DOI https://doi.org/10.30525/978-9934-26-091-9-8

DIGITIZATION OF THE CRIMINAL PROCESS: YESTERDAY, TODAY, TOMORROW

Krytska I. O.

INTRODUCTION

Undoubtedly, it seems relevant to identify possible directions for adapting criminal procedural law to the digital realities of today and the challenges of the near future, given the obsolescence of the relevant provisions of the Criminal Procedure Code of Ukraine in comparison not only with similar regulations in other countries, but even in other procedural areas of law (administrative, economic, civil). It is also important to outline the directions of digital transformation of pre-trial investigation in the field of proving through the prism of increasing its effectiveness in the digitalization of society and taking into account the need to ensure the rights and legitimate interests of the individual, their general characteristics. In this regard, it should be noted that the current criminal procedure law is somewhat archaic regarding the latest manifestations of illegal actions in the network, as they contain general rules for protecting the rights and legitimate interests of individuals from threats in reality without taking into account the possibility of criminal offenses in Internet space. Therefore, traditional methods of preventing and combating criminal offenses are not always effective; in addition, difficulties may arise at the stage of establishing the fact of the offense.

In considering the issue of digital technologies in criminal proceedings, it seems appropriate to identify three main areas of our study, namely:

(1) "yesterday" – to consider what has already been introduced and taken into account in domestic law (in particular, to focus on remote procedural actions in criminal proceedings, operation of automated systems in criminal proceedings, application of measures for ensuring of criminal proceedings to digital media;

(2) "today" – to reveal those areas that can already be improved on the basis of existing regulations (first of all, to draw attention to the need to change conceptual approaches to the collection, research, use of digital information in criminal proceedings and its various forms (e.g. digital tracks);

(3) "tomorrow" – to outline potential "futuristic" vectors of criminal proceedings in this direction (which now seem to be the distant future), namely to identify possible vectors for the introduction of artificial intelligence technologies in criminal proceedings.

1. “Yesterday” (what has already been introduced and taken into account in domestic law)

First, the current Criminal Procedure Code of Ukraine (hereinafter – the CPC) enshrines regulations governing the possibility of remote procedural actions in criminal proceedings. Thus, there is a possibility of interrogation, identification by videoconference during the pre-trial investigation (Article 232), the procedure for conducting remote court proceedings is regulated (Articles 336, 354), the interrogation procedure at the request of the competent authority of a foreign state by holding a video or telephone conference is regulated (Article 567). At the same time, given that the CPC requires that the use of technical means and technologies to ensure proper image and sound quality, as well as information security (i.e. security of information and supporting infrastructure) – a person involved in proceedings must be or in the premises of a pre-trial investigation body or court, or in a pre-trial detention facility or penitentiary institution.

Secondly, the functioning of the automated document management system of the court is provided (Article 35). These include: automated distribution of criminal proceedings and determination of jury; providing legal entities and individuals with information on the status of consideration of materials in criminal proceedings; issuance of documents; transfer of materials to the E-archive; preparation of statistics; correspondence registration; centralized storage of texts of procedural documents. However, the constant delay in the start of the unified judicial information and telecommunication system raises significant issues.

Third, the current CPC provides for instructions aimed at preventing illegal violation of individual rights in the seizure of digital media – in particular, temporary access to electronic information systems or parts thereof, mobile terminals of communication systems is carried out by removing a copy of information contained in such electronic information systems or their parts, mobile terminals of communication systems, without their removal (paragraph 2, part 1 of Article 159 of the CPC); seizure of electronic information systems or their parts, mobile terminals of communication systems for the study of physical properties that are important for criminal proceedings, is carried out only if they are directly specified in the court decision (paragraph 2, part 2 of Article 168 of the CPC) and other.

At the same time, the analysis of a large number of draft laws (in particular, № 9484 from 17.01.2019[1], № 2740 from 15.01.2020[2],

[1] Проект закону про внесення змін до кримінального процесуального кодексу України та кримінального кодексу україни (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) (реєстр. № 9484 від 17.01.2019 р.). url: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65354

[2] Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) (реєстр. № 2740 від 15.02.2020 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67884

№ 4003[3] and № 4004 from 01.09.2020[4], etc.), aimed at regulating certain issues, related to digital transformation, testifies to the relevance of this issue. In addition, the scientific community has long justified the need, in particular, the introduction of new approaches to the search related to interference with electronic information systems, the need to improve the regulatory model of measures to ensure criminal proceedings (especially those related to access to information contained on digital media). However, the use of electronic information still remains almost unregulated in national criminal procedure law. This puts on the agenda, on the one hand, the issue of ensuring the prompt receipt and use of this type of information and its media in evidence in criminal proceedings, and on the other – prevention of illegal and unjustified violations or restrictions on the rights and legitimate interests of individuals and legal entities.

In light of this, it should be added that, despite the fact that Ukraine ratified the Convention on Cybercrime on September 7, 2005[5], some provisions of this international agreement have not yet been implemented into national law. In view of this, the analysis of some proposals formulated in the draft law №4003 of 01.09.2020[6], which are directly aimed at resolving this issue, becomes especially relevant.

Thus, the draft law proposes to introduce a new measure in the domestic CPC to ensure criminal proceedings, namely – "urgent preservation of information". Systematic analysis of these proposals requires attention to some aspects, in particular:

(1) the use of the term "information" in the name of the action. Thus, it seems more appropriate to use the term "data", because, first, it is used to denote this measure in Art. 16 of the Convention on Cybercrime. And, secondly, such a designation seems more successful, because the data can be transformed into information by analysis, identification of links, highlighting the most important facts, their synthesis; that is, information is data that is transformed into meaningful form for appropriate use. At the same time, at the time of application of such a security measure, analysis and selection is not yet taking place, and therefore it is more correct to talk about the concept of "data";

[3] Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам (реєстр. № 4003 від 01.09.2020 р.). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

[4] Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів (реєстр. № 4004 від 01.09.2020 р.). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

[5] Конвенція про кіберзлочинність: ратифіковано Загоном України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

[6] Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам (реєстр. №4003 від 01.09.2020 р.). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

(2) the inexpediency of limiting the list of corpus delicti in criminal proceedings in respect of which the application of this measure to ensure criminal proceedings will be permitted. Thus, the comparison of this list with Art. 2-10 of the Budapest Convention indicates that the drafters of the bill tried to cover only those crimes that are explicitly specified in these rules. However, it should be noted that according to Part 2 of Art. 14 of this international agreement, the application of such measures is appropriate not only to criminal offenses established in accordance with Articles 2 to 11 of this Convention (paragraph a), but also to other criminal offenses committed by the using of computer systems (paragraph c). In light of this, it is possible to mention the possibility of committing even certain crimes against human life and health using computer systems and networks (for example, leading to suicide through correspondence on social networks). In view of this, we propose to consider the possibility of expanding the list of criminal offenses in criminal proceedings in respect of which the use of urgent storage of information is allowed.

It seems appropriate to dwell also on the analysis of proposals for the introduction of a procedure for temporary access to urgently stored information. Study of the content of the proposed version of Part 3 of Art. 159 of the CPC, which provides for the possibility of the investigator, prosecutor on the basis of his decision without a decision of the investigating judge to gain temporary access to certain types of urgently stored information, indicates that the definition of such information is quite abstract, leaving considerable room for law enforcement discretion.

Instead of Art. Art. 17 and 18 of the Convention on Cybercrime[7] clearly define the scope of such information, while distinguishing that the disclosure of information on the movement of information is an integral part and logical continuation of the procedure of urgent data retention, and therefore does not require a separate decision that ensures maximum efficiency in obtaining such data by the investigator, prosecutor.

At the same time, the procedure for submitting (Article 18 of the Convention on Cybercrime), which in its legal content and purpose is similar to such a measure of criminal proceedings enshrined in national criminal procedure law as temporary access, regulates the procedure for providing data on the type of communication service used , its technical regulations and the period of use of the service; the identity of the user of the services, postal or geographical address, telephone and other access number, information on invoices and payments, which can be obtained through an agreement or agreement on the supply of services; any other information on the location of the communication equipment that can be obtained through an service agreement.

[7] Конвенція про кіберзлочинність: ратифіковано Загоном України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

In view of this, in our opinion, such a way of resolving this issue may be more expedient. However, in this case it is necessary to take into account that temporary access should be carried out under such conditions only on the basis of the decision of the investigating judge. In our opinion, such a more accurate implementation of Art. 17 and Art. 18 of the Budapest Convention[8], (according to which the essence of such a convention measure as urgent storage and partial disclosure of information on the movement of information is that the telecommunications service provider who received the order of urgent storage, promptly discloses such a volume of information on traffic data), which will be sufficient to enable the identification of other providers and establish a "route" of communication), will increase the effectiveness of appropriate measures.

Fourth, it is now possible to file application about criminal offenses online (for example, the system of electronic application of citizens to the National Police (in particular, cyberpolice), electronic notification of corruption offenses to NABU, the form for reporting criminal offenses on the official website State Bureau of Investigation, etc.).

Fifth, an attempt is now being made in a test mode to launch an e-CASE e-criminal justice system at the “triad” level of anti-corruption bodies (NABU, Specialized Anti-Corruption Prosecutor’s Office and the Supreme Anti-Corruption Court), which provides for:

1) online pre-trial investigation planning;

2) remote exchange of procedural documents (electronic document flow) between participants;

3) the implementation of procedural guidance online. However, the issues of integration into the system of all registers necessary for the operation of the system, as well as the possibilities of access to the system by the defense side, are still debatable and not completely resolved.

2. “Today” (those areas that can already be improved on the basis of existing regulations)

1. Determining the place of digital information and its carriers in the system of procedural sources of evidence. In light of this, it is worth noting the existence of significant plurality to address this issue in the theory of criminal procedure: from the desire to attribute this category of objects to traditional procedural sources of evidence (only documents, or only physical evidence, or both to the first and second, depending from what information has probative value in criminal proceedings) to the recognition of the urgent objective need to separate digital sources of evidence as an independent procedural source.

In the context of this discussion, we note that due to the lack of a constant connection between digital information and its physical medium, it

[8] Конвенція про кіберзлочинність: ратифіковано Загоном України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

seems difficult to deny the presence of such specific features as broadcastability (possibility of being transferred from one medium to another), multiplicity (possibility of one and that information simultaneously on different, unrelated and unconnected media), as well as variability (possibility to be deleted, fully or partially changed, etc. in the absence of direct "physical" access or without human participation using the appropriate software) [9]. Therefore, in our opinion, it is more appropriate not to try to "inscribe" digital information and its media in a constant, perhaps for several decades, the system of evidence and their procedural sources, but, given not denying its specifics, the recognition of these objects of independent evidentiary value, and, accordingly, expanding the range of procedural sources of evidence.

This issue becomes especially relevant given the emergence of completely new, intangible manifestations of evidence, such as the so-called "track of electronic-digital traces", ie the system of trace formation in the information and telecommunications network, which consists of several chronologically located and logically related records on the passage of computer information by communication lines through the switching equipment of the communication operator (s) from the computer of the offender to the computer of the victim [10].

This question necessitates, first of all, the need to clarify the legal meaning of the term "digital footprint". In this regard, it should be pointed out that there is a pluralism of approaches even to the very phrase used in the science of criminal procedure and criminalistics to denote this legal phenomenon. Thus, the analysis of various scientific publications in this perspective shows that most scientists operate with such concepts as "virtual footprint" (VA Meshcheryakov, AB Smushkin, LB Krasnova, V. Yu. Agibalov and others), "Binary trace" (VA Milashev), "electronic trace" (VB Vekhov), "digital trace" (OR Rossinskaya, IA Ryadovsky, AI Semikalenova, etc.). In our opinion, the use of the word construction "digital footprint" in this context seems more successful, because it allows to cover the various manifestations of this phenomenon and reflects its real technical nature of creation. In addition, this approach fits perfectly into the now common terminology: "digitalization" and so on. However, it should be noted that the phrase "electronic trace" is also quite accurate.

With regard to the definitions of this concept, it should also be noted the existence of a fairly large range of different views. In particular, VA Meshcheryakov defines a "virtual trace", apparently based on a broad understanding of the trace in criminology, namely as any change in the state

[9] Пашнєв Д. В. Властивості компютерної інформаціх та особливості збирання компютерних слідів. *Учен. зап. Таврич. нац. ун-та им. В. И. Вернадского. Серия «Юрид. науки»*. 2006. Т. 19 (58), № 2. С. 296-300. (С. 297-298).

[10] Электронные носители информации в криминалистике : монография / под ред. О С. Кучина. Москва : Юрлитинформ, 2017. 304 с. (С. 164).

of the automated information system associated with the crime and recorded in the form of computer information». Such traces, according to the scientist, occupy a conditionally intermediate position between material and ideal traces – on the one hand, they really exist on a tangible medium, but do not have an inseparable connection with the device by which the information was recorded, and are unstable, brings them closer to ideal traces; on the other hand, classifying virtual traces as ideal would be erroneous, because they are stored not in human memory, but on material objects[11].

It seems that the definition proposed by scientists, although consistent with the general forensic interpretation of this concept, but still too broad, especially in the context of the phrase "digital footprint", and closer to understanding the category of "digital information". In addition, commenting on the definition given by VA Meshcheryakov, it should also be noted that the place of detection of digital traces can be not only tangible but also intangible objects, such as Internet resources, a person's profile on a social network and more.

In this context, a more precise definition is proposed by OR Rossinskaya and IA Ryadovsky, who believe that the digital footprint is a forensic computer information about events or actions reflected in the material environment in the process of its occurrence, processing, storage and transfer[12]. It is also necessary to support the approach formulated by PS Pastukhov, according to which such information is followed by electronic information resulting from a criminal act, which was generated in the information environment as a consequence of the crime, ie information formed during and as a result of the crime, and not in connection with the communication between the participants in the process[13].

As an example of digital traces, researchers indicate a fairly extensive list of objects – all kinds of information recorded on media in the form of digitally encoded sequences (RAM dumps and traffic dumps, files and their parts, service information about such files, etc. – A. And Semikalenov); identification features that will uniquely identify the surveillance subscriber, telecommunication network, terminal equipment (IP address of the computer in the network, MAC address of the network equipment, e-mail address, social network identifier, bank card number, transactions made from it, telephone number , data of geolocation systems, etc. – Yu. V. Gavrilin); as well as information databases of mobile communications, credit and

[11] Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. *Издательство Воронежского государственного университета*. 2002. С. 94–119. (С. 97-98).

[12] Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике. *Аубакировские чтения: материалы Международной научно-практической конференции* (19 февраля 2019 г.). Алматы, 2019. С. 6-8. (С. 7).

[13] Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества. Автореф. дисс. … д-ра юрид. наук. М. 2015. 66 с. (С. 20).

discount cards, travel documents protected by magnetic code, personal computers connected to the Internet, electronic product tags, special chips and other similar devices (EP Ishchenko) , which are generally tangible carriers of digital information rather than digital footprints.

In order to narrow the scope of the objects, in our opinion, it is advisable to refer to the definition of "digital footprint", formulated in scientific publications in this area. In particular, it means a system of trace formation in the information and telecommunication network, consisting of several sequentially arranged and logically connected records of the passage of computer information through communication lines through the switching equipment of the communication operator (s) from computer of the offender to the computer of the victim[14]. The component tracks of digital traces were identified by VB Vekhov[15].

Finally, it should be noted that the need to take into account the specific properties of digital information (including its variety – digital tracks), namely: multiplicity, broadcastability, latency, lack of constant communication with the media, etc., requires compliance with certain rules when collecting and researching such evidentiary information in criminal proceedings. Among them are the following: (1) involvement of a specialist in carrying out procedural actions, during which relevant information may be found (search, inspection, removal of information from electronic information systems, temporary access to things and documents); (2) taking into account the restrictions regulated by para. 2 h. 1 st. 159, para. 2-4 h. 2 st. 168 of the CPC, regarding the methods of access to digital media and the exclusive grounds for their seizure; (3) given that the digital footprint track itself is not available for direct presentation and examination during the trial, it is necessary to involve an expert and conduct an examination during its collection and study (including in order to identify destroyed information, establish the facts of unauthorized access to it, its changes, distortions, etc.).

2. Expansion of legally regulated methods of forming evidentiary information in criminal proceedings. This is a significant update of the system of methods of collecting and examining evidence enshrined in the criminal procedure law. In our opinion, the introduction of point changes, such as the provision of rules on the mandatory participation of specialists in investigative (search) actions, during which the question of obtaining digital information and seizure of its media may not be able to fully respond to modern information and technological reality. It is necessary to change the view in general on the system of existing procedural actions and

[14] Электронные носители информации в криминалистике: монография/ под ред. докт. юрид. наук О. С. Кучина. Москва: Юрлитинформ, 2017. 304 с. (С. 164).

[15] Вехов В. Б. Особенности судебного компьютерно-технического исследования «дорожки» электронных следов. *Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы: сборник научных трудов II Международного форума*. Москва: Московский университет МВД России имени В.Я. Кикотя, 2019. С. 57-61. (С. 58-59).

understanding of their legal nature. In this perspective, it is also important to note a certain fragmentation and inconsistency of the proposals mentioned above. First of all, there are some provisions of the draft Law "On Amendments to Certain Legislative Acts Concerning the Implementation of the Provisions of the Convention on Cybercrime and Improving the Effectiveness of the Fight against Cybercrime"[16], according to which a search warrant automatically allows authorized persons to access electronic information systems or their parts, mobile terminals, communication systems, information (automated), telecommunication, information and telecommunication systems or integral parts of these systems, as well as the possibility of obtaining such access even in exceptional cases when they are not subject to a search permit. As will be illustrated below, this approach completely eliminates the idea of the need for double judicial review – separately on the restriction of the right to inviolability of the home or other property of a person, and separately on the restriction of the right to privacy.

To continue the research, we will use a concrete example to demonstrate situations related to possible interference in private communication as a result of actions such as search and inspection. In particular, in recent law enforcement cases, the so-called "review of the subject – digital device" (smartphone, tablet, computer, etc.) in order to detect and copy digital information stored on these media for research and use in criminal proceedings. At the same time, the investigator, removing a certain digital device (phone, computer, tablet) and examining the object, is usually not limited to visual observation of its external features (which is an examination of the object in its traditional sense), but tries to obtain information of another nature – SMS – messages, messages in Viber, Whats -up, Telegram, listen to recorded phone conversations (because some smartphones provide this feature). The nature of such actions essentially means interfering in a person's private communication, which requires mandatory judicial review. In addition, it is obvious that the examination of the object in its classical sense as a visual observation of the features of a particular material object does not correspond to the nature of the actions taken to examine the information that can be stored in the device.

Paying attention to this problem, RI Okonenko proposes to use the concept of "digital device search", because it, according to the researcher, will correspond to the nature of the investigative action, which is carried out in this case[17]. Reflecting on this perspective, AV Shilo emphasizes that since the information contained in the electronic devices seized during the

[16] Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) (реєстр. № 2740 від 15.02.2020 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1? pf3511=67884

[17] Оконенко Р. И. Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации **:** дис. …канд. юрид. наук. Москва, 2016. 158 с. (С. 120-121).

proceedings cannot be identified with the electronic device itself as its physical medium, such information is a separate object of ownership and object of the right to privacy, and therefore its withdrawal and / or copying requires obtaining a separate court decision – the decision of the investigating judge to involve an expert to conduct an examination[18]. Without denying the rationality and validity of these proposals, in our opinion, it is more appropriate to apply in this case the order of temporary access to digital information by reviewing it and copying it. Moreover, if such access requires overcoming the logical protection (ie the digital device is password protected), it is necessary to involve a specialist.

In the context of this proposal, we also support the conclusions of A. Skrypnyk on the need to adapt the experience of individual countries to domestic criminal procedure legislation on the introduction of the rule of "closed container", which would provide for two-stage judicial control over the restriction of privacy[19].

3. Changing conceptual approaches to the examination and evaluation of evidence in criminal proceedings. The modern "digital" person always has a smartphone or tablet at hand; a significant part of streets, communal and private buildings are equipped with video surveillance; cars are equipped with devices capable of recording changes in speed, time and location in space, as well as video recorders. Given this, almost any of us can potentially become a "collector" of evidence that will be important in establishing the circumstances of a criminal offense. In addition, such information in digital form, created using these gadgets, can be instantly transmitted to the Internet and posted on public sites. However, given the current regulatory issues related to the examination and evaluation of evidence, such a property as admissibility, this digital information, despite its importance and force, often can not be used as evidence in criminal proceedings.

That is why there is an urgent need to change the legislative approaches to the regulation of the procedure for verification and evaluation of evidence, the criteria of admissibility of the latter. The initial value should not be strict adherence to established, often too "formalized" rules for obtaining evidence and its media, but the technical possibility of verifying the authenticity of

[18] Шило А. В. Використання в кримінальному провадженні відомостей, отриманих у результаті проведення негласних слідчих (розшукових) дій: автореф. дис. ... канд. юрид. наук : 12.00.09; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2019. 20 с. (С. 14).

[19] Скрипник А. Правило «закритого контейнеру» в українських правових реаліях. *Кримінальний процес: сучасний вимір та проспективні тенденції : II Харк. кримінал. процесуал. полілог : присвяч. актуал. питанням застосування заходів забезпечення кримінал. провадження* (м. Харків, 12 груд. 2019 р.) / редкол. О. В. Капліна, В. І. Маринів, О. Г. Шило. Харків : Право, 2020. С. 29-31.

digital information submitted to the court for research[20]. That is, in our opinion, the primary criterion for the admissibility of the use of digital information and its media in criminal proceedings as a means of proving circumstances relevant to criminal proceedings should be the availability of technical capabilities to confirm the authenticity of such information.

This, in our opinion, causes the emergence of an urgent need to change the conceptual views on the regulation of the procedure for verification and evaluation of digital evidence. Thus, according to C.I. Kuvychkov, it is necessary to give priority to technical guarantees of verification of the authenticity of information submitted to the court, in relation to compliance with the formal requirements for the admissibility of evidence, primarily related to their recording. That is, provided that the technical capabilities allow to confirm the authenticity of electronic information, it may have probative value[21]. In light of the above, it is necessary to cite the legal position formulated in the decision of the Supreme Court of 07.08.2019 (case № 607 / 14707/17). Thus, in particular, the court of cassation agreed with the conclusion of the appellate court that the video disc from the surveillance cameras of the store, which was the basis of of the conviction by the court of first instance, is inadmissible as evidence because it was received from the victim by an unauthorized pre-trial official (by an operative) and without complying with the requirements of the criminal procedure law (outside the criminal proceedings, ie before entering information into the ERDR, as well as before inspecting the scene)[22]. This conclusion clearly illustrates the currently dominant approach - giving preference to the unconditional need to comply with the formal requirements of the procedural design of evidence over its significance, strength, weight to prove the circumstances relevant to criminal proceedings. However, it seems that, especially with regard to digital evidence, such a view should be shifted towards the possibility of verifying the authenticity of electronic information, rather than formalized requirements for its recording.

In this context, it is also worth paying attention to the main arguments against this kind of reasoning. They are usually technical in nature and come down to the fact that such information is unreliable because it is multiplicative and broadcast, and therefore easily changeable, and in some cases it is difficult to establish its authenticity, as well as to identify facts of falsification and fabrication of such information.

PS Pastukhov opposes such arguments, emphasizing that verifiability is the main property of evidence containing electronic information, because in

[20] Кувычков С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде : дисс. … канд. юрид. наук. Нижний Новгород, 2016. 273 с. (С. 13).

[21] Там само.

[22] Постанова колегії суддів Третьої судової палати Касаційного кримінального суду ВС від 07.08.2019 р. (справа № 607/14707/17). URL: http://reyestr.court.gov.ua/Review/83589933

the case of using this type of information there are significant opportunities to verify its identification and authentication using technical means, in addition to verification integrity and immutability of information on electronic media is primarily a technical task, and the subjective factor here plays a much smaller role[23]. And it is difficult to disagree with this statement, because despite the fact that digital information can indeed be changed with the help of application software, but such an intervention can just as easily be established by conducting appropriate expert research.

To continue our research, it is appropriate to turn to the analysis of the meaning of concepts that have already been used by us, but have not found their disclosure – "authentication" and "verification". A systematic analysis of domestic legislation gives grounds to state that laws and bylaws in various fields contain more than ten definitions of each of these concepts. It seems that for criminal procedural purposes, the authentication of digital evidence should be understood as the process of establishing identity of information contained in them, its origin and integrity, immutability, and under the verification of digital evidence we offer to understand their verification, research to establish the accuracy of information contained in them and confirmation of the absence of facts of its illegal change (modification).

It seems important to determine the necessary ways and means of authentication and verification of digital evidence. In light of this, we note, first of all, that the International Organization for Computer Evidence has developed some principles in this direction, namely:

(1) when working with digital evidence, all general judicial requirements and expert procedural principlesmust be observed,

(2) actions to examine the seized digital evidence should not change them,

(3) if it is necessary to provide someone with access to the original digital evidence, such person should be properly trained and instructed,

(4) all activities, with regard to confiscation (seizure), access, storage and transfer of digital evidence must be fully documented and available for inspection,

(5) the person in possession of digital evidence is fully responsible for all actions taken on this evidence[24].

Clarifying these principles, NA Zigura points to the need to comply with the following rules when checking computer information: (a) the establishment of the technical means from which such information was obtained or copied (if possible); (b) verification of compliance of the type, model, company of the manufacturer of the material carrier of computer

[23] Пастухов П.С. Модернизация уголовно–процессуального доказывания в условиях информационного общества: автореф. дис. … д-ра юрид. наук. Москва, 2015. 64 с. (С. 17, 21).

[24] Международная организация по компьютерным (цифровым) доказательствам (International Organization on Computer Evidence – ЮСЕ) (назва з екрану). URL: https://ceur.ru/library/spravochnik/katalog_kompanijj/item126250/

information with the parameters specified in the protocol of investigative action, in the conclusion of the specialist; (c) the installation of the software by which this information was obtained [25].

PS Pastukhov considers means of verification of digital proofs in detail, distinguishing the following aspects: detailed fixing in the protocol of characteristics of software (type of operating system, registration number), the computer information (file type, its volume, time of creation, time of editing) , opening time, user information), software used to ensure the integrity (immutability) of the data (this, for example, may be the principle of hashing). Thus, according to the researcher, there is a whole arsenal of verification of the reliability of electronic evidence, with a special means of verifying electronic evidence is a computer-technical examination [26].

special role for the authentication and verification of digital information is played by the so-called "chain of legal possession" ("chain of custody"). The essence of this principle is the step-by-step registration of all information about the identification properties, production, storage and movement of the file from user to user, until the study in court – and if necessary to demonstrate this to participants in the process. Thus, it is a step-by-step documentation of the identification properties of the file from the moment of its registration, translation, storage and movement from one medium to another [27] [28].

Quite interesting in the context of our work are the recommendations made in Module 4 "Introduction to Digital Forensics" (developed under the Education for Justice Initiative (E4J), which is a component of the Global Doha Declaration Drugs and Crime (UNODC), Vienna, 2019). In particular, it is proposed to divide all digital evidence into 3 groups and appropriate advice for each of these categories: 1) content generated by one or more persons (for example, e-mail text, text editor documents) – can be considered admissible evidence if it is reliable and plausible (ie it can be established that it belongs to any person); 2) content generated by a computer or digital device without the participation of the user (for example, data logs) – may be considered admissible evidence if it can be proved that the device functioned properly at the time of data generation, and if it can be shown that at the time of generation data protection mechanisms were in

[25] Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России : дис… канд. юрид. наук. Челябинск, 2010. С. 144

[26] Пастухов П.С. Средства проверки надежности «электронных» доказательств в ходе досудебного производства по уголовному делу. *Пробелы в российском законодательстве*. 2015. № 3. С.170-173. (С. 170-171).

[27] Там само. (С. 171).

[28] Галяшина Е.И. Оценка достоверности цифровых фонограмм в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве. Материалы международной научно–практической конференции, посвященной памяти доктора юрид. наук, профессора Полины Абрамовны Лупинской: сборник научных трудов. Москва : ООО «Изд–во «Элит», 2011. С. 135.

place to prevent data changes; 3) content generated by both the user and the device (for example, dynamic tables in programs such as Microsoft Excel) – must apply both of the previous rules [29].

Thus, taking into account the above tools and recommendations when using digital evidence in criminal proceedings will help to algorithmize the procedure of its verification, and it will allow to further shift the emphasis in the aspect of verification and evaluation of evidence regarding their admissibility from complying with purely formal requirements during the collection to establish the possibility of their identity and authenticity.

3. "Tomorrow" (potential "futuristic" vectors of criminal proceedings in this direction)

Jurisprudence, as well as other areas of our public life, will gradually be "filled" with digital technologies. The criminal process is not left out either, although among other procedural branches of law it still remains in a transitional stage in some issues (in particular, compared to other procedural codes, the CPC did not single out electronic evidence as an independent procedural source of evidence). At the same time, along with some issues of digitalization of criminal proceedings, which are already taken into account in domestic law, ideas for the introduction of electronic justice and improving methods of collecting and examining digital evidence during pre-trial investigation, which are permanently developed at the level of legislative activity already now, at least among scientists, "futuristic" proposals (which now seem to be something far away and fantastic), in particular on the introduction of artificial intelligence technologies in the criminal process, also are formulated.

Turning directly to the issue of artificial intelligence in criminal proceedings, we should first determine the general understanding of this concept. Thus, if we summarize the basic views on the definition of this category and try to explain its meaning in simple words, in the context of our work we can consider "artificial intelligence" as a system of methods, software algorithms aimed at solving certain problems that usually require human consciousness, human understanding. These are certain systems of knowledge processing, knowledge management, which allow to solve certain tasks, suggest possible algorithms of actions, etc.

In the future, assessing the advantages and disadvantages of introducing artificial intelligence technologies in the criminal process, it is certainly appropriate to emphasize such important positive manifestations as saving

[29] Модуль 4 ««Вступ до цифрової криміналістики» (розроблений в рамках ініціативи «Освіта для Правосуддя» (E4J), що є компонентом Глобальної програми по здійсненню Дохінской декларації, Управління Організації Об'єднаних Націй з наркотиків і злочинності (УНЗ ООН), м. Віна, 2019 р.). URL: https://www.unodc.org/documents/e4j/Cybercrime_Module_4_Introduction_to_Digital_Forensics_RU.pdf

time, human and material resources, relieving people from excessive monotonous, typical work in favor of increasing attention to creative tasks, justification key procedural decisions that require evaluation based on internal conviction, etc. At the same time, among the disadvantages or risks of the introduction of artificial intelligence, we can pay attention to some problems associated with possible bias, discrimination arising from the underlying algorithms of artificial intelligence technologies. For example, the situation with the violation of ethical norms by the algorithms used in the COMPAS program when assessing the risks of recidivism by defendants by the US courts is well known in the light of the issue under consideration. In particular, there is racial bias, where the algorithm is twice as likely to label defendants who were African-Americans as recidivists, while whites were usually identified as low-risk individuals [30].

In this context, attention should be paid to certain legal guidelines that have already been established. In particular, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was adopted, ratified by Ukraine on 06.07.2010[31], as well as the Convention on Cybercrime, ratified on 07.09.2005[32]. At the same time, these international documents concern, first of all, the general use of digital technologies and digital evidence in criminal proceedings. Instead, the key standards for the introduction of artificial intelligence in the judiciary, including criminal, are defined in the European Charter of Ethics for the use of artificial intelligence in judicial systems and the realities around them (adopted by the European Commission on Justice Efficiency on 3–4 December 2018 in Strasbourg)[33].

The analysis of this document gives grounds to single out the basic principles of using artificial intelligence technologies in justice, namely:

(1) the principle of observance of fundamental human rights – the use of relevant technologies must comply with the fundamental rights guaranteed, in particular, by the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. That is, artificial intelligence-based technical

[30] Штучний інтелект у правосудді. *Центр демократії та верховенства права.* URL: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/

[31] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: ратифікована Україною 06.07.2010 р. *Законодавство України*: база даних / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

[32] Конвенція про кіберзлочинність: ратифікована законом № 2824-IV 07.09.2005 р. *Законодавство України*: база даних / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

[33] Європейська етична хартія використання штучного інтелекту в судових системах та реаліях, що їх оточують (прийнята Європейською комісією з ефективності правосуддя 3-4 грудня 2018 р. у м. Страсбург). URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4

means should in no way impede access to justice and the right to a fair trial, and their application should be fully in line with the rule of law and the independence of the judiciary;

(2) the principle of inadmissibility of discrimination – means that when processing certain data according to established algorithms, the methods of analysis used should not deepen inequality, for example, by taking into account purely racial, ethnic, religious, genetic data. Neutralization of such risks should take place by providing for measures aimed at adjusting, increasing the level of intervention of stakeholders in the establishment of such facts of discrimination;

(3) the principle of quality and security – it is, first of all, the use of certified data sources that allow maintaining the confidentiality of personal data, prevent attempts to illegally interfere with the right to privacy and unlawful alteration of data entered into the system and processed by it;

(4) the principle of implementation "under the control of the user" – it is the person who should be informed in detail about the results of data processing and should be responsible for the results of decisions. Also in the light of this principle, it should be possible at any time to review the judgment and the data used to obtain the outcome of the case;

(5) the principle of openness, impartiality, transparency – provides for the possibility of external audit at the stages of development, design, implementation and operation of artificial intelligence technologies. However, it should be noted that the implementation of this principle is perhaps the most difficult, as it requires finding a reasonable balance between its action and guaranteeing the intellectual property rights of developers, the need to protect trade secrets[34].

Based on the above, we outline the main vectors of possible introduction of artificial intelligence technologies in the criminal process:

– assessment of prospects, ie forecasting possible court decisions based on the analysis of similar situations that have already taken place and have been resolved;

– automation of drafting basic procedural documents or their parts, when there is no need to motivate or present arguments, etc.;

– consulting, in particular in the perspective of proposing optimal or acceptable (possible) algorithms of actions of participants in criminal proceedings in a particular situation;

– technicalization, automation of certain procedures in court records (namely, automatic copying of documents in the required number, their distribution to participants in the proceedings, sorting by groups / types / episodes, etc.);

[34] Європейська етична хартія використання штучного інтелекту в судових системах та реаліях, що їх оточують (прийнята Європейською комісією з ефективності правосуддя 3-4 грудня 2018 р. у м. Страсбург). URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4

– data processing and systematization in criminal proceedings;

– assessment of risks when making certain procedural decisions (for example, risks of negative behavior of a suspect, accused in case of application or non-application of a certain preventive measure in criminal proceedings) on the basis of coefficients, data on his previous behavior, data characterizing this person, etc.

Finally, we emphasize once again that the definition of promising areas for the introduction of artificial intelligence in the criminal process should be based, in our opinion, on the idea of its additional, ancillary nature, and not one that can completely replace a person, especially in key procedural decisions related to the resolution of criminal proceedings on the merits, restriction or deprivation of constitutional rights and freedoms, etc. Indeed, the "machine" can perform certain standardized, typical actions instead of a person, at the same time, creativity, creativity, empathy, ethics, justice – purely human qualities that can not be passed on to anyone.

CONCLUSIONS

In conclusion, it is worth noting that the current CPC already regulates certain aspects related to the use of digital technologies in criminal proceedings (first of all, the possibility of remote proceedings, the functioning of an automated document management system, seizure of digital media during pre-trial investigation, etc.). In addition, the test mode is currently introducing an electronic criminal system (E-case), which will further significantly optimize the time, material and human resources. However, some issues, in particular, regarding the balanced application of ensuring measures ofcriminal proceedings (temporary access to digital media, their temporary seizure and seizure), as well as the use of hardware and software in remote proceedings and the operation of electronic judicial information and telecommunications system still remains on the agenda.

In addition, given the foreign experience, as well as the settlement of these aspects in other procedural law, there is an urgent need to determine the place of digital evidence in the system of procedural sources of evidence, with further regulation of new approaches to their collection, research, evaluation, based on the peculiarities of their technical nature and the need for their authentication and verification.

As a promising direction, the possible introduction of artificial intelligence technologies in the criminal process is identified, taking into account international ethical principles, in particular, in formulating templates of standard procedural documents, systematizing materials of criminal proceedings according to various criteria, assessment of prospects for making procedural decisions and resolving the case on the merits, automatic processing of materials with their copying, mailing, etc.

SUMMARY

The paper identifies the relevance of the use of digital technologies in criminal proceedings, taking into account the state of development of Ukrainian society and legislation at the present stage with an emphasis on the gradual and inevitable digitalization of most spheres of life, including legal. It is proposed to explore three key aspects of this issue, namely: 1) to analyze those regulations that are already enshrined in the current CPC or the possibility of their implementation is already being tested in a test mode (so to speak, "yesterday"); 2) identify (especially within the issues of evidentiary law) those areas, the regulation of which has long been discussed in science, but has not yet been enshrined in the CCP ("today"); 3) outline possible further prospects for the introduction of digital technologies (primarily, artificial intelligence technologies) and criminal proceedings ("tomorrow").

Within the first aspect, attention was paid to the regulated possibility of conducting remote procedural actions, functioning of the automated court document management system, introduction of the electronic criminal case system, application of precautionary measures of criminal proceedings to digital media, etc. At the same time, the article highlights some problems that exist in resolving these issues.

Within the second vector, attention is focused on the legal nature and place of digital evidence in the system of procedural sources of evidence (in particular, and some of their types – digital footprints). In view of this, the need to change conceptual approaches to the methods of collecting and studying digital evidence, criteria for assessing their admissibility and reliability, etc. has been identified.

Finally, within the third direction, the definition of artificial intelligence is given, taking into account the provisions of international documents, the principles of its use in the judiciary (including criminal) are defined and promising vectors for the use of artificial intelligence technologies in criminal proceedings.

REFERENCES

1. Вехов В.Б. Особенности судебного компьютерно-технического исследования «дорожки» электронных следов. *Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы: сборник научных трудов II Международного форума*. Москва: Московский университет МВД России имени В.Я. Кикотя, 2019. С. 57–61.

2. Галяшина Е.И. Оценка достоверности цифровых фонограмм в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве. Материалы международной научно–практической конференции, посвященной памяти доктора

юрид. наук, профессора Полины Абрамовны Лупинской: сборник научных трудов. М.: ООО «Изд–во «Элит», 2011. С. 131–141.

3. Європейська етична хартія використання штучного інтелекту в судових системах та реаліях, що їх оточують (прийнята Європейською комісією з ефективності правосуддя 3–4 грудня 2018 р. у м. Страсбург). URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4

4. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России : дис. … канд. юрид. наук. Челябинск, 2010. 234 с.

5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: ратифікована Україною 06.07.2010 р. *Законодавство України*: база даних / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

6. Конвенція про кіберзлочинність: ратифікована законом № 2824-IV 07.09.2005 р. *Законодавство України*: база даних / Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

7. Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде : дисс. … канд. юрид. наук. Нижний Новгород, 2016. 273 с.

8. Международная организация по компьютерным (цифровым) доказательствам (International Organization on Computer Evidence – ЮСЕ) (назва з екрану). URL: https://ceur.ru/library/spravochnik/katalog_kompanijj/item126250/

9. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. *Издательство Воронежского государственного университета*. 2002. С. 94–119.

10. Модуль 4 «Вступ до цифрової криміналістики» (розроблений в рамках ініціативи «Освіта для Правосуддя» (E4J), що є компонентом Глобальної програми по здійсненню Дохінской декларації, Управління Організації Об'єднаних Націй з наркотиків і злочинності (УНЗ ООН), м. Віна, 2019 р.). URL: https://www.unodc.org/documents/e4j/Cybercrime_Module_4_Introduction_to_Digital_Forensics_RU.pdf

11. Оконенко Р.И. Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дис. … канд. юрид. наук. Москва, 2016. 158 с.

12. Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества : автореф. дисс. … д-ра юрид. наук. Москва, 2015. 66 с.

13. Пастухов П.С. Средства проверки надежности «электронных» доказательств в ходе досудебного производства по уголовному делу. *Пробелы в российском законодательстве*. 2015. № 3. С. 170–173.

14. Пашнєв Д.В. Властивості компютерної інформаціх та особливості збирання компютерних слідів. *Учен. зап. Таврич. нац. ун-та им. В. И. Вернадского. Серия «Юрид. науки»*. 2006. Т. 19 (58), № 2. С. 296–300.

15. Постанова колегії суддів Третьої судової палати Касаційного кримінального суду ВС від 07.08.2019 р. (справа №607/14707/17). URL: http://reyestr.court.gov.ua/Review/83589933

16. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) (реєстр. № 9484 від 17.01.2019 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65354

17. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження) (реєстр. № 2740 від 15.02.2020 р.). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67884

18. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам (реєстр. №4003 від 01.09.2020 р.). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69770

19. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів (реєстр. № 4004 від 01.09.2020 р.). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771

20. Россинская Е.Р., Рядовский И.А. Концепция цифровых следов в криминалистике. *Аубакировские чтения: материалы Международной научно-практической конференции* (19 февраля 2019 г.). Алматы, 2019. С. 6–8. (С. 7).

21. Скрипник А. Правило «закритого контейнеру» в українських правових реаліях. *Кримінальний процес: сучасний вимір та проспективні тенденції : II Харк. кримінал. процесуал. полілог : присвяч. актуал. питанням застосування заходів забезпечення кримінал. провадження* (м. Харків, 12 груд. 2019 р.) / редкол. О.В. Капліна, В.І. Маринів, О.Г. Шило. Харків : Право, 2020. С. 29–31.

22. Шило А. В. Використання в кримінальному провадженні відомостей, отриманих у результаті проведення негласних слідчих (розшукових) дій : автореф. дис. ... канд. юрид. наук : 12.00.09; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2019. 20 с. (С. 14).

23. Штучний інтелект у правосудді. *Центр демократії та верховенства права.* URL: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/

24. Электронные носители информации в криминалистике: монография / под ред. О.С. Кучина. Москваа : Юрлитинформ, 2017. 304 с.

Information about the author:
Krytska Iryna Oleksandrivna,
orcid.org/0000-0003-3676-4582
Candidate of Law,
Associate Professor at the Department of Criminal Procedure
Yaroslav Mudryi National Law University
77, Pushkinska str., Kharkiv, 61024, Ukraine