance on verifiable evidence when formulating conclusions; the preservation of data integrity, authenticity, and confidentiality; appropriate documentation and auditability of investigative procedures; and transparency and accountability throughout the digital evidence life cycle.

Taken together, these findings demonstrate that a coherent ethical framework for digital investigations is essential for ensuring the lawful, proportionate, transparent, and scientifically sound use of digital technologies in criminal justice. Such a framework would strengthen the protection of fundamental rights and personal data, improve the reliability and integrity of digital evidence, and enhance public confidence in digital investigative practices.

REFERENCES

Association for Computing Machinery. (2018). *ACM code of ethics and professional conduct*.

Association of Police and Crime Commissioners. (n.d.). *About the APCC*. <https://www.apccs.police.uk/about-the-apcc/>

Astanov, I., & Xamidov, B. (2021). General theoretical issues related to electronic or digital evidence: Problems and solutions. *Society and Innovations*, 2(7/S), 259–278. <https://doi.org/10.47689/2181-1415-vol2-iss7/S-pp259-278>

Balogun, A. M., & Zuva, T. (2017). Open ethical issues in digital forensic systems. *International Journal of eBusiness and eGovernment Studies*, 9(1), 55–69.

Decree of the President of the Republic of Uzbekistan No. PF–6079. (2020, October 5). *On approving the Digital Uzbekistan — 2030 strategy and measures for its effective implementation*.

Decree of the President of the Republic of Uzbekistan No. PQ–3250. (2017, August 30). *On measures to further expand the introduction of modern information and communication technologies into the activities of courts*.

Dehghantanha, A., & Franke, K. (2014). Privacy-respecting digital investigation. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST)* (pp. 129–138). IEEE. <https://doi.org/10.1109/PST.2014.6890932>

Deloitte. (n.d.). *Survey of chief officer representatives from UK police forces*.

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: A framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, 21(2), 257–290. <https://doi.org/10.1108/JIC-05-2019-0097>

GOST ISO/IEC 29100:2021: *Information technology—Security techniques—Privacy framework—Guidelines for privacy management*. (2021).

International Association of Computer Investigative Specialists. (n.d.). *PRECEPT framework resource*.

ISO/IEC 27043: *Information technology—Security techniques—Incident investigation principles and processes*. (n.d.).

ISO/IEC 29100:2011: *Information technology—Security techniques—Privacy framework*. (2011).

Judicial Ethics Code of the Republic of Uzbekistan. (2018). Resolution No. SOKQ–490–III, arts. 5–10.

Khamidov, B., & Askerov, B. (2023). Ethical principles for organizing digital investigation in the process of digital transformation: Uzbekistan and foreign experience. *International Bulletin of Applied Science and Technology*, 3(4), 917–920.

Law of the Republic of Uzbekistan No. O'RQ–547. (2019, July 2). *On personal data*.

Merck KGaA. (2021). *Code of digital ethics* (Version 1.0).

Nikkel, B. J. (2014). Fostering incident response and digital forensics research. *Digital Investigation*, 11(4), 249–251.

Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 645. (2021, October 15). *On measures for the widespread introduction of modern information technologies into the activities of internal affairs bodies*.

Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. *Journal of Digital Forensics, Security and Law*, 10(2), 43. <https://doi.org/10.15394/jdfsl.2015.1201>

South Yorkshire Police and Crime Commissioner. (n.d.). *Digital policing ethics report*. <https://southyorkshire-pcc.gov.uk/app/uploads/2020/01/Digital-Policing-Ethics-Final-for-PAB-1.pdf>

Toshev, O., & Murodkosimov, B. (2023). Digitalization of court activities contributes to ensuring justice. *Digitalization of Court Activities: Current and Prospective Tasks*, 1(1), 162–175.

Uzbekistan population exceeds 36 million people. (n.d.). <https://yuz.uz/news/ozbekiston-aholisi-36-million-kishidan-oshdi>

Xamidov, B. (2021). Verification and evaluation of digital forensic results. *Society and Innovations*, 2(3), 91–97. <https://doi.org/10.47689/2181-1415-vol2-iss3-pp91-97>



TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC
SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 3
SEPTEMBER 2026