HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

CYBERCRIME AND THE ADMISSIBILITY OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: LEGAL CHALLENGES AND SAFEGUARDS

Yakubbayeva Shaxnoza Xabibullayevna
English language teacher at the H.K. Muhitdinova Academic Lyceum under Tashkent State University of Law.
E-mail: shahnozasaydullo@gmail.com
Doi: https://doi.org/10.5281/zenodo.23600195

Abstract. The rapid development of information and communication technologies has transformed criminal activity and created new challenges for criminal investigations and judicial proceedings. Digital evidence, including electronic communications, computer logs, mobile device data, cloud records, and blockchain transactions, has become increasingly important in establishing criminal liability. However, its admissibility raises complex legal and technical questions concerning authenticity, integrity, reliability, lawful acquisition, privacy, and the preservation of the chain of custody. This article examines the principal legal challenges associated with digital evidence in criminal proceedings and evaluates safeguards designed to protect the rights of defendants while ensuring effective criminal prosecution. Using doctrinal, comparative, and analytical methods, the study considers international legal instruments, digital forensic standards, and fair-trial principles. It argues that reliable digital evidence requires a transparent evidentiary process, effective judicial scrutiny, independent forensic examination, and meaningful opportunities for the defence to challenge prosecution evidence. The article concludes by proposing a comprehensive framework for improving the admissibility and evidentiary value of digital evidence.

Keywords: cybercrime, digital evidence, electronic evidence, admissibility, criminal proceedings, digital forensics, chain of custody, authenticity, data integrity, fair trial, privacy, human rights.

Introduction. The widespread use of digital technologies has fundamentally changed the nature of criminal activity and the methods employed by law enforcement authorities to investigate offences. Crimes such as unauthorized access to computer systems, online fraud, identity theft, cyberstalking, ransomware attacks, and the distribution of illegal digital content frequently involve electronic information that may be stored across multiple devices, networks, and jurisdictions. At the same time, digital evidence is increasingly relevant to conventional criminal offences, including fraud, corruption, organized crime, and other activities in which electronic communications or transaction records may establish the circumstances of the alleged offence. The United Nations Office on Drugs and Crime (UNODC) emphasizes that the admissibility of digital evidence depends on both legal and technical considerations, including the authority under which data was obtained, the relevance and authenticity of the evidence, the integrity of the acquisition process, and the reliability of forensic examination [1]. Consequently, the mere existence of a digital file does not necessarily establish its authenticity, its connection to a particular person, or its reliability as proof of criminal conduct. International instruments provide important foundations for addressing these challenges. The Council of Europe Convention on Cybercrime, commonly known as the Budapest Convention, establishes a framework

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

for criminalizing specified cyber-related conduct, adopting procedural powers to secure electronic evidence, and facilitating international cooperation [2]. The Convention does not, however, create a single universal law of admissibility applicable to every national criminal justice system. The assessment of evidence remains closely connected to domestic procedural law and applicable human rights obligations. The right to a fair trial is equally significant. Article 14 of the International Covenant on Civil and Political Rights recognizes equality before courts and tribunals and guarantees fundamental procedural protections in criminal proceedings [3]. These protections require that defendants have a meaningful opportunity to challenge the evidence relied upon against them. Accordingly, digital evidence must be evaluated not only in terms of technical accuracy but also in relation to procedural fairness, equality of arms, and the practical ability of the defence to examine its reliability. The research problem addressed in this article is the tension between the increasing evidentiary importance of digital information and the legal safeguards necessary to prevent unreliable, unlawfully obtained, or improperly interpreted data from influencing criminal judgments. The research objectives are to: Examine the conceptual and legal foundations of digital evidence. Identify the principal challenges concerning authenticity, integrity, reliability, and chain of custody. Analyse the relationship between digital evidence collection, privacy, and fair-trial guarantees. Assess the significance of international legal instruments and forensic standards. Develop recommendations for improving legal frameworks and evidentiary procedures. The research argues that the admissibility of digital evidence should be assessed through an integrated framework combining lawful acquisition, technical integrity, reliable interpretation, transparent documentation, and effective judicial and defence scrutiny.

Literature review. The scholarly and institutional literature on digital evidence has developed around several interconnected themes: the legal regulation of cybercrime, the scientific principles of digital forensics, evidentiary reliability, and the protection of procedural rights. The United Nations Office on Drugs and Crime has made a substantial contribution to the practical understanding of digital evidence through its educational materials on cybercrime investigation and evidence admissibility. Its analysis emphasizes that courts should consider the legality of searches and seizures, the relevance and authenticity of the material, the integrity of forensic procedures, and the competence of the experts responsible for examination [1]. This approach demonstrates that admissibility cannot be reduced to the production of an electronic record. Instead, it requires scrutiny of the entire process through which the record was obtained, preserved, analysed, and presented. A related contribution is provided by the Council of Europe's *Electronic Evidence Guide*, which addresses the identification, collection, preservation, and examination of electronic evidence. The Guide highlights the importance of maintaining a documented chain of custody and demonstrating who collected the evidence, how it was obtained, and who subsequently controlled or accessed it [4]. These principles are particularly important where evidence passes between investigators, forensic laboratories, prosecutors, and courts.

The Budapest Convention represents a major international legal reference point for cybercrime legislation and electronic evidence cooperation. Its provisions address substantive cybercrime offences, procedural powers, and international cooperation, including the preservation and disclosure of computer data under applicable legal conditions [2]. Its importance lies in recognizing that effective cybercrime investigations require both domestic procedural powers and mechanisms for obtaining evidence located abroad. Nevertheless, international cooperation must operate within the legal safeguards applicable to the relevant jurisdictions. The Commonwealth's *Guidelines on the Treatment*

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

of Electronic Evidence in Criminal Proceedings, adopted by Commonwealth Law Ministers in 2025, provide a further contemporary contribution. They recognize the need for legal systems to accommodate electronic evidence while addressing the risks associated with manipulation, distortion, deletion, and unequal access to technical expertise. The Guidelines also emphasize a fair balance between prosecution and defence and recognize that the ultimate evidentiary value of electronic material must be determined under applicable national law [5].

Despite these contributions, an important analytical challenge remains: technical integrity and legal admissibility are related but distinct questions. A technically accurate forensic copy may have been obtained unlawfully, while lawfully acquired data may be unreliable because of inadequate attribution, incomplete context, or methodological errors. A comprehensive approach must therefore consider legal authorization, forensic integrity, evidentiary relevance, reliability, and procedural fairness together. This article builds on the above literature by proposing an integrated model in which admissibility is assessed through five connected dimensions: legality, authenticity, integrity, reliability, and procedural fairness. The model is intended as an analytical framework rather than a universally binding legal test, since the precise rules of admissibility differ between jurisdictions.

Research methodology. The research employs doctrinal legal analysis, comparative legal analysis, and conceptual synthesis.

Doctrinal legal analysis is used to examine international instruments and institutional guidelines relevant to cybercrime investigations and digital evidence. Particular attention is given to the Budapest Convention, the International Covenant on Civil and Political Rights, the UNODC's materials on digital evidence admissibility, and the Commonwealth Guidelines on the Treatment of Electronic Evidence. Comparative legal analysis is applied to identify common principles across different legal approaches to digital evidence. The comparison focuses on legal authorization, authentication, chain of custody, forensic reliability, disclosure obligations, and the right to challenge evidence. The objective is not to claim that national evidentiary rules are identical, but to identify safeguards that may be relevant across different procedural systems. Conceptual analysis is used to distinguish admissibility from evidentiary weight. Admissibility concerns whether evidence may legally be considered by the court, whereas evidentiary weight concerns the degree to which that evidence supports a particular factual conclusion. The distinction is essential because digital evidence may satisfy a jurisdiction's threshold requirements for admission while remaining insufficient, by itself, to prove identity, intent, or guilt beyond the applicable standard of proof. Synthesis is used to develop a proposed five-dimensional framework for evaluating digital evidence. The framework considers legality, authenticity, integrity, reliability, and procedural fairness as related but independently important factors. The study is qualitative and primarily based on documentary sources. It does not employ a statistical dataset, experimental forensic testing, or an empirical survey of judges, prosecutors, defence lawyers, or forensic experts. Accordingly, its findings constitute a normative and analytical assessment rather than a statistical measurement of the prevalence of evidentiary failures in criminal proceedings.

Results. The analysis identifies five principal dimensions that should be considered when assessing digital evidence in criminal proceedings.

Lawful acquisition of digital evidence. The first requirement is that digital evidence must be obtained in accordance with the applicable law. Searches of computers, mobile devices, online accounts, and cloud storage may reveal highly sensitive personal information, including private

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

communications, financial transactions, medical information, and location histories. The scope of investigative access must therefore be justified by an appropriate legal basis and comply with the relevant procedural requirements. The Budapest Convention provides an international framework for procedural measures in cybercrime investigations, including the expedited preservation of stored computer data and the collection of specified forms of electronic information, subject to applicable conditions and safeguards [2]. However, the existence of an international framework does not eliminate the need to comply with domestic rules governing search warrants, production orders, consent, disclosure, and the handling of privileged or confidential material. An unlawful acquisition may affect admissibility, depending on the applicable national legal system. Even where exclusion is not automatic, the manner in which evidence was obtained may be relevant to the fairness of the proceedings and the reliability of the resulting material.

Authenticity and attribution. Authenticity concerns whether the evidence is what its proponent claims it to be. Attribution concerns whether a particular record can reliably be connected to a specific person, device, account, or activity. For example, a screenshot of a social media conversation may show text attributed to a defendant, but the screenshot alone may not establish who created the messages, whether the account was compromised, whether the displayed content was altered, or whether relevant portions of the conversation were omitted. A more reliable assessment may require examination of the original data where available, associated metadata, account records, device information, server logs, and corroborating evidence. Investigators should also consider alternative explanations, including shared devices, spoofed identities, unauthorized account access, and automated system activity. Authentication must therefore be based on a reasoned evaluation of the available material rather than the assumption that electronic information is inherently reliable.

Integrity and chain of custody. Digital evidence can be modified, intentionally or unintentionally, during collection, transfer, storage, or analysis. Maintaining integrity requires appropriate acquisition procedures, secure storage, documentation, and the use of suitable forensic techniques. A central safeguard is the chain of custody: a documented record of the identification, collection, transfer, storage, examination, and presentation of evidence. Such a record should identify the individuals who handled the material, the relevant dates and times, the purpose of each transfer or access, and any incident that may have affected the evidence. Cryptographic hash values can support integrity verification by allowing investigators to compare the digital fingerprint of a file or forensic image at different stages. However, a matching hash value does not independently prove that the original data was authentic, lawfully acquired, correctly attributed, or complete. It establishes a more limited proposition: that the compared digital objects have matching hash values under the algorithm used. The UNODC's guidance emphasizes documentation throughout the collection and preservation process and recognizes the importance of maintaining a chain of custody [1]. These safeguards are necessary to enable courts and opposing parties to examine whether the evidence may have been altered or mishandled.

Fair-trial guarantees and the rights of the defence. The admissibility of digital evidence must be considered alongside the defendant's right to challenge the prosecution's case. Article 14 of the International Covenant on Civil and Political Rights provides fundamental guarantees relating to a fair hearing and the opportunity to defend oneself [3]. In digital cases, effective defence participation may require access to relevant forensic reports, acquisition records, metadata, and information concerning the tools and methods used. Where disclosure is restricted for legitimate reasons, the court should

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

consider whether alternative arrangements can preserve both the protected interest and the defendant's ability to challenge the evidence. The right to challenge digital evidence must be practical rather than merely formal. If the prosecution relies on a complex technical conclusion that the defence cannot meaningfully examine, the court may have difficulty evaluating the evidence fairly. Depending on the circumstances and applicable law, access to independent expert assistance, supplementary examination, or a hearing on disputed technical issues may be necessary.

The five dimensions identified above are summarized in Table 1.

Table 1. Principal legal and technical requirements for the admissibility of digital evidence

Dimension	Core question	Principal safeguard
Legality	Was the evidence obtained under lawful authority?	Judicial authorization where required, lawful scope, and procedural compliance
Authenticity	Is the evidence what it is claimed to be?	Source verification, metadata examination, and corroboration
Integrity	Has the evidence remained sufficiently protected from alteration?	Forensic acquisition, hash verification where appropriate, and documented chain of custody
Reliability	Are the methods and conclusions technically dependable?	Qualified examiners, validated methods, transparent reporting, and independent review
Procedural fairness	Can the defendant meaningfully challenge the evidence?	Disclosure, access to relevant records, expert assistance where necessary, and judicial scrutiny

Source: Developed by the author through a synthesis of UNODC guidance, international legal instruments, and electronic-evidence guidelines [1–5].

The table demonstrates that digital evidence admissibility is a multidimensional issue. No single technical measure, such as hash verification, can replace lawful acquisition, proper authentication, reliable interpretation, and procedural safeguards.

Discussion. The findings suggest that the principal challenge in digital evidence proceedings is not simply the increasing volume of electronic information but the difficulty of ensuring that this information can be transformed into legally reliable proof. Digital evidence may be highly probative, yet its evidentiary value depends on how it was obtained, what it actually demonstrates, and whether its interpretation can withstand scrutiny. A key distinction must be maintained between the admissibility of evidence and its ultimate probative value. In some legal systems, unlawfully obtained evidence may be excluded under specific rules; in others, the legal consequences may depend on the nature of the violation and the applicable judicial test. It would therefore be inappropriate to propose a universal rule that every procedural defect automatically renders digital evidence inadmissible. Nevertheless, serious defects affecting authenticity, integrity, or the fairness of proceedings should receive careful judicial attention. The European Court of Human Rights' approach reinforces the importance of evaluating fairness in the proceedings as a whole. Its case law does not establish a single, comprehensive European rule governing the admissibility of all digital evidence. Rather, the Court examines whether the proceedings complied with fair-trial requirements, including whether the defence had an adequate opportunity to challenge evidence and whether the courts sufficiently addressed relevant questions of reliability [6]. The case of *Yüksel Yalçınkaya v. Türkiye* is particularly

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

instructive because it demonstrates how the interpretation and use of digital information can raise questions beyond the technical existence of a digital record. The evidentiary significance attributed to data, the reasoning used to connect that data to an individual, and the opportunities available to challenge the relevant conclusions may all affect the fairness of criminal proceedings [6]. Cross-border evidence presents another significant challenge. Digital information may be stored by a service provider in one country, accessed from another, and relevant to a criminal investigation in a third. Differences between national laws regarding data preservation, disclosure, privacy, and investigative authority can complicate the acquisition and subsequent use of evidence. International cooperation mechanisms can help address these difficulties, but cooperation should not eliminate the need to assess legality, authenticity, integrity, and procedural fairness in the receiving jurisdiction.

Conclusion. Digital evidence has become an essential component of contemporary criminal investigations and prosecutions. Its capacity to preserve communications, reconstruct events, identify digital activity, and connect individuals with alleged offences offers substantial advantages to criminal justice systems. At the same time, the distinctive characteristics of digital information create serious challenges concerning authenticity, integrity, attribution, reliability, privacy, and procedural fairness. The analysis demonstrates that the admissibility of digital evidence should not be determined solely by its electronic form or by the apparent sophistication of the technology used to collect it. Instead, courts and investigative authorities should assess whether the evidence was lawfully obtained, whether its origin and integrity can be established, whether the forensic methods are reliable, and whether the defendant has had a meaningful opportunity to challenge the evidence. The article proposes a five-dimensional analytical framework based on legality, authenticity, integrity, reliability, and procedural fairness. Although the precise legal consequences of evidentiary defects differ between jurisdictions, these dimensions provide a structured basis for evaluating digital evidence and identifying weaknesses in its collection or use. Ultimately, a reliable digital evidence system must protect both the integrity of criminal investigations and the rights of individuals subject to prosecution. By strengthening procedural standards, forensic transparency, independent scrutiny, disclosure, and international cooperation, states can improve the evidentiary value of digital information while preserving the legitimacy and fairness of criminal proceedings.

References

1. Council of Europe. (2001). Convention on Cybercrime. Budapest, 23 November 2001, ETS No. 185. Available at: https://www.coe.int/en/web/digital-governance/cybercrime.
2. Council of Europe. (2022). Electronic Evidence Guide, Version 3.0. Cybercrime Programme Office.
3. Commonwealth Secretariat. (2025). Guidelines on the Treatment of Electronic Evidence in Criminal Proceedings. London: Commonwealth Secretariat. https://doi.org/10.14217/tmkw7381.
4. European Court of Human Rights. (2023). Yüksel Yalçınkaya v. Türkiye [GC], Application No. 15669/20, Judgment of 26 September 2023.
5. United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. United Nations, Vienna.
6. Brezinski, D., & Killalea, T. (2002). Guidelines for Evidence Collection and Archiving. RFC 3227. Internet Engineering Task Force. https://doi.org/10.17487/RFC3227.

HSR (LONDON),
HOUGHTON STREET REVIEW JOURNAL
ISSN: 2058-5519|Impact factor-15.9
http://houghtonstreetreview.com/index.php/hsr

7. National Institute of Standards and Technology (NIST). (2006). Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.SP.800-86.
8. Maras, M.-H. (2014). Computer Forensics: Cybercriminals, Laws, and Evidence. 2nd ed. Burlington, MA: Jones & Bartlett Learning.