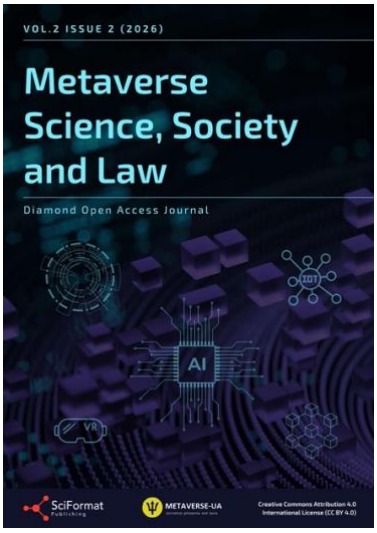

Metaverse Science, Society and Law

Vol. 2, Issue 3 (2026)

SciFormat Publishing

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: THE CONCEPT, RELATIONSHIP WITH RELATED CATEGORIES, AND PROSPECTS FOR LEGAL CODIFICATION
DOI	https://doi.org/10.69635/mssl.2026.2.3.58
RECEIVED	06 April 2026
ACCEPTED	17 August 2026
PUBLISHED	04 September 2026
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: THE CONCEPT, RELATIONSHIP WITH RELATED CATEGORIES, AND PROSPECTS FOR LEGAL CODIFICATION

Alisher Kadyrbekov
Master of Laws (LLM), PhD candidate in Public Law, Institute of Graduate Studies, Anadolu University, Turkey
ORCID ID: 0009-0003-3941-5553

ABSTRACT

This article examines the category of 'digital evidence' within the context of criminal proceedings. The relevance of the topic stems from the rapid digitalisation of social relations and the shift of criminal activity into the digital environment, which necessitates a comprehensive approach to the use of digital evidence in criminal proceedings. The author's aim is to formulate an original definition of "digital evidence" and to distinguish it from the related categories of "electronic evidence" and "virtual trace".

The methodological basis of the study consists of comparative-legal and terminological methods of analysis. The article examines the current criminal procedure legislation of Kazakhstan, Ukraine, Kyrgyzstan and Türkiye, as well as the provisions of the Digital Codes of Kazakhstan and Kyrgyzstan, which define the concepts of 'digital data' and 'digital record'. Particular attention is paid to international experience – the legislation of China and the Philippines, as well as the provisions of the Budapest Convention on Cybercrime. It is established that none of the countries examined formally enshrines the term 'digital evidence' in criminal legislation: related categories are used instead – 'electronic evidence' (Ukraine, in civil and administrative proceedings), 'electronic data' (China), or an open-ended list of evidence without further detail (Türkiye).

The author proposes an original definition of digital evidence that takes into account its immaterial nature, its suitability for automated processing, and the procedural manner of its acquisition. Four alternative legislative solutions are set out for national legal systems – ranging from avoiding detailed regulation to introducing digital evidence as an independent category of evidence. The findings may be used to improve criminal procedure legislation and in further research on the digitalisation of evidence law.

KEYWORDS

Evidence, Digital Evidence, Electronic Evidence, Virtual Trace, Electronic Form, Digital Data, Digital Information, Criminal Procedure, Digitalisation

CITATION

Alisher KADYRBEKOV. (2026). Digital Evidence in Criminal Proceedings: The Concept, Relationship with Related Categories, and Prospects for Legal Codification. *Metaverse Science, Society and Law*. Vol. 2, Issue 3. doi: 10.69635/mssl.2026.2.3.58

In today's world, almost all spheres of human activity are subject to the process of digitalisation. Judicial proceedings and the rule of law are no exception. Here, in addition to the application of Artificial Intelligence with its prospects and risks, the pressing question naturally arises regarding the use of digital evidence in judicial proceedings, particularly in criminal proceedings – specifically, the pre-trial investigation and the examination of such evidence in court.

The research methodology employed in this study comprises the general legal method of comparative legal analysis, with regard to legal acts and other legislation at both national and international levels. It also involves a terminological analysis of established concepts and definitions found in legal and other acts.

The aim of this article is to develop a universal approach to the use of digital evidence in criminal proceedings.

The objectives of the study are:

1. To propose the author's definition of 'digital evidence';
2. To compare and attempt to distinguish between the concepts of 'digital evidence', 'electronic evidence' and 'digital footprint';
3. To analyse the current legislation of certain countries with regard to the establishment of the concept of 'digital evidence'.

With the advent of digitalisation and artificial intelligence in the judicial system and the work of law enforcement agencies – including those conducting pre-trial investigations, administering justice and those defending the interests and rights of citizens – a serious question has arisen regarding the use, in addition to traditional evidence, of its digital equivalents (digital evidence) in their work. This is also linked to the fact that, in this age of advanced technology, crime has transformed and adapted to the new digital environment, where cybercrime is the primary threat to the rule of law.

However, in order to discuss digital evidence, we must first define the nature of the traditional concept of evidence. In criminal law theory, evidence *'must exclude all reasonable doubt to secure a* conviction'[1].

In practical terms, we must draw on examples from the current criminal procedure legislation of certain developing countries that are actively digitising their judicial systems and developing a unique approach to AI technologies. Such countries include Kazakhstan, Kyrgyzstan, Ukraine and Türkiye.

For example, Article 111 of the Code of Criminal Procedure of the Republic of Kazakhstan establishes the following definition: *'1. Evidence in a criminal case consists of factually established data obtained lawfully, on the basis of which the preliminary enquiry body, the preliminary enquiry officer, the investigator, the prosecutor, the court establish the existence or absence of an act provided for in the Criminal Code of the Republic of Kazakhstan, the commission or non-commission of that act by the suspect, accused or defendant, their guilt or innocence, as well as other circumstances relevant to the correct resolution of the case. 2. The facts relevant to the proper resolution of a criminal case are established by: the statements of the suspect, the accused, the victim, a witness, a witness entitled to defence, an expert or a specialist; the opinion of an expert or specialist; material evidence; records of procedural actions and other* documents'[2];

In the Criminal Procedure Code of Ukraine: *'1. Evidence in criminal proceedings consists of factual data obtained in accordance with the procedure laid down in the Code of Criminal Procedure, on the basis of which the investigator, the prosecutor, the investigating judge and the court establish the existence or absence of facts and circumstances relevant to the criminal proceedings and subject to proof. 2. Procedural sources of evidence include witness statements, physical evidence, documents and expert* reports'[3];

The Turkish legislature has stipulated in Article 217 of the Code of Criminal Procedure that *'Assessment of evidence (1) A judge may base his or her decision only on evidence presented at the court hearing and discussed in his or her presence. The judge shall assess this evidence according to his or her inner conviction. (2) The offence with which the defendant is charged may be proven by any evidence obtained* lawfully'[4].

Based on an analysis of the examples given, it can be said that the legislators of Kazakhstan, Ukraine and Türkiye take a similar stance on the concept of 'evidence', the common feature being that it *consists of lawfully obtained factual data upon which a charge of committing a particular criminal offence is based*.

[1] Edwards, J. (2018). Theories of criminal law. // https://plato.stanford.edu/entries/criminal-law/?o=600605&l=dir&qsrc=990&qo=contentPageRelatedSearch&ad=dirN#CrimProcEvid

[2] Criminal Procedure Code of the Republic of Kazakhstan No. 231-V of 4 July 2014 // https://prg.kz/document/?doc_id=31575852&ysclid=mthhg1w2ai821484984

[3] Criminal Procedure Code of Ukraine No. 4651-VI of 13 April 2012 // https://prg.kz/document/?doc_id=31197178&doc_id2=31197178&pos=116;252&pos2=1728;244

[4] Criminal Procedure Code of Türkiye No. 5271 (CMK) // https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf

However, one difference should be noted – the level of detail and the specific list of types of evidence set out in the relevant articles of the criminal procedure legislation of Kazakhstan and Ukraine: *witness statements; expert or specialist reports; material evidence; records of procedural actions; and other documents*. Whereas the Turkish legislature leaves this list fairly open-ended, using the wording *'any evidence obtained lawfully'*.

It is precisely in this distinctive aspect that the Turkish legislature has left itself room for manoeuvre, not only with regard to the recognition of evidence in its classical sense (witness evidence; expert or specialist reports; physical evidence; and other documents), but also those dictated by the demands of the times and technological progress – that is, the evidence which is the subject of our study at: 'Digital Evidence'. This example may serve as a model of sorts for other national legislations seeking to keep pace with the times.

In addition to the definition of evidence in Kazakhstan's national legislation, there is the concept of 'digital data', enshrined in Article 16 of the Digital Code of the Republic of Kazakhstan: *'Digital data is information provided in digital form and suitable for automated and/or analytical collection, storage, processing, use, transmission, dissemination or deletion, regardless of the method of its acquisition and the form of its digital* provision'[1].

Similarly, Article 25 of the Digital Code of the Kyrgyz Republic stipulates that *'Digital data is freely transferred between any entities and processed for these purposes without restriction, and cannot in itself be the subject of digital rights... Digital records are the subject of their owner's digital rights, unless otherwise provided for by the Digital Code or by a contract between parties to legal relations in the digital environment... 3. Rights to digital records constituting virtual assets are governed by the legislation of the Kyrgyz Republic on virtual assets. Rights to digital records constituting intellectual property are governed by the legislation of the Kyrgyz Republic in the field of intellectual* property'[2].

Furthermore, Article 52 of the Digital Code of Kyrgyzstan stipulates that *'Digital records as the basis for the creation, modification and termination of legal relationships in the digital environment 1. The grounds for the creation, modification and termination of legal relationships in the digital environment are legal facts expressed in digital records, including those presented in the form of digital documents or as part of digital resources. 2. The certification of the creation, modification and termination of legal relationships in the digital environment is carried out, inter alia, by means* of *trusted* services'[3].

Article 21 of the Digital Code of Kazakhstan also provides a definition of a digital record: *'1. A digital record is recognised as a distinct digital object comprising information recorded in digital form, or details concerning such information, possessing unique identifying characteristics that enable the content, source, structure or purpose of the record to be established. 2. Digital records are classified as follows: 1) identification digital records – which record information or details of a factual, personal or official nature and are intended to identify digital data; 2) digital records certifying rights – certifying the creation, ownership, transfer, encumbrance or termination of rights to digital and/or tangible objects, including items, goods, raw materials and other assets, as well as claims relating to such* objects'[4].

Based on the above provisions, we can conclude that Kazakhstan and Kyrgyzstan take a similar stance on the distinction between the categories of 'digital data' and 'digital records'; however, differences lie in the legislature's approach to these categories. Thus, in Kazakhstan, the Digital Code defines the types of digital objects and their legal nature. In Kyrgyzstan, by contrast, a digital record is linked to digital rights and legal facts, which may subsequently be accepted as evidence. It is also significant that the Digital Code of Kyrgyzstan addresses the issue of metadata, which contains general information about when, where, by whom, and on what device such digital records were created or stored (when they were last modified, by whom, and who owns them). All of this may be relevant in pre-trial investigations into criminal cases.

It is also worth considering some of the concepts of digital evidence proposed by various scholars:

1) *'Digital evidence is any probative information stored or transmitted in electronic form that any party to legal proceedings may use at trial'*[5].

2) *'Electronic evidence consists of digital objects which were the means or instrument used to commit a criminal offence, which retained electronic or digital traces of the offence, which were the subject or object*

[1] Code of the Republic of Kazakhstan No. 255-VIII of 9 January 2026 'Digital Code of the Republic of Kazakhstan' // https://prg.kz/document/?doc_id=38546537&pos=241;64

[2] Digital Code of the Kyrgyz Republic No. 178 of 31 July 2025 // https://prg.kz/document/?doc_id=37462686&pos=593;136

[3] Ibid.

[4] Ibid.

[5]Bhatti, N. (2026). The Use of Digital Evidence in Criminal Proceedings. American Journal of Society and Law, 5(1), 10–19. // https://www.researchgate.net/publication/403273766_The_Use_of_Digital_Evidence_in_Criminal_Proceedings

of the commission of a criminal offence, or which contain other information that may be used as evidence of facts or circumstances established in the course of criminal proceedings'[1].

3) *'Electronic evidence comprises data which served as a means or instrument for committing a criminal offence, which retains electronic or digital traces of the offence, or which was the subject or object of the criminal offence. Among the main characteristics of electronic evidence, the following are identified: intangible form; it cannot exist outside a technical medium or communication channel; transmission via an electronic network; a specific procedure for recording; and remote transmission. The principles that characterise electronic evidence include: admissibility; authenticity; completeness; reliability; comprehensibility; and plausibility. It is essential to pay attention to the specific nature of electronic information and its use in case files; consequently, amendments should be made to criminal procedure legislation to regulate the concept and procedure for the use of electronic evidence'*[2].

Furthermore, some scholars are attempting to classify digital evidence, including within it such items as:

1. Data stored on a computer – stored on hard drives or solid-state drives: files, documents, databases, emails and spreadsheets. Function: determining authorship; recovering deleted files; and obtaining metadata[3].
2. Network and internet data – internet protocol logs, web logs, email logs, social media logs, server logs and communication logs. Function: to identify participants; to determine or establish a digital presence at a particular location or at a particular time[4].
3. Evidence from mobile devices – text messages, call history and GPS location data, app data, photographs and messaging app content. Function: tracking location; reconstructing correspondence; and establishing a chronology of events[5].
4. Cloud-based evidence – information stored on third-party servers: emails, documents, backups, and records from collaboration platforms. Function: retrieval of data not stored locally; synchronised activity records from multiple devices are available[6].
5. Internet of Things (IoT) and smart device data – Home records on smart devices, medical records on wearable devices, vehicle records via telematics, data on the operation of domestic appliances. Function: verification of circumstances and behaviour; presence of suspects at crime scenes; chronology[7].
6. Blockchain and distributed ledgers – records of cryptocurrency transactions, records of smart contract execution, data from an immutable distributed ledger. Function: tracking of illegal financial transactions; tracing of transaction links; provision of verifiable audit trails[8].

Thus, having examined the provisions of criminal law theory and the national legislation of Kazakhstan, Ukraine, Kyrgyzstan and Türkiye, we can attempt to formulate our own – the author's – concept of 'digital evidence', which would be more relevant and in line with contemporary realities.

Thus, **digital evidence** *refers to digital data or digital records obtained in accordance with the procedure laid down by law, including the information, metadata and other details contained therein, which are relevant, admissible and reliable, and on the basis of which a criminal prosecution authority (an investigator, a prosecutor or a court) establishes the existence or absence of circumstances that are relevant to criminal proceedings and are subject to proof. Furthermore, digital evidence may exist both in a stored state and whilst being transmitted via computer systems, information and telecommunications networks, digital platforms, electronic devices, cloud services, distributed information networks and other digital technologies*.

This definition of digital evidence helps to distinguish the term from 'electronic evidence', since electronic evidence primarily refers to a form of information (text messages, photographs, videos, electronic files, correspondence via email and messaging apps, etc.). Compared with electronic evidence, digital evidence is not merely an electronic form, but data of a digital nature that is suitable for automated processing, identification, transmission, analysis and reproduction (which is consistent with Article 16 of the Digital Code of the Republic of Kazakhstan).

[1] Degtyareva, O. (2021). Evidence in criminal proceedings based on electronic evidence. // https://library.megu.edu.ua:9443/jspui/handle/123456789/2819
[2] Ibid.
[3] Bhatti, N. (2026). The Use of Digital Evidence in Criminal Proceedings. American Journal of Society and Law, 5(1), 10–19. // https://www.researchgate.net/publication/403273766_The_Use_of_Digital_Evidence_in_Criminal_Proceedings
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

Moving on to the distinction between digital evidence and a digital trace, it should be noted that a digital trace is not, by its very nature, evidence in its own right. It is, first and foremost, the result of digital interaction, which may potentially have procedural significance and acquire the status of evidence.

An example of such interaction is a simple login to an online platform; the mere fact that you have registered or logged in to that site does not, in itself, constitute a significant legal fact.

However, if you have logged in to an online shop or other platform where goods or items withdrawn from civil circulation are sold, and have purchased them via an online transaction, and subsequently committed a criminal offence involving that item – then the investigating authority, having received such information, may attach it to the case file as digital evidence of your involvement in the case under investigation.

In other words, a digital footprint objectively exists as a result of a specific action carried out in the digital environment, whilst digital evidence acquires procedural status as a result of its collection, recording and assessment within the framework of criminal proceedings.

When considering the established term 'digital evidence' in the national legislation of certain countries, the experiences of Ukraine, China, Vietnam, Indonesia and the Philippines serve as illustrative examples.

Thus, in Ukraine, Article 100 of the Code of Civil Procedure provides that *'1. Electronic evidence is information in electronic (digital) form containing data on circumstances relevant to the case, in particular, electronic documents (including text documents, graphic images, plans, photographs, video and audio recordings, etc.), websites (web pages), text, multimedia and voice messages, metadata, databases and other data in electronic form. Such data may be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other storage locations for data in electronic form (including on the Internet). 2. Electronic evidence shall be submitted in the original or as an electronic copy bearing a qualified electronic signature in accordance with the requirements of the Ukrainian laws 'On Electronic Documents and Electronic Document Management' and 'On Electronic Identification and Electronic Trust Services'. The law may provide for a different procedure for certifying an electronic copy of electronic* evidence…'[1].

A similar definition is also given in Article 96 of the Commercial Procedural Code of Ukraine (Arbitration Procedure) of 6 November 1991 No. 1798-XII[2]. In Article 72 of the Code of Administrative Procedure of Ukraine of 6 July 2005 No. 2747-IV *'Evidence in administrative proceedings comprises any information on the basis of which the court establishes the existence or absence of circumstances (facts) substantiating the claims and defences of the parties to the case, and other circumstances relevant to the correct resolution of the case. 2. Such information is established by the following means: 1) written, material and electronic evidence; 2) expert opinions; 3) witness testimony...'*[3].

From the Ukrainian legislative acts cited above, we can see that digital evidence is referred to as 'electronic evidence'; however, this does not alter its essence. It is also worth noting that the submission of this type of evidence is not an issue in civil and administrative proceedings; however, there is no such provision at the level of criminal law. Nevertheless, Ukrainian scholars have formed a general understanding of digital evidence in criminal proceedings, and their position is as follows: *'the term "electronic evidence" is understood to mean data or information generated as a result of the use of digital technology and relevant software, which may be used in court* proceedings'[4].

However, it cannot be said that criminal legislation makes no provision whatsoever for digital evidence, as Part 5 of Article 106 of the Code of Criminal Procedure of Ukraine states that '*…the handling of electronic documents in criminal proceedings, insofar as not regulated by the Code of Criminal Procedure of Ukraine, is governed by other laws on electronic documents and electronic document* management…'[5]. In other words, the legislator refers to the provisions of other legislative acts (including those mentioned above).

[1] Civil Procedure Code of Ukraine of 18 March 2004 No. 1618-IV // https://prg.kz/document/?doc_id=30418564&doc_id2=30418564&pos=129;233&pos2=1479;202

[2] Commercial Procedure Code of Ukraine (Arbitration Procedure Code) of 6 November 1991 No. 1798-XII // https://prg.kz/document/?doc_id=30418667

[3] Code of Administrative Procedure of Ukraine of 6 July 2005 No.2747-IV // https://prg.kz/document/?doc_id=30418335&pos=1213;190

[4]Milimko, L. V., & Zhidovtsev, Ya. V. (2025). Electronic evidence in criminal proceedings in Ukraine. Scientific Bulletin of Uzhhorod National University. Series: Law, 3(88), 302–308. // https://visnyk-pravo.uzhnu.edu.ua/article/view/330827/320168

[5]Criminal Procedure Code of Ukraine of 13 April 2012 No. 4651-VI // https://prg.kz/document/?doc_id=31197178&pos=1973;130

Article 3(u) of the Implementing Rules and Regulations (IRR) of Act No. 9175/2012 (Cybercrime Prevention Act) (Philippines) provides an explicit definition: *'Electronic evidence means evidence the use of which is permitted under the applicable rules of evidence in establishing the truth of a fact in legal proceedings, and which has been obtained, recorded, transmitted, stored, processed, retrieved or presented in electronic* form'[1].

Article 50 of the Criminal Procedure Code of the People's Republic of China states: *'All materials that may be used to prove the facts of a case constitute evidence. Evidence includes: (1) Physical evidence; (2) Documentary evidence; (3) Witness statements; (4) statements by the victim; (5) confessions and defences by suspects and accused persons; (6) expert opinions; (7) records of inspections, examinations, identifications and investigative experiments; (8) audiovisual materials and electronic data. Evidence must be verified as authentic before it can be used as the basis for* a verdict'[2]. Here, we also see that the legislator specifically refers to 'electronic data', providing a broad scope for selecting items falling under this definition; however, we have not found any more detailed or explicit provision regarding 'digital evidence'.

When discussing international instruments, it is also necessary to mention the Budapest Convention of 23 November 2001, also known as the Convention on Cybercrime (ETS No. 185) (hereinafter referred to as the Convention). This Convention sets out the fundamental principles for the investigation of offences relating to computer systems and computer technology.

The term 'digital evidence' is not explicitly mentioned in the document; however, the concept in question can be inferred from the context. Thus, the word 'evidence' appears eight times in the Convention. The first mention is in the preamble, which states: *'…computer networks and electronic information may also be used to commit offences, and that evidence relating to such offences may be stored and transmitted via these networks…*[3]. Further on in the text, in the same preamble: *'…with a view to enhancing the effectiveness of criminal investigations and proceedings relating to offences involving computer systems and data, and to ensuring that evidence in electronic form relating to an* offence *can be* collected'[4]. Subparagraph C of paragraph 2 of Article 14 of the Convention refers to *'the collection of evidence in electronic form relating to a crime*'[5]. Articles 23 and 25 of the Convention enshrine the principle of international co-operation regarding *'the collection of evidence in electronic form relating to a* crime'[6]. In turn, Articles 35 and 45 of the Convention refer to the ongoing exchange of information on cybercrime, as well as to *the 'exchange of information on significant legal, political or technological developments relating to cybercrime and the collection of evidence in electronic* form'[7].

Thus, whilst we have not found the term 'digital evidence' explicitly enshrined in the text of the Convention, based on the context, we can derive a basic understanding of such evidence: *it is information relating to a crime committed in the digital environment (cybercrime) using computer technology. Such information includes data in the form of computer data or in any other form that is stored or in the process of being transmitted by a service provider (subscriber information; traffic data; content data)*.

[1] Rules and Regulations Implementing Republic Act No. 10175, ("Cybercrime Prevention Act of 2012") // https://www.wipo.int/wipolex/en/legislation/details/13667
[2] Criminal Procedure Code of the People's Republic of China of 26 October 2018 // https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/bgt/art/2025/art_48b3b0c3f954448e996602a71fc6f878.html
[3] Convention on Cybercrime (ETS No. 185), 23 November 2001, Budapest // https://rm.coe.int/1680081561
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.

Conclusions

Having analysed the current legislation of a number of countries, and taking into account the international instrument known as the Budapest Convention, we have reached the following conclusion: there is no official enshrinement of the term 'digital evidence' in the criminal law of the countries cited in this article. There are isolated references to and provisions for such a category, but under the term 'electronic evidence', which, in our view, is not entirely accurate or correct.

Digital evidence, by its very nature, forms part not of the physical world but of the digital realm, and possesses its own specific characteristics and nature. Our definition is not the only correct one and may become outdated in the foreseeable future; however, it is as close as possible to contemporary realities and is intended to distinguish 'digital evidence' from its electronic form of expression, as well as from an ordinary 'digital footprint'.

In our view, modern legislators may adopt one of the options proposed below:

1) Simplify their decision by avoiding excessive detail and adopt the wording *'any* evidence', whilst providing for discretion within criminal procedure law regarding the concept of evidence and its types (Türkiye);

2) Attempt to introduce a definition of '*digital* evidence' into national legislation, providing detailed provisions but limiting its scope to civil and administrative proceedings (Ukraine);

3) Not to introduce a separate category, but to provide for electronic forms of evidence in criminal proceedings (China and the Budapest Convention);

Accept the reality of the situation, set out in detail a separate type of evidence or source of evidence – '*Digital* evidence', as proposed by the author – and avoid discretion in the interpretation of the rules, as well as delineate this concept and avoid confusion with electronic forms of evidence.

REFERENCES

1. Edwards, J. (2018). *Theories of criminal law*. https://plato.stanford.edu/entries/criminal-law/?o=600605&l=dir&qsrc=990&qo=contentPageRelatedSearch&ad=dirN#CrimProcEvid
2. *Code of Criminal Procedure of the Republic of Kazakhstan No. 231-V of 4 July 2014*. (2014). https://prg.kz/document/?doc_id=31575852&ysclid=mthhg1w2ai821484984
3. *Criminal Procedure Code of Ukraine No. 4651-VI of 13 April 2012*. (2012). https://prg.kz/document/?doc_id=31197178&doc_id2=31197178&pos=116;252&pos2=1728;244
4. *Criminal Procedure Code of Türkiye No. 5271 (CMK).* (n.d.). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf
5. *Code of the Republic of Kazakhstan No. 255-VIII of 9 January 2026 "Digital Code of the Republic of Kazakhstan."* (2026). https://prg.kz/document/?doc_id=38546537&pos=241;64
6. *Digital Code of the Kyrgyz Republic No. 178 of 31 July 2025*. (2025). https://prg.kz/document/?doc_id=37462686&pos=593;136
7. Bhatti, N. (2026). The use of digital evidence in criminal proceedings. *American Journal of Society and Law, 5*(1), 10–19. https://www.researchgate.net/publication/403273766_The_Use_of_Digital_Evidence_in_Criminal_Proceedings
8. Degtyareva, O. (2021). *Evidence in criminal proceedings based on electronic evidence*. https://library.megu.edu.ua:9443/jspui/handle/123456789/2819
9. *Civil Procedure Code of Ukraine of 18 March 2004 No. 1618-IV*. (2004). https://prg.kz/document/?doc_id=30418564&doc_id2=30418564&pos=129;233&pos2=1479;202
10. *Commercial Procedure Code of Ukraine (Arbitration Procedure Code) of 6 November 1991 No. 1798-XII*. (1991). https://prg.kz/document/?doc_id=30418667
11. *Code of Administrative Procedure of Ukraine of 6 July 2005 No. 2747-IV*. (2005). https://prg.kz/document/?doc_id=30418335&pos=1213;190
12. Milimko, L. V., & Zhidovtsev, Ya. V. (2025). Electronic evidence in criminal proceedings in Ukraine. *Scientific Bulletin of Uzhhorod National University. Series: Law, 3*(88), 302–308. https://visnyk-pravo.uzhnu.edu.ua/article/view/330827/320168
13. *Criminal Procedure Code of Ukraine of 13 April 2012 No. 4651-VI.* (2012). https://prg.kz/document/?doc_id=31197178&pos=1973;130
14. *Rules and regulations implementing Republic Act of Philippines No. 10175 ("Cybercrime Prevention Act of 2012").* (n.d.). https://www.wipo.int/wipolex/en/legislation/details/13667
15. *The Criminal Procedure Code of the People's Republic of China of 26 October 2018*. (2018). https://www.samr.gov.cn/zw/zfxxgk/fdzdgknr/bgt/art/2025/art_48b3b0c3f954448e996602a71fc6f878.html
16. *Convention on Cybercrime (ETS No. 185).* (2001, November 23). https://rm.coe.int/1680081561