

American Journal of Social and Humanitarian Research

**Vol. 7 Issue** 11 | **pp.** 74-83 | **ISSN:** 2690-9626
**Available online @** https://globalresearchnetwork.us/index.php/ajshr

*Article*

# International Legal Mechanisms and Cooperation in the Field of Forensic Computer-Technical Expertise

**Medetbaeva Aksungul Sharapatdin kizi[1]***

1. Lecturer of the training institute for lawyers under the Ministry of Justice, PhD student of the Republican Center of Forensic Expertise named after Kh. Suleymanova under the Ministry of Justice of the Republic of Uzbekistan, Scientific research institute of forensic expertise

* Correspondence: aksumedetbaeva@gmail.com; ORCID: 0009-0007-1157-4359

**Abstract:** The article examines the international legal mechanisms that govern cooperation in the field of digital forensics. It is argued that the transnational and volatile nature of digital evidence makes international cooperation an indispensable condition for the effectiveness of such examinations. The author analyses the procedural provisions of the Council of Europe Convention on Cybercrime and its Second Additional Protocol, the United Nations Convention against Cybercrime of 2024, the Minsk Convention of 1993, the cooperation framework of the Shanghai Cooperation Organization and the European Union rules on electronic evidence, as well as the ISO/IEC standards and the best-practice guidelines of ENFSI and INTERPOL. The degree to which these mechanisms are reflected in the legislation of the Republic of Uzbekistan is assessed, and the principal obstacles to cross-border cooperation jurisdictional uncertainty, delays in mutual legal assistance, encryption, data localization and methodological divergence - are identified. On this basis, proposals are formulated for improving national legislation, institutional arrangements and expert practice.

**Keywords:** digital forensics, digital evidence, electronic evidence, international cooperation, mutual legal assistance, Budapest Convention, UN Convention against Cybercrime, chain of custody, forensic standards, Republic of Uzbekistan.

**Citation:** Kizi, M. A. S. International Legal Mechanisms and Cooperation in the Field of Forensic Computer-Technical Expertise. American Journal of Social and Humanitarian Research 2026, 7(11), 74-82.

Received: 04th Aug 2026
Revised: 05th Sep 2026
Accepted: 08th Oct 2026
Published: 06th Nov 2026

**Copyright:** © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

## 1. Introduction

The digital transformation of social relations has fundamentally altered the evidentiary landscape of contemporary justice. Information stored on, processed by or transmitted through computer systems — from mobile devices and cloud repositories to network logs and blockchain records — now features in a growing proportion of criminal, civil and economic disputes. In the Republic of Uzbekistan, this shift is reflected in the procedural rules governing the appointment and conduct of expert examinations and the evaluation of expert opinions as a source of evidence [1]. It is also reflected in the Law "On Forensic Examination", which establishes the legal, organizational and methodological foundations of forensic examination [2]. The Law "On Cybersecurity" defines the legal framework for protecting information systems and responding to cyber incidents [3]. The Strategy "Digital Uzbekistan-2030" sets the goal of the comprehensive digitalization of public administration, the economy and the social sphere [4].

The distinctive feature of digital evidence, however, is its inherent transnationality. Data relevant to a single offence may be physically dispersed across several jurisdictions, held by service providers incorporated abroad, or replicated across data centers whose location is uncertain even to the provider itself. The comprehensive study of cybercrime prepared by the United Nations Office on Drugs and Crime demonstrated that a substantial share of cybercrime investigations has a transnational dimension, while formal mutual legal assistance procedures remain slow and poorly adapted to the volatility of electronic data [5]. Consequently, a forensic computer-technical examination conducted within a purely national framework frequently encounters objects, data and questions that lie beyond the reach of domestic authorities.

Digital evidence is, moreover, inherently fragile: it may be altered, overwritten or destroyed through the ordinary use of a device or by deliberate action, and its integrity can be demonstrated only through scientifically sound methods of acquisition and documentation [6]. These two properties — transnationality and fragility — explain why international legal mechanisms of cooperation have become indispensable for forensic computer-technical examination. The Council of Europe Convention on Cybercrime of 2001 is the first of the two principal frameworks of broad geographical reach in this field [7]. The second is the United Nations Convention against Cybercrime adopted in 2024 [8]. Each devotes particular attention to the expedited preservation, disclosure and transfer of electronic evidence.

The purpose of this article is to analyze the international legal mechanisms that govern cooperation in forensic computer-technical examination, to evaluate the extent to which these mechanisms are reflected in the legislation of the Republic of Uzbekistan, and to formulate scientifically grounded proposals for the improvement of national law and practice. To achieve this purpose, the following tasks are set: first, to clarify the legal nature of forensic computer-technical examination as an object of international cooperation; second, to examine universal, regional and comparative instruments; third, to assess the technical and methodological standards that ensure the cross-border acceptability of expert findings; and fourth, to identify the principal obstacles to cooperation and the ways of overcoming them.

## 2. Methods

### *2.1. Research materials*

The research is based on the national legislation of the Republic of Uzbekistan governing criminal procedure, forensic expert activity, cybersecurity and digital development, on international treaties of universal and regional character, on the empirical findings of international organizations concerning cross-border cooperation in cybercrime cases, and on foreign scholarly literature on digital evidence. These sources are supplemented by international technical standards, the best-practice guidelines of international forensic networks and specialized doctrinal studies, each of which is referenced at the point of its analysis.

### *2.2. Research methods*

The methodological basis of the study comprises the formal-legal (dogmatic) method, used to interpret the content of national and international norms; the comparative-legal method, used to juxtapose the cooperation models of the Council of Europe, the United Nations, the Commonwealth of Independent States, the Shanghai Cooperation Organization and the European Union; the systemic-structural method, used to identify the interrelation between legal, institutional and methodological dimensions of cooperation; and the method of legal modelling, used to formulate proposals for the improvement of the legislation of Uzbekistan. The combination of these methods ensures that the conclusions rest both on the normative text and on the practical conditions of expert work.

## 3. Results

The analysis yielded four groups of findings. They concern the legal nature of forensic computer-technical examination as an object of international cooperation, the universal and supranational instruments, the regional and comparative mechanisms, and the technical and methodological standards that make expert findings acceptable across borders.

### *3.1. Forensic computer-technical examination as an object of international cooperation*

In legal doctrine, forensic computer-technical examination is understood as a procedural action consisting of the study, by a person possessing special knowledge in computer science and information technology, of hardware, software, data and networks, conducted on the basis of a decision of the competent authority in order to establish facts relevant to a case. Under the legislation of Uzbekistan, the expert opinion constitutes an independent source of evidence [1]. Its preparation is subject to the principles of legality, independence of the expert, objectivity, comprehensiveness and completeness of research [2]. These principles are not purely domestic in character: they correspond to internationally recognized requirements for the reliability of expert evidence, which presuppose that the methods applied are tested, reproducible and properly documented.

Casey divides the digital forensic process into the stages of identification, preservation, collection, examination, analysis and reporting, emphasizing that errors committed at the earliest stages cannot be remedied by even the most sophisticated subsequent analysis [6]. Mason and Seng observe that the law of evidence in many jurisdictions has been slow to recognize the specific nature of electronic records, often attempting to fit them into categories developed for paper documents, which creates uncertainty in the assessment of their authenticity and integrity [9]. The international standard ISO/IEC 27037:2012 addresses this problem by formulating universal requirements for the identification, collection, acquisition and preservation of digital evidence, built on the principles of auditability, repeatability, reproducibility and justifiability [10].

Kerr argues that digital evidence has generated a new criminal procedure, because traditional rules on search and seizure, designed for tangible objects, do not fit the two-stage process in which a device is first seized and only later searched forensically [11]. This observation is directly relevant to international cooperation: when a device or a data set is obtained in one state and examined in another, the legal regime governing each stage may differ substantially. The analysis and interpretation of data — the core of the expert's work — are subject to separate standardization in ISO/IEC 27042:2015, which requires that the examiner's conclusions be traceable to the underlying data and that alternative explanations be duly considered [12].

Accordingly, international cooperation in forensic computer-technical examination encompasses at least four interrelated dimensions: (a) procedural-legal cooperation in obtaining, preserving and transferring digital evidence; (b) institutional cooperation among forensic laboratories and expert bodies; (c) methodological cooperation aimed at the harmonization of techniques and standards; and (d) educational and scientific cooperation, including joint training, proficiency testing and research. Only the combination of these dimensions ensures that an expert opinion prepared with the involvement of foreign elements will be recognized as admissible and reliable.

### *3.2. Universal and supranational instruments*

The Council of Europe Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, was the first binding international treaty addressing crimes committed through computer networks [7]. Its procedural part obliges the parties to provide for the expedited preservation of stored computer data, the expedited preservation and partial disclosure of traffic data, production orders, the search and seizure of stored computer data, and the real-time collection of traffic data and interception of content data [7]. Chapter III establishes the regime of international cooperation: the general principles of mutual assistance; the expedited preservation of stored data at the request of another party; the expedited disclosure of preserved traffic data; mutual assistance in accessing

stored data; trans-border access to stored data with consent or where the data are publicly available; and a network of contact points available twenty-four hours a day, seven days a week [7].

For forensic examination, the significance of these provisions lies in the fact that a preservation order "freezes" data before they can be lost, thereby creating the conditions for a subsequent qualified expert study. Clough nevertheless observes that the Convention achieved the harmonization of substantive and procedural law only to a limited degree, since it leaves considerable discretion to the parties and permits numerous reservations, which in practice results in uneven levels of implementation [13]. In other words, the Convention establishes a common minimum, but not a uniform procedure, and an expert working with evidence obtained under it must still take into account the national rules of the state in which the data were secured.

The Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence, opened for signature on 12 May 2022, responds directly to the challenges of cloud computing [14]. It provides for requests for domain name registration information; direct cooperation with service providers in other parties for the disclosure of subscriber information; giving effect to orders from another party for the expedited production of data; expedited disclosure in emergencies; emergency mutual assistance; video conferencing; and joint investigation teams, all accompanied by a detailed regime for the protection of personal data [14]. The provision on video conferencing is of particular importance for forensic science, since it allows an expert located in another state to be heard without his or her physical presence, while joint investigation teams create a legal basis for experts from several states to work together on the same evidentiary material.

The United Nations Convention against Cybercrime, adopted by General Assembly resolution 79/243 of 24 December 2024, is the first treaty in this field negotiated within a universal forum [8]. It covers criminalization, procedural measures and international cooperation, including the collection and sharing of evidence in electronic form, the expedited preservation of stored data, mutual legal assistance and a network of points of contact, together with provisions on technical assistance and capacity building [8]. Significantly, its cooperation mechanisms extend not only to offences against information systems but also to the gathering of electronic evidence of other serious crimes [8]. For states that are not parties to the Budapest Convention, including the Republic of Uzbekistan, the United Nations Convention therefore opens a universal channel of cooperation that does not depend on membership of a regional organization, and its mechanisms are relevant to the entire spectrum of computer-technical examinations rather than only to cases concerning offences against information security.

### *3.3. Regional and comparative mechanisms*

Within the Commonwealth of Independent States, the principal legal basis for cooperation of Uzbekistan in criminal matters remains the Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters, signed in Minsk on 22 January 1993 [15]. Under this Convention, legal assistance includes the performance of procedural actions, among them the conduct of expert examinations, and requests are executed in accordance with the law of the requested party, which may, at the request of the requesting party, apply the procedural rules of the latter insofar as they do not contradict its own legislation [15]. The Minsk Convention thus permits an expert examination to be ordered in another member state; however, it was designed for the era of paper documents and contains neither mechanisms for the expedited preservation of volatile data nor rules on direct cooperation with service providers.

The Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security, signed in Yekaterinburg on 16 June 2009, identifies the use of information and communication technologies for criminal purposes as one of the principal threats and provides for cooperation among competent authorities, the exchange of information, and joint research and training [16]. This instrument creates a valuable

political and institutional framework for Uzbekistan in its regional environment, yet it is largely declaratory in nature and does not establish procedural mechanisms for the preservation, transfer and expert examination of digital evidence.

The legislation of the European Union offers an instructive comparative model. Regulation (EU) 2023/1543 introduces European Production Orders and European Preservation Orders, enabling a judicial authority of one member state to address a service provider established in another member state directly [17]. Providers must respond within ten days, or within eight hours in emergency cases, and the Regulation has applied since 18 August 2026 [17]. The Regulation distinguishes between subscriber data, data requested for the sole purpose of identifying the user, traffic data and content data, attaching differentiated safeguards to each category [17]. Although it does not apply to Uzbekistan, it clearly demonstrates the global trend of moving from classical state-to-state mutual legal assistance towards direct, time-bound cooperation with providers — a trend that national legislators cannot ignore.

The comparative characteristics of the instruments examined above are summarised in Table 1.

**Table 1. Comparative characteristics of international instruments on cooperation in obtaining and examining digital evidence**

| Instrument | Nature and scope | Mechanisms relevant to forensic examination | Significance for Uzbekistan |
|---|---|---|---|
| Budapest Convention, 2001 | Council of Europe treaty open to non-member states | Expedited preservation and disclosure; production orders; search and seizure; 24/7 network | Not a party; accession possible upon invitation |
| Second Additional Protocol, 2022 | Supplement to the Budapest Convention | Direct cooperation with providers; emergency assistance; video conferencing; joint investigation teams | Available only to parties to the Convention |
| UN Convention against Cybercrime, 2024 | Universal treaty | Collection and sharing of electronic evidence of serious crimes; preservation; 24/7 network; capacity building | Potential universal basis for cooperation |
| Minsk Convention, 1993 | CIS multilateral treaty on legal assistance | Conduct of expert examinations upon request; execution under the law of the requested party | In force; principal channel with CIS states |
| SCO Agreement, 2009 | Regional framework agreement | Information exchange; cooperation of competent authorities; joint research and training | Member state; framework without procedural tools |
| Regulation (EU) 2023/1543 | Supranational EU act | European Production and Preservation Orders; 10-day and 8-hour deadlines | Not applicable; comparative model |

### *3.4. Technical and methodological harmonisation*

Legal mechanisms alone are insufficient: the results of an examination conducted in one jurisdiction must also be scientifically acceptable in another. The Best Practice Manual for the Forensic Examination of Digital Technology adopted by the European Network of Forensic Science Institutes sets out a comprehensive framework covering case assessment, the handling of evidence, examination methods, the validation of tools and methods, documentation, reporting and quality assurance, including participation in

proficiency tests [18]. The Global Guidelines for Digital Forensics Laboratories issued by INTERPOL in 2019 contain recommendations on the establishment and operation of laboratories, the competence of personnel, infrastructure, the handling of digital evidence at every stage and the importance of accreditation against internationally recognized standards [19]. Together with the ISO/IEC standards discussed above, these documents form a common methodological language that enables experts from different legal systems to understand, verify and rely upon each other's findings.

For the Republic of Uzbekistan, this means that the accreditation of the computer-technical divisions of forensic institutions against international standards, the documented validation of software and hardware tools, and the maintenance of chain-of-custody records in a form compatible with international practice would substantially increase the cross-border recognition of national expert opinion.

Particular attention should be paid to the chain of custody. When digital evidence is obtained through international cooperation, it must be accompanied by documentation recording the cryptographic hash values of the acquired data, the tools and versions used, the time and circumstances of acquisition, and every subsequent transfer. In the absence of such documentation, an expert in the requesting state cannot confirm that the material examined is identical to the material seized abroad, and the evidentiary value of the entire examination is called into question. It is therefore advisable to develop a standard form for requests concerning digital evidence and for the transmission of such evidence, setting out the minimum technical information that must accompany the data.

## 4. Discussion

### *4.1. Principal obstacles to cooperation*

The findings show that, even where suitable instruments exist, five principal obstacles impede effective cooperation in forensic computer-technical examination.

The first obstacle is jurisdictional uncertainty. In cloud environments, data may be fragmented and continuously moved between servers in different countries, so that the traditional territorial link between data and the state in which they are stored becomes weak or entirely lost. As a result, it is often unclear to which state a request should be addressed and which law governs access to the data. This uncertainty affects the forensic expert directly, since the legality of the method by which the data were obtained determines whether the subsequent expert opinion may be used as evidence.

The second obstacle is time. Formal mutual legal assistance proceedings frequently take months, whereas log files, cached data and volatile memory may be lost within hours or days. Expedited preservation mechanisms and 24/7 networks are designed precisely to address this asymmetry [7]. Yet they can be used only by states that participate in the relevant instruments. The third obstacle is technological: widespread encryption, anti-forensic techniques and the rapid evolution of devices and operating systems demand constant updating of expert methods and tools, which is beyond the capacity of any single laboratory acting in isolation.

The fourth obstacle concerns the protection of personal data and the localization of data. The Law of the Republic of Uzbekistan "On Personal Data" regulates the cross-border transfer of personal data and, following its subsequent amendments, establishes requirements for the storage of personal data of citizens of Uzbekistan on technical means located within the territory of the Republic [20]. This approach facilitates access by national authorities to data held domestically, but it may complicate the execution of incoming foreign requests and creates expectations of reciprocity in outgoing ones. The experience of the Second Additional Protocol, which integrates detailed data-protection safeguards into the cooperation mechanism itself, shows that the effectiveness of cooperation and the protection of privacy can be reconciled through clear procedural guarantees [14].

The fifth obstacle is the divergence of procedural models. In continental systems, including that of Uzbekistan, the expert is appointed by the competent authority and his or her opinion constitutes an independent source of evidence, whereas in adversarial systems expert testimony is typically introduced by the parties and tested through cross-

examination. Consequently, the evidentiary value of an expert opinion prepared abroad, or of the findings of a foreign specialist, must be resolved through the general rules on the admissibility and evaluation of evidence established by the Criminal Procedure Code [1]. Finally, disparities in technical capacity among states hinder equal participation in cooperation. For this reason, the United Nations Convention gives particular weight to technical assistance and capacity building [8]. The INTERPOL guidelines likewise stress the development of laboratory capacity [19].

### *4.2. Directions for improving the legislation and practice of Uzbekistan*

On the basis of the foregoing analysis, the following proposals are formulated. **First**, it is advisable to consider the participation of the Republic of Uzbekistan in the United Nations Convention against Cybercrime as a universal basis for cooperation in the gathering and sharing of electronic evidence [8]. It is also advisable to study the possibility of acceding to the Budapest Convention, which would open access to the mechanisms of its Second Additional Protocol [14]. These tracks are not mutually exclusive, and their parallel use would maximize the number of states with which effective cooperation can be established.

**Second**, the Criminal Procedure Code should be supplemented with detailed rules on cross-border electronic evidence, including the expedited preservation of computer data at the request of a foreign state, the expedited disclosure of traffic data, the hearing of experts by video conference and the participation of national experts in joint investigation teams, drawing on the procedural models of the international instruments examined above [1]. **Third**, it is expedient to designate a national contact point operating twenty-four hours a day, seven days a week, with the mandatory involvement of specialists in forensic computer-technical examination, so that requests for preservation are formulated in a technically correct manner from the outset.

**Fourth**, the requirements for the acquisition, preservation and documentation of digital evidence should be consolidated in departmental methodological documents in a manner consistent with ISO/IEC 27037 [10]. The interpretation of data should likewise follow ISO/IEC 27042 [12]. The forensic computer-technical divisions of national expert institutions should be accredited against international standards and participate regularly in international proficiency tests. **Fifth**, the conclusion of memoranda of cooperation between national forensic institutions and foreign forensic laboratories, as well as the use of the platforms of INTERPOL and the Shanghai Cooperation Organization for joint training and research, would strengthen the institutional and educational dimensions of cooperation. **Sixth**, the provisions of the Law "On Personal Data" on cross-border transfer should be supplemented with clear procedures for the disclosure of data in response to foreign requests in criminal matters, accompanied by safeguards comparable to international standards [20].

## 5. Conclusion

The study has shown that the transnational and fragile nature of digital evidence makes international cooperation an indispensable condition for the effectiveness of forensic computer-technical examination. Such cooperation is multidimensional and includes procedural-legal, institutional, methodological and educational components, each of which is necessary for an expert opinion with foreign elements to be recognized as admissible and reliable.

At the international level, the Budapest Convention and its Second Additional Protocol have created an advanced system of expedited preservation, disclosure and direct cooperation with service providers, while the United Nations Convention against Cybercrime offers, for the first time, a universal framework open to all states. The European Union rules on production and preservation orders illustrate the global trend towards direct and time-bound cooperation. At the same time, the instruments currently applicable to Uzbekistan — the Minsk Convention and the cooperation framework of the Shanghai Cooperation Organization — do not contain procedural mechanisms adapted to the specific features of digital evidence.

National legislation of Uzbekistan provides a solid foundation for forensic expert activity and for cybersecurity and digital development, yet it requires further development with respect to cross-border electronic evidence. The implementation of the proposals formulated in this article — participation in universal instruments, the supplementation of the Criminal Procedure Code, the establishment of a 24/7 contact point, the harmonization of methodological requirements with international standards, the accreditation of expert divisions and the refinement of personal data legislation — would integrate national forensic computer-technical examination into the global system of cooperation and enhance the protection of the rights and legitimate interests of citizens in the digital environment.

**REFERENCES**


[1] Criminal Procedure Code of the Republic of Uzbekistan, Sep. 22, 1994. [Online]. Available: https://lex.uz/mact/111460

[2] Law of the Republic of Uzbekistan "On Forensic Examination." [Online]. Available: https://lex.uz/docs/6809379

[3] Law of the Republic of Uzbekistan "On Cybersecurity," No. LRU-764, Apr. 15, 2022. [Online]. Available: https://lex.uz/en/docs/6997403

[4] President of the Republic of Uzbekistan, "On approval of the 'Digital Uzbekistan-2030' Strategy and measures for its effective implementation," Decree No. PD-6079, Oct. 5, 2020. [Online]. Available: https://lex.uz/en/docs/5031048

[5] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime: Draft*. New York, NY, USA: United Nations, 2013. [Online]. Available: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[6] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. Waltham, MA, USA: Academic Press, 2011.

[7] Council of Europe, *Convention on Cybercrime*, ETS No. 185, Budapest, Hungary, Nov. 23, 2001. [Online]. Available: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[8] United Nations General Assembly, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, Res. 79/243, Dec. 24, 2024.

[9] S. Mason and D. Seng, Eds., *Electronic Evidence and Electronic Signatures*, 5th ed. London, U.K.: Univ. London Press, Inst. Advanced Legal Studies, 2021.

[10] *Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, ISO/IEC 27037:2012, Int. Org. Standardization, Geneva, Switzerland, 2012.

[11] O. S. Kerr, "Digital evidence and the new criminal procedure," *Columbia Law Rev.*, vol. 105, no. 1, pp. 279–318, 2005.

[12] *Information Technology — Security Techniques — Guidelines for the Analysis and Interpretation of Digital Evidence*, ISO/IEC 27042:2015, Int. Org. Standardization, Geneva, Switzerland, 2015.

[13] J. Clough, "A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation," *Monash Univ. Law Rev.*, vol. 40, no. 3, pp. 698–736, 2014.

[14] Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, CETS No. 224, May 12, 2022. [Online]. Available: https://rm.coe.int/1680a49c9d

[15] *Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters*, Minsk, Belarus, Jan. 22, 1993. [Online]. Available: https://lex.uz/docs/2741647

[16] *Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security*, Yekaterinburg, Russia, Jun. 16, 2009.

[17] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *Off. J. Eur. Union*, L 191, pp. 118–180, Jul. 28, 2023.

[18] European Network of Forensic Science Institutes, *Best Practice Manual for the Forensic Examination of Digital Technology*, ENFSI, 2015.

[19] INTERPOL, *Global Guidelines for Digital Forensics Laboratories*. Lyon, France: INTERPOL, 2019.

[20] Law of the Republic of Uzbekistan "On Personal Data," No. LRU-547, Jul. 2, 2019. [Online]. Available: https://lex.uz/docs/4831939