CYBERSECURITY OF DIGITAL CRIMINAL JUSTICE INFRASTRUCTURE IN UKRAINE: A PROCEDURAL SAFEGUARD OF ELECTRONIC EVIDENCE INTEGRITY AND FAIR TRIAL

Nataliia Stashevska
LL.M., CBAP, CCA,
Independent Researcher
e-mail: stashevskaya.nata@gmail.com, orcid.org/0009-0002-6120-9011

Summary

The digitalisation of criminal justice has transformed the procedural environment in which evidence is created, stored, transmitted, examined, and challenged. In proceedings involving electronic evidence, evidentiary reliability increasingly depends not only on formal rules of admissibility and proof, but also on the cybersecurity of the digital infrastructure through which such evidence is handled. This article argues that cybersecurity of digital criminal justice infrastructure in Ukraine is better conceptualised not merely as a technical or organisational function of information protection, but as a procedural safeguard of electronic evidence integrity and fair trial.

The article examines the procedural significance of cybersecurity safeguards for ensuring the integrity, authenticity, provenance, traceability, and verifiability of electronic evidence in Ukrainian criminal proceedings. It applies formal-dogmatic, systemic-structural, and limited comparative legal methods and analyses Ukrainian criminal procedure, legislation on electronic documents, electronic identification and trust services, cybersecurity regulation, selected doctrinal sources, European human rights standards, and international cybersecurity guidance.

The analysis demonstrates that the integrity, traceability, and verifiability of electronic evidence increasingly depend on cybersecurity measures embedded within digital justice systems. Accordingly, Ukrainian criminal procedure should more clearly integrate cybersecurity safeguards into evidentiary handling, judicial assessment, and defence verification.

Key words: electronic evidence, cybersecurity, criminal proceedings, evidence integrity, traceability, fair trial, equality of arms, Ukraine.

DOI https://doi.org/10.23856/7647

1. Introduction

Digitalisation has transformed criminal justice from a predominantly paper-based process into an environment increasingly dependent on electronic communication, digital records, information systems, and electronic forms of evidence. In contemporary criminal proceedings, relevant information may exist in the form of e-mails, messages, CCTV recordings, digital financial records, cloud-stored documents, device data, system logs, and other digital traces. As a result, evidentiary reliability can no longer be analysed solely through traditional categories of admissibility and proof. It also depends on the technological environment in which digital material is created, stored, transmitted, and examined *(Nazarko, 2023; Council of Europe, 2019).*

This transformation is particularly important for electronic evidence. Unlike traditional paper documents or physical objects, electronic evidence is inseparable from the digital

conditions of its existence. Its authenticity, integrity, provenance, and reliability may depend not only on the content of the evidentiary item itself, but also on metadata, timestamps, system logs, access records, audit trails, integrity-verification mechanisms, and the security of the systems through which the evidence has been handled *(NIST, 2022; UNODC, n.d.)*.

In Ukraine, this issue has acquired growing significance due to the broader digitalisation of public administration, electronic document circulation, trust services, and justice-related information systems. Ukrainian law regulates criminal procedure, electronic documents, electronic identification and trust services, cybersecurity, and related matters relevant to digital interaction. Yet the legal and doctrinal treatment of this transformation remains fragmented. Ukrainian law recognises the importance of electronic evidence and regulates certain digital instruments, but it does not yet provide a coherent procedural model that conceptualises cybersecurity as a safeguard of evidentiary integrity and verifiability *(Figurskyi, 2023; Predmestnikov et al., 2026)*.

The research problem addressed in this article is therefore the following: Ukrainian criminal procedure increasingly relies on electronic evidence and digital interaction, but the legal regulation of cybersecurity and the legal regulation of criminal evidence still operate largely in parallel. As a result, access control, logging, metadata preservation, integrity verification, and incident response are often treated as technical or administrative matters rather than as mechanisms directly relevant to evidentiary reliability and procedural fairness *(Ablamskyi & Romaniuk, 2024; Politova & Chekhlai, 2025)*.

The purpose of this article is to substantiate that cybersecurity of digital criminal justice infrastructure in Ukraine should be understood not merely as a technical or organisational function of information protection, but as a procedural safeguard necessary for ensuring the integrity, authenticity, traceability, and verifiability of electronic evidence and, consequently, for supporting fair trial guarantees in criminal proceedings.

The article uses formal-dogmatic, systemic-structural, and limited comparative legal methods. The formal-dogmatic method is used to analyse the Criminal Procedure Code of Ukraine, legislation on electronic documents, trust services, and cybersecurity. The systemic-structural method makes it possible to examine evidentiary rules, digital infrastructure, and procedural guarantees as parts of one procedural ecosystem. A limited comparative approach is used to situate the Ukrainian discussion within selected international standards and fair trial principles relevant to digital evidence *(Council of Europe, 2019; Stoykova, 2023)*.

2. Digital Criminal Justice Infrastructure in Ukraine

The digitalisation of criminal justice in Ukraine has developed at the intersection of several legal regimes. These include criminal procedure law, legislation on electronic documents and electronic document management, legislation on electronic identification and trust services, cybersecurity legislation, and broader rules governing the protection of information systems. Although these frameworks were not originally designed as one integrated model of digital criminal justice, their interaction increasingly determines how procedural information and electronic evidence are created, transmitted, preserved, and evaluated *(Criminal Procedure Code of Ukraine, 2012; Law of Ukraine on Electronic Documents and Electronic Document Management, 2003; Law of Ukraine on Electronic Identification and Electronic Trust Services, 2017; Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine, 2017)*.

The Criminal Procedure Code of Ukraine establishes the general framework for the collection, submission, examination, and evaluation of evidence. It remains the central source

governing proof, admissibility, procedural rights, and judicial control. At the same time, its evidentiary rules increasingly operate in digital environments that the Code itself does not fully conceptualise. Where information exists in digital form or is generated through information systems, criminal procedure intersects with other areas of regulation that shape the legal status and handling of digital material *(Criminal Procedure Code of Ukraine, 2012).*

Legislation on electronic documents and electronic document management establishes the legal recognition of electronic documents and regulates their use in legal circulation. For criminal proceedings, its significance lies in defining the conditions under which digital documents may be created, preserved, and relied upon as evidentiary material *(Law of Ukraine on Electronic Documents and Electronic Document Management, 2003).* Legislation on electronic identification and trust services is also relevant because electronic signatures, seals, timestamps, and related mechanisms may help establish authorship, time of signing, and formal integrity of digital records *(Law of Ukraine on Electronic Identification and Electronic Trust Services, 2017).*

Cybersecurity legislation forms another important layer. At first glance, cybersecurity law may appear to concern primarily national security, resilience of digital systems, or protection of state information resources. In criminal proceedings, however, its significance is broader. Cybersecurity regulation shapes the conditions under which digital systems are protected against unauthorised access, interference, data loss, compromise, or disruption. Where procedural information and electronic evidence are stored or processed through such systems, cybersecurity safeguards become relevant to evidentiary integrity *(Law of Ukraine on Protection of Information in Information and Communication Systems, 1994; Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine, 2017).*

For the purposes of this article, digital criminal justice infrastructure may be defined as the set of legal, organisational, institutional, and technological arrangements through which criminal justice actors create, receive, store, transmit, access, process, preserve, and examine procedural information and evidence in digital form. This concept is broader than any single information system. It includes technological tools, institutional procedures, legal recognition of digital records, and safeguards that protect integrity and traceability.

This broader concept is necessary because electronic evidence does not exist in a procedural vacuum. A file, message, image, database extract, or digital log may formally appear as a discrete evidentiary object, but the reliability of such digital material often depends on the digital environment from which it originates and through which it has been handled. The question is not only what the electronic evidence contains, but whether the conditions of its creation, preservation, and transmission allow the court and the parties to trust that it is authentic, complete, and unchanged *(Council of Europe, 2019; NIST, 2022; UNODC, n.d.).*

The institutional structure of criminal proceedings reinforces this conclusion. Digital evidentiary material may pass through multiple actors and stages: investigators, prosecutors, experts, courts, and the defence. At the pre-trial stage, electronic evidence may be identified, copied, extracted, preserved, and transmitted by investigative authorities. The prosecutor may rely on it and disclose it to the defence. The court may later need to evaluate not only the content of the digital material, but also the conditions of its collection and handling. The defence may need access to metadata, extraction records, or system-handling information to challenge authenticity or integrity. These institutional dynamics show that evidentiary reliability depends not only on the digital item itself, but on the integrity of the environment through which it moved *(NIST, 2022; Stoykova, 2023).*

Thus, digital criminal justice infrastructure is better conceptualised not as a neutral technical background, but as a legally relevant evidentiary environment.

3. Electronic Evidence and the Problem of Verifiability

The growing role of digital technologies has transformed the evidentiary landscape of criminal proceedings. A substantial part of information relevant to criminal cases now exists in digital form: messages, e-mails, photographs and videos, geolocation data, server logs, financial records, cloud-stored files, social media content, and data generated by online services. In many cases, such materials may serve as central evidence of communication, chronology, identity, intent, access, possession, or financial activity *(Council of Europe, 2019; Nazarko, 2023).*

In Ukrainian criminal proceedings, however, the legal treatment of electronic evidence remains conceptually complex. Digital material may enter the case as a document, as material evidence, as information contained on physical carriers, as audio-visual data, or through expert conclusions based on extracted digital information. This reflects the reality that such evidence is not defined by one single physical form. At the same time, it creates doctrinal uncertainty because the evidentiary object presented to the court is often not the original digital environment itself, but a copy, export, screenshot, recording, printout, or reconstructed set of data *(Figurskyi, 2023).*

Electronic evidence differs from traditional evidence not only in format, but in its dependence on the digital environment from which it originates. A digital file may be copied without physical degradation, but it may also be altered, deleted, reformatted, partially extracted, or stripped of metadata. A screenshot may show a conversation, but by itself it may not prove who controlled the account, whether the message was modified, whether the conversation was selectively captured, or whether metadata confirming timing and origin has been preserved *(NIST, 2022; Predmestnikov et al., 2026).*

From this perspective, electronic evidence should be understood functionally rather than purely formally. It is not enough to ask whether a file or digital record falls within one evidentiary category or another. What matters is whether the criminal process has sufficient tools to assess its origin, authenticity, integrity, provenance, completeness, and reliability *(Hryshchuk, 2026; Nazarko, 2023).*

The key doctrinal difficulty is that the reliability of digital material often depends on whether it can be meaningfully verified. In criminal proceedings, admissibility is not the only question. The court must also be able to assess whether the evidence is authentic and reliable, and the opposing party must have a realistic opportunity to challenge it. In the context of electronic evidence, this means that the system of proof must provide a basis for assessing whether digital information is what it purports to be, whether it remained unchanged, whether it can be linked to a particular source, and whether the opposing party can contest those claims *(Ablamskyi & Romaniuk, 2024; Stoykova, 2023).*

Several interrelated categories become central here. Authenticity concerns whether the digital material is what it purports to be. Provenance concerns the origin and history of the evidence. Integrity concerns whether the digital material remained unchanged, complete, and free from unauthorised modification. Verifiability concerns whether the court and the parties have a meaningful basis for checking those claims.

Ukrainian law increasingly recognises the practical significance of electronic evidence, yet it does not fully articulate a coherent procedural model of verifiability. One aspect of this gap concerns the relationship between the evidentiary object and the evidentiary environment. In digital cases, reliability cannot always be assessed without information about the environment in which the evidence was created, stored, copied, transferred, and preserved *(Council of Europe, 2019; NIST, 2022).*

A second gap concerns the distinction between possession of digital content and proof of evidentiary reliability. In practice, the acquisition of a file, screenshot, chat export, or video recording may be treated as sufficient for evidentiary use, while questions of authenticity or integrity are postponed until challenged or referred to expert examination. In digital cases, however, the absence of built-in verification may itself create procedural vulnerability *(Politova & Chekhlai, 2025; Predmestnikov et al., 2026).*

A third gap concerns traceability. In relation to physical evidence, criminal procedure recognises the importance of documenting seizure, storage, transfer, and examination. In the digital context, traceability may require more: documentation of how data was extracted, whether forensic copying was used, whether integrity indicators were generated, who accessed the data after collection, whether it was transferred between systems, and whether metadata was preserved *(SWGDE, 2018; Council of Europe Cybercrime Programme Office, 2023).*

Finally, there is a broader conceptual gap between technical reliability and procedural fairness. Criminal procedure speaks the language of admissibility, burden of proof, judicial evaluation, and party rights. Cybersecurity speaks the language of confidentiality, integrity, availability, access control, and incident response. What remains underdeveloped is the doctrinal bridge between these vocabularies: an account of how technical safeguards and failures affect evidentiary reliability, party challenge, and fair trial guarantees *(Stoykova, 2023; Predmestnikov et al., 2026).*

4. Cybersecurity as a Procedural Safeguard

If the reliability of electronic evidence depends on the conditions of its creation, storage, transfer, and verification, the next question is which features of digital systems preserve that reliability. The answer lies in cybersecurity and digital-governance safeguards that are often treated as technical controls but, in criminal proceedings, perform a broader evidentiary function.

These safeguards include access control, authentication and authorisation, logging, audit trails, metadata preservation, integrity verification, secure storage, controlled copying, and incident response *(NIST, 2006; NIST, 2022; SWGDE, 2018).*

Access control matters because it determines who can view, copy, modify, delete, export, or otherwise interact with digital material. If electronic evidence is stored in an environment where access is not properly restricted, the possibility of unauthorised interference increases and later evidentiary trust may be weakened. Authentication and authorisation mechanisms are similarly important because they help establish whether actions affecting digital evidence can be attributed to specific users or roles *(Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine, 2017; NIST, 2006).*

Logging and audit trails are also central. Logs may record access, downloads, uploads, modifications, deletions, transfers, or other system actions. In the context of electronic evidence, logs may answer procedural questions: who accessed the evidence, when it was accessed, whether it was copied, and whether changes occurred. Audit trails can create a structured history of evidentiary handling and help reconstruct the path of electronic evidence from collection to courtroom *(Council of Europe Cybercrime Programme Office, 2023; NIST, 2022).*

Metadata preservation is another essential safeguard. Metadata may contain information about creation time, modification time, file origin, system attributes, transmission history, device identifiers, and other contextual details relevant to authenticity and provenance. In many digital cases, metadata is not peripheral but evidentially central *(Council of Europe, 2019; NIST, 2022).*

Integrity-verification mechanisms, including hashes, also play a crucial role. Their value lies in creating a reference point against which later versions of a digital file or image can be compared. If a forensic copy is created and its hash value recorded, later examination may show whether the evidentiary item remains identical to the collected version *(SWGDE, 2018; NIST, 2022)*.

The procedural significance of these safeguards follows from a simple proposition: in digital criminal proceedings, the reliability of electronic evidence depends not only on the content of the evidentiary item, but on whether the parties and the court can meaningfully verify how that item was created, handled, preserved, and protected from unauthorised interference *(Council of Europe, 2019; Stoykova, 2023)*.

First, cybersecurity safeguards support proof of evidentiary integrity. In the digital environment, alteration may occur invisibly and without obvious traces. If a file can be modified, copied, partially deleted, or reformatted without the change being externally apparent, evidentiary integrity cannot be reliably assessed without system-level safeguards.

Second, cybersecurity safeguards support provenance and attribution. Electronic evidence is often challenged not because its content is implausible, but because its source is disputed. A message may be denied by the alleged sender; a document may be said to have been created or altered by someone else; a database extract may be challenged as incomplete or taken out of context. These questions may require metadata, access records, account histories, timestamps, extraction documentation, and other traces of system interaction.

Third, cybersecurity safeguards support contestability of evidence. The defence must have a meaningful opportunity to challenge authenticity, integrity, provenance, and completeness. In many cases, such challenge is impossible unless handling of the evidence has left verifiable traces: logs, extraction records, integrity checks, metadata, or audit trails documenting the path of the evidence *(Stoykova, 2023)*.

The inverse proposition is equally important: cybersecurity failures may create evidentiary risk. If electronic evidence is stored in a system to which unauthorised persons gained access, the evidentiary question is not limited to whether information-security policy was violated. The key issue is whether the evidence may have been viewed, copied, altered, deleted, or otherwise affected in a manner relevant to the criminal case.

Likewise, if integrity-verification mechanisms are absent or poorly documented, it may be difficult to distinguish between a faithful copy and a modified version of the same evidence *(NIST, 2006; UNODC, n.d.)*.

For these reasons, cybersecurity in digital criminal justice should not be conceptualised as an external matter of infrastructure protection. It should therefore be treated as a procedural safeguard of evidentiary trust. Cybersecurity remains technical in implementation, but its legal significance becomes procedural where integrity, traceability, and contestability of proof depend on it.

5. Fair Trial and Defence Verification

The procedural significance of cybersecurity becomes most apparent when electronic evidence is examined through fair trial guarantees. Criminal proceedings are not concerned only with formal admission of evidence; they are concerned with whether the evidentiary process allows the accused to understand, challenge, and respond to the case against them *(European Convention on Human Rights, 1950, Art. 6; Stoykova, 2023)*.

Digital evidence creates specific fair trial challenges because its reliability may depend on information that is not visible from the evidence itself. A digital file, message, database extract, or system log may appear persuasive on its face, but its evidentiary value may depend on source, metadata, access history, preservation, extraction method, and system integrity. A fair trial framework must therefore take account of the fact that digital evidence often cannot be meaningfully assessed without contextual information about the way it was created and handled *(Council of Europe, 2019; NIST, 2022).*

This does not mean that Article 6 ECHR requires a technical cybersecurity audit in every case involving electronic evidence. Rather, where reliability of electronic evidence is contested, or where circumstances raise reasonable concerns about authenticity, integrity, provenance, or completeness, the procedural system must provide mechanisms through which those concerns can be examined. In the digital context, fair trial does not demand technical perfection; it demands a fair opportunity to test reliability where reliability is reasonably in issue *(Jasper v. the United Kingdom, 2000; Stoykova, 2023).*

Equality of arms is central here. The prosecution may rely on digital materials obtained from devices, platforms, databases, surveillance systems, or state information systems. The defence, however, may not have direct access to the original digital environment, extraction process, system logs, or metadata necessary to test reliability. In such circumstances, the prosecution's practical control over the evidentiary environment may create an asymmetry that goes beyond ordinary differences in litigation resources *(Rowe and Davis v. the United Kingdom, 2000; Edwards and Lewis v. the United Kingdom, 2004).*

A meaningful opportunity to verify electronic evidence may require information about the source of the evidence, the method of collection or extraction, metadata, timestamps, logs, chain of handling, and, where relevant, cybersecurity incidents or system compromise. A screenshot may show text, but not necessarily prove authorship, timing, or completeness. A digital file may contain relevant content, but not necessarily prove that it remained unchanged or corresponds to the original source *(Council of Europe Cybercrime Programme Office, 2023; NIST, 2022).*

At the same time, the defence's right to verification must be balanced against legitimate interests such as privacy, protection of sensitive systems, confidentiality of investigative methods, and security of state information resources. Not every case will justify unrestricted disclosure of technical infrastructure. Yet legitimate limitations do not remove the procedural problem. They require mechanisms that allow relevant verification while protecting legitimate interests. Such mechanisms may include controlled expert examination, disclosure of extracted metadata, production of logs in limited form, judicial review of sensitive materials, or appointment of independent experts *(Foucher v. France, 1997; Jasper v. the United Kingdom, 2000).*

Traceability concerns the ability to reconstruct the history of electronic evidence. Transparency concerns the availability of sufficient information for the court and parties to evaluate that history. Challengeability concerns the practical ability of the defence to contest reliability, authenticity, integrity, or completeness. Cybersecurity safeguards are procedurally relevant because they support all three conditions. Logging supports traceability. Metadata preservation supports transparency and attribution. Access control supports accountability. Integrity verification supports challengeability *(Council of Europe Cybercrime Programme Office, 2023; Stoykova, 2023).*

The broader implication is that cybersecurity of digital criminal justice infrastructure should be understood as a condition of trust in digital criminal adjudication. Its importance lies not only in protecting state information systems, but in supporting the reliability of proof, rights of the defence, transparency of evidentiary handling, and the court's ability to make reasoned decisions based on digital material.

6. Conclusions

The digitalisation of criminal justice has changed the conditions under which evidence is created, preserved, transmitted, examined, and challenged. In proceedings involving electronic evidence, the reliability of proof increasingly depends not only on formal procedural rules, but also on the digital infrastructure through which evidentiary material is handled. The analysis demonstrates that cybersecurity has procedural significance extending beyond the protection of information systems. Where criminal proceedings rely on electronic evidence, cybersecurity safeguards directly influence the integrity, traceability, and verifiability of evidentiary material and, consequently, the practical implementation of fair trial guarantees.

First, cybersecurity in digital criminal justice has procedural significance because it supports the conditions under which electronic evidence can be authenticated, traced, preserved, verified, and challenged. Access control, logging, audit trails, metadata preservation, integrity verification, secure storage, and incident-response mechanisms are technical in implementation, but procedural in evidentiary effect.

Second, Ukrainian law contains important normative elements relevant to digital criminal justice, including criminal procedure rules, legislation on electronic documents, electronic identification and trust services, and cybersecurity regulation. However, these elements do not yet form a sufficiently coherent procedural-legal model linking cybersecurity safeguards with evidentiary integrity, authenticity, provenance, traceability, and verifiability.

Third, digital evidentiary material should not be analysed only through formal evidentiary categories or through visible content. Its evidentiary value may depend on the digital environment in which it was generated, collected, copied, stored, transferred, and presented. For this reason, admissibility and evidentiary weight in cases involving electronic evidence may require attention to metadata, access records, system logs, integrity checks, extraction methods, and chain-of-custody documentation.

Fourth, Article 6 ECHR and equality of arms require that the accused have a meaningful opportunity to challenge evidence used against them. In digital cases, such opportunity may depend on access to information necessary to verify electronic evidence, including its source, metadata, handling history, and integrity safeguards. Where those conditions are absent, the defence may be deprived of an effective opportunity to contest the prosecution's digital case.

On this basis, Ukrainian criminal procedure should more clearly recognise the procedural relevance of electronic evidence integrity, authenticity, provenance, and traceability. Evidentiary-handling protocols should include clearer requirements for preserving metadata, documenting extraction and copying methods, maintaining access records, and ensuring integrity verification. Procedural rules should also address evidentiary consequences of cybersecurity incidents affecting systems that store or process electronic evidence. Courts should be provided with clearer guidance on how to evaluate challenges based on alleged alteration, incomplete extraction, metadata loss, or system compromise.

In sum, cybersecurity of digital criminal justice infrastructure should be conceptualised as an integral part of procedural fairness in the digital age. It is not only a matter of protecting systems from technical threats. It is a condition for preserving the integrity of electronic evidence, enabling meaningful defence challenge, supporting reasoned judicial evaluation, and maintaining trust in digital criminal justice. Ultimately, the legitimacy of digital criminal justice depends not only on the existence of electronic evidence, but on the procedural ability of courts and parties to trust, verify, and challenge it.

References

1. Ablamskyi, S. Ye., & Romaniuk, V. V. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. Law and Safety, 93(2), 140–150. https://doi.org/10.32631/pb.2024.2.13

2. Council of Europe Cybercrime Programme Office. (2023). Electronic evidence guide: A basic guide for police officers, prosecutors and judges. Council of Europe. https://www.coe.int/en/web/cybercrime/-/iproceeds-2-launching-of-the-electronic-evidence-guide-v-3-0

3. Council of Europe. (2019). Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. https://search.coe.int/cm?i=0900001680902e0c

4. Criminal Procedure Code of Ukraine, No. 4651-VI (2012, April 13). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/4651-17?lang=en

5. Edwards and Lewis v. the United Kingdom, Applications nos. 39647/98 and 40461/98, European Court of Human Rights. (2004).

6. European Convention on Human Rights. (1950). Council of Europe.

7. Figurskyi, V. M. (2023). Evidence in electronic form in criminal proceedings. Galician Studies: Legal Sciences, 4, 97–105. https://doi.org/10.32782/galician_studies/law-2023-4-14

8. Foucher v. France, Application no. 22209/93, European Court of Human Rights. (1997).

9. Guttman, B., White, D. R., & Walraven, T. (2022). Digital evidence preservation: Considerations for evidence handlers (NIST IR 8387). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8387

10. Hryshchuk, V. R. (2026). Elektronni (tsyfrovi) dani u kryminalnomu provadzhenni: vid elektronnoho slidu do dokazu [Electronic (digital) data in criminal proceedings: From electronic trace to evidence]. Naukovyi Visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo, 93(5). https://doi.org/10.24144/2307-3322.2026.93.5.9

11. Jasper v. the United Kingdom, Application no. 27052/95, European Court of Human Rights. (2000).

12. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

13. Law of Ukraine on Electronic Documents and Electronic Document Management, No. 851-IV. (2003, May 22). Verkhovna Rada of Ukraine.

14. Law of Ukraine on Electronic Identification and Electronic Trust Services, No. 2155-VIII. (2017, October 5). Verkhovna Rada of Ukraine.

15. Law of Ukraine on Protection of Information in Information and Communication Systems, No. 80/94-VR. (1994, July 5). Verkhovna Rada of Ukraine.

16. Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine, No. 2163-VIII. (2017, October 5). Verkhovna Rada of Ukraine.

17. Nazarko, A. (2023). E-evidence in Ukrainian criminal justice: Exploring the legal realities and theoretical perspectives. Naukovyi Visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia: Pravo, 80(2), 183–188. https://doi.org/10.24144/2307-3322.2023.80.2.28

18. Politova, A. S., & Chekhlai, T. O. (2025). Dopustymist tsyfrovykh dokaziv u kryminalnomu provadzhenni: analiz sudovoi praktyky [Admissibility of digital evidence in criminal proceedings: Analysis of judicial practice]. Visnyk Mariupolskoho Derzhavnoho Universytetu. Seriia: Pravo, 29, 104–115. https://doi.org/10.34079/2518-1319-2025-15-29-104-115

19. Predmestnikov, O. H., Tatarnikova, T. O., & Semeniuk-Prybaten, A. V. (2026). Pravove rehuliuvannia vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnomu protsesi [Legal regulation of the use of electronic (digital) evidence in criminal proceedings]. Akademichni Vizii, 54. https://doi.org/10.66556/2786-586X.54.predmestnikov-o
20. Rowe and Davis v. the United Kingdom, Application no. 28901/95, European Court of Human Rights. (2000).
21. Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence. Computer Law & Security Review, 49, Article 105801. https://doi.org/10.1016/j.clsr.2023.105801
22. SWGDE. (2018). Best practices for digital evidence collection. Scientific Working Group on Digital Evidence. https://www.swgde.org/documents/published-complete-listing/18-f-002-best-practices-for-digital-evidence-collection/
23. UNODC. (n.d.). Digital evidence / Handling of digital evidence. United Nations Office on Drugs and Crime. https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html