Legal and Institutional Challenges of Digital Forensics: An Integrated Regulatory Model

Kamran Khalilov
Baku State University, Baku, Azerbaijan
Heydar Aliyev Academy of the State Security Service, Baku, Azerbaijan
kamran.khalilov.isa@bsu.edu.az

***Abstract*— The development of digital technologies has significantly transformed the nature of evidence and its use in criminal proceedings. This study examines the legal and institutional challenges of digital forensics, focusing on proportionality, reliability of evidence, jurisdiction, technological oversight, and artificial intelligence. The research is based on doctrinal and comparative legal methods. The analysis demonstrates that the existing legal framework does not fully align with technological capabilities, creating risks for legal certainty, reliability of evidence, and fair trial guarantees. To address these challenges, the study proposes a legally integrated model that conceptualizes digital evidence within a unified and systematic legal framework.**

Keywords*— *digital forensics; electronic evidence; proportionality principle; cross-border data access; artificial intelligence.

I. INTRODUCTİON

The rapid development of digital technologies has significantly affected the nature of the evidentiary system and its mechanisms of application in criminal proceedings [1]. A substantial portion of the information used in modern criminal investigations is no longer created, stored, and transmitted in a physical environment, but rather within digital platforms. This transformation is not limited to an increase in the types of evidence; it also reshapes the rules governing the collection, preservation, evaluation, and admissibility of evidence before courts [2].

Traditional criminal procedural law has been based on the stability and observable characteristics of physical evidence. However, digital evidence possesses a fundamentally different ontological nature. It is inherently changeable, easily reproducible, and dependent on technical systems. These features complicate the application of classical legal categories and necessitate their adaptation to the digital environment [2]. For instance, investigative measures such as search and seizure, originally designed for physical objects, may lead to excessively broad intrusions into private life when applied in digital contexts [3]. At the same time, the determination of evidentiary authenticity is no longer linked to a physical carrier, but rather to the technical integrity of the data.

This transformation requires a reconsideration of law not only at the normative level but also at the institutional and technological levels. Digital forensics should no longer be viewed merely as a technical field of expertise, but as a domain that plays a significant role in the formation of legal decisions. Within this system, legal norms, technical protocols, and algorithmic tools interact with one another [4].

In the Republic of Azerbaijan, recent amendments to criminal procedural legislation may be regarded as important steps toward the recognition of electronic evidence and the establishment of procedures related to digital data [5]. Nevertheless, the existing approach still lacks a systematic character and does not provide a comprehensive model regulating the legal regime of digital evidence.

In this context, the aim of this study is to analyse the legal and institutional challenges of digital forensics across five key dimensions:

- legality and proportionality;
- chain of custody and authenticity of evidence;
- jurisdiction and digital sovereignty;
- code-based regulation;
- artificial intelligence and algorithmic transparency.

Relying on doctrinal and comparative legal methods, the study examines national legislation in light of international legal standards and academic approaches. The main thesis of the research is that the effective and legitimate use of digital evidence cannot be ensured solely by expanding technical capabilities, but also requires strengthening constitutional safeguards, procedural transparency, and institutional accountability.

II. LEGAL AND INSTİTUTİONAL CHALLANGES IN DIGITAL FORENSIC

The challenges associated with digital forensics are not limited to technical issues alone. The difficulties arising in this field also have a direct impact on the application of fundamental principles of criminal procedural law. The collection, preservation, and evaluation of evidence in digital environments do not fully correspond to classical legal approaches, giving rise to a number of new challenges. The analysis conducted demonstrates that the legal regime of digital evidence faces difficulties in several key areas. These challenges are particularly evident in defining the limits of state interference and in applying the principle of proportionality.

2.1. Principles of Legality and Proportionality in the Collection of Digital Evidence

The collection of evidence in the digital environment

DOI: 10.25045/forensic.gov.2026.78

represents one of the most sensitive issues in criminal procedural law. Under the traditional approach, investigative measures such as search and seizure are carried out in relation to physical objects. However, the characteristics of digital devices and information systems complicate the application of these rules. For this reason, the application of the principles of legality and proportionality in the digital context becomes particularly important.

In constitutional law doctrine, the principle of proportionality serves as a key instrument for assessing the legitimacy of state interference [6]. According to Article 71.2 of the Constitution of the Republic of Azerbaijan, restrictions on rights and freedoms must be proportionate to the intended objective pursued by the state [7]. In legal doctrine, the balancing approach developed by Robert Alexy provides that any interference with a right can be justified only if three conditions are met: the legitimacy of the objective, the necessity of the measure, and the proportionality of its application [8]. This approach is particularly relevant in the context of digital evidence, as the object of interference is no longer a specific physical space, but rather the digital environment related to an individual's private life.

Digital devices are not merely technical tools; they constitute an information environment reflecting almost all aspects of an individual's daily life. In this respect, their examination entails a significantly broader and deeper interference compared to traditional search methods. This perspective is indirectly supported by the case law of the European Court of Human Rights. In Benedik v. Slovenia, the Court held that access to data related to the identification of an internet user must be assessed within the framework of the protection of private life. This approach demonstrates that digital data is not purely technical in nature and that its collection always requires proper legal justification [3].

In this context, the main problem lies in the fact that traditional search mechanisms are based on the principle of the full seizure of an object. In the case of physical evidence, this approach is generally justified, as the evidentiary value is directly linked to the integrity of the object itself. However, in the digital environment, such an approach creates significant risks. The seizure of a device effectively provides access to all data stored on it, including personal communications, photographs and videos, financial information, and other sensitive data. This may result in investigative authorities gaining control over information that is unrelated to the criminal case [9].

The principle of proportionality requires limiting state interference in such situations. Specifically, investigative authorities should have access only to data relevant to the criminal offence, while interference with unrelated data must be minimized. This approach is commonly described as a "targeted access" model and has been gaining increasing importance in contemporary European legal practice. According to this model, digital search measures should be conducted based on predefined parameters, ensuring that only data relevant to the specific offence is selected [10].

Recent amendments to the criminal procedural legislation of the Republic of Azerbaijan may be considered an important step toward the recognition of electronic evidence [5]. However, the specification of the principle of proportionality at this level has not yet been fully ensured. The existing provisions primarily regulate the fact of evidence collection, but do not sufficiently define clear limitations regarding the scope and content of the data obtained. This creates broad discretion in practice and poses risks to the protection of individual rights.

Furthermore, the intensity of interference in the digital environment cannot be measured through classical legal categories. For instance, a physical search is typically a one-time measure limited in duration. In contrast, access to digital data often has a continuous character and allows for further analysis at later stages. This requires the assessment of interference not only at the initial stage, but throughout the entire process [11].

In this context, the principle of legality also acquires a new dimension. Legality requires not only the formal existence of a legal basis for interference, but also that such interference be regulated in a sufficiently precise and foreseeable manner. If the normative framework grants investigative authorities broad and undefined powers, this may be considered inconsistent with the principle of legal certainty [12].

The above considerations demonstrate that the main challenge in the collection of digital evidence lies in the mismatch between the breadth of technical capabilities and the adequacy of legal safeguards. Addressing this mismatch requires improvements in criminal procedural legislation in several key areas. First, specific and narrowly defined authorization mechanisms for digital search measures should be established. In addition, it must be ensured that investigative authorities have access only to data relevant to the specific offence, while interference with excessive or unrelated data is prevented. At the same time, both legal and technical mechanisms should be developed to protect data unrelated to the offence. Finally, the application of the principle of proportionality must be ensured at all stages of the interference.

As can be observed, the development of digital forensics requires a reassessment of the principles of legality and proportionality not only in their formal sense, but also in their substantive dimension. The recognition of digital devices as tools that contain information related to an individual's private life serves as a key approach in this regard and provides a theoretical basis for future legal reforms.

2.2. Chain of Custody and the Problem of Authenticity of Digital Evidence

Once issues of legality and proportionality in the collection of digital evidence have been established, the next major concern relates to how its reliability is ensured. While legal justification plays a central role at the stage of evidence collection, at subsequent stages—namely, preservation, transfer, and presentation—the key issue becomes ensuring its authenticity and integrity.

In traditional criminal procedural law, this issue is addressed through the institution of the "chain of custody." This mechanism requires the documentation and control of all stages through which evidence passes, from the moment it is obtained to its presentation in court. For physical evidence, this approach

is generally considered effective, as the identification and integrity of an object can be determined through its visual and physical characteristics.

However, this approach cannot be applied in the same manner in the digital environment. Unlike physical evidence, digital data does not possess a stable character. It can be altered, copied, and presented in different formats within a very short period of time. Therefore, the reliability of digital evidence depends less on the medium on which it is stored and more on how it is obtained and preserved. As noted by Eoghan Casey, the primary focus in this field lies on the proper identification and preservation of data. This indicates that the originality of digital evidence is not defined by the notion of a "first copy," but rather by the technical verification of its integrity. For this reason, hash functions play a crucial role in verifying the integrity of digital evidence [1].

A hash function generates a unique digital summary of a given dataset, and even the slightest modification to the data results in a change in this summary. This property provides an objective and reliable mechanism for verifying the integrity of digital evidence [13]. In contemporary forensic practice, a bit-by-bit copy of the evidence is created at the time of acquisition, and a hash value is calculated for that copy. At later stages, this value is used to determine whether the data has been altered.

Nevertheless, the legal challenge lies in the fact that these technical procedures are often not regulated with sufficient precision at the normative level. As noted in the legal literature by Stephen Mason and Daniel Seng, the admissibility of digital evidence depends not only on its existence, but also on whether the process of its acquisition and preservation is transparent and verifiable [2].

In international practice, certain standards have been developed in this area. For instance, ISO/IEC 27037:2012 establishes technical and methodological principles for the identification, collection, and preservation of digital evidence [14]. Although these standards do not constitute binding legal rules, they are widely used as guiding frameworks for procedural activities in many jurisdictions and are taken into account by courts in the evaluation of evidence.

In the criminal procedural legislation of the Republic of Azerbaijan, the regulation of the chain of custody of digital evidence remains largely general in nature. Although the existing provisions define the procedures for the seizure and formalization of evidence, the question of how its technical integrity should be ensured remains insufficiently addressed. In particular, several elements have not been clearly specified at the normative level: a) the procedure for creating copies of digital data; b) the calculation and documentation of digital fingerprint (hash) values; c) the recording of subsequent operations performed on the evidence (such as analysis, copying, etc.); d) the tracking of who accessed and used the evidence, and how, at different stages.

These gaps create significant legal risks in practice. If the integrity of evidence cannot be technically verified, its admissibility as reliable evidence before a court may be called into question. In such cases, the evidentiary value may depend on subjective assessment, which could conflict with the presumption of innocence [15].

Another important issue concerns the reinterpretation of the concept of the "chain of custody" in the digital environment. The classical approach is based on tracking the physical movement of evidence. However, for digital evidence, a more appropriate model should be based on the "integrity of the process" [16]. Within this model, primary attention is given to the method of data acquisition, the technical tools used, the applied methodology, and the consistent documentation of all operations performed. This approach makes it possible to track not only where the evidence is, but also what has been done with it.

The development of digital forensics demonstrates that the reliability of evidence is no longer ensured solely through legal procedures, but also through technical means. This requires a closer integration between law and technology. Taking this reality into account, legislation should define the legal status of technical procedures. In this regard, several improvements may be considered necessary within Azerbaijani criminal procedural law. First, the application of hash-based verification mechanisms in the collection of digital evidence should be formally recognized at the normative level [13]. In addition, uniform standards should be established for documenting all stages of evidence processing, and the reliability and suitability of the technical tools used should become subject to legal oversight. Furthermore, the defence should be provided with effective opportunities to verify the technical integrity of the evidence [17].

Thus, the concept of the chain of custody, in its classical form, is insufficient for the digital environment. It should be replaced by a more complex model based on the principles of technical verification, transparency of the process, and verifiability. The formal recognition of such a model at the legal level constitutes one of the fundamental conditions for ensuring the legitimacy of digital forensics.

2.3. Jurisdiction and Digital Sovereignty: The Legal Paradox of Cross-Border Access to Evidence

Once the technical and procedural aspects of the collection and preservation of digital evidence have been established, the next fundamental issue concerns how such evidence is regulated within the framework of jurisdiction. Classical criminal procedural law closely links the collection of evidence to the territorial sovereignty of the state. According to this approach, investigative authorities may directly access evidence located within their own jurisdiction, while in other cases they must rely on mechanisms of international legal assistance.

However, the digital environment fundamentally alters this approach. Data is no longer tied to a specific physical location; it may be stored on multiple servers, exist simultaneously across several jurisdictions, or be distributed within cloud infrastructures. This situation complicates the application of the traditional territorial principle. For this reason, as noted by Jennifer Daskal, control over data should be determined not by its physical location, but by who has actual control over it.

This transformation creates a significant legal paradox. On the one hand, states seek rapid access to digital evidence to

ensure effective criminal investigations. On the other hand, such access often requires interference with data located in different jurisdictions, raising sensitive issues related to sovereignty and human rights. As a result, the concept of "digital sovereignty" is emerging as an alternative to the classical model of sovereignty.

At the international level, one of the primary mechanisms addressing this issue is the 2001 Convention on Cybercrime (Budapest Convention). While the Convention facilitates cooperation between states, it also requires the protection of human rights in the exercise of procedural powers. In particular, Article 15 of the Convention establishes the principles of legality, proportionality, and necessity as fundamental conditions for the collection of evidence. Nevertheless, traditional mutual legal assistance mechanisms (MLATs) are associated with significant limitations in the digital context. These procedures are often time-consuming and lose effectiveness in the face of rapid technological development. Since digital evidence can be quickly altered or deleted, delays increase the risk of its loss. For this reason, recent years have seen growing efforts to develop more flexible mechanisms.

In this context, the Second Additional Protocol to the Budapest Convention (2022) is of particular importance. This instrument allows, in certain cases, for direct cooperation between states and service providers, enabling faster access to data. However, this approach raises new legal questions: can direct requests to service providers be regarded as interference with the jurisdiction of other states? How will individual rights be protected in this process?

Within the European Union, a different approach has been developed under Regulation (EU) 2023/1543. This framework aims to accelerate the collection of evidence by imposing direct legal obligations on service providers. At the same time, it is accompanied by procedural safeguards and oversight mechanisms designed to maintain a proper legal balance.

At the national level, this issue is of particular relevance. While Azerbaijan is part of the international system for combating cybercrime, it also depends on global platforms and foreign service providers for access to digital evidence. This dependence limits the practical effectiveness of classical jurisdictional mechanisms. Although the existing legal framework is primarily based on international legal assistance procedures, the speed and flexibility of these mechanisms do not fully meet the demands of the digital environment.

On the other hand, the expansion of cross-border access mechanisms without adequate legal safeguards increases the risk of violations of individual rights. Fundamental rights such as the protection of personal data, the confidentiality of communications, and the right to a fair trial play a central role in this process. In this regard, the issue of jurisdiction should be understood not only as a technical or institutional problem, but also as a constitutional and human rights concern.

For this reason, the contemporary approach requires balancing two key objectives: ensuring rapid access to evidence for the effective functioning of investigative authorities, and safeguarding individual rights and state sovereignty. Achieving this balance necessitates improvements in several areas. First, more flexible mechanisms for cross-border access to evidence should be established, accompanied by appropriate legal safeguards, and transparency in legal procedures should be ensured within the framework of cooperation with service providers. In addition, the application of human rights standards in the process of accessing data must be strengthened.

As a result, the concept of jurisdiction in the digital environment moves away from the classical territorial principle and evolves into a more complex and multi-layered structure. The notion of "digital sovereignty" serves as the legal expression of this transformation and redefines states' ability to access evidence. However, this process should be assessed not only in terms of efficiency, but also from the perspective of legal legitimacy and the protection of human rights.

2.4. *"Code-Based Regulation" and "Lex Informatica": The Technological Transformation of Law in Digital Forensics*

The challenges related to the collection, preservation, and cross-border access to digital evidence cannot be explained solely by normative gaps or the insufficiency of institutional mechanisms. A deeper cause of these problems lies in the inability of classical forms of law to adapt to technological structures operating within the digital environment. In this context, the approaches of "code-based regulation" and "lex informatica" are of particular importance.

The core idea of this approach was first systematically articulated by Lawrence Lessig. According to his well-known thesis that "code is law," behavior in the digital environment is regulated not only through legal norms, but also through the architecture of software systems [18]. In other words, code is not merely a technical tool, but also functions as a mechanism that effectively enforces legal norms.

This approach is particularly relevant in the field of digital forensics. The tools used by investigative authorities for data extraction, filtering, and analysis determine how evidence is presented and, ultimately, which facts are "visible" to the court. In this respect, legal decisions are shaped not only by the application of normative rules, but also by the characteristics of the technological tools employed.

This situation raises a new legal question: if the processes of selecting and presenting evidence are influenced by technological algorithms, should these algorithms themselves become subject to legal evaluation? In response, the concept of "lex informatica," advanced by Joel Reidenberg, suggests that rules in the information environment are shaped not only through legal acts, but also through technological design [19].

This perspective has been further developed by Mireille Hildebrandt, who argues that it raises serious concerns from the standpoint of the rule of law. If legal outcomes depend on the internal logic of software systems, and that logic is not transparent, the predictability of law and individuals' ability to align their behavior with legal requirements are undermined [20].

In the context of digital forensics, this problem manifests itself in concrete situations. For example, determining which files are considered relevant during data extraction, filtering large volumes of data to isolate information related to a specific case, accurately interpreting timestamps indicating when files

were created, modified, or accessed, and the methods used to recover deleted data are all of particular importance in this regard.

Each of these processes has a direct impact on the legal outcome. However, in most cases, these technical operations are only described in general terms in legal documents, without detailed explanation of how they are carried out. This raises questions regarding the objectivity of the evidence. The core of the problem is that, although law formally exists, the actual decision-making process is significantly influenced by technological systems. This creates a reality not fully anticipated by the classical model of law and results in a gap between normative rules and technological design [21].

To address this gap, the integration of law and technology is considered essential. This integration should not be limited to the application of technical standards, but must also include the establishment of legal oversight mechanisms. Specifically, the tools used in digital forensics should meet several requirements. First, the methodology of the software employed should be transparent at least to a minimum extent, and the results produced by algorithms should be verifiable and reproducible. In addition, the processes of evidence selection and filtering must be properly documented. This approach is also consistent with the principles of "privacy by design" and "accountability by design," which require that legal safeguards be embedded within the architecture of the system itself, rather than applied solely through ex post control mechanisms [22].

For Azerbaijan, this issue remains at an early stage of development. Existing legislation primarily regulates the procedures for the collection and use of evidence, but the legal status of the technological tools used in these processes, as well as the mechanisms for their oversight, are not sufficiently clear. This may lead, in practice, to the automatic acceptance of the outputs generated by investigative tools as reliable. Such a situation should be regarded as problematic from the perspective of the rule of law [23]. If the technological instruments that shape the information on which legal decisions are based remain outside effective oversight, this undermines the objectivity of the legal process.

Thus, the concept of "code-based regulation" in the field of digital forensics demonstrates that law is entering a new stage of development. Law can no longer be understood solely as a system of written norms, but must be seen as a complex regulatory mechanism implemented through technological systems [24]. This reality requires that the technological dimensions of the legal system also be brought under normative and institutional control.

2.5. Artificial Intelligence and the "Black Box" Problem: Algorithmic Transparency and the Right to a Fair Trial in Digital Forensics

The development of digital forensics is not limited to changes in the methods of data collection and analysis; it also affects how such data is evaluated. One of the key issues in this field is the use of artificial intelligence technologies in investigative and forensic activities. Modern forensic tools no longer merely present data; they process, categorize, and in some cases generate conclusions. This creates new legal challenges.

At the core of these challenges lies the "black box" phenomenon. As described by Frank Pasquale, modern algorithmic systems are often opaque to users, making it difficult to understand how decisions are made [25]. This characteristic poses particular risks in the context of digital forensics, as investigative and judicial decisions may rely on the outputs generated by such systems.

The use of AI-based tools offers several advantages, including the rapid analysis of large volumes of data, the identification of patterns, and the detection of relationships that may not be easily observable by humans. However, these advantages raise significant legal questions in terms of procedural safeguards. The central issue concerns the legal status of the outputs generated by these systems. Should they be accepted as direct evidence, or should they be treated merely as expert opinion?

This issue is closely linked to the fundamental elements of the right to a fair trial. Where judicial decisions are based on the outputs of artificial intelligence systems, the ability of the defence to challenge those outputs may be limited. In particular, when the functioning of an algorithm is unknown or protected as a commercial secret, the parties do not have equal opportunities to access and contest the evidence. This is inconsistent with the principle of equality of arms as developed in the case law of the European Court of Human Rights. As stated in Dombo Beheer B.V. v. the Netherlands, a fair trial cannot be ensured without equality in the parties' ability to access and challenge evidence. In that case, the Court emphasized that each party must be given a reasonable opportunity to present its case and to contest the evidence of the opposing party [26]. This approach demonstrates that both parties must be afforded real and effective participation in the process of evaluating evidence.

Accordingly, if the prosecution relies on an AI-based tool, the defence must be provided with effective opportunities to verify and challenge its outputs. In the absence of such opportunities, the proceedings may appear formally balanced but are, in substance, unequal. From this perspective, the key legal conclusion is that results generated by artificial intelligence should not be treated as independent and conclusive evidence, but rather as expert opinion that is subject to verification and contestation [27]. This issue is not merely theoretical, but has clear practical implications. Certain algorithms used in digital forensic tools perform functions such as automated filtering, risk assessment, or behavioural analysis. The criteria and models underlying these processes are often not disclosed to the user. As a result, the way in which the information forming the basis of a legal decision is generated remains unclear.

In this context, an important approach within the European legal framework has been developed on the basis of the Artificial Intelligence Act adopted in 2024. This regulation classifies artificial intelligence systems according to their level of risk and categorizes certain systems used in law enforcement as "high-risk". For such systems, specific requirements are established, including transparency, human oversight, risk management, and documentation [28].

This approach demonstrates that the lawful use of artificial intelligence systems should be assessed not only in terms of their effectiveness, but also with regard to their accountability and verifiability. In the context of digital forensics, this requires the application of several key principles: the explainability of

algorithmic outputs; the possibility of independent verification; the provision of human oversight; and the assessment of risks such as errors and bias [29]. In the absence of these principles, the legal value of outputs generated by artificial intelligence systems should be significantly limited.

In Azerbaijan, this issue has not yet been comprehensively regulated, either at the legislative or doctrinal level. The current legal framework does not contain specific provisions governing the use of artificial intelligence in the field of digital forensics. This may lead to uncertainty in practice regarding how AI-generated outputs should be evaluated.

In conclusion, the "black box" problem represents one of the most complex challenges in digital forensics. It is not merely a matter of technical transparency, but also concerns legal legitimacy and the principles of a fair trial [30]. Ensuring the effective and safe use of artificial intelligence within the legal system requires not only normative regulation, but also the development of institutional and technical oversight mechanisms.

III. A Legal Integration Model Of Digital Forensics

The findings of this study demonstrate that the challenges in the field of digital forensics stem not from isolated normative gaps, but from a mismatch between legal and technological elements. The collection, preservation, and evaluation of digital evidence are not regulated in a fully systematic manner within the current criminal procedural framework, which weakens both legal certainty and fair trial guarantees.

For this reason, the study proposes a legal integration model for digital forensics. This model conceptualizes the legal regime of digital evidence within a unified framework and incorporates five key dimensions. The structure of this model is illustrated in Figure 1.

The first dimension concerns the proportionality of interference. In the digital environment, the collection of evidence should not take the form of broad and general intrusion, but must be limited to data directly related to a specific criminal offence [31]. This approach restricts the scope of interference and serves to protect other data related to private life.

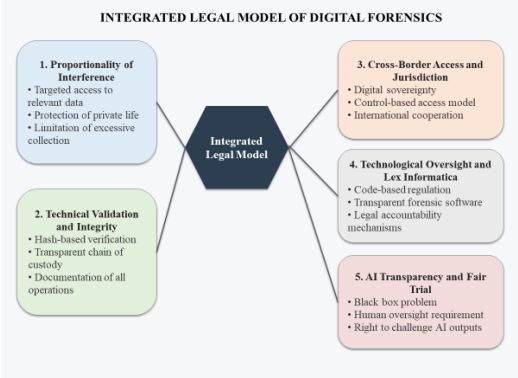

Figure 1. Integrated legal model of digital forensics.

The second dimension relates to the technical validation of digital evidence. In this context, the reliability of evidence is determined not by its physical carrier, but by its preservation without alteration and proper documentation. The use of cryptographic tools and the systematic documentation of all operations are therefore of particular importance. This approach introduces a new dimension to the concept of the chain of custody.

The third dimension addresses cross-border access. Since digital data is not tied to a specific territory, the classical approach to jurisdiction becomes insufficient. Therefore, control over data should be determined not only by its location, but also by the ability to exercise actual control over it [11]. This approach requires a reconsideration of international cooperation mechanisms.

The fourth dimension concerns legal oversight of technological tools. The software and algorithmic instruments used in digital forensic processes directly influence the formation of evidence. Accordingly, their use must be transparent and subject to legal oversight.

The fifth dimension relates to the use of artificial intelligence. Results generated by AI systems should not be treated as independent and conclusive evidence, but rather as information that is subject to verification and contestation. The defence must be provided with the opportunity to examine and challenge such outputs.

The main advantage of the proposed model lies in its ability to address the challenges of digital forensics not in isolation, but as part of an interconnected system. This approach ensures alignment between legal principles and technological capabilities, enabling their integrated application.

In conclusion, the effective regulation of digital forensics should not be limited to the adoption of new legal norms, but must also involve the development of a systematic approach that reflects technological realities. The proposed model may serve as a conceptual foundation in this regard.

Conclusion

The development of digital forensics demonstrates that the traditional approach of criminal procedural law does not fully correspond to the characteristics of the digital environment. The main challenge in this field arises from the mismatch between legal rules and technological capabilities.

The analysis shows that the effective and legitimate use of digital evidence cannot be achieved solely by addressing individual issues, but requires their consideration within a unified framework. In this regard, the legal integration model proposed in this study provides a coherent approach to addressing the key challenges of digital forensics.

In conclusion, the primary objective in this field is to ensure a balance between investigative efficiency, the protection of individual rights, and technological transparency. It is precisely this balance that forms the foundation for the legally acceptable and reliable use of digital evidence.

References

[1] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. San Diego, CA, USA: Academic Press, 2011, pp. 15–42.

[2] S. Mason and D. Seng, Eds., Electronic Evidence, 4th ed. London, UK: Institute of Advanced Legal Studies, 2017, pp. 35–68.

[3] European Court of Human Rights, "Case of Benedik v. Slovenia," Application no. 62357/14, Apr. 24, 2018.

[4] L. Lessig, Code: Version 2.0. New York, NY, USA: Basic Books, 2006, pp. 121–137.

[5] Law of the Republic of Azerbaijan on Amendments to the Criminal Code and the Criminal Procedural Code of the Republic of Azerbaijan, No. 373-VIIQD, Mar. 3, 2026. https://president.az/az/articles/view/71955

[6] Barak, Proportionality: Constitutional Rights and Their Limitations. Cambridge, UK: Cambridge University Press, 2012, pp. 131–174. doi: 10.1017/CBO9781139151023

[7] The Constitution of the Republic of Azerbaijan, adopted Nov. 12, 1995 (amended 2016). https://e-qanun.az/framework/897

[8] R. Alexy, A Theory of Constitutional Rights. Oxford, UK: Oxford University Press, 2002, pp. 388–425.

[9] O. S. Kerr, "Searches and Seizures in a Digital World," Harvard Law Review, vol. 119, no. 2, pp. 531–585, 2005.

[10] 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, OJ L 191, 2023.

[11] J. Daskal, "The Un-Territoriality of Data," Yale Law Journal, vol. 125, no. 2, pp. 326–398, 2015.

[12] European Court of Human Rights, "Case of Roman Zakharov v. Russia," Application no. 47143/06, Dec. 4, 2015.

[13] N. Jain and D. R. Kalbande, Digital Forensic: The Fascinating World of Digital Evidence. New Delhi, India: Wiley, 2017, pp. 145–168.

[14] ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence, ISO, 2012. https://www.iso.org/standard/44381.html

[15] A. Ashworth, "Four Threats to the Presumption of Innocence," The International Journal of Evidence & Proof, vol. 10, no. 4, pp. 241–279, 2006. doi: 10.1350/ijep.2006.10.4.241J

[16] J. Cosic and Z. Cosic, "Chain of custody and life cycle of digital evidence," Computer Technology and Application, vol. 3, no. 2, pp. 126–144, 2012.

[17] European Court of Human Rights, "Case of Rook v. Germany," Application no. 1586/15, July 25, 2019.

[18] L. Lessig, Code: Version 2.0. New York, NY, USA: Basic Books, 2006, pp. 1–38.

[19] J. R. Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology," Texas Law Review, vol. 76, no. 3, pp. 553–593, 1997. https://ssrn.com/abstract=40560

[20] M. Hildebrandt, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham, UK: Edward Elgar Publishing, 2015, pp. 162–184. doi: 10.4337/9781782549222

[21] K. Yeung, "Can We Employ Design-based Regulation while Embodying Respect for the Rule of Law?," Law, Innovation and Technology, vol. 3, no. 1, pp. 1–29, 2011. doi: 10.5235/175799611796399812

[22] A. Cavoukian, Privacy by Design: The 7 Foundational Principles. Toronto, ON, Canada: Information and Privacy Commissioner of Ontario, 2009.

[23] J. Waldron, The Rule of Law in the 21st Century. Cambridge, UK: Cambridge University Press, 2024, pp. 88–110.

[24] P. De Filippi and S. Hassan, "Blockchain-based Regulation and the Rule of Law," Policy and Society, vol. 43, no. 1, pp. 12–29, 2024. doi: 10.1093/polsoc/puad015

[25] F. Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge, MA, USA: Harvard University Press, 2015, pp. 1–25. doi: 10.4159/harvard.9780674736061

[26] European Court of Human Rights, "Case of Dombo Beheer B.V. v. the Netherlands," Application no. 14448/88, Oct. 27, 1993.

[27] L. Edwards and M. Veale, "Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?," IEEE Security & Privacy, vol. 16, no. 3, pp. 46–54, 2018. https://doi.org/10.1109/MSP.2018.2701157

[28] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L, 2024. http://data.europa.eu/eli/reg/2024/1689/oj

[29] L. Floridi, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford, UK: Oxford University Press, 2023, pp. 112–135. doi: 10.1093/oso/9780198883654.001.0001

[30] R. Binns, "Human Oversight and Algorithmic Accountability," Law, Innovation and Technology, vol. 14, no. 1, pp. 1–28, 2022. doi: 10.1080/17579961.2022.2047048

[31] D. J. B. Svantesson, Solving the Internet Jurisdiction Puzzle. Oxford, UK: Oxford University Press, 2021, pp. 156–180.