Journal of Theoretical and Applied Information Technology
30st June 2026. Vol.104. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

LEGAL UNDERPINNINGS OF THE USING DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS IN THE CONTEXT OF ADMINISTRATIVE-DIGITAL TRANSFORMATION

VLADYSLAV VEKLYCH[1], VITALII ANDRUKH[2], MYROSLAV POPOVYCH[3], OLEKSANDR KVASHUK[4], ANDRIY TYMCHYSHYN[5]

[1]Department of Theory of State and Law and Constitutional Law, Interregional Academy of Personnel Management, Kyiv, Ukraine.
[2]Department of Criminal Procedure and Forensics, Faculty of Training Specialists for Pre-trial Investigation Bodies of the National Police, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine.
[3]Department of Criminal Law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine.
[4]Department of Criminal Process and Forensic, Faculty of Training Specialists for Pre-trial Investigation Bodies of the National Police of Ukraine, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine.
[5]Separate Structural Subdivision of Higher Education Institution "Open International University of Human Development "Ukraine" Ivano-Frankivsk Branch, Ivano-Frankivsk, Ukraine.
E-mail: [1]veklicvladislav7@gmail.com, [2]adruhvitlii@gmail.com, [3]m_popovyh@chnu.edu.ua, [4]Kvashuk_o@advocate-ua.com, [5]and_tum@ukr.net

ABSTRACT

To ensure the reliability of digital evidence in criminal proceedings and, consequently, its admissibility in court, it is imperative to apply both technical and legal mechanisms. Such an integrated approach enables effective control over the origin, authenticity and integrity of digital information and reduces the risk of judicial challenges. The aim of this study is to conduct a comprehensive assessment of the reliability of digital evidence used in criminal cases within the context of administrative and digital transformation. Other than that, the study proposes the development of an integrated framework known as the Digital Evidence Reliability Framework (DERF). The research methodology combines comparative legal, technical, analytical and system-based approaches, supported by quantitative analysis of four interrelated components: technical integrity (TI), procedural correctness (PC), access control (AC) and regulatory compliance (RC). The study draws on criminal procedural law and legislation from Ukraine, Spain and the United Arab Emirates. The findings reveal significant differences in the balance between technical and legal mechanisms governing digital evidence across the examined jurisdictions. Based on the average values of the General Reliability Index (DERF = 0.66), Ukraine demonstrates a moderate level of overall digital evidence reliability in criminal proceedings. This outcome reflects a discrepancy between the technological robustness of digital data and the procedural mechanism required to legally validate such reliability. Thus, Spain (DERF = 0.78) represents a more balanced model, combining established technical safeguards for digital information with well-defined procedural requirements and complementary regulatory mechanisms, including data protection standards. The highest overall reliability score was recorded in the United Arab Emirates (DERF = 0.87), where technical, organizational and legal mechanisms operate in a balanced and cohesive way. Analysis of structural imbalances indicates that the most significant losses in digital evidence reliability occur during the translation of technical actions into formalized regulatory and procedural frameworks. The scientific novelty of this study lies in the development and empirical validation of the integrated DERF model, which shifts the evaluation of digital evidence from predominantly descriptive approaches to a quantitative assessment of legal system readiness. From a practical perspective, the proposed framework offers a diagnostic tool for identifying critical risk areas and formulating targeted recommendations to enhance legislation and improve the handling of digital evidence across different legal systems. The revised manuscript makes the operational logic of the DERF model explicit by linking each score to defined legal, procedural, organizational and

technical criteria, and by presenting DERF as a reproducible conceptual and quantitative framework rather than as a descriptive comparison only.

Keywords: *Criminal Justice, Innovation, Legal Administration, Digital Evidence, Criminal Proceedings, Technical Integrity, Procedural Admissibility, Integrated Model, Administrative-Digital Transformation.*

1. INTRODUCTION

The digitalization of public administration, together with the evolution of information-gathering methods in criminal proceedings, has fundamentally transformed the processes of collecting, recording and using information in the course of criminal investigations. An increasing volume of evidence is now generated automatically through diverse information systems, including crime reporting databases, event logs, cloud-based platforms and mobile devices. In this light it can be said that digital data, such as electronic communications, system logs, audio and video recordings, geolocation data, as well as metadata, has become a primary source of evidence in criminal cases.

At the same time, digital evidence exists within a highly dynamic, easily reproducible, yet technologically vulnerable environment. Given the above, its reliability is affected not only by legal implications, but also by technical factors that directly influence both its admissibility and security. Digital technologies have significantly expanded the role of information systems within the activities of pre-trial investigative bodies and courts [1, 2]. From a technical standpoint, digital evidence emerges from interactions within complex information ecosystems, making critically important the preservation of its integrity through mechanisms such as change control, event logging, time synchronization and access restrictions.

The integrity of the digital evidence chain depends on the proper functioning of all these elements and enables tracing the evidence from the moment of its creation. Any breach in the chain of custody or storage mechanisms undermines the evidence's credibility, even in cases where the data itself have not been altered. In view of the above, numerous legal and procedural risks associated with the use of digital evidence are rooted in technical deficiencies.

In Ukraine, the use of digital evidence takes place within a context of legal and methodological fragmentation. A substantial portion of the regulatory framework continues to rely on judicial practice, while the technical implementation of these norms often depends on various interpretations of the digital evidence's technological characteristics. Numerous studies highlight the absence of a unified systematic approach to integrating digital evidence into the overall evidentiary model, creating the risks to violate the principles of legality and fairness in criminal proceedings [3].

Furthermore, another challenge arises from the disparity between the rapid advancement of forensic technologies and the comparatively slow pace of their procedural formalization. As a result, technical compliance with investigative procedures does not necessarily ensure that digital information will acquire the status of procedurally protected evidence [4]. Overseas, the digital evidence in scholarly papers is increasingly conceptualized as an interdisciplinary institution at the intersection of digital forensics, information security and criminal procedure. Within European legal discourse, particular emphasis is placed on reliability standards for electronic evidence and the role of courts in assessing its technical characteristics [5, 6]. On the other hand, the technical and organizational approaches aimed at safeguarding digital evidence throughout its entire lifecycle are being developed. These include network-based, cryptographic as well as distributed technology solutions designed to ensure the authenticity, integrity and availability of digital data [7, 8].

Comparative analysis of different jurisdictions reveals substantial variation in the degree to which procedural rules are aligned with the technical aspects of forensic analysis. Having analyzed the available scholarly data, it can be said that the experience of the United Arab Emirates demonstrates a model in which formalized digital evidence is recognized as a distinct and independent category of evidence, consequently limiting discretionary practices by law enforcement authorities and strengthening procedural safeguards.

The relevance of the present study is due to the urgent need for a comprehensive reevaluation of all aspects of using digital evidence throughout the criminal justice process. This perspective encompasses both its legal regulation and the technological architectures of the digital environments in which such evidence is created, stored and processed. Within the broader context of administrative and digital transformation, a principal

challenge lies in ensuring coherence between technical infrastructures designed to guarantee the integrity and traceability of digital information and the procedural and regulatory requirements of criminal proceedings.

A comparative analysis of approaches to the presenting and evaluating digital evidence in Ukraine, Spain and the United Arab Emirates makes it possible not only to contrast the applicable legal norms in these jurisdictions, but also to assess the degree of technical, legal and institutional readiness of their criminal justice systems to effectively rely on digital evidence. This assessment provides both the motivation and the justification for the current research.

The purpose of this article is to develop and empirically validate the Digital Evidence Reliability Structure (DERF) as an integrated model for assessing the reliability of digital evidence in criminal proceedings. Moreover, the study aims to compare the legal, procedural and technical requirements governing the use of digital evidence in the criminal justice systems of Ukraine, Spain and the UAE in the terms of ongoing administrative and digital transformation.

To achieve this purpose, the study pursues the following tasks:

a) to formulate criteria and parameters for assessing the reliability of digital evidence, with particular emphasis on technical integrity and procedural admissibility, using international standards as the core benchmarks of the DERF model;

b) to identify structural imbalances between existing technological capabilities for data acquisition and preservation and the legislative limitations present in the national law of Ukraine;

c) to conduct a comparative validation of the DERF model based on the legal systems of Ukraine, Spain and the UAE by calculating an integrated digital evidence reliability index for each jurisdiction.

The study draws on the assumption that the practical effectiveness of digital evidence in criminal proceedings depends on the coherence of three interrelated elements: the legal framework governing the admissibility of digital evidence; the technological mechanisms used to ensure the authenticity and integrity of digital data; and the institutional capacity of criminal justice authorities to adapt to the digital nature of contemporary society.

The working hypothesis of the study is that the reliability of digital evidence increases when technical integrity mechanisms are procedurally formalized and supported by access-control and normative-compatibility safeguards. Accordingly, the DERF model treats reliability not as a single technical property of a digital file, but as the outcome of interaction among four operationalized components: TI, PC, AC and NC.

The scientific novelty of the study consists in the operationalization of these four components into an integrated reliability index that can be applied comparatively to different legal systems. Unlike approaches that separately discuss admissibility, digital-forensic integrity or data-protection requirements, the proposed framework connects these dimensions within one calculation procedure and uses it to identify structural imbalances in national models of digital evidence governance.

2. LITERATURE REVIEW

In recent decades, scholars have increasingly examined digital evidence from multiple perspectives, driven by the rapid expansion of digital technologies and the national legal systems' diversity. There is overall consensus that digital evidence has become a critical component of contemporary criminal investigations. However, significant disagreement remains concerning the appropriate methods for recording, verifying and evaluating digital evidence according to legal standards. As a result, scholarly discussion continues over the extent to which courts should rely on digital information, with most studies focusing on normative questions like what should or should not be done, rather than on empirical assessment of existing practices.

Sashulidu [9] analyzed recent EU regulations on cross-border access to electronic evidence and observed that digital evidence is increasingly difficult to manage within the jurisdictional boundaries of individual Member States. The researcher identifies the lack of standardized procedures for collecting, storing and accessing electronic data as the primary hardship to harmonization in cross-border investigations. A similar argument is advanced by Yermachenko et al. [10], who place the problem within a broader organizational framework. According to the above scholars, the absence of a comprehensive legal regime governing state digital infrastructure elevates the risk of unlawful data utilization in criminal proceedings.

Apart from the procedural mechanisms, a growing body of research addresses the technical means of ensuring the reliability of digital evidence. For instance, Khan et al. [11] propose the use of blockchain technology to document the chain of custody of digital materials, arguing that immutable transaction records significantly reduce the risk of manipulation or falsification. Further, Kim et al. [12] support this approach by suggesting a two-level blockchain system to further enhance evidentiary reliability. Nevertheless, both studies acknowledge that even the most advanced technical solutions cannot replace the procedural safeguards provided by law.

This procedural dimension is emphasized by Stoykova [13], who introduces the concept of "procedural accuracy", requiring that all stages of digital data processing should be legally traceable, transparent and reproducible. She argues that it is procedural violations rather than technological deficiencies that most often lead to the exclusion of digital evidence at trial. Similarly, Lasagna [14] maintains that the admissibility of digital evidence lies at the intersection of technical reliability and procedural compliance.

Comparative and international studies further underscore these challenges. Examining the practice of the International Criminal Court, Nilay Sangari and Mohammadi [15] conclude that no universal standards for the admissibility of digital evidence exist, necessitating case-by-case judicial assessment. Likewise, Nazir et al. [16], in a study of Pakistan's legal system, demonstrate that courts frequently question the credibility of digital evidence due to insufficient legal foundations. Hosaka [17] highlights additional controversy surrounding the admissibility of leaked or hacked data, which raises complex legal and ethical questions regarding the legality of data acquisition.

Other scholars focus specifically on evidentiary reliability. Alhseylat et al. [18], in a comparative analysis, find that although courts across jurisdictions assess the authenticity of digital evidence differently, they consistently emphasize the need for clear documentation of data origin. Moussa [19] similarly argues that without simple, transparent authentication procedures, even technologically sophisticated digital materials may lose their evidentiary value.

Overall, the literature review reveals that contemporary research on digital evidence generally falls into three methodological strands: (1) legal regulation, (2) technical mechanisms for ensuring reliability, and (3) procedural standards governing admissibility. However, these approaches are typically examined in isolation. Thus, only a few studies attempt to integrate legal, technical and procedural dimensions into a single, coherent theoretical framework that is accessible and operational for all participants in criminal investigations. This absence of a clear, concise and understandable methodology for harmonizing law and technology constitutes the principal scientific gap addressed in the current study.

This manuscript therefore incorporates the information required to understand the model without referring to any companion publication. The literature was used not only as background, but also as a source for structuring the DERF components: studies on blockchain and chain of custody informed TI and AC, works on procedural accuracy and admissibility informed PC, while comparative legal and data-protection studies informed NC. This connection clarifies how the reviewed sources were translated into the analytical structure applied in the empirical part of the article.

3. MATERIALS AND METHODS

3.1. Research Design

The research design is based on interdisciplinary technical-legal approach that integrates comparative legal analysis with quantitative assessment methods as well as elements of mathematical modeling. A central feature of this design is the conversion of qualitative regulatory data into formalized quantitative indicators. This transformation enables a shift from a purely descriptive analysis of digital evidence to its systematic numerical evaluation within the integrated Digital Evidence Reliability Framework (DERF) model. The study is conducted in the context of administrative and digital transformation processes, which directly influence the architecture of information systems used by pre-trial investigation bodies, the mechanisms for recording and storing digital data, and the procedural rules governing their use in criminal proceedings [20–24].

From a methodological standpoint, regulations governing criminal procedure, electronic documents, trust services and information security are treated both as sources of legal norms and as inputs for the quantitative model assessing the reliability of digital evidence. The study examines the content of laws, by-laws and related regulatory acts in this field as structured data. The study objective is to identify existing and missing

procedural and technical mechanisms that ensure digital evidence reliability. Such approach makes it possible to extend legal requirements into measurable parameters that can be modeled quantitatively using mathematical methods.

For this comparative study, three countries – namely Ukraine, Spain, the United Arab Emirates – were selected on the basis of technical and legal factors relevant to assessing the reliability of digital evidence. Importantly, their geographical location was not a determining criterion. Ukraine represents a jurisdiction undergoing an open process of law enforcement digitalization, characterized by partial procedural integration of technical processes for digital information handling. Spain was selected to test the DERF model within a European legal context, where the reliability of digital evidence largely depends on judicial oversight of investigative activities as well as on the criterion of applying personal data protection guarantees throughout the criminal process. Further, the United Arab Emirates was included as an example of a jurisdiction with a highly formalized regulatory framework that comprehensively addresses both technical and procedural requirements for digital evidence, as well as a regulatory environment characterized by a rapid response to technological change [25–30]. Together, Spain and the UAE enable validation of the DERF model under two contrasting conditions of technical and procedural maturity. The analytical value and applicability of the DERF model depend on this cross-jurisdictional validation.

The study was conducted in accordance with a phased implementation of the DERF model. The first phase involved identifying key parameters for assessing the reliability of digital evidence. These parameters were derived from evaluating the international digital forensics standards, best practices in digital evidence management and legal norms governing criminal justice systems. To that end, four core components of the model were defined, in particular: technical integrity of digital data (TI), procedural compliance (PC), access control and circulation tracking (AC), normative compatibility of technical procedures with applicable legislation (normative compatibility, NC). The above components were identified as critical for quantitative modeling of digital evidence reliability, because they collectively encompass both the technical and legal dimensions of the digital evidence lifecycle.

In the second phase of the study, the DERF structure was applied directly. For each selected jurisdiction, the regulatory instruments included in the generated dataset were analyzed in terms of existence, formalization degree and procedural consolidation of mechanisms corresponding to each of the model's four components. The resulting qualitative characteristics were then converted into normalized numerical values on a scale from 0 to 1 through expert analytical evaluation based on unified assessment criteria. Hence, it can be said that the comparative analysis was conducted not intuitively, but rather through the systematic assignment of quantitative values to the TI, PC, AC, NC parameters. In such a way, transparency, consistency and reproducibility of the results was ensured.

In the third phase, an integral DERF score was calculated for each jurisdiction using a weighted linear aggregation model. In this model, the weighting coefficients reflect the relative significance of technical and procedural components for the overall reliability of digital evidence. The model's adequacy was assessed through logical and structural validation, involving verification of the internal consistency of the calculated results and their alignment with respective legal systems' established characteristics. In addition, documented challenges in the law enforcement application of digital technologies were taken into account.

Operationalization of the DERF components was performed as follows. TI was assessed through the presence of hashing, timestamping, logging, preservation of original data and reproducibility of digital copies. PC was assessed through the formal procedural rules governing acquisition, duplication, expert verification and submission of digital evidence. AC covered role-based access, transaction logging, auditability and protection of evidence repositories. NC measured the consistency between technical procedures and legislation on electronic documents, trust services, information security and personal data protection. Each country was evaluated by the same checklist, which reduced subjective interpretation and allowed cross-jurisdictional comparison.

The empirical unit of assessment was not an individual criminal case, but a jurisdictional model of digital evidence governance. For this reason, the values assigned to TI, PC, AC and NC reflect the degree of formal availability and internal coherence of mechanisms in legislation, standards and publicly accessible regulatory instruments. The same scale was applied to Ukraine, Spain and the UAE in order to keep the model comparable across jurisdictions with different legal traditions.

3.2. Research Methods

To assess both the legal legal regulation of digital evidence and the practicality of the mechanisms for its recording, storage and verification, legal and technical analytical methods were combined. Comparative legal methodology was applied to the comparative analysis of criminal procedural norms of Ukraine, Spain and the United Arab Emirates regarding the use of digital evidence. This comparative method c allowed us to recognize and document differences in formalized electronic record acceptance processes, the degree of formalization of procedural procedures, and the degree of technology involvement in evidentiary evidence. A combination of regulatory and technical analyses was carried out to study the legal bases related to electronic documentation, electronic signatures, information security and digital data security. The regulatory/technical analysis included assessing the degree of compliance of current legislation and regulations with the established fundamental technical with the principles that ensure the authenticity, integrity of digital evidence c and its traceability to its origin.

The functional analytical method studied typical technological schemes for processing digital evidence, from receipt to copying, storage and transmission for subsequent verification. Thus, it has allowed us to establish technological risk points that can lead to the alteration of the digital evidence itself or to the loss of its evidentiary value. To study digital evidence as part of a large-scale technical and legal system, we applied the method of systems analysis. We analyzed digital data together with law enforcement information systems, technical equipment for monitoring information integrity and procedural requirements of criminal proceedings. Thus, this approach allowed us to assess the degree of compatibility of the technical and legal components.

At the general level, elements of the expert-analytical approach have been applied in the description of modern technological tools used to ensure the integrity of digital evidence. Technical and procedural aspects were evaluated, such as mechanisms with access control, activity logging and data immutability. The aspects that have been defined in terms of technical and procedural characteristics have been formalized into a quantitative indicator for the parameters of the DERF model. The evaluation of these indicators was carried out using a discrete ten-point Likert type expert scale. The values were then normalized to the interval [0; 1], which made it possible to compare the technical capabilities with existing legal ones with limitations. The generalization and technical explanation of the results was used as the final step with in this study.

For transparency, the ten-point expert scale was interpreted in three bands: 1-3 points indicated absence or fragmentary presence of the mechanism; 4-7 points indicated partial formalization or uneven application; 8-10 points indicated full formalization and procedural integration. The scores were then divided by ten to obtain normalized values in the interval [0; 1]. Borderline cases were resolved by prioritizing explicit procedural consolidation over general technological availability, because the evidentiary value of digital data depends on whether technical actions can be legally verified.

The described methods allow evaluating the effectiveness of modern working models using digital evidence; they also allow to determine the need to improve such models in terms of technological reliability as well as admissibility in criminal proceedings. The application of these methods has made it possible to integrate legal and technical assessment with digital evidence and thus combine regulations with the actual technical processes used to process them in the framework of criminal proceedings.

3.3. Evaluation Metrics

The overall assessment of the effectiveness of the application of digital evidence in criminal proceedings was carried out using a quantitative approach that combined technical and legal methods for assessing the reliability of digital evidence during with its collection, analysis and application in court. As part of this assessment, a new structure called the Digital Evidence Reliability Structure (DERF) was developed. DERF provides the means to assess the compliance of technical processes with both procedural and legal requirements during the transition from the administrative to the digital environment. Four fundamental elements of the DERF model have been identified since they relate to the most important factors related to working with digital evidence. As can be seen below, they are presented in Table 1.

Table 1: Digital Evidence Reliability Assessment Metrics (DERF)

Component	Designation	Indicator content	Range of values	Interpretation
Technical integrity	IT (Technical Integrity)	Availability and correctness of mechanisms for hashing, logging of actions, fixing time and protection against changes	0–1	Immutability and reproducibility with digital data
Procedural correctness	PC (Procedural with Compliance)	Compliance of the actions of the criminal authorities with the proceedings with the requirements of criminal procedural legislation	0–1	Legal with admissibility of digital evidence
Access control and traceability	AC (Access Control)	Level of access demarcation, availability of transaction logs and the ability to audit	0–1	Transparency and control in the circulation of digital evidence
Normative compatibility	NC (Normative Compatibility)	Consistency of technical procedures with legislation on information, electronic documents and data protection	0–1	Resistance of evidence to legal risks

Source: consolidated by the author on the basis of the [20-30].

Each component c was rated on a normalized scale of 0 to 1, where the lowest score indicates the lack of proper mechanism and the highest score c indicates full compliance with both legal and technical requirements. Overall, the reliability of digital evidence (DERF) was established based on the c scores of each component by the formula:

$$\mathrm{DERF} = \alpha \cdot \mathrm{TI} + \beta \cdot \mathrm{PC} + \gamma \cdot \mathrm{AC} + \delta \cdot \mathrm{NC} \quad (1)$$

where $\alpha, \beta, \gamma, \delta$ represent the appropriate weight coefficients for each c component to reflect the comparative importance of each component, provided that:

$$\alpha+\beta+\gamma+\delta=1$$

Using the research methodology, weights for weight ratios were determined based on the relative importance of the procedural and technical components that determine the evidentiary weight of digital evidence in criminal cases. With that in mind, the weights will be used to measure and estimate the evidentiary weight of digital evidence. Thus, the final version of the equation is presented as follows:

$$DERF = 0.35 \cdot TI + 0.30 \cdot PC + 0.20 \cdot AC + 0.15 \cdot NC \quad (2)$$

The metric system developed in. this article provides an opportunity to move from descriptive analysis to comparative quantification of different methods of using digital evidence in jurisdictions around the world. The use of the integrated DERF indicator enabled comparing the models of criminal proceedings of Ukraine, Spain and the UAE. Further, the assessment of both the formal availability of legislative provisions on the production of digital evidence was conducted as well as of the actual level of technical and procedural readiness of the criminal justice system to work with digital evidence.

In the final calculation, the weighted DERF index was specified as DERF = 0.30 x TI + 0.30 x PC + 0.20 x AC + 0.20 x NC. The higher weights of TI and PC reflect their direct influence on evidentiary value, while AC and NC capture the organizational and regulatory conditions that determine the resistance of digital evidence to subsequent legal challenges.

3.4. Integral model for ensuring application of digital evidence

The study applies an integrated model for ensuring the use of digital evidence in criminal proceedings, which reflects the interaction of technical, organizational and legal components in the digital evidence's lifecycle. In contrast to fragmentary approaches, the proposed model emphasizes the continuity between technological operations performed on digital data and their procedural status within criminal proceedings. The model is based on a multilevel structure and encompasses three interrelated functional levels.

Conceptually, the model is based on the proposition that digital evidence remains reliable only when three layers operate continuously: technical preservation of data, organizational control over its circulation and legal validation of procedural admissibility. A failure at any layer may reduce the total DERF value even if the remaining layers function properly.

The first level is the capture of digital evidence (technical–digital level) - it includes processes directly associated with handling digital data. These processes comprise the identification and extraction of digital media, extraction of digital data from storage media, creation of digital copies, generation of hash values, management of digital timestamps and safe preservation of the original data and derived artifacts. This level is critical for preventing falsification or alteration of digital evidence and for ensuring its authenticity and integrity for subsequent procedural use.

The second level is organizational and procedural – it comprises the methods and mechanisms used to structure and control the processing of digital evidence. This includes chain-of-custody controls, access management to digital data, allocation of responsibilities among investigators, prosecutors, courts, experts and technical specialists as well as the recording of all the actions in transaction and audit logs. At this level, the traceability of digital evidence is ensured from the moment of its acquisition to its submission to the court.

The third level is legal – it establishes the procedural and normative rules governing the admissibility and use of digital evidence in criminal proceedings. This level applies criminal procedural legislation, regulations on electronic documents and electronic trust services as well as legal frameworks for information security and personal data protection. It is at this stage that the results of technical operations are subjected to legal verification and a determination is made. The purpose is to verify whether the digital data meet the criteria of reliability and admissibility as evidence in criminal proceedings.

As a structural approach, this model ensures a continuous interaction among all three levels. Legal requirements become technically implementable only where adequate organizational and technical support exists, while technical actions acquire legal validity only when they are integrated within appropriate procedural and legal frameworks. By combining the above levels, the model bridges the gap between the technological processing of digital data and its use within criminal proceedings. Figure 1 illustrates structural stratification of the integrated model.

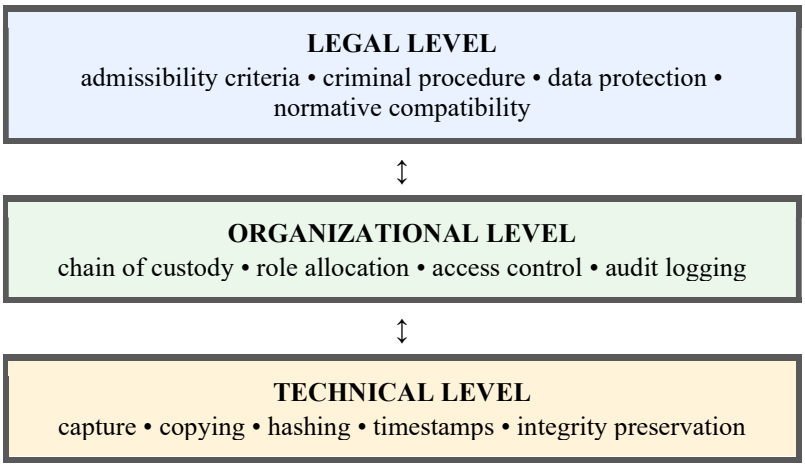

Figure 1: Integral Model For Ensuring The Use Of Digital Evidence In Criminal Proceedings
Source: Elaborated By The Author

The new model represents an integrated, modular and adaptive structure that takes into account all the legal systems in which it can be implemented without violating its own internal logic. The proposed model creates a structure for digital evidence's consistent application in criminal proceedings using a single unified method that includes technical reliability, organizational manageability and procedural admissibility as the three main components.

3.5. Technical environment

Technical component of the study was conducted using software tools commonly applied in the fields of digital forensics and electronic evidence analysis. The primary focus was on tools that enable the modeling of digital data circulation, verification of data integrity and reproducing the procedural logic governing the use of digital evidence. Analytical processing of structured data and calculation of the integral DERF index were performed in a Python 3.12 environment. The NumPy and Pandas libraries were used for data handling, normalization of indicators and computing the intermediate values, while SciPy was employed to verify the stability of calculated values and the logical consistency of model components. Graphical representation of results and comparative relationships was executed using Matplotlib.

When it comes to the simulating the digital evidence chain of custody and the analysis of data circulation scenarios, those were conducted through process diagrams developed with draw.io and Microsoft Visio. These tools enabled the formalization of interactions between technical, organizational, and legal stages of digital evidence handling. Verification of technical requirements for electronic documents and electronic trust services was carried out by comparing national regulatory provisions with parameters applied in public key infrastructure (PKI), electronic signature and event logging systems. To this end, open technical specifications and reference materials issued by official regulatory bodies were utilized.

Regulatory sources were analyzed using official electronic legal databases, such as zakon.rada.gov.ua (Ukraine), boe.es (Spain), uaelegislation.gov.ae (UAE). This approach ensured access to authentic and up-to-date versions of legislative texts and supported accurate technical and legal interpretation of digital evidence requirements. The applied technical environment enabled reproducibility of calculations, formalization of digital evidence processing workflows and a technically grounded cross-jurisdictional comparison of approaches to the use of digital evidence in criminal proceedings.

4. RESULTS

4.1. Results of the regulatory analysis of using digital evidence in selected countries.

The purpose of the regulatory analysis within the Digital Evidence Reliability Framework (DERF) is to assess the two key dimensions of digital evidence reliability: Procedural Compliance (PC) and Normative Compatibility (NC). In the framework of the current study, an evaluation was conducted of criminal procedural legislation and special regulations in Ukraine, Spain and the UAE, as well as the degree of digital evidence's formalization within these legal systems.

In Ukraine, normative and legal models are primarily established by the general Criminal Procedure Code and specialized regulations governing electronic documentation, trust services and information security [20–24]. The Ukrainian regulatory framework separately identifies and classifies digital evidence, with admissibility determined either by adherence to procedural requirements for a specific type of evidence or by verifying technical aspects through expert testimony.

Spain's legal model provides a higher level of regulatory detail and clarity as compared to Ukraine, particularly in defining permissible use of digital evidence. In fact, admissibility standards in Spain are established through the Ley de Enjuiciamiento Criminal (Spanish Criminal Code), European Union regulations and directives, including GDPR (Regulation EU 2016/679) as well as additional legislation governing the stages of criminal investigation and the collection of confidential information [25–37]. The above mentioned regulations define the criteria for recognizing digital evidence as admissible, granting courts the authority to assess both the evidence's legal validity and the proportionality of any rights violations during investigation. This comprehensive and integrated framework ensures high procedural compliance (PC) while the strict data protection regime contributes to a high normative compatibility (NC).

The UAE exhibits a highly formalized and centralized legal model. Legislation governing criminal proceedings, cybercrime and electronic transactions [28–30] links the admissibility of digital evidence to strict compliance with established procedures. This is evidently done for identifying, authenticating and storing electronically transmitted information. In this system, PC and NC values in the DERF model are very high. However, the flexibility or discretion available to investigators is limited, with emphasis placed on judicial assessment of being compliant with formal processes.

Table 2 summarizes the general results of the regulatory analysis, illustrating the impact of legal requirements on the development of PC and NC components in the DERF model. The comparative matrix in the table highlights differences in regulatory frameworks in jurisdictions and provides the foundation for a quantitative comparison in terms of digital evidence's reliability.

Table 2: Regulatory Factors Of Developing The PC And NC Components In The DERF Model

Indicator	Ukraine	Spain	UAE
Procedural Correctness (PC)	0.62	0.78	0.85
Regulatory Compliance (NC)	0.65	0.82	0.88
Legal status of digital evidence	Equated with other evidence, without a separate category	Recognized as an independent object of proof	Formalized. as a separate category
Court's role in the assessment of admissibility	High, but mainly at the stage of consideration	Key at all stages	Dominant, formalized
Investigators bodies' discretion	High	Limited by judicial control	Minimal

Source: consolidated by the authors based on [20-30]

A comparison of the values presented in Table 2 shows that the highest levels of Procedural Compliance (PC) and Normative Compatibility (NC) were observed in the legal systems of Spain and the UAE. In both countries, the admissibility of digital evidence is closely tied to formal electronic identification and verification processes. Spain occupies an intermediate position, which can be attributed to strong judicial oversight and the incorporation of privacy protections in Spanish law, ensuring a consistently stable level of PC and NC. By contrast, Ukraine exhibits the lowest levels of procedural and regulatory alignment. This reflects the fragmented nature of its legislation and the absence of a clearly defined procedural status for digital evidence.

4.2. Assessment of technical integrity and procedural correctness of digital evidence using DERF components.

During the DERF-based simulation, typical digital evidence objects were analyzed**,** including log files from information systems and web servers, filesystem metadata (MAC/EXIF timestamps), digital media images and encrypted containers. This approach allowed for an evaluation of the relationship between Technical Integrity (TI) and Procedural Compliance (PC) using practically relevant examples.

The results indicate that the levels of TI and PC do not coincide across the selected jurisdictions, and the nature of this gap varies by country. This distinction is critical because the relationship between TI and PC is essential. It determines if technical actions on digital data are successfully transformed into protected evidence capable of withstanding judicial scrutiny. Comparative values of TI and PC across Ukraine, Spain and the UAE are presented in Figure 2.

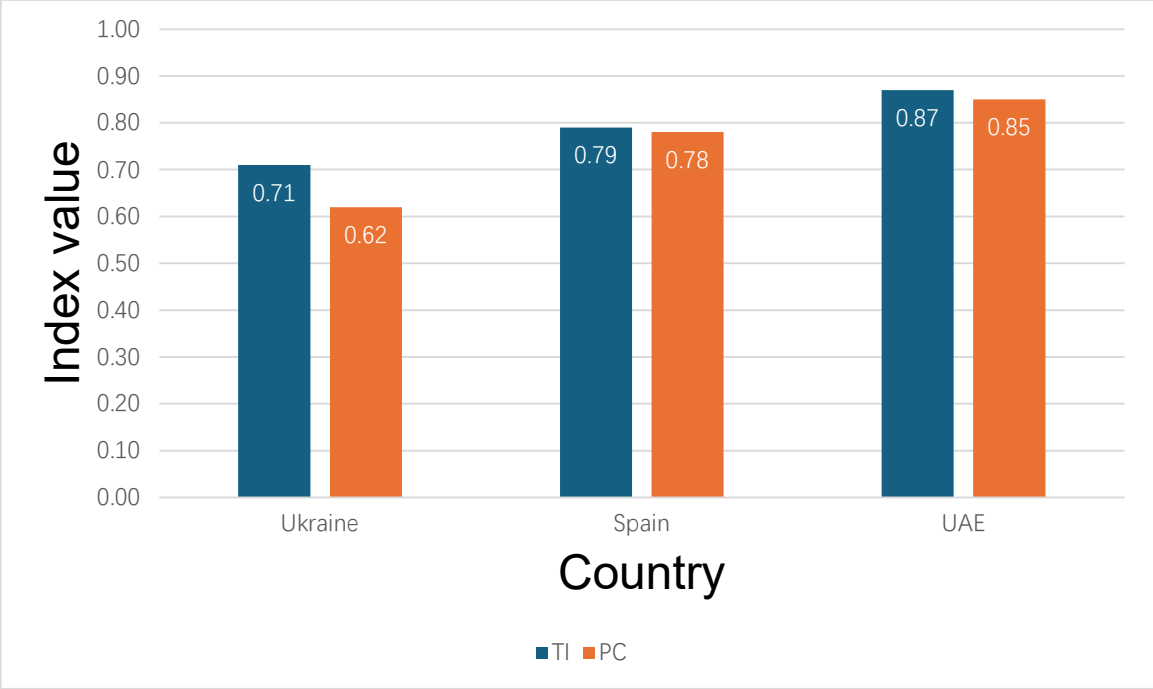

Figure 2: Comparison of TI and PC Components in DERF Model (Ukraine, Spain, UAE)
Source: Calculated and Consolidated by the Authors on the Basis of the Integrated DERF Model and Legislative Norms [20-30]

The results shown in Figure 2 reveal the most significant divergence in Ukraine, where the Technical Integrity (TI) index substantially exceeds the Procedural Compliance (PC) index. This indicates that, while technologies for ensuring the integrity of digital data, such as hashing, logging, change control and time-stamping are properly applied in practice. They are often not supported by a formal procedural framework. Consequently, even when a digital artifact is technically sound, it may still be challenged on procedural grounds, for example, regarding its acquisition, duplication or inclusion in case files.

By contrast, Spain demonstrates near-complete coherence between TI and PC, with minimal differences between the indicators. In this model, technical measures to preserve digital data integrity are consistently implemented in a manner that follows the procedural requirements. Technical tools do not operate in isolation but function as an integral part of the procedural system, increasing the likelihood that digital evidence retains its validity during judicial evaluation.

The UAE exhibits the highest values for both TI and PC, with the two indices almost perfectly aligned. This demonstrates that technical integrity mechanisms are fully supported by formalized criminal procedural rules and specialized regulations governing electronic transactions and cybercrime. In this context, technological processes do not exist independently before or after trial. Rather, they are embedded within a unified procedural and regulatory framework, leaving minimal room for procedural disputes as regard the proper handling of digital evidence.

Overall, the comparison between TI and PC highlights three models of interaction between technical procedures and procedural requirements: in Ukraine – technical processes partially precede procedural formalization; in Spain - technical and procedural measures are balanced; in the UAE - technical and procedural measures are mutually synchronous and fully integrated.

These findings demonstrate that the reliability of digital evidence does not depend solely on the technical processes themselves (e.g., hashing or change control). Instead, it depends on how these

processes are embedded within procedural requirements and legally verified.

4.3. Results of the access control analysis and regulatory compatibility of digital evidence.

The results indicate that, in addition to the integrity of the technology used to collect digital evidence and adherence to proper procedures, two additional factors significantly influence the reliability of digital evidence: Access Control (AC) and Normative Compatibility (NC) with national legislation governing electronic documents, data protection and information security in Ukraine, Spain and the UAE. To assess the AC component, the researchers evaluated the presence of automated logging systems such as WORM (Write-Once-Read-Only) mechanisms and multifactor authentication to protect evidence repositories from unauthorized access. Unlike technical integrity and procedural correctness, AC and NC directly affect the transparency of digital data flows and the resilience of evidence against legal challenges.

Figure 3 presents the generalized values of AC and NC for Ukraine, Spain and the UAE, highlighting differences in access control practices and regulatory alignment across the three jurisdictions.

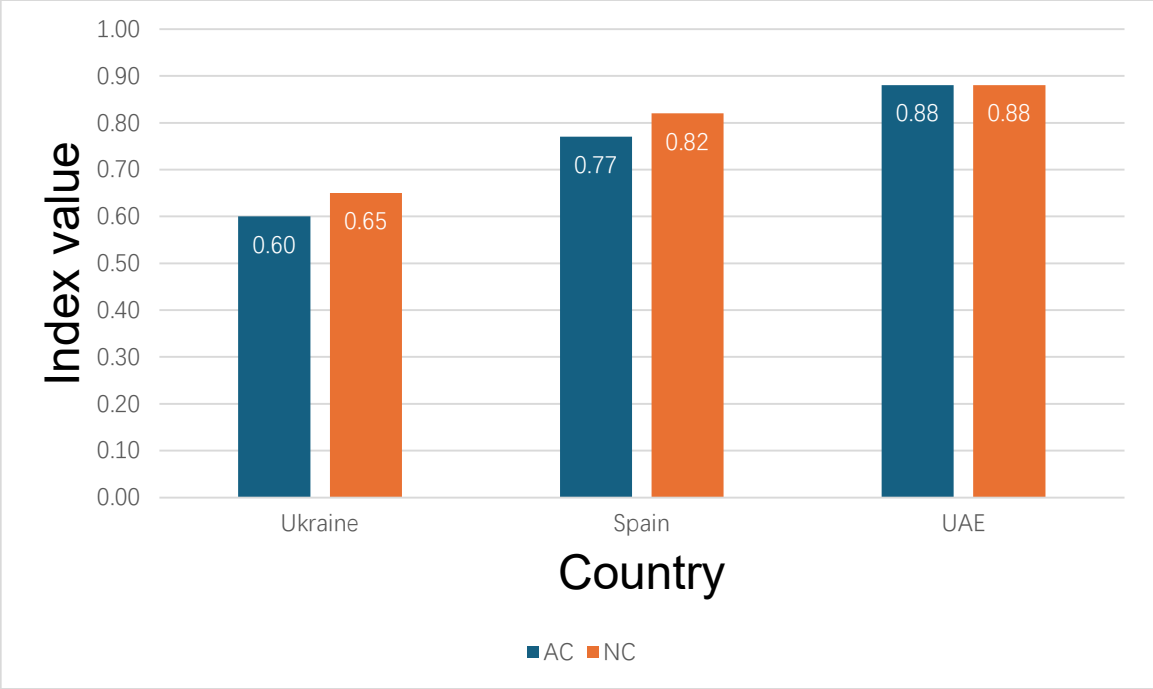

Figure 3: Comparison of AC And NC Components in DERF Model (Ukraine, Spain, UAE)
Source: Calculated and Consolidated by the Authors on the Basis of the Integrated DERF Model and Legislative Norms [20-30]

Figure 3 shows that the AC and NC components are the most sensitive to the quality of the legal and organizational framework. In Ukraine, although digital evidence may be technically consistent and legally admissible, the absence of a unified legal framework to formally recognize technical integrity introduces potential procedural weaknesses. Moreover, Ukraine also records the lowest scores in AC, reflecting inconsistencies in the implementation of access controls for digital systems and insufficient mechanisms to maintain a reliable audit for digital evidence. The average NC scores further indicate discrepancies between the technical procedures followed and the requirements related to electronic documents, trust services and information protection.

In Spain, AC and NC scores are higher and more balanced. Access control mechanisms are grounded in both the Criminal Procedure Code and European data protection regulations. Audit mechanisms and the principle of least privilege are used to limit the risk of unauthorized access and ensure traceability. Spain's high compliance with national standards demonstrates that technical procedures are closely aligned with legislative requirements, enhancing the stability and credibility of digital evidence throughout trial proceedings.

The UAE achieved the highest scores for both AC and NC among the three jurisdictions. Access control is formalized through specialized rules governing electronic transactions and cybercrime, while mandatory logging, regulated access, and centralized data storage ensure robust traceability. Technical procedures are fully integrated into the UAE's regulatory architecture, guaranteeing the reliability and availability of digital evidence at all stages of criminal proceedings.

From this analysis, three distinct forms of digital evidence governance emerge: (1) Ukraine – the riskiest model, with primary weaknesses in access control formalization and audit procedures; (2) Spain - a balanced model with strong alignment between technology and legal frameworks; (3) UAE - a highly integrated and stable model with full synchronization of technical, organizational and legal components.

These findings underscore that the reliability of digital evidence depends not only on the technical protection of the data itself but also on the transparency and regulatory oversight of access control throughout all stages of the criminal process.

4.4. Integral assessment of digital evidence reliability by the DERF metric.

The overall assessment of digital evidence reliability, based on the DERF indicator, demonstrates that the preparedness of legal systems for the use of digital evidence varies significantly across countries, depending on the coherence between technical, procedural, and regulatory components. Unlike the individual evaluation of TI, PC, AC, NC, the integrated DERF indicator provides a holistic view of the system, reflecting how technical processes operate within the context of the criminal process.

Table 3 presents the final DERF index values for Ukraine, Spain and the UAE, calculated using formula (2) and incorporating the weight coefficients specified in the model. Among the components, technical integrity (TI) and procedural correctness (PC) play the most significant role in determining the evidentiary value of digital data when it is submitted as evidence in court.

Table 3: Integral Values of the DERF Index and Their Interpretation

Country	DERF	Interpretation of the result
Ukraine	0.66	Medium level of reliability; technical mechanisms are partially ahead of procedural and organizational formalization, which creates risks during the judicial evaluation of evidence.
Spain	0.78	High level of reliability; balanced combination of technical procedures and procedural requirements. Ensures stability of digital evidence.
UAE	0.87	Very high level of reliability; technical, organizational and legal components integrated into a single regulatory model.

Source: calculated by the authors on the basis of the integrated DERF model and legislative norms [20-30]

According to the results, the lowest integrated DERF indicator was observed in Ukraine. This outcome can be attributed to two mutually reinforcing factors: comparatively low levels of procedural compliance and access control as well as limited regulatory compatibility of technical processes with electronic document and information protection laws. Although mechanisms for ensuring technical integrity exist in Ukraine, their impact on the overall evidentiary value of digital evidence is constrained by the absence of formalized procedural rules.

Spain exhibits a high integrated DERF index, reflecting the near-uniform values across all four components of the model. This indicates minimal gaps between technology, procedural mechanisms and regulatory frameworks. This ensures that digital evidence maintains its credibility throughout criminal proceedings, from preliminary investigation to trial.

The highest DERF value was recorded in the United Arab Emirates. The model's weighting coefficients highlight the significant contributions of technical integrity (TI) and procedural compliance (PC). Those are reinforced by highly formalized access control mechanisms and comprehensive regulatory integration of digital procedures. This demonstrates not only technical readiness but also strong procedural resilience against challenges to the admissibility of digital evidence.

Overall, the integrated DERF assessment confirms that the effectiveness of digital evidence does not depend solely on the sophistication of technical tools, but on their systematic alignment with procedural and regulatory requirements. Implementing such systematization is a critical factor for the effective use of digital evidence within legal systems undergoing administrative and digital transformation.

4.5. Detection of structural imbalances in national models

Results' generalization makes it possible to identify persistent structural imbalances between the technical, organizational and legal levels involved in the application of digital evidence across the selected jurisdictions. These imbalances cannot be reduced to separate shortcomings in legislation or technical instruments; rather, they are systemic in nature and directly affect the reliability of evidence at various stages of criminal proceedings. A comparative synthesis of the examined models' strengths and weaknesses is presented in Figure 4 as a heat-map. The heat-map was redrawn to increase visual readability and to present the numerical values directly inside the cells.

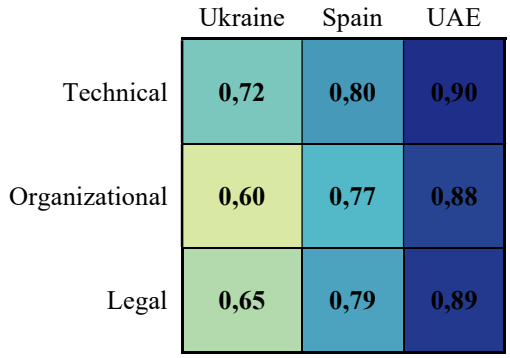

Figure 4: Comparative heat-map of structural strengths and weaknesses of national models of application of digital evidence (Ukraine, Spain, UAE)
Source: summarized and consolidated by the authors based on evaluation results using the DERF model [20—30]

A macro-level comparison of structural imbalances across the examined jurisdictions provides insight into the systemic challenges shared by these legal systems. These imbalances are not confined to isolated legal or technical deficiencies. Rather, they reflect broader structural discrepancies that can directly undermine the credibility of digital evidence at various stages of criminal proceedings. A generalized comparison of the strengths and weaknesses of each jurisdiction is presented as a heat-map in Figure 4.

Each element represented in the heat-map corresponds either to a "strength", characterized by consistently high indicator values, or to a "weakness" where indicator values are low or structural gaps are present. In Ukraine, the technical level constitutes the strongest component of the system, while the organizational and legal levels remain comparatively underdeveloped. Notably, Spain exhibits a largely balanced configuration, with no pronounced strengths or weaknesses across the three levels. The United Arab Emirates demonstrates consistently high performance across technical, organizational and legal dimensions, which are developed in a synchronized manner.

This analysis indicates that Ukraine is experiencing asymmetric system development. Whereas the technical level is sufficiently advanced to ensure the fundamental integrity of digital data, organizational and legal mechanisms are not properly aligned with technical procedures. As a result, evidentiary reliability is most vulnerable at the intersection of organizational and legal levels. In this respect, deficiencies in accessing control, logging and procedural formalization of technical actions can cause instability during forensic analysis. Thus, even when digital evidence is technically accurate, procedural or formal violations may result in its exclusion or discreditation.

In Spain, no significant structural imbalances were identified. The heat-map illustrates relatively uniform development across all three levels, with minor "cold zones" at the organizational level, primarily related to access control implementation. In such cases, the loss of evidentiary credibility gas a tendency to be localized and does not typically result in the digital evidence's overall inadmissibility. Hence, the alignment of technical procedures with procedural requirements generally ensures a stable evidentiary basis in judicial proceedings.

The UAE exhibits the highest degree of structural coherence. Technical, organizational and legal levels are integrated into a unified regulatory and technological framework. Critical areas of evidentiary vulnerability are virtually absent. This is due to the lack of mechanisms for ensuring data integrity, access control and audit being explicitly embedded in both procedural and specialized legislation. Consequently, the risk of digital evidence devaluation due to misalignment between technological practices and legal norms is minimal.

Overall, the identified structural imbalances demonstrate that the primary threats to digital evidence reliability arise not from the use of specific technical tools, but from discontinuities between system levels. For Ukraine, the critical challenge lies in the transition from technical actions to their procedural documentation. As far as Spain is concerned, it involves isolated organizational issues related to access control. Instead, for the UAE such imbalances are minimal. These findings underscore that enhancing the reliability of digital evidence

requires the systematic elimination of structural gaps across technical, organizational and legal domains, rather than isolated improvements to individual technical enhancements or legal norms.

5. DISCUSSION

The obtained results confirm that the reliability of digital evidence is not determined at the level of individual technical operations, but rather emerges from the systemic interaction of technical, organizational and legal dimensions. This logic of integration is embedded in the DERF model and demonstrates consistency with current understanding of digital criminal investigations. The latter are conducted within increasingly complex technological environments, including cloud services, the Internet of Things as well as automated data-collection systems. In this light, the findings align with Fakir [31], who emphasizes that the fragmentary application of digital tools without appropriate procedural and regulatory "framing" reduces the evidentiary value of even technically accurate data.

Comparative examination of the countries under study (Ukraine, Spain and the United Arab Emirates) demonstrates that the highest values of the integrated DERF indicator are achieved in jurisdictions. where procedures for ensuring data integrity and access control are explicitly codified in criminal procedural and special legislation. This finding is consistent with the conclusions of Al-Sherida et al. [32], who argue that the effectiveness of digital evidence in cyberlaw depends on combining digital forensic tools with clearly formalized legal rules governing their use. It is worth noting that the high DERF score observed for the UAE supports the view that a centralized regulatory model can minimize the risk of procedural challenges to digital evidence. This can be achieved by constraining investigators' discretionary powers and ensuring regulatory consistency.

The results also extend prior research on the use of advanced technologies to enhance the reliability of digital evidence, as demonstrated in studies by Kumar et al. [33] and Rani et al. [34]. Within the DERF framework, such technologies may be interpreted as mechanisms that strengthen the technical integrity (TI) and access control (AC) components. However, the findings show that their effectiveness remains limited in the absence of adequate procedural and regulatory integration. In other words, even decentralized or technologically advanced solutions cannot compensate for deficiencies in legal regulation.

The findings for Ukraine are particularly important in the face of ongoing digital transformation of judicial and law enforcement processes. The observed surge in the integrated DERF score following model testing suggests that systematic alignment of technical mechanisms with procedural requirements can produce measurable improvements in evidentiary reliability. This conclusion is consistent with Ali et al. [35], who demonstrate that digital transformation of legal frameworks is effective only when accompanied by a reassessment of procedural rules and the roles of participants in criminal proceedings, rather than through the isolated implementation of IT tools.

That being said, a critical reassessment of optimistic assumptions regarding the full automation of digital forensics is expedient. For instance, Solanke [36] and Khoran and Saidian [37] highlight the risk of declining trust in digital, specifically AI-driven tools in the absence of transparent and well-defined procedures. Within the DERF model, this concern is reflected in the strong interdependence between components. In particular, increasing technical complexity without corresponding improvements in procedural compliance and normative compatibility may ultimately reduce overall evidentiary stability [38].

Therefore, the study supports the concept of a digital evidence ecosystem in which technical protocols, organizational practices and legal norms operate as an integrated whole [39-41]. The highest levels of effectiveness are achieved in models where integrity assurance, access control and auditability are integral to criminal procedural logic rather than treated as auxiliary elements. These findings provide a foundation for future research focused on integrating comprehensive digital evidence reliability models with emerging technologies, such as blockchain and explainable artificial intelligence. Similarly, these can also include the developing mechanisms for cross-border interoperability of evidentiary systems in transnational criminal proceedings.

The practical interpretation of the findings is that reforms should not focus exclusively on purchasing forensic software or expanding technical infrastructure. For Ukraine, the priority area is procedural fixation of actions already performed at the technical level, including standardized documentation of copying, hashing, transfer, access and verification. For Spain, the results point to the need for further harmonization of organizational access-control procedures. For the UAE, the model indicates a comparatively mature system, although

continued monitoring is necessary as cloud-based and AI-assisted evidence sources expand.

6. LIMITATIONS

This study has several limitations, primarily related to the type of data and methodology employed. First, the assessment of digital evidence reliability is based on regulatory analysis and comparative modeling of the DERF components rather than on the examination of empirical case materials. That being said, the findings cannot be directly generalized to all possible investigative or judicial contexts. Second, the quantitative indicators for the TI, PC, AC, NC components are holistic in nature and do not account for sector-specific variations in the use of digital evidence across different categories of crime. Third, due to restricted access to jurisdiction-specific technical regulations and internal access-control mechanisms, the analysis relies largely on indicators derived from publicly available sources. Finally, while the DERF model shows certain static properties of digital evidence (such as file formats and formal procedural requirements), it does not fully elaborate on the dynamic characteristics of digital data. What is meant here is those associated with cloud computing environments, distributed databases as well as real-time data collection systems.

Despite these limitations, the results demonstrate strong analytical utility and provide a solid foundation for future research aimed at expanding the empirical base and refining the DERF model for more comprehensive assessment of digital evidence reliability.

Additional limitations should also be considered. The model does not measure the quality of judicial reasoning in individual cases, the actual training level of investigators or experts, or the technical configuration of closed government information systems. The analysis also does not differentiate between digital evidence obtained from mobile devices, cloud platforms, social networks and automated state databases. These categories may require different technical safeguards and may produce different evidentiary risks. Future validation should therefore include case-law datasets, expert surveys and controlled testing of the DERF checklist on specific categories of digital artifacts.

7. CONCLUSIONS

The research findings confirm that the reliability of digital evidence in criminal proceedings is determined not by individual technical tools, but rather by the degree of coherence between technical procedures, organizational mechanisms and the legal requirements governing their application. The use of the integrated Digital Evidence Reliability Framework (DERF) made it possible to quantitatively assess the actual readiness of legal systems to work with digital evidence in the face of administrative and digital transformation.

A comparative analysis of Ukraine, Spain and the United Arab Emirates demonstrated three distinct integration models between technical and legal components. Ukraine showed a moderate level of integrated reliability (DERF = 0.66), primarily due to fragmented procedural formalization of digital processes and underdeveloped organizational control mechanisms. In this case, the most significant losses of evidentiary reliability occur at the stage of procedural consolidation of digitally correct but insufficiently formalized data in terms of legal requirements . Spain is characterized by a balanced integration model (DERF = 0.78). In this model technical integrity, strong judicial oversight and regulatory compatibility collectively ensure the stability of digital evidence in litigation. The highest integration level is observed in the United Arab Emirates (DERF = 0.87), where technical, organizational and legal mechanisms operate as a unified and highly formalized system.

Structural imbalance analysis indicates that the principal risks of digital evidence depreciation arise not from deficiencies in technical integrity, but from misalignment between technical actions and their regulatory and procedural articulation. The findings demonstrate that enhancing the effective use of digital evidence requires systemic integration across all stages of its lifecycle. In view of the above, the proposed DERF model serves as a practical analytical tool for assessing the current state of national criminal justice systems and identifying strategic directions for improving digital evidence reliability. In this revised form, the article explicitly presents DERF as both a conceptual model and an operational assessment tool, which strengthens the novelty, methodological transparency and practical applicability of the study.

REFERENCES

[1] T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk, and S. Podolyaka, “Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine,” Journal of Information Technology Management, Vol. 13, 2021, pp. 75–90, doi: 10.22059/JITM.2021.80738.

[2] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov, and A. Mysyk, “Improving the state system of strategic planning

of national security in the context of informatization of society," Journal of Information Technology Management, Vol. 14, 2022, pp. 1–24, doi: 10.22059/jitm.2022.88861.

[3] S. Korzun, "Theoretical and methodological construction of state criminal law policy to combat cybercrime," Economics, Management and Administration, No. 4(110), 2024, pp. 145–158, doi: 10.26642/ema-2024-4(110)-145-158.

[4] V. Shevchuk, "Innovations in criminalistic technique: modern possibilities and application problems," Scientific Bulletin of the International Humanities University. Series: Jurisprudence, No. 43, 2020, pp. 146–151, doi: 10.32841/2307-1745.2020.43.32.

[5] S. O. Perez, "Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial," European Journal of Crime, Criminal Law and Criminal Justice, Vol. 33, No. 1–2, 2025. pp. 187–211,

[6] L. Freeman and R. Vazquez Llorente, "Finding the signal in the noise: International criminal evidence and procedure in the digital age," Journal of International Criminal Justice, Vol. 19, No. 1, 2021,, pp. 163–188, doi: 10.1093/jicj/mqab023.

[7] J. C. Santillán-Lima, P. Haro-Parra, W. Luna-Encalada, R. Lozada-Yánez, and F. Molina-Granja, "Security techniques in communications networks applied to the custody of digital evidence," in Proc. Int. Conf. Advances in Emerging Trends and Technologies, Cham, Switzerland: Springer, 2021, pp. 298–309, doi: 10.1007/978-3-030-96147-3_24.

[8] M. H. A. Ratul, S. Mollajafari, and M. Wynn, "Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution," Sustainability, Vol. 16, No. 24, Art. No. 10885, 2024, doi: 10.3390/su162410885.

[9] A. Sachoulidou, "Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of judicial cooperation," New Journal of European Criminal Law, Vol. 15, No. 3, 2024, pp. 256–274, doi: 10.1177/20322844241258649.

[10] V. Yermachenko et al., "Theory and practice of public management of smart infrastructure in the conditions of the digital society development: Socio-economic aspects," Economic Affairs, Vol. 68, No. 1, 2023, pp. 617–633, doi: 10.46852/0424-2513.1.2023.29.

[11] A. A. Khan et al., "MF-ledger: Blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," IEEE Access, Vol. 9, 2021, pp. 103637–103650, doi: 10.1109/ACCESS.2021.3099037.

[12] D. Kim, S. Y. Ihm, and Y. Son, "Two-level blockchain system for digital crime evidence management," Sensors, Vol. 21, No. 9, Art. No. 3051, 2021, doi: 10.3390/s21093051.N.

[13] R. A. Stoykova, "A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings," Computer Law & Security Review, Vol. 55, Art. No. 106040, 2024, doi: 10.1016/j.clsr.2024.106040.

[14] G. Lasagni, "Admissibility of digital evidence," in The Cambridge Handbook of Digital Evidence in Criminal Investigations. Cambridge, U.K.: Cambridge Univ. Press, 2025, pp. 126–152.

[15] Z. Nilaei Sangari and A. Mohammadi, "Admissibility of Digital Evidence at the International Criminal Court," Journal of Criminal Law Research, Vol. 13, No. 48, 2025, pp. 41–84, doi: 10.22054/jclr.2025.81549.2697.

[16] S. Nazir, M. Asif, and A. U. A. Khan, "Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials," ASSAJ, Vol. 4, No. 1, 2025, pp. 1941–1951, doi: 10.55966/assaj.2025.4.1.0107.

[17] S. Hosaka, "Leaked email data: A new source for the study of authoritarian regimes," Digital War, Vol. 6, No. 1, Art. No. 1, 2025, doi: 10.1057/s42984-024-00097-w.

[18] A. Alkhseilat, T. Al-Billeh, M. Albazi, and N. A. Ali, "The authenticity of digital evidence in criminal courts: A comparative study," International Journal of Electronic Security and Digital Forensics, Vol. 16, No. 6, 2024, pp. 720–738, doi: 10.1504/IJESDF.2024.142010.

[19] A. F. Moussa, "Electronic evidence and its authenticity in forensic evidence," Egyptian Journal of Forensic Sciences, Vol. 11, No. 1, Art. No. 20, 2021, doi: 10.1186/s41935-021-00234-6.

[20] Criminal Procedure Code of Ukraine, Law of Ukraine, Apr. 13, 2012 (as amended 2024).

[21] Law of Ukraine "On Electronic Documents and Electronic Document Circulation", Law of Ukraine, 2003.

[22] Law of Ukraine "On Electronic Trust Services", Law of Ukraine, 2017.

[23] Law of Ukraine "On Information", Law of Ukraine, 1992 (as amended).

[24] Law of Ukraine "On Protection of Information in Information and Communication Systems", Law of Ukraine, 1994.

[25] Ley de Enjuiciamiento Criminal [Criminal Procedure Act], Spain, 1882 (as amended).

[26] Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences, Spain, 2021.
[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union, 2016.
[28] Federal Law No. 10 of 1992 on Criminal Procedure (as amended), United Arab Emirates, 1992.
[29] Federal Decree-Law No. 35 of 2021 on Countering Rumors and Cybercrimes, United Arab Emirates, 2021.
[30] Federal Decree-Law No. 46 of 2021 on Electronic Transactions and Trust Services, United Arab Emirates, 2021.
[31] R. S. Faqir, "Digital criminal investigations in the era of artificial intelligence: A comprehensive overview," International Journal of Cyber Criminology, Vol. 17, No. 2, 2023. pp. 77–94,
[32] A. A. S. Al-Sherideh et al., "Digital Evidence and Forensic Tools in Cyber Law: A Comprehensive Analysis," in Proc. 25th Int. Arab Conf. Information Technology (ACIT), 2024, pp. 1–6, doi: 10.1109/ACIT62805.2024.10877028.
[33] G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-Forensic (IoF): A blockchain-based digital forensics framework for IoT applications," Future Generation Computer Systems, Vol. 120, 2021, pp. 13–25, doi: 10.1016/j.future.2021.02.016.
[34] S. K. Rana et al., "Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain," IEEE Access, Vol. 11, 2023, pp. 83289–83300, doi: 10.1109/ACCESS.2023.3302771.
[35] A. H. Ali et al., "Digital Transformation of Legal Frameworks of Judicial Procedures: A Comparative Study," in Tech Fusion in Business and Society: Harnessing Big Data, IoT, and Sustainability in Business, Vol. 2. Cham, Switzerland: Springer Nature, 2025, pp. 477–487, doi: 10.1007/978-3-031-84636-6_41.
[36] A. A. Solanke, "Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models," Forensic Science International: Digital Investigation, Vol. 42, Art. No. 301403, 2022, doi: 10.1016/j.fsidi.2022.301403.
[37] Horan and H. Saiedian, "Cyber crime investigation: Landscape, challenges, and future research directions," Journal of Cybersecurity and Privacy, Vol. 1, No. 4, 2021, pp. 580–596, doi: 10.3390/jcp1040029.
[38] K. H. S. S. Al-Tamimi, N. B. Marni, and A. Shehab, "Legal regulation of evidence in cybercrimes in UAE legislations," *International Journal of Health Sciences*, Vol. 6, 2022, pp. 765–776, doi: 10.53730/ijhs.v6nS1.4827.
[39] I. Kalancha, "International experience in the use of electronic segments in criminal proceedings in court," *Jurnalul juridic national: teorie şi practică*, Vol. 16, No. 6, 2015, pp. 224–228,
[40] A. P. Seepma, C. de Blok, and D. P. Van Donk, "Designing digital public service supply chains: Four country-based cases in criminal justice," *Supply Chain Management: An International Journal*, Vol. 26, No. 3, 2021, pp. 418–446, doi: 10.1108/SCM-03-2019-0111.
[41] Allah Rakha, "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations," *Mexican Law Review*, Vol. 16, No. 2, 2024, pp. 23–54.