*UDC 343.1*
*DOI https://doi.org/10.24144/2788-6018.2025.05.3.46*

# DIGITAL EVIDENCES IN CRIMINAL PROCEEDINGS: PROBLEMS OF AUTHENTICITY AND ADMISSIBILITY

**Shyshenko A.A.,**
*4th year student*
*faculty of International and European Law*
*Yaroslav Mudryi National Law University*

**Shyshenko A.A. Digital evidences in criminal proceedings: problems of authenticity and admissibility.**

Everyday life is filled with information technology, which is developing very rapidly. In all of this, digital evidence has its place and is becoming increasingly important in crime investigations, helping to establish the truth and ensure justice. However, their use in such cases leads to numerous legal, procedural and technical problems that are the subject of scientific reflection. This article demonstrates the definition of digital evidence in accordance with national legislation, doctrine and international acts, in particular the Convention on Cybercrime (the Budapest Convention). It also provides a classification of the main types, such as: emails, messages in messengers (e.g. WhatsApp, Facebook, etc.), photos and videos, files, metadata, IP addresses, geolocation data, information from social networks, cloud storage, etc. Particular attention is paid to the comparison of digital evidence with its traditional types (physical, paper, etc.), which differ from each other in their changing form, high dependence on digital media and the risk of being lost forever. Specific attention is focused on the issue of authenticity of this type of evidence, which calls into question its origin, integrity and permanence. The research includes a study of the technical risks of falsification of digital traces, the lack of a single clear mechanism for verifying the authenticity of digital evidence, and discussions on the need for forensic examinations. The study analyses how the authenticity of digital evidence used in pre-trial investigation and court proceedings is assessed in court practice. The admissibility of digital evidence is an equally important topic for research. The requirements for them arise from the provisions of the Criminal Procedure Code of Ukraine (in particular, Articles 84, 86, 87, 99), as well as the case law of the European Court of Human Rights. The article focuses on such conditions as compliance with the procedure for obtaining them, proper procedural design and ensuring the rights of the parties to the proceedings, in particular the right to defence and privacy (Articles 6 and 8 of the European Convention on Human Rights). The case law of Ukraine and the ECHR is also presented, where digital evidence has become a key factor in the case and allowed to assess the current state of law enforcement and the challenges faced by the judiciary. From all the analysed material, a certain conclusion has been drawn that indicates the urgent need for legislative regulation of issues related to the verification and processing of digital evidence, the development of clear standards for its collection, storage and presentation in criminal proceedings.

**Key words:** criminal procedure, digital evidence, authenticity of evidence, admissibility of evidence, digital forensics, problems of digital data verification.

**Шишенко А.А. Цифрові докази у кримінальному процесі: проблеми автентичності та допустимості.**

Повсякденне життя наповнене інформаційними технологіями, які розвиваються дуже швидко. У всьому цьому цифрові докази займають своє місце і набувають все більшого значення у розслідуванні злочинів, допомагаючи встановити істину та забезпечити справедливість. Однак їх використання в таких справах призводить до численних правових, процесуальних і технічних проблем, які є предметом наукової рефлексії. У цій статті наведено визначення цифрових доказів відповідно до національного законодавства, доктрини та міжнародних актів, зокрема Конвенції про кіберзлочинність (Будапештської конвенції). Також надається класифікація основних видів, таких як: електронні листи, повідомлення в месенджерах (наприклад, WhatsApp, Facebook тощо), фото та відео, файли, метадані, IP-адреси, геолокаційні дані, інформація з соціальних мереж, хмарних сховищ тощо. Особливу увагу приділено порівнянню цифрових доказів з їх традиційними видами (речовими, паперовими тощо), які відрізняються між собою мінливою формою, високою залежністю від цифрових носіїв та ризиком бути втраченими назавжди. Окрему увагу приділено питанню автентичності цього виду доказів, що ставить під сумнів їхнє походження, цілісність і незмінність. Дослідження включає вивчення технічних ризиків фальсифікації цифрових слідів, відсутність єдиного чіткого механізму перевірки автентичності цифрових доказів, а також дискусії щодо необхідності

проведення судових експертиз. У дослідженні проаналізовано, як у судовій практиці оцінюється автентичність цифрових доказів, що використовуються під час досудового розслідування та судового провадження. Не менш важливою темою для дослідження є допустимість цифрових доказів. Вимоги до них випливають з положень Кримінального процесуального кодексу України (зокрема, статті 84, 86, 87, 99), а також практики Європейського суду з прав людини. У статті зосереджено увагу на таких умовах, як дотримання процедури їх отримання, належне процесуальне оформлення та забезпечення прав учасників провадження, зокрема права на захист та приватність (статті 6 та 8 Європейської конвенції з прав людини). Також представлено судову практику України та ЄСПЛ, де цифрові докази стали ключовим фактором у справі та дозволили оцінити поточний стан правозастосування та виклики, з якими стикається судова система. З усього проаналізованого матеріалу зроблено певний висновок, який свідчить про нагальну потребу законодавчого врегулювання питань, пов'язаних із перевіркою та обробкою цифрових доказів, розробкою чітких стандартів їх збирання, зберігання та представлення у кримінальному провадженні.

**Ключові слова:** кримінальний процес, цифрові докази, автентичність доказів, допустимість доказів, цифрова криміналістика, проблеми перевірки цифрових даних.

**Statement of the problem:** Digital technologies are developing very rapidly and this leads to their active use by law enforcement agencies, including in criminal proceedings, as digital evidence. At the same time, they have certain specifics, and it gives rise to a number of problems, such as authentication and ensuring the admissibility of such evidence in court. The scientific analysis of this topic is due to the fact that there are no clear legislative norms (criteria), it is difficult to verify digital data and there is a certain risk of violation of the rights of participants in the process, and for this purpose it is necessary to improve procedural regulation in this area.

**Purpose of the study:** This study aims to provide a comprehensive analysis of the legal nature of digital technologies, namely digital evidence in criminal proceedings, to identify the problems associated with ensuring their authenticity and admissibility, and to propose ways to improve the regulatory framework and practice of their use, taking into account international standards and case law.

**State of development of the problem:** The issue of authenticity and admissibility of digital evidence in criminal proceedings is increasingly attracting the attention of Ukrainian and foreign scholars. In general, legal research revolves around the legal status of digital evidence, its classification, procedural registration and use in criminal proceedings. The following scholars are also actively researching this issue: D.S. Stepanets, A.I. Zazulin, D.V. Filin, O.V. Sirenko, Eoghan Casey, J.W. Chisum and others. However, there is an understanding that the issue has not yet been properly considered, so most scientific research simply does not fully cover the interaction of technical, procedural and law enforcement aspects of the authenticity and admissibility of digital evidence, which indicates that further scientific understanding of this topic is needed.

**Main material:** The emergence of digital technologies has had a significant impact on the means of recording, transmitting and storing information. The criminal process has also begun to adopt the most modern technology to facilitate the investigation of crime, namely digital evidence, which is data in digital form that can be used to provide important facts for the investigation. However, it should not be forgotten that such evidence still has its own specific nature, which tends to affect the procedural approaches to its receipt, processing and evaluation. [1, p. 256-260]

The Criminal Procedure Code of Ukraine does not provide a precise definition of digital evidence, but Article 84 defines evidence as factual data obtained in accordance with the procedure prescribed by law, on the basis of which circumstances relevant to criminal proceedings are established, while Article 99(2)(1) of the same Code states that photographic, sound recording, video recording and other media (including computer data) may be classified as material evidence. This provision allows for some digital data to be classified as material evidence or documents (Articles 98 and 99 of the CPC respectively), but this depends on their form of presentation and content. [2]

The scientific doctrine presents digital evidence as electronic information that contains potential evidentiary value and is stored on an electronic medium or in another digital sphere. The international legal environment is also developing the use of digital evidence in criminal proceedings. The Council of Europe Convention on Cybercrime (Budapest Convention, 2001), which is the main international document in the field of combating crimes in cyberspace, does not have a direct term for digital evidence, but its article uses the concept of computer data and it can already be the object of investigative actions (Articles 16-21). [3] There is also the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (2022), which emphasises the need for common standards for the collection, transmission and use of digital information in criminal proceedings. [4]

There are several basic types of digital information and, according to certain criteria, it can be divided into: emails (for example, correspondence between the thief and the victim); messages in various messengers (Viber, Telegram, WhatsApp, etc.), which may contain text messages, voice recordings, photos and videos; surveillance camera footage (both public and private - shops, cafes, gyms, etc.); access logs, IP addresses, geolocation data (used to establish the location of a person) and data from cloud services or online accounts. [5, p.42-53] The difference between digital evidence and other types of evidence is the different form of storage, ease of modification or destruction, the need for technical processing and examination to verify accessibility, and dependence on the digital environment. [6, p. 418–421; 7, p. 208–212]

Each piece of evidence has its own characteristics, but the key one is authenticity. In general, the concept of authenticity means the actual source from which the information originates and remains intact and unchanged from the moment it is created or received until it is presented in court. In criminal proceedings, this is understood to mean that digital evidence is exactly what it is presented as and has not been tampered with, altered, falsified, etc. [5, p. 42-53]

A significant challenge in ensuring the authenticity of digital evidence is that it exists in a virtual environment and undergoes transformations when copied, moved or processed. It is a well-known fact that almost any digital information can be easily edited without any visible signs of tampering. For example, photos, audio or video files can be edited or altered using various programs, and metadata can be completely erased or deleted. This makes it impossible to confirm authenticity without technical analysis. The court practice records cases when parties of proceedings provided screenshots of emails as evidence without any confirmation of the source, which put the authenticity and admissibility of digital evidence in doubt. [8, p. 119–123]

Ukrainian criminal procedure legislation currently lacks a single clear procedure and technical standard that would help pre-trial investigation authorities or courts confirm the authenticity of digital evidence. For example, there are many cases when digital data is transferred on flash drives, digital media or even in printed form without an accompanying technical protocol, which prevents the requirements for preserving the original data structure and thus raises doubts about its authenticity. [9, p.56–60] The case law is full of cases where emails or messages from messengers are presented as digital evidence, but without an electronic signature, technical log or full archive, and this does not allow verifying their origin at all without additional information. In such cases, lawyers have the full right to challenge the admissibility of such evidence, or the court cancels it completely, accepting it as inadequate.[8, p. 119–123; 10, p. 23–27]

Most of the digital evidence belongs to the ecosystems of international private companies such as Google, Apple, Meta (Facebook), Telegram, Microsoft, etc. Critical data is stored on the servers of these companies, and they often refuse to provide information or require compliance with a complex international procedure (MLAT – Mutual Legal Assistance Treaty). Equally important is that some of these servers use certain data encryption, namely end-to-end encryption, which makes it impossible to gain access without the company's consent, even for law enforcement agencies. For Ukraine, this means that it is impossible to verify digital evidence if it comes from a closed digital ecosystem.

Almost all digital evidence requires technical or computer forensic examination due to the complexity of the structure of digital data and the risks of its falsification. These types of examinations can establish the presence of traces of editing or tampering, the authenticity of data sources, the time and geographical parameters of creation, and the presence of malware that could have influenced the alteration of the original information. However, not all participants in a criminal investigation use this right, which leads to a decrease in the level of protection of the parties' rights and the objectivity of the trial. [11, p. 131–167]

The problem of admissibility of digital evidence is related to the problem of its authenticity. Its significance lies in the fact that it affects whether such evidence will be taken into account by the court when passing a verdict or rejected by it. The admissibility of evidence is a guarantee of its procedural quality, which shows that the evidence was obtained legally and in accordance with the established requirements of the law.[12, p. 140–150]

Article 84 of the CPC provides that factual data confirming or refuting the existence of circumstances to be proved must be obtained in accordance with the procedure prescribed by law. This directly links the admissibility and legality of obtaining certain evidence, including digital evidence. The significance of Article 86 lies in the fact that it sets out a special detailed procedure for the collection of evidence and once again states that all evidence must be obtained legally, otherwise it will be inadmissible. But Article 87 already refers to the grounds for inadmissibility of evidence. Among them are the following: obtaining evidence as a result of human rights violations or by an unauthorised person is also not permitted, and the absence or distortion of the investigative protocol is also an important violation of

the collection procedure. Of course, all of this applies not only to physical evidence and documents, but also to digital evidence. [2]

The above legislative norms form certain criteria for the admissibility of digital evidence in criminal proceedings. First and foremost, the legality of obtaining any evidence is a key requirement, and this can only be done by an investigating judge's decision, through a search, temporary access to things and documents, or with the consent of the person. Furthermore, the evidence must come from a legally authorised entity (this may be a prosecutor, judge or other law enforcement officer) or be voluntarily provided by the person. Equally important is the relevance of the evidence to a particular case, as it must relate to the case and be subject to bringing the case to a logical conclusion with a judge's verdict based on the legal evidence presented. [12, p. 140–150]

Obviously, there are problems associated with the admissibility of evidence, including digital evidence. Firstly, the process of obtaining evidence is most often violated. For example, a phone was seized, but without an investigating judge's ruling, or data was copied from a computer, but this was not recorded in the relevant search report. There are many such cases in court practice that simply lead to the non-admission of digital evidence into the evidence base. [8, p. 119–123] Second, improper collection of evidence often leads to a violation of the right to privacy, which is also a violation of the European Convention on Human Rights (Article 8). In general, interference with private life, including confidential digital communication, should only take place on the basis of the law and by lawful means, which is indicative of proportionality. [13] Due to the lack of clear legislative regulation of these issues, cases of incorrect procedural notification often arise. For example, screenshots without technical verification, copies of documents without originals, or without confirmation of the integrity of information are all procedural deficiencies. This leads to the fact that such evidence raises doubts about its reliability and procedural value. [9, p. 56–60]

As for the roles of judges and attorneys in this process, this is an important issue that requires separate consideration. Speaking about an investigating judge, his/her main function as he/she is the one who grants permission for certain types of procedural actions such as temporary access to digital media, search, covert investigative actions, etc. Provided that these decisions are sufficiently justified and legal, the evidence has further admissibility. The investigating judge has the power to dismiss the application, as he or she may conclude that the interference with digital information is disproportionate or insufficiently justified. In turn, an attorney acts as a guarantor of the procedural rights of the defence. He or she, like an investigating judge, has the right to declare digital evidence inadmissible by filing a motion (according to Article 89) or may initiate an alternative examination. One of the options for declaring evidence inadmissible for a lawyer is to draw the judge's attention to the procedure for obtaining the same evidence that was violated. In practice, it is quite clear that proper advocacy prevents the unreasonable use of unreliable digital evidence [2; 11, p. 131–167].

The issue of the use of digital evidence in criminal proceedings is a central one in judicial practice both in Ukraine and internationally. Certainly, challenges with authentication, admissibility and verification of the procedure for obtaining evidence are constantly emerging. In such cases, having a sustainable approach to the assessment of digital evidence is important and helps to maintain a high level of compliance with the principles of fair trial and human rights protection. At present, Ukrainian court practice lacks a clear mechanism for evaluating digital evidence and their unified standards in criminal proceedings. However, the Criminal Court of Cassation of the Supreme Court (CCC SC) has repeatedly spoken out on the admissibility and relevance of electronic data as a type of evidence. For example, screenshots cannot be recognised as evidence without proper verification, such as examination or technical verification, which can confirm their authenticity. Or there are often situations with violations of the protocol when obtaining digital data (for example, copying information from a mobile phone), which leads to the court's recognition of such evidence as inadmissible. Considering the practice of the courts of first instance, it can be concluded that the lack of a unified approach to the assessment of digital evidence creates legal uncertainty and the risk of procedural abuse, since some courts of this instance may accept such evidence as screenshots without objection, provided that they are attached by the prosecution or the defence, while others, on the contrary, require confirmation of the source of information, a technical protocol or an expert opinion [8, p. 119–123; 9, p. 56–60].

Turning to the practice of European countries, the difference with the case law of Ukraine is quite noticeable. The European Court of Human Rights already has experience in considering such cases involving digital evidence, with the focus on the right to privacy and fair trial (Articles 8 and 6 ECHR respectively). For example, in the case of R.E. v. the United Kingdom (2015), the Court recognised that any action aimed at seizing digital data without a clear judicial procedure violates Article 8 of the Convention [13; 14]. The Court emphasised the importance of effective judicial control over access to

personal electronic data by states. The court also notices the illegality of using video recordings from surveillance cameras without a court order and without warning the person about the video recording, thus violating the right to privacy. The Court often finds that states do not have a clear technical procedure for preserving and protecting digital evidence, which raises doubts about its authenticity [15, p. 80–85; 16, p. 11–18].

EU countries are already gradually developing a common policy on digital evidence. This is also based on EU Directive 2016/680, which focuses on the protection of personal data in criminal proceedings and proposes the use of digital evidence exchange within the European Electronic Evidence Platform (e-Evidence). [17] Currently, most European countries have formed special forensic units to work with digital evidence, which operate in accordance with common standards (ISO/IEC 27037:2012) [18]. The US experience has a basic practice called the Federal Rules of Evidence, which has more than 1100 rules [19]. For the US court, it is essential to know whether the evidence is authentic, and for this purpose they widely use expert opinions of digital forensics specialists. In their practice, there was such a case (United States v. Ganias (2014)), where a federal appellate court ruled that digital evidence was inadmissible, that it was seized from a computer without time or scope limits, and that this violated the right to privacy in digital space under the Fourth Amendment [20].

With the rapid development of technology, the criminal process is increasingly moving towards the creation of specialised structures - digital forensics units - that can operate as part of the police, prosecutors or expert institutions. The United States and EU countries are already actively using such structures and have created unified methods for capturing, copying, storing and documenting digital evidence, which increases the authenticity and admissibility of such evidence. Ukraine is just beginning to integrate such new structures into the system, and they are being formed on the basis of the activities of the National Police's cyber units and expert centres of the Ministry of Internal Affairs. However, insufficient funding and legal restrictions, such as the lack of a fixed status for such units, significantly slow down the entire process and limit their effectiveness [15, p. 80–85; 16, p. 11–18].

Improving approaches to digital evidence in the criminal procedure of Ukraine is relevant because it is a period of rapid digitalisation of society. Currently, the existing regulatory framework does not have an adequate level of legal certainty, technical accuracy and security of the process related to obtaining, storing or otherwise handling digital evidence in criminal proceedings. This creates a certain risk of human rights violations, incorrect results of investigative actions and a decrease in the efficiency of criminal proceedings in general. First of all, it is recommended to create and implement a single, unified system of digital data verification. This will establish rules for recording, storing, copying and documenting digital information and will take into account requirements such as immutability, integrity and source authenticity [16, p. 11–18]. This system should be based on and comply with international standards such as ISO/IEC 27037 and use digital hash identifiers, secure protocols, etc. [18]. Mandatory expert assessment of digital evidence should also be introduced as a reform in criminal procedure. There are cases where digital material is essential for a verdict, so it must be authenticated by appropriate technical expertise to be truly legitimate evidence of guilt or innocence of a person. This process will help reduce the risks of falsification, manipulation and procedural abuse. The need to develop the digital competencies of judges, lawyers and investigators should also be emphasised. This can be done in the form of specialised training in digital forensics, explanations of the technical nature of electronic evidence and the basics of authentication. Such actions will help legal professionals to perform their functions more effectively and protect the rights of the parties to criminal proceedings [7, p. 208–212; 8, p. 119–123]. It is also necessary to improve the Criminal Procedure Code of Ukraine by including special articles or sections on digital evidence and everything that may be related to it for procedural guarantees. The positive experience of EU countries and the provisions of the Budapest Convention may be useful not only for improving Ukrainian evidence practice, but also for adapting to the requirements of the international legal environment [3; 4; 9, p. 56–60].

**Conclusion.** This study explains the benefits to the criminal process from the introduction of digital technologies, which include transforming approaches to the collection, verification and evaluation of digital evidence. As of today, this particular area of criminal procedure is the least regulated element of Ukrainian criminal procedure legislation. The Criminal Procedure Code of Ukraine does not currently contain any definitions, procedures or criteria related to digital evidence, which in turn leads to practical difficulties in criminal proceedings.

The study identified a number of problems: first, the lack of a unified procedure for verifying digital evidence, which prevents timely identification of the immutability, integrity and relevance of the source of origin. Secondly, doubts about the admissibility of digital evidence arise from violations of the

procedural procedure for obtaining it, deficiencies in recording, lack of expert assessment and legal uncertainty.

The problems mentioned above create equal risks for human rights violations. The ECtHR case law frequently deals with Articles 6 and 8 ECHR violations which is why it stresses that digital privacy interference must have clear regulations and proportionate measures with effective judicial oversight. The Ukrainian legal system lacks specific procedural safeguards which results in distorted court proceedings.

The article presents solutions to address digital evidence problems through three main approaches: adding specific provisions to the CPC regarding digital evidence collection procedures and authentication methods and evaluation processes and usage protocols; requiring technical expertise for essential digital evidence; creating a standardized digital verification process that follows international standards; and establishing training programs for judges and investigators and lawyers who handle digital data while adopting Budapest Convention approaches.

Thus, the proper legal status of digital evidence together with its procedural registration and verification stands as a fundamental requirement for criminal proceedings to operate effectively in the digital age. Systemic updates of legislative and practical mechanisms should be observed to achieve a balance between criminal prosecution effectiveness and human rights respect which aligns with modern European standards.

**REFERENCES:**


1. Tsekhan D.M. Digital evidence: concept, features and place in the system of evidence. *Scientific Bulletin of the International Humanitarian University*. Jurisprudence. 2013. No. 5. P. 256–260.
2. Criminal Procedure Code of Ukraine: Law of Ukraine dated 13.04.2012 No. 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/en/4651-17#Text (date of access: 29.06.2025).
3. Convention on Cybercrime. URL: https://rm.coe.int/1680081561 (date of access: 30.06.2025).
4. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. URL: https://rm.coe.int/1680a49dab (date of access: 30.06.2025).
5. Metelev O.P. Digital evidence in criminal procedure: typological characteristics. *Herald of criminal justice*. 2023. No. 1-2. P. 42–53.
6. Kozytska O.H. On the concept of electronic evidence in criminal proceedings. *Juridical scientific and electronic journal*. 2020. No. 8. P. 418–421.
7. Sirenko O.V. Electronic evidence in criminal proceedings. *International Legal Bulletin: Current Problems of Modernity (Theory and Practice*). 2019. No. 14. P. 208–212.
8. Petryk V.V. The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation. *Uzhhorod National University Herald.* Series: Law. 2025. Vol. 4, no. 87. P. 119–123.
9. Taran O. Practical problems of verifying electronic evidence in criminal proceedings. Scientific Review, 2021, 42(2), P. 56–60.
10. Vitkovska I. Authenticity of electronic evidence: practical aspect. *Law and State.* 2020, 48(1), P. 23–27.
11. Groshevy Yu.M., Myroshnychenko T.M., Filin D.V. Criminal Process. Kharkiv: Pravo, 2010. 608 p.
12. Romaniuk, V.V. and Ablamskyi, S.Y. Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law and Safety*. 93(2), 2024 P. 140-150.
13. European Convention on Human Rights. URL: https://www.echr.coe.int/documents/d/echr/convention (date of access: 29.06.2025).
14. Case of R.E. v. The United Kingdom. HUDOC - European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng?i=001-158159 (date of access: 01.07.2025).
15. Shevchenko O. International experience in the use of electronic evidence: lessons for Ukraine. *Criminal Law*. 18(3), 2022, P. 80–85.
16. "International Experience in the Use of Electronic Evidence." *International Journal of Criminal Law*. 2020, 38(4), P. 11–18.
17. Directive – 2016/680 – EN – Law Enforcement Directive; LED - EUR-Lex. The official portal for European data data.europa.eu. URL: http://data.europa.eu/eli/dir/2016/680/oj (date of access: 01.07.2025).
18. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. ISO - International Organization for Standardization. URL: https://www.iso.org/obp/ui#iso:std:iso-iec:27037:ed-1:v1:en (date of access: 02.07.2025).

19. Federal Rules of Evidence. United States Courts. URL: https://www.uscourts.gov/sites/default/files/2025-02/federal-rules-of-evidence-dec-1-2024_0.pdf (date of access: 01.07.2025).
20. Fourth Amendment – Search and Seizure and Evidence Retention – Second Circuit Creates a Potentional "Right to Deletion" of Imaged Hard Drives. United States v. Ganias, 755 F.3d 125 (2d Cir. 2014). *Harvard Law Review*. URL: https://harvardlawreview.org/wp-content/uploads/2014/12/united_states_v_ganias.pdf (date of access: 02.07.2025).