

Electronic Evidence and Its Application in International Criminal Law

Gafurova Shoiri

Doctoral student, Tashkent state university of law, Uzbekistan

Received: 30 March 2026; **Accepted:** 25 April 2026; **Published:** 16 May 2026

Abstract: This article discusses the concept of electronic evidence in international criminal law and its practical application, which is one of today's most pertinent issues. The development of technology has led to numerous changes in the field of legal science. Scholars hold differing views on the concept of electronic evidence; some refer to materials obtained through computers, mobile communication devices, drones, and cameras as "electronic evidence" while others prefer the term "digital evidence". Electronic evidence is also a new area for the International Criminal Court, as it is not specified in the Rome Statute. Furthermore, the article examines the legislation of foreign countries and cases considered by international courts, studying their experience and practice in this regard.

Keywords: Electronic evidence, digital evidence, International Criminal Court, international criminal law, evidence, Rome Statute, means of proof.

Introduction: In The development of information technologies and the widespread implementation of digitalization are significantly impacting modern reality, as well as the economic, political, and legal spheres. Researchers have repeatedly highlighted a significant transformation in the characteristics of modern crime and a shift in offenders' interests toward cyberspace. [1, P.695] The illegal use of computer information, remote management of banking operations, and a number of other crimes committed in this domain not only violate the rights of individuals but also undermine the national security of the state. This creates the necessity to codify these types of crimes in substantive law and to develop procedural laws that facilitate their investigation and exposure.

Electronic evidence currently signifies information that exists in an electronic format. This concept has not yet been reflected in criminal procedural legislation. Nevertheless, it is possible to introduce electronic evidence, which is broader in meaning and may include, for example, records stored by network or internet providers, into the proving process.[2, P.46-51]

Results and discussions

Electronic means of proof are any legal and technical capabilities that, in accordance with criminal procedural legislation, allow for the use of information in electronic form during the proving process. These include digital data, electronic information carriers, and the legal norms for their identification, recording, copying, seizure, storage, and use in criminal proceedings. Electronic information can be presented in the form of traditional evidence—either as physical evidence or as other documents. In the near future, a gradual transition to electronic document circulation in criminal proceedings is expected, which will completely replace the analog method of recording information obtained during investigations and trials. At the same time, physical evidence and other documents in electronic form require additional procedural guarantees to ensure their authenticity.

Currently, there is some disagreement among scholars on whether to label this evidence as "electronic" or "digital". For example, S.V. Kalitin, a Candidate of Technical Sciences and an Associate Professor at the Department of Information Systems and Technologies of the Khabarovsk State Academy of Economics and Law, has expressed his views on the matter under

consideration. He proposes classifying evidence according to its form of presentation as follows: Oral and written (handwritten, printed, information signals [analog, digital]); and physical (electronic, chemical, biological, mechanical, etc.). After evidence, referred to as "electronic" in modern legal terminology, is obtained and attached to a criminal case, there is a tendency to classify it as physical evidence. To facilitate its examination and subsequent use in court proceedings, its main and essential features and characteristics are summarized and transferred to written documents printed on paper. If the evidence involves files that can only be reproduced using electronic devices or instruments, then they must be reproduced using only those means. For example, an electron microscope makes it possible to view small objects or biological cells that are invisible to the naked eye. In this case, the recorded state of the cells is not called ELECTRONIC, as it does not depend on the electronics (electronic technology) that recorded the beam of electrons passing through the sample. Similarly, if a microscope with glass lenses were used, the resulting image of the observed sample would not be called a "glass" image. [3]

In the United States, electronic (digital) evidence is understood to be information and data that is stored, received, or transmitted via electronic devices. [4] We propose the following as a complete and meaningful definition of electronic information: electronic information is data presented in a digital format suitable for identification, processing, or storage using a computer or information system, which exists in the form of files, logs, and metadata.

Established in 1998, the International Criminal Court (ICC) is the world's first permanent international criminal court. It is tasked with investigating and prosecuting the most serious crimes of concern to the international community: genocide, crimes against humanity, war crimes, and the crime of aggression. At the time of the ICC's establishment, the future revolution in digital technologies and its impact on the Court could not have been foreseen. However, more than two decades later, the court's evidentiary procedures and judicial processes for corroborating evidence have become outdated. While new technologies have great potential to transform the process of international criminal justice in many ways, the Court is currently not fully equipped to handle the complex tasks of authenticating and verifying digital evidence. [5, pp. 554-555]

The ICC grants judges broad discretion in admitting evidence. The Rome Statute, the founding treaty of the ICC, serves as the Court's primary legal document. In addition, the Rules of Procedure and Evidence provide

detailed guidance on the admission and handling of evidence. Rule 63 (2) states: "In accordance with article 64, paragraph 9, the Chamber has the authority to freely assess all evidence submitted in order to determine its relevance or admissibility in accordance with article 69." [6] In other words, judges have the authority to resolve any issues related to the authenticity or reliability of digital evidence. The Court relies on the experience and expertise of judges to properly weigh the admitted evidence. This flexible approach to the admission of evidence is also a result of the ICC's limited powers. While law enforcement agencies in domestic criminal investigations have the power to compel parties through subpoenas and search warrants, ICC investigative teams do not possess such authority. The ICC's general approach to the admissibility of evidence involves a sequential three-step test, in which all of the following criteria must be met:

Relevance: According to Articles 64 (9) (a) and 69 (4) of the Rome Statute, as well as the Rules of Procedure and Evidence, evidence is considered relevant if "the evidence presented makes the existence of the fact in dispute more or less probable." In other words, evidence may be found relevant if it is *prima facie* significant to the case. [7]

Probative value: Probative value generally means that the evidence is sufficiently useful in proving a significant part of the legal proceedings. Essentially, probative value measures the extent to which the evidence presented can influence the determination of a fact or issue. According to Article 69 (4) of the Statute, an item's probative value must be assessed before it can be admitted as evidence. There is no exhaustive list of criteria for assessing probative value. Instead, "the probative value is determined on the basis of a number of considerations relating to the specific characteristics of the evidence." Therefore, the court must weigh the probative value of the item against its prejudicial effect on the accused. [8]

Weighing probative value against prejudicial effect: In accordance with Rules 69 (4) and 63 (2), the evidence presented must be "sufficiently relevant and probative to overcome any prejudicial effect or consequences that its admission may entail." In other words, the weight given to the evidence must fully respect the rights of all parties, not be manifestly unfair to either the prosecution or the defence, and not undermine the overall fairness of the trial.

When using electronic evidence, it is crucial to examine its criteria for admissibility and reliability in comparison to other forms of evidence. This is because as technologies advance, their capabilities increase.

Altering and adding to images, videos, and audio recordings presented as electronic evidence through artificial intelligence is becoming commonplace. For this reason, the process of admitting and using them as evidence in a court case is considerably time-consuming.

European countries do not provide a clear definition of electronic evidence in their legislation. Furthermore, there are no national rules on the admissibility of electronic evidence. In some states, electronic documents are equated to paper documents and are given significance as evidence in court proceedings. In certain countries, an electronic signature is equated to a traditional signature, and their significance before the court is recognized as being the same. Practice shows that the majority of European judges consider electronic evidence to be equivalent to traditional evidence. Legal scholars do not view them as a separate category. Electronic evidence is one of the forms of presenting evidence, which allows the obtained information to be observed with the human senses. Additionally, evidence can also be in analog form, in the form of a physical object, or in written (paper) form. [9, pp.64-66]

In the legislation of the Republic of Uzbekistan, an amendment regarding the use of electronic evidence was introduced to the law in 2024, adding the terms "electronic" and "digital evidence" to the list of evidence in Articles 81, 87, and 89 of the Criminal Procedure Code. According to Article 81 of the Criminal Procedure Code:

Any factual data that serves as a basis for an inquirer, investigator, and the court to determine, in the manner prescribed by law, whether or not a socially dangerous act occurred, the guilt or innocence of the person who committed this act, and other circumstances relevant to the correct resolution of the case, shall be considered evidence in a criminal case. It is stipulated that these data are established by the testimony of a witness, victim, suspect, accused, or defendant; an expert's conclusion; physical, written, and digital evidence; materials consisting of audio recordings, video recordings, films, and photographs; protocols of investigative and judicial actions; and other documents. [10]

The ICC has already begun to address questions about how to evaluate digital evidence in two notable cases, namely Al-Mahdi and Al-Verfalli (Freeman and Vasquez Llorente 2021, 179).

In the Al Mahdi case, internet videos and satellite imagery were used to bring charges against Ahmad Al Faqi Al Mahdi, suspected of being affiliated with the Al-Qaeda network, for the destruction of cultural heritage

sites in Timbuktu, Mali. However, because the defendant pleaded guilty, the authenticity of the evidence was never challenged, and technical experts were not called to testify on the digital evidence presented. Similarly, in the 2017 case of *The Prosecutor v. Mahmoud Mustafa Busyf Al-Werfalli*, the court relied on several videos posted on Facebook to issue an arrest warrant for Major Mahmoud Mustafa Busyf Al-Werfalli, a high-ranking Libyan military officer accused of murdering 33 people. As Al-Werfalli is not currently in ICC custody, the impact of presenting the social media evidence remains to be seen. The Al-Mahdi and Al-Werfalli cases demonstrate that courts are willing to evaluate digital evidence in entirely new ways. In the Al-Werfalli case, it is likely the case would not have been brought at all if not for the Facebook videos of these alleged crimes. Although digital evidence has not yet played a decisive role in the final judgment of any case before the ICC, these two instances indicate that this change is inevitable. [11]

Conclusion.

Thus, the practice of working with electronic evidence shows its necessity and the need for further legal regulation of the rules for its use in criminal proceedings. It is essential to establish a unified, clear, and logical procedure for procedural actions involving electronic evidence, as this can serve as a sufficient criterion for its admissibility. In this regard, the relevance and reliability of electronic evidence will depend entirely on its verification in the manner prescribed by law. The International Criminal Court has not been able to fully adapt to the specific challenges of authenticating and verifying digital evidence. Not only is the primary mechanism for authenticating digital files from the electronic court record cryptographically broken and unusable, but judges are also inadequately prepared to fulfill their duties in resolving disputes over the authenticity of digital evidence. The rapid development of technology, a disruptive information environment, and the large volume of fragile, ephemeral, and time-sensitive data indicate that disputes over the authenticity of digital evidence are inevitable. New forms of digital evidence increase the level of doubt in authentication and verification, raising serious questions about how the ICC should approach complex areas of technology and what judicial oversight should look like under such conditions.

References:

1. "Electronic evidence" in the regulatory system of criminal procedural evidence // Perm Legal Almanac. – 2019. – No. 2. – pp. 695-707.
2. Zuyev S. V. Electronic evidence in criminal

- proceedings: concept and significance. - Pravoporyadok: istoriya, teoriya, praktika [Law and Order: History, Theory, Practice] No. 3 (26) / 2020 pp. 46-51.
3. Baranov A.M. "Electronic evidence: an illusion of the 21st century criminal process." Russian Journal of Criminal Law No. 13 UDC 343.14 doi: 10.17223/23088451/13/12.
 4. Vladimirovna A.Ch. Digital (electronic) evidence in criminal proceedings - <https://cyberleninka.ru/article/n/tsifrovye-elektronnye-dokazatelstva-v-ugolovnom-sudoproizvodstve/viewer>
 5. Ch.Quilling The Future of Digital Evidence Authentication at the International Criminal Court May 20, 2022 <https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminacourt#:~:text=Relevant%20ICC%20Cases&text=However%2C%20because%20the%20defendant%20pleaded,Freeman%20and%20Vazquez%20Lorente%202021>).
 6. Rules of Procedure and Evidence. ICC, Rule 63(2).
 7. Prosecutor v. Thomas Lubanga Dyilo. Trial Chamber I. "Decision on the admissibility of four documents." ICC-01/04-01/06-1399. (2008)
 8. Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui. Trial Chamber II. "Decision on the Prosecutor's Bar Table Motions." ICC-01/04-01/07. (2010)
 9. The Admissibility of Electronic Evidence in Court // ITU [Международный союз электросвязи]. URL: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf
 10. Jinoyat protsessual kodeksi - <https://lex.uz/docs/-111460?ONDATE=21.11.2024%2000#edi-7234037>
 11. Ch.Quilling The Future of Digital Evidence Authentication at the International Criminal Court May 20, 2022 <https://jpia.princeton.edu/news/future-digital-evidence-authentication-international->