AJEE
ACCESS TO JUSTICE IN EASTERN EUROPE
Peer-reviewed Journal

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Case Note

ELECTRONIC EVIDENCE IN PROVING CRIMES OF DRUGS AND PSYCHOTROPIC SUBSTANCES TURNOVER[1]

Dmytro Golovin[2]
Yehor Nazymko[3]
Oleh Koropatov[4]
Maksym Korniienko[5]

1 The study was conducted as part of research work No. 0114U004013 'Ensuring the rights and freedoms of citizens in administrative (police) activities', Department of Administrative Activities of the Odesa State University of Internal Affairs, and as part of research work No. 0121U109271 'Security and protection of rights, freedoms and legal interests of participants in criminal proceedings', Department of Criminal Procedure of Odesa State University of Internal Affairs, as well as the concept of the program of informatization of the Ministry of Internal Affairs of Ukraine and central executive bodies, whose activities during 2021-2023 are directed and coordinated by the Cabinet of Ministers. See 'Development of digital infrastructure and creation of digital services for citizens is a priority of the program of informatization of the system of the Ministry of Internal Affairs' (22 April 2021 No. 301) <https://mvs.gov.ua/en/press-center/news/rozvitok- cifrovoyi-infrastrukturi-ta-stvorennya-cifrovix-servisiv-dlya-gromadyan-prioritet-programi-informatizaciyi-sistemi-mvs> accessed 30 January 2022.

2 Graduate Student in Law, Department of Criminology and Psychology, Odesa State University of Internal Affairs, Odessa, Ukraine dmytro_golovin@ukr.net https://orcid.org/0000-0002-6394-8937 **Corresponding author**, responsible for data curation, supervision, and project administration. The corresponding author is responsible for ensuring that the descriptions and the manuscript are accurate and agreed by all authors.

3 Dr. Sc. (Law), Professor at the Department of State and Legal Disciplines and Public Administration, Vice-Rector of Donetsk State University of Internal Affairs, Mariupol, Ukraine nazymko8190@acu-edu.cc https://orcid.org/0000-0002-7825-4057 **Co-author**, responsible for exploration of sources and for writing.

4 PhD in Law, Associate Professor, Professor at the Department of Administrative Activity and Affiliation, Odesa State University of Internal Affairs, Odessa, Ukraine koropatov8190@edu-knu.com https://orcid.org/0000-0003-0996-3455 **Co-author**, responsible for formal analysis and writing methodology.

5 Dr. Sc. (Law), Professor, Head of the Department of Administrative Activity of Police, Odesa State University of Internal Affairs, Odessa, Ukraine korniienko8190@sci-univ.com https://orcid.org/0000-0003-2449-9814 **Co-author**, responsible for writing and editing.

Competing interests: All co-authors declare no conflict of interest of relevance to this topic. **Disclaimer:** The authors declare that they were not involved in any state bodies, courts, or any other organisation's activities related to the discussed views and case-law.
Managing editor – Dr Olena Terekh. **English Editor** – Dr Sarah White
The content of this article was translated with the participation of third parties under the authors' responsibility.

How to cite: D Golovin, Ye Nazymko, O Koropatov, M Korniienko 'Electronic Evidence in Proving Crimes of Drugs and Psychotropic Substances Turnover' 2022 No 2 (No 14) Access to Justice in Eastern Europe 156-166. DOI: 10.33327/AJEE-18-5.2-n000217
First published online: 14 Mar 2022 (https://doi.org/10.33327/AJEE-18-5.2-n000217)
Last published: 16 May 2022

Submitted on 30 Jan 2022 / Revised 1st 14 Feb 2022 / Revised 2nd 23 Feb 2022 /
Approved 07 Mar 2022 / Published online: 14 Mar 2022 // Last published 16 May 2022

ABSTRACT

Background: *This article is prompted by the increasing levels of crime in the sphere of illicit trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors using information and telecommunication systems. The aim of the article is a comprehensive analysis of the problem of the use of electronic evidence in proving crimes of trafficking in these substances.*

Methods: *A number of methods were used in this article, namely: theoretical analysis – the study and analysis of official documentation, scientific, methodological, and educational literature, summarising information to determine the theoretical and methodological foundations of the study; logical analysis – to formulate basic concepts and classification; concrete-historical analysis – to demonstrate the dynamics of development of the use of electronic evidence in criminal proceedings; the dialectical method – to reveal the meaning of concepts of 'electronic evidence'. The judicial practice of the Supreme Court of Ukraine regarding the recognition of electronic proof as appropriate evidence in cases is disclosed. The definition of electronic proof in the Ukrainian legal system, as well as the forms and features of electronic proof, are also considered.*

Results and Conclusions: *It is established that the main causes of drug trafficking crimes include insufficient legal regulation of cyberspace, the lack of geographical boundaries, the spread of information about drugs on the Internet, especially on the Darknet, and the uncontrolled development of the cryptocurrency market.*

Keywords: *electronic evidence; criminal process; narcotics; information technologies; evidence.*

1 INTRODUCTION

Over the past decade, Ukraine has made significant strides in informatising society, as evidenced by statistics from GlobalLogic, which found that 60% of Ukraine's population is already registered on social networks, the most popular of which is YouTube, with users at 96% of the population. As for the dynamics of growth, from the beginning of 2020 to the beginning of 2021, the Ukrainian audience of social networks increased from 19 million to 26 million users, that is, by 7 million people.[6]

At the state level, the development of informatisation in our country is considered one of the national priorities, as exemplified by the mobile application, web portal, and brand of the digital state, developed by the Ministry of Digital Transformation of Ukraine (DIIA), which has an ambitious goal to translate 100% of public services online.[7] According to the Minister of Digital Transformation of Ukraine, M. Fedorov, over the next two years,

6 During the year of quarantine, the number of Ukrainians on social networks increased by seven million (2021). <https://www.dw.com/en/za-rik-karantUnu-kilkist-ukraintsiv-u-sotsmereznakn-zrosla-na-sim-milioniv/a-56899697> accessed 30 January 2022.

7 DIIA (service) <https://diia.gov.ua> accessed 30 January 2022.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

electronic voting tools may be introduced that will operate during referendums and elections in Ukraine. But along with the necessary information changes in the public life of every person, it is natural that there are new schemes of illegal behaviour and criminal elements to which the law enforcement system must respond. Such a reaction must be on a par with modern information technology, which unfortunately almost never happens. This is a problem not only in Ukraine but also globally.

The public danger of crimes in the sphere of illegal circulation of drugs and their analogues, committed using computer technologies, is determined along with other signs of an increase in the criminality of the information space of the global network, influencing various spheres of society and causing inappropriate social and criminal behaviour of individuals or groups of people. This is due to the general availability and openness of the global network and insufficient legal regulation of its activities. Criminal elements are the first to have the most advanced software – they have the opportunity to hire the most professional workers, as well as to operate in different legal systems in different countries. For example, the UN Program on International Drug Control and Crime Prevention contains the Model Law on the Punishment of Drug-Related Crimes, which prohibits the use of computer data exchange networks to facilitate or advance the production, manufacture, trafficking, and illicit use of drugs. In some foreign countries, the use of the global network in the commission of crimes in the sphere of illicit drug trafficking is criminalised either as a mandatory sign of the main *corpusdelicti* or as a qualifying sign. This testifies to the increased attention of the world community to the problem of drug distribution via the Internet. It should be noted that the main source of law in the countries of the Romano-Germanic legal family, including Ukraine, is a legal act, and the legal norm is considered an abstract, general, and impersonal rule of conduct that can be repeatedly applied to an indefinite number of cases and persons.

Electronic evidence and the issue of its use in the judicial process of Ukraine remain controversial topics in the legal community. The concept of 'electronic evidence' appeared in the 1970s with the advent of machine documents. According to Art. 2 of the Model Law on Electronic Commerce of 1997, recommended by the UN General Assembly, it is defined as information prepared, sent, received, or stored by electronic, optical, or similar means, including electronic data exchange, e-mail, telegraph, or fax. As for the typical schemes of committing crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors, these have undergone significant changes over the past ten years. The results of human activity are increasingly reflected in electronic (digital) forms, including those that acquire the meaning of legal facts. There are no more real meetings for the sale of drugs – all communication has moved online for the sake of anonymity. Therefore, a large share of drug sales is made through such means of communication as messengers (Telegram, Viber, WhatsApp, and Signal) and social networks (Instagram, Facebook, and Twitter). This makes the issue of the use of electronic evidence especially relevant in the investigation of crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors.

Analysis of the current reality in the field of procedural law of Ukraine8 shows its transformation into case law when the court's own conviction takes precedence over legal norms so that it is impossible to consider them a unified tool for establishing the truth. Indicative in this aspect is the use of electronic evidence in criminal proceedings. Various aspects of electronic evidence in criminal procedure legislation have been studied

8 S Studennykov, 'Electronic evidence in procedural law: how it works in Ukrainian realities' (2019) Jud & Leg Newspaper <https://sud.ua/en/news/publication/138354-elektronni-dokazi-v-protsesualnomu-pravi-yak-tse- pratsyuye-v-ukrayinskikh-realiyak> accessed 30 January 2022; VI Zavydniak, Introduction of judicial precedent in the criminal process of Ukraine (SFS University of Ukraine 2019).

by Ukrainian scholars. But there are still several practical and scientific inconsistencies regarding electronic evidence and their recognition as appropriate and admissible in court, which led to our study.

The purpose of the present article is an analysis of the problem of using electronic evidence in proving crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors. The study was conducted based on practical experience gained in senior positions of the Main Directorate of the National Police of Ukraine in the Odessa region during the implementation of professional activities, as well as during scientific and pedagogical activities in higher education institutions of the Ministry of Internal Affairs of Ukraine.

To achieve this goal, a number of scientific methods were used, namely: theoretical analysis – to study and analyse official documentation, scientific, methodological, and educational literature and to generalise information to determine the theoretical and methodological foundations of the study; logical analysis – to formulate the basic concepts and classification; concrete-historical analysis – to demonstrate the dynamics of development use of electronic evidence in criminal proceedings; the dialectical method – to reveal the meaning of the concepts of 'electronic proof', 'electronic traces', and signs of electronic evidence, as well as to establish the content and features of the constituent elements of the implementation and application of electronic evidence in law enforcement; empirical methods – for the generalisation of practical experience, observation, and discussion. The formal-legal method was used in the analysis of current national legislation, identifying inherent advantages and disadvantages in the use of electronic evidence, as well as formulating proposals to improve the procedural use of electronic evidence in Ukraine.

2 SCIENTIFIC APPROACHES: VIEW FROM UKRAINE

The current state of crime in the sphere of illegal drug trafficking, including crimes committed using the Internet, is characterised by a high level of latency. This is due to the lack of mechanisms for automatic detection of resources on the network containing illegal information about drugs or those used for illegal activities, as well as identification of offenders. The emergence of such resources is monitored and analysed using search engines, and the result depends on the development of information retrieval and what encryption programs are used by offenders. In addition, in the case of identification of sites on the Internet registered outside the territory of Ukraine and used for the distribution of drugs and involvement in their consumption, it becomes difficult to prosecute the owners of such resources. As a rule, the only measure applied to the owners of prohibited resources on the Internet is for providers to restrict access.

Also, such activities can be conducted in other countries from the territory of Ukraine, despite the establishment of access restrictions for the Ukrainian consumer, which significantly limits Ukrainian law enforcement officers in the methods of detecting such activities. The possibilities of the Internet in the commission of crimes in the sphere of trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors have undergone significant changes. The characteristic features of these acts include:

- the remote nature of illegal actions in the absence of physical contact between 1) the drug dealer and the purchaser, 2) the person who posted information about the manufacture or processing of drugs and the person who manufactures or processes them, 3) the person who posted information aimed at inducement to the use of drugs and the person who is being persuaded;

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

- the increased secrecy of the commission of a crime, provided by the specifics of the network space (developed mechanisms of anonymity, the complexity of the infrastructure);
- the cross-border nature of drug crimes, in which the perpetrator, the object of the criminal offence, and/or the victim may be under the jurisdiction of different states;
- the high level of preparedness of offenders and the intellectual nature of their illegal activities (preparation and commission of drug crimes require special knowledge and skills);
- the special nature of the crime scene. Traces of criminal actions are distributed over a variety of objects (computer systems of the criminal, provider, intermediate network nodes, etc.);
- the non-standard, complex, diverse, and frequently updated ways of committing drug crimes and the special means used, including the development of the cryptocurrency market;
- the multi-episode nature of illegal actions;
- the possibility of committing a crime in an automated mode, the implementation of complex scenarios by one person when combining the resources of individual computers;
- the absence of witnesses of illegal actions, such as persons who observed the event of the crime and are able to identify the offender.

Before considering the peculiarities of proving crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors, it is necessary to explore the concept of 'electronic evidence' because there is the problem of insufficient fixation in Ukrainian legislation. Therefore, in accordance with Part 1 of Art. 100 of the Civil Procedure Code of Ukraine, electronic evidence is information in an electronic (digital) form, containing data on the circumstances relevant to the case, in particular, electronic documents (including text documents, graphics, plans, photographs, video and audio recordings, etc.), websites (pages), text, multimedia and voice messages, metadata, databases, and other data in electronic forms.

Such data can be stored on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other places of data storage in electronic form (including the Internet).[9]

In accordance with para. 3 of Part 2 of Art. 99 of the Criminal Procedure Code of Ukraine (hereafter, CrPC), the documents may also include media on which procedural actions are recorded by technical means, if they are compiled in the manner prescribed by the CrPC. In Part 4 of Art. 99 of the CrPC states that a duplicate of the document (a document made in the same way as its original), as well as copies of information contained in information (automated systems, telecommunications systems, information and telecommunications systems, their integral parts, made by the investigator or prosecutor with the involvement of a specialist), are considered by the court as an original document.

According to Art. 84 of the CrPC, evidence in criminal proceedings are factual data obtained in the manner prescribed by this Code, on the basis of which the investigator,

9 Civil Procedure Code of Ukraine: Law of Ukraine No 1618-IV <https://zakon.rada.gov.ua/laws/show/1618-15#Text> accessed 30 January 2022.

prosecutor, investigating judge, and court establish the presence or absence of facts and circumstances relevant to criminal proceedings and subject to proof. Procedural sources of evidence are testimony, physical evidence, documents, and expert opinions.[10] Among the definitions provided by scientists, the most common among them are the electronic evidence is a set of information stored electronically on any type of electronic media and electronic means,[11] including evidence in criminal proceedings in electronic form.[12]

The concept of 'electronic traces' is also reflected in domestic forensic literature. The electronic digital traces are materially invisible traces that can be detected, recorded, and studied by digital electronic devices and contain any forensic material information (information, data) recorded in electronic digital form on physical media. This definition focuses on the principles of working with electronic traces but, unfortunately, lacks due attention to their nature.

It should be noted that both the criminal procedure legislation and the scientific doctrine of some foreign countries are currently at a slightly higher level of development in relation to electronic sources compared to domestic ones. At the beginning of the development of computer technology, the problem of using digital information in evidence arose in the United States, where, at that time, the rules for the use of 'novel evidence' were first expressed. According to the peculiarities of the Anglo-American legal system, the source of such rules is the case law in *Frye v. the United States*, which concerned the use of new data and methods of science in evidence and consisted of two elements: the court must determine first, which field of scientific knowledge data and techniques underlie the evidence, and second, whether the leading scientists in this field recognise the principle on which the evidence is formed.[13]

There are also differing views on the place of electronic evidence in the system of procedural sources of evidence. A. Bilousov proposes that we consider computer objects one of the varieties of a separate group of physical evidence.[14] Yu. Orlov and S. Cherniavskyi believe that electronic evidence is similar to physical evidence in relation to criminal proceedings.[15] A. Stolitnii and A. Kalancha emphasise that a document as a source of evidence in criminal proceedings can be in both paper and electronic form. D. Tsekhan argues that digital information and its media, due to its unique characteristics (especially the intangible ones), cannot be attributed to any qualification group.[16] Tsekhan also notes that when detecting digital information, investigators have many difficulties in capturing it, taking into account the requirements of criminal procedure law for evidence and further use in criminal proceedings.[17] This is due to the ability to quickly change the content of a site, the physical location of servers in other countries, and the use of anonymous software. V. Markov and R. Savchenko determine the absence

10 Criminal Procedure Code of Ukraine: Law of Ukraine No 4651-VI (2012) <http://law.rada.gov.ua/laws/show/4651- 17> accessed 30 January 2022.

11 DO Alekseeva-Protsyuk, OM Briskovskaya, 'Electronic evidence in criminal proceedings: concepts, features and problematic aspects of application' (2018) 2 Sci Bull of Publ and Priv L 250.

12 OO Volkov, 'The main sources of forensic information about malware are related to malware' (2018) 3(22) Inn Sols in Modern Sci 15.

13 DM Tsekhan, 'Digital evidence: concepts, features and place in the system of proof' (2013) 5 Sci Bull of the Intern Hum Univ. Ser: Jur 258.

14 AS Bilousov, *Forensic analysis of objects of computer crimes* (Classic Private University 2008).

15 YuYu Orlov, SS Cherniavskyi, 'Electronic reflection as a source of evidence in criminal proceedings' (2017) 1(13) Leg J of the NAIA 12-22.

16 Tsekhan (n 12) 258.

17 Ibid 256-260.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

of grounds for inadmissibility of electronic evidence obtained from any digital media and the legal order obtained in accordance with the CrPC.[18]

G. Chyhryna singles out the lack of knowledge of the subjects of evidence in the field of computer hardware and software and the need to develop and improve existing special training programs for law enforcement officers so they can work with media computer (electronic) information, detection, analysis, and imaging.[19] V. Muradov also notes that due to the lack of basic knowledge in the field of IT and a well-established method of collecting and using such evidence, it is necessary to involve specialists (and appoint examinations), remove a large amount of equipment, or spend a lot of time finding and fixing them.[20]

Thus, for electronic evidence, the following features can be identified:

- existence in intangible form;
- the need to use certain technical means for reproduction;
- the ability to transfer or copy to different devices without losing performance;
- the original electronic proof can exist in many places at the same time.

In particular, A. Kalamayko identifies the following features:

> 1) the impossibility of direct perception of information, which necessitates the use of hardware and software to obtain information; 2) the presence of a technical storage medium that can be used repeatedly; 3) a specific process of creating and storing information, which allows you to easily change the media without losing content and vice versa, provides the ability to make changes to the content without leaving traces on the media; 4) the absence of the concept of "original" electronic means of proof due to the complete identity of electronic copies; 5) the presence of specific "details", the so-called metadata – information of a technical nature, which is encoded within the files.[21]

In our opinion, there is no need to single out electronic evidence as an independent procedural source of evidence, but it is necessary to clearly define the preservation of electronic data, which must be integral and unchangeable. We must therefore define in regulations the algorithm of obtaining, recording, using, storing, and analysing data. In addition, certain algorithms should be immediately introduced into the curricula of higher education for the formation of high-quality modern knowledge and skills in the field of information and telecommunications. When working with electronic evidence, certain principles must be followed:

1. Legality. Employees of law enforcement agencies conducting investigations and investigating evidence in electronic forms have an obligation to comply with current legislation and general procedural and forensic principles.
2. Data integrity. The actions of the specialist should not lead to material changes in the data, electronic devices, or media that can be used as evidence.
3. Documenting the process. Any actions performed in relation to electronic evidence must be documented, and these documents must be stored in case of verification so that an independent third party could repeat these steps and get a similar result.

18 BB Markov, RR Savchenko, 'Principles of reliance on electronic evidence obtained from mobile devices' (2014) 1(52) L&S 89-95.

19 G Chyhpyna, 'Electronic documents: involvement of a specialist in the closure and use during the criminal conduct' (2017) 1 Nat Leg J: Theory & Practice 136.

20 VV Muradov, 'Electronic evidence: a forensic aspect of use' (2013) 3(2) Comparative-Analytical Law 314.

21 AYu Kalamayko, *Electronic means of proof in civil process* (Yaroslav Mudriy National University of Law 2016).

4. Expert support. If it is assumed that during the inspection (search), electronic evidence may be detected, support from specialists (specialists) providing, if possible, their presence at the scene is required.
5. Appropriate professional training. If in the process of inspection (search), there are no specialists from electronic evidence, priority actions at the scene are carried out by persons who have the necessary knowledge and skills to identify and gather evidence.
6. Reasonable caution. Avoid any intentional or unintentional actions that can damage potential evidence presented in digital form.[22]

3 THE PRACTICE OF THE ELECTRONICAL EVIDENCE USING IN PROVING CRIMES

Let us move on to practical analysis. Because today, the sale of narcotic drugs, psychotropic substances, their analogues, or precursors mostly takes place through messengers, the Supreme Court investigating whether a screenshot of messages from a phone can be proper proof is particularly important[23]. The plaintiff stated that in the phone correspondence between herself and her ex-husband concerning organisational meetings with her son, he had made open threats, insulted her, humiliated her honour and dignity, and used obscene language regarding the applicant and her family.

The court of first instance upheld the claim in part. A restrictive order was issued. The following measures of temporary restriction of rights for a period of six months were established: it was forbidden for the ex-husband to conduct correspondence, telephone conversations, or communicate through any other means of communication with the applicant and the child personally or through third parties. The Court of Appeal upheld the decision of the court of first instance. Disagreeing with the court's decision, the ex-husband filed a cassation appeal. Considering the case, the Supreme Court referred to Part 1.3 of Art. 100 of the CPC, which we previously cited, and further noted that such data may be stored on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other places of data storage in electronic form (in including the Internet). The parties to the case had the right to submit electronic evidence in paper copies, certified in the manner prescribed by law.[24] Even so, a paper copy of an electronic proof is not considered written proof. Thus, the Supreme Court emphasised that in support of the claims, the applicant had provided screenshots of telephone and tablet messages and Viber printouts, which the trial court and appellate court considered appropriate and admissible evidence.

The content of specific phrases, vocabulary, and the nature of the language used by the ex-husband in correspondence with his ex-wife and young son provided grounds to conclude that his actions should be classified as domestic violence, and the court reasonably prohibited him from correspondence, telephone conversations, and communications through other means with the ex-wife and child personally and through third parties. Thus, the Supreme Court dismissed the cassation appeal and upheld the decision of the court of first and appellate instance, recognising the screenshots of the messages as evidence in the case.[25]

22 IP Ponomarev, 'Digital alibi and its verification' (2011) 2 Bull of VSU 440.

23 Resolution of the Supreme Court of Ukraine of 13 July 2020 No 753/10840/19 (2020) <https://reyestr.court.gov.ua/Review/90385050> accessed 30 January 2022.

24 Civil Procedure Code of Ukraine: Law of Ukraine No 1618-IV (n 10).

25 Resolution of the Supreme Court of Ukraine of 13 July 2020 No 753/10840/19 (2020) <https://reyestr.court.gov.ua/Review/90385050> accessed 30 January 2022.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Contrary to the above-mentioned decision, the Supreme Court noted in the other case [26]that an electronic copy of written evidence is not considered electronic evidence. Thus, in the cassation appeal, the cassator pointed out that the cassation appeal concerns the issue of law, which is fundamental for the formation of a unified law enforcement practice, namely, the use of electronic evidence in the form of electronic correspondence, including messengers (Skype, Viber, and WhatsApp). He also pointed out that correspondence via messengers (in the form of text and multimedia messages) fully meets the requirements of electronic proof.

However, in response to the cassation appeal, the defendant considered unfounded the plaintiff's arguments about the existence of a contractual relationship between them. Thus, the defendant pointed out that the plaintiff provided the court with electronic correspondence, screenshots, and copies of documents to confirm his arguments, which cannot be considered appropriate evidence. The Supreme Court noted that if a copy (paper copy) of the electronic evidence is submitted, the court may, at the request of the party to the case or on its own initiative, request the original electronic evidence from the person concerned. If the original electronic evidence is not submitted, and the party to the case or the court questions the compliance of the submitted copy (paper copy) of the original, such evidence is not taken into account by the court (Part 5 of Art. 96 of the CPC). The Court also concluded that the party to the case has the right to submit electronic evidence in the following forms to substantiate his claims and objections:

1) the original;
2) an electronic copy certified by an electronic digital signature;
3) a paper copy certified in the manner prescribed by law.[27]

It should also be noted that on 14 February 2019, the Grand Chamber of the Supreme Court[28] decided that the electronic digital signature is the main requisite of this form of electronic evidence. The absence of such details in an electronic document excludes grounds to consider it original and therefore appropriate evidence in the case[29].

4 CONCLUSIONS

The main reasons for drug crimes on the Internet include insufficient legal regulation of cyberspace, a lack of geographical boundaries, dissemination of information about drugs on the Internet, and the uncontrolled development of the cryptocurrency market. The main conditions for drug crimes on the network include anonymity, public availability of information disseminated via the Internet, virtualisation (lack of material component when working on the Internet), lack of methodological developments in the investigation of law enforcement agencies, and improper organisation of the work of telecommunication service providers (providers). In today's conditions, the use of electronic means of proof,

26 Resolution of the Supreme Court of Ukraine of 29 January 2021 No 922/51/20 (2021) <https://reyestr.court.gov.ua/Review/94517830?fbclid=IwAR2NHSc2-GkGdPohIKGbS5b2KsOreDLF3kVyblnRrBflii48jLcojXikgDQ> accessed 30 January 2022.

27 Ibid.

28 Decision of the Supreme Court of Ukraine of 14 February 2019 No 9901 / 43/19 (2019) <https://verdictum.ligazakon.net/document/79883385> accessed 30 January 2022.

29 A similar legal position was expressed by the Supreme Court in the decision of 19 December 2018 in case No. 226/1204/18, from 4 December 2018 in case No. 2340/3060/18, from 23 November 2018 in case No. 813/1368/18, and from 14 December 2018 in case No. 804/3580/18. Therefore, both the original and a copy of the electronic document must be certified by a Single Digital Signature.

their admissibility, and their probative value are becoming increasingly important. In practice, and especially when proving crimes in the field of trafficking in narcotic drugs, psychotropic substances, their analogues, or precursors, as this type of illegal activity has almost completely gone online, there are many questions about the possibility of using information from messengers, social networks, network games, or proprietary programs. In the course of the research, we came to the conclusion that the issues of electronic evidence are poorly regulated by law and especially by the CPC.

According to the practice of the Supreme Court of Ukraine, electronic evidence can be stored on portable devices (memory cards, mobile phones, etc.), servers, backup systems, and other places of data storage in electronic form (including the Internet). According to the above provisions, an original electronic document is an electronic copy of the document with the required details, including the electronic signature of the author. Messenger correspondence (in the form of text and multimedia messages) fully meets the requirements of electronic proof. However, the court may not take into account a copy (paper copy) of the electronic evidence if the original electronic evidence is not submitted, and the party to the case or the court questions the responsibility of the submitted copy (paper copy) of the original.

Also, in our opinion, there is no need to distinguish electronic evidence as an independent procedural source of evidence, but it is necessary to clearly define the preservation of electronic data, which must be integral and unchangeable. Therefore, we need to define in regulations the algorithm for obtaining, recording, using, storing, and analysing this data. The independence of the concept of electronic evidence depends on the characteristics of the data carrier. In addition, certain algorithms should be immediately introduced into the curricula of higher education for the formation of the latest high-quality modern knowledge and skills in the field of information and telecommunications.

To achieve this aim, we need an appropriate procedural form that would ensure that the judge and other parties to the process can demonstrate the facts of the case and present the necessary evidence and make information technologies serve litigation purposes more effectively. The solutions to those questions are closely linked to the understanding of the essence of electronic evidence, as well as its place in the trial process. Thus, the current negative trends of drug-related crime on the Internet and the peculiarities of its existence and reproduction in the global network dictate the need for further research into the criminological characteristics of the crimes under consideration and the grounds for criminalising the method of drug distribution.

REFERENCES

1. Alekseeva-Protsyuk DO, Briskovskaya OM, 'Electronic evidence in criminal proceedings: concepts, features and problematic aspects of application' (2018) 2 Sci Bull of Public & Private L 247-253.
2. Bilousov AS, *Forensic analysis of objects of computer crimes* (Classic Private University 2008) 18.
3. Chyhpyna G, 'Electronic documents: involvement of a specialist in the closure and use during the criminal conduct' (2017) 1 Nat Leg J: Theory & Practice 134-137.
4. Kalamayko, AYu *Electronic means of proof in civil process* (Yaroslav Mudriy National University of Law 2016).
5. Markov BB, Savchenko RR, 'Principles of reliance on electronic evidence obtained from mobile devices' (2014) 1(52) L&S 89-95.

Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

6. Muradov VV, 'Electronic evidence: a forensic aspect of use' (2013) 3(2) Comparative-Analytical L 313-315.
7. Orlov YuYu, Cherniavskyi SS, 'Electronic reflection as a source of evidence in criminal proceedings' (2017) 1(13) Leg J of the NAIA 12-22.
8. Ponomarev IP, 'Digital alibi and its verification' (2011) 2 Bull of VSU 437-444.
9. Studennykov S, 'Electronic evidence in procedural law: how it works in Ukrainian realities' (2019) Judicial and Legal Newspaper <https://sud.ua/en/news/publication/138354-elektronni-dokazi-v- protsesualnomu-pravi-yak-tse-pratsyuye-v-ukrayinskikh-realiyak> accessed 30 January 2022.
10. Tsekhan DM, 'Digital evidence: concepts, features and place in the system of proof' (2013) 5 Sci Bull of the Int Hum Univ. S: Jur 256-260.
11. Volkov OO, 'The main sources of forensic information about malware are related to malware' (2018) 3(22) Inn Sol in Mod Sci 15.
12. Yesimov SS, 'Electronic documents as evidence in cases of administrative offenses' (2016) Bull of the Nat Univ 'Lviv Polytechnic' Leg Sci 72.
13. Zavydniak VI, *Introduction of judicial precedent in the criminal process of Ukraine* (SFS University of Ukraine 2019).