MELNICHUK R. V.,
Candidate of Legal Sciences,
Associate Professor at the Department of
(State and Legal Disciplines European University)

УДК 343.13:004(477)
DOI https://doi.org/10.32842/2078-3736/2025.4.2.30

CURRENT ISSUES OF DIGITALISATION OF CRIMINAL PROCESS IN UKRAINE

The article focuses on the current prospects and peculiarities of introduction of digital tools and technologies into the criminal process in Ukraine. Digitalisation of the criminal process is a significant step forwards the development of legal system of the state; nevertheless, it also entails a number of legal and practical aspects that require careful analysis. The introduction of digital technologies in criminal proceedings raises many issues related to efficiency, protection of the participants' rights in criminal process and compliance with the principles of a fair trial. Due to the special role of criminal process in the system of Ukrainian law that becomes even more important during a full-scale war in Ukraine, the introduction of electronic and digital innovations is accompanied by a high degree of risks; and, therefore, their implementation in practice requires significant theoretical and legal understanding, appropriate level of technical equipment and use of empirical experience gained by borrowing ready-made working digital tools of criminal process, used in foreign countries as well.

At the same time, arbitrary and meaningless digitalisation of criminal process without taking into account its nature and inherent features, increases the risk of miscarriages of justice, the number of incorrectly resolved cases and human rights violations. The article examines the main areas for the introduction of digital technologies into pre-trial and trial proceedings in criminal process in Ukraine. The author identifies the main prospects for the transition to digital criminal process, outlines the problems of this process and formulates proposals for overcoming them.

Key words: *digitalisation, digital technologies, criminal procedure, electronic evidence, information and communication technologies, cybersecurity, criminal proceedings, electronic criminal procedure, Criminal Procedure Code of Ukraine.*

Мельничук Р. В. Сучасні проблеми цифровізації кримінального процесу в Україні

Стаття присвячена дослідженню сучасних перспектив та особливостей запровадження цифрових інструментів та технологій у сферу кримінального процесу в Україні. Цифровізація кримінального процесу є значним кроком вперед у розвитку правової системи держави, проте вона також тягне за собою низку правових та практичних аспектів, які вимагають уважного аналізу. Впровадження цифрових технологій у кримінальний процес порушує багато питань, пов'язаних з ефективністю, захистом прав учасників процесу та дотриманням принципів справедливого суду. Через особливу роль кримінального процесу в системі українського права, яка стає ще більше важливою під час повномасштабної війни в Україні, запровадження електронних і цифрових нововведень супроводжується високим ступенем ризиків, у зв'язку з чим їхнє втілення в практичну діяльність вимагає суттєвого теоретичного правового осмислення,

відповідного рівня технічного оснащення та використання емпіричного досвіду, здобутого шляхом запозичення вже готових робочих цифрових інструментів, які використовуються в кримінальному судочинстві в тому числі й в зарубіжних країнах.

Водночас, довільна та беззмістовна цифровізація кримінально-процесуальної діяльності без урахування її природи, притаманних їй особливостей збільшує ризик судових помилок, кількості неправильно вирішених справ та порушень прав людини. У статті розглянуто основні напрями для запровадження цифрових технологій у досудове та судове провадження у кримінальному процесі України. Визначені основні перспективи переходу до цифрового кримінального процесу, окреслено проблеми цього процесу та сформульовано пропозиції щодо їх подолання.

Ключові слова: *цифровізація, цифрові технології, кримінальний процес, електронні докази, інформаційно-комунікаційні технології, кібербезпека, кримінальне провадження, електронний кримінальний процес, Кримінальний процесуальний кодекс України.*

Introduction. In many countries of the world the practice of investigating criminal offences is based on the systematic integration of modern technologies into the criminal process and, in particular, into judicial proceedings. The use of the latest technical means in criminal proceedings is gradually being introduced. Technological progress and digitalisation of most spheres of the modern state and society activity accelerates promising changes in the field of criminal process legal relations. The acceleration of the relevant modern digital transformations was facilitated by the rapid spread of the coronavirus pandemic in 2020. Therefore, it is not surprising that the current stage of development of our society is already fully connected with the use of information technology.

It should be noted that Ukraine has been creating conditions for the effective work of state bodies for some time now; and the electronic document management system has been operating for quite some time, which has had a positive impact on the speed of receiving information by the addressee and making appropriate decisions. However, the prospects for the use of information and communication technologies in the activities of judicial institutions are of particular interest, as these state bodies apply the law to ensure the rights of individual subjects of law and society as a whole. In Ukraine, electronic innovations within the criminal process are of particular interest, given its importance for the state and the public as an effective means used to bring people to criminal liability for committing socially dangerous acts.

The scientific literature has already considered various aspects of digitalisation of criminal process, for example, such scholars as V.Y. Chumachenko, N.V. Hlynska, D.I. Klepka, O.I. Marochkin, L.V. Milimko, M.I. Pashkovskyi, N.M. Senchenko, V.V. Shablystyi, Y.V. Zhydovtsev, and other scholars have already studied the peculiarities of implementation of digitalisation of criminal process in Ukraine and in the world. The analysis of existing studies shows that digitalisation of criminal process can significantly increase its efficiency, although, it also poses new challenges to the legal system.

Purpose statement of the research paper is to identify and analyse the current problems of introducing digitalisation into criminal process and to develop recommendations for their elimination. The study aims to formulate proposals for improving the legal regulation of criminal process relations due to regard for current challenges and trends in the field of criminal justice.

Main part of the research paper. Digitalisation processes are increasingly affecting justice systems around the world. A number of countries are actively implementing e-justice and e-case systems. Information technologies are emerging in various areas of the judiciary. The positive impact of such technologies on the judicial system has been repeatedly recognised by many researchers both in Ukraine and abroad. According to the modern Ukrainian authors of the monographic study ‘Conceptual Foundations of Digitalisation of Criminal Proceedings in Ukraine’,

‘digitalisation of criminal process is a multidimensional concept, which in the operational sense is both a process of reasonable introduction (reasonable equipment) of digital and IT into the criminal procedural form, accompanied by adaptation of criminal proceedings to the specifics of the digital environment and the specifics of cybercrime investigation, while maintaining the necessary balance between increasing the efficiency in investigation and trial and ensuring the rights and legitimate interests of individuals in this area. The digital transformation of criminal process is a natural result of the process of digitalisation of criminal proceedings, the qualitative certainty of which is characterised by a certain level of transformation of criminal proceedings due to the transition to new ways of operating using digital technologies, adaptation to the specifics of the digital environment (digital information)’ [3, p. 443]. At the same time, the authors rightly note that ‘the acceleration of this process is due to a combination of diverse circumstances, including socio-political, regulatory, criminogenic, and praxeological ones. These factors are elements of their multidimensional system, which not only contribute to accelerating the process of digital transformation of national criminal justice, but also actualise the implementation of a conceptual study of digitalisation of criminal proceedings. The quarantine restrictions imposed during the Covid-19 pandemic; the fact that Ukraine is under martial law; acceleration of Ukraine's European integration are clear factors in the actualisation of digitalisation of criminal proceedings of a social and political nature’ [3, p. 442].

The digitalisation era of criminal process in Ukraine began in 2021 with the adoption of the Law of Ukraine ‘On Amendments to the Criminal Procedure Code of Ukraine on the Introduction of the Information and Telecommunication System of Pre-trial Investigation’ No. 1498-IX, which defined the procedure for the functioning of ‘a system that ensures the creation, collection, storage, search, processing and transmission of materials and information (data) in criminal proceedings’[7]. This system was used to digitise all criminal proceedings entered into the Unified Register of Pre-trial Investigations after 15 December 2021, which was a global step towards a full-fledged electronic criminal process in Ukraine. At the same time, the ‘iCase’ information and telecommunication system for pre-trial investigation was created having similar functions; and its main task was to ‘create a single electronic space for the system's subjects, which stores materials and information on criminal proceedings’[6]; to ensure interaction with other systems and collect accurate analytical data [6]. According to V.V. Shablystyi, ‘the functioning of the ‘iCase’ IT system of pre-trial investigation contributes to significant automation of pre-trial investigation processes in general, as well as individual procedures related to organisational, managerial, analytical, information and telecommunication and other needs of the system users. This, in particular, has facilitated the defence's access to the criminal proceedings in accordance with the Article 221 of the Criminal Procedure Code of Ukraine [4] (hereinafter – the CPC of Ukraine) [4], and will allow the investigating judge to promptly consider motions and complaints of the parties to the proceedings at the pre-trial investigation stage within a reasonable time, without the need to physically request materials from the pre-trial investigation body or the prosecutor's office, which significantly saves time’ [10, p. 631]. At the same time, the practice of using the ‘iCase’ system based on the experience of electronic interaction between the National Anti-Corruption Bureau of Ukraine, the Specialised Anti-Corruption Prosecutor's Office and the High Anti-Corruption Court of Ukraine has revealed a number of problems, namely: ‘1) not all criminal proceedings are included in the ‘iCase’ system, which is why some motions are filed in paper form; 2) there is a limited possibility to file other types of motions with the investigating judge; 3) there is no possibility of electronic interaction between the defence and the prosecution; 4) there are problems with the integration of the ‘iCase’ system with higher courts’[2].

Along with the problems with the information content and technical support of electronic criminal justice systems, it is worth highlighting the issue of imperfect legal regulation of criminal procedural relations, as well as disagreements over how new technologies should be integrated into the criminal process in order not to violate human rights and fair trial guarantees. One of the key issues in the application of digital criminal proceedings is the use of electronic evidence. With the advent of digital technologies, there is a need to define the legal status of such evidence,

its admissibility, and to determine how it can be presented in court. It is especially important to emphasise the importance of enshrining in the legislation the entire range of definitions related to this institute of criminal process law. We are talking about such terms as 'electronic evidence', 'electronic media', 'digital evidence' and a number of others. These innovations are fully justified in the context of digitalisation of the criminal process, especially since the relevant conceptual apparatus is already widely used in provisions of other branches of Ukrainian legislation. It is known that 'in 2017, the Civil Procedure Code, the Commercial Procedure Code and the Code of Administrative Procedure of Ukraine were amended to include 'electronic evidence' as a means of proof. The adoption of the Law of Ukraine 'On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine 'On Electronic Communications' to improve the efficiency of pre-trial investigation 'in hot pursuit' and 'countering cyber attacks' No. 2137-IX dated 15 March 2022 has significantly improved the legal regulation of the process of proving with the help of electronic evidence' [9, p. 2]. For example, the Article 100 of the Civil Procedure Code of Ukraine states that '1. Electronic evidence shall mean the information in 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 form. Such data can be stored, in particular, on portable devices (memory cards, mobile phones, etc.), servers, backup systems, other places of data storage in electronic form (including the Internet). 2. Electronic evidence shall be submitted in the original or in an electronic copy certified by an electronic digital signature, equated to a handwritten signature under the Law of Ukraine 'On Electronic Digital Signature'. The law may provide for a different procedure for certifying an electronic copy of an electronic evidence' [11]. At the same time, scholars L.V. Milimko and Y.V. Zhydovtseva propose to understand 'the concept of 'electronic evidence in criminal proceedings' as information about the facts and circumstances of criminal proceedings, which is recorded in electronic form and considered to be different from evidence in electronic form; obtained in the manner prescribed by the criminal process legislation. The forms of displaying information in electronic evidence (sources of electronic evidence) are characterised by diversity and are not sustainable sources due to the intensive development of information technology' [5, p. 306-307]. At the same time, the scholars propose to highlight the characteristic features that distinguish electronic evidence from other evidence in the criminal justice system: 'a) information in electronic (digital) form; b) this information is reflected in the form of electronic documents or other visually expressed forms – text, multimedia and voice messages, in the form of metadata, databases and other data in electronic form; c) such information is stored on memory cards, mobile phones, servers, backup systems (USB flash drives, hard drives (external hard drives), etc.); c) it can be either created by a person or generated automatically; d) it moves freely in the electronic network; e) it requires a specific procedure for collection, verification and evaluation' [5, p. 307].

Modern criminal law doctrine has also formed the idea that 'electronic evidence in criminal process can be defined as factual data obtained in accordance with the procedure provided for by the CPC of Ukraine, which exist in electronic (digital) form, recorded on electronic (digital) media and used to establish the circumstances to be proved in criminal process. The proposed definition focuses on the criminal procedural aspects of the use of electronic evidence and does not contain a significant technical terminology component, which is obviously the subject of research in other fields of knowledge. It seems appropriate to separate electronic evidence into a separate procedural source. According to the essential features, electronic evidence can be classified as follows: 1) by status, electronic evidence can be divided into originals, duplicates and copies; 2) by degree of protection, electronic evidence can be divided into objects with general access and objects with restricted access; 3) by location, electronic evidence can be divided into objects, located in computer, smartphone, tablet, in the Internet space, etc.; 4) by form, electronic evidence can be divided into files containing video, audio, photos, text, graphic images, information in another form, etc; 5) according to the procedure of creation, electronic evidence can be divided into objects, created by a person and objects, formed as a result of the execution of technical devices by the laid down

algorithms; 6) according to the presence of changes in electronic evidence, one can distinguish objects that exist in their original form and objects that have been amended; 7) according to the content of data in electronic evidence, one can distinguish basic and metadata'[3, c. 446-447].

In addition, the authors N.M. Senchenko and V.Y. Chumachenko note that 'in the context of Ukraine's aspiration to become a full member of the European Union, the adoption of EU regulations on electronic evidence will play an important role in ensuring effective cross-border cooperation among the Member States in criminal matters' [9, p. 9], pointing to the Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 and the Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023.

In view of mentioned above, it can be assumed that Ukrainian legislation needs to be updated and improved in order to ensure its compliance with the modern realities of the digital world. The legislator should take into account new technologies and their impact on the criminal process, as well as the necessity to develop clear rules on the admissibility of electronic evidence, data protection and the use of new technologies. This will create a more transparent and efficient justice system. The development of digital technologies will require significant reform of criminal process legislation in the near future. The following measures should be taken to improve the legal regulation of digitalisation relations in criminal process:

1. Developing clear legal rules on electronic evidence, a separate procedure for collecting, storing and presenting electronic evidence in court, and set requirements for its authenticity and integrity;

2. Introducing to the Article 3 of the CPC of Ukraine 'Definition of the main terms of the Code' [4] concepts that would reveal the meaning of the terms 'electronic document', 'electronic/cloud servers', 'electronic storage medium', 'criminal case format', 'electronic criminal case', as well as other definitions that may be used in electronic criminal process;

3. Amending the current criminal procedure legislation to include clear and understandable regulatory provisions on the use of digital technologies;

4. Identifying the problematic provisions of criminal process that can be resolved through the emergence of modern digital technologies. Unfortunately, today many provisions of the CPC of Ukraine do not allow for the use of fully accessible technologies that do not require global technological developments. The refusal to use the possibilities of video communication is often not a consequence of limited digital capabilities, but a direct result of the gaps in the criminal procedure law;

5. Considering the issue of regulating the procedure for the admissibility of electronic evidence at the legislative level. Regulatory consolidation of such a procedure will contribute to the formation of a unified opinion of both theorists and practitioners on the admissibility of electronic evidence. This step will undoubtedly have a significant impact on the quantity and quality of evidence, expand the possibilities of proof and have a positive impact on law enforcement practice. Therefore, "the topical issues of using electronic evidence in criminal proceedings, in terms of determining the requirements for them, are: 1) peculiarities of the procedural form of collecting electronic evidence to ensure its admissibility; 2) peculiarities of recording criminal proceedings in connection with the use of electronic evidence; 3) peculiarities of storing electronic evidence to ensure its admissibility; 4) peculiarities of studying electronic evidence by the court; 5) peculiarities of determining the status of electronic evidence (original, duplicate, copy); 6) peculiarities of studying the material carrier of electronic evidence; 7) peculiarities of assessing the weight of electronic evidence in criminal proceedings; 9) peculiarities of assessing the admissibility of electronic evidence in the investigation of certain categories of criminal offences and in certain criminal proceedings; 10) peculiarities of using electronic evidence obtained with the use of a computer polygraph; 11) peculiarities of determining the sufficiency of evidence in the assessment of electronic evidence' [3, c. 447]

Thus, in the process of harmonising criminal procedure legislation, it is important to ensure the protection of the rights of suspects, accused and victims by ensuring that electronic evidence is accumulated and processed in accordance with established norms and standards. At any historical stage of society's development, legislation must respond in a timely manner to the changes taking

place in it, meet modern needs and be mobile. Innovations caused by the development of information progress are necessary for a more complete reflection of existing social relations in the rules of law, and for the establishment of a unified legal regime for the use of the latest developments in law enforcement practice.

Another important aspect that requires attention is cybersecurity. As the volume of data processed in criminal proceedings increases, so the threat of information leakage or forgery does. The legal system must be prepared to ensure the protection of personal data and prevent cyberattacks, which requires the development of new norms and standards.

Unequal access to digital technology opportunities, especially in the context of martial law in Ukraine, is another serious challenge for the legal system and citizens. Access to modern technologies may be limited among certain groups of the population in the temporarily occupied territories and in the regions of hostilities, which creates the risk unequal opportunities in the criminal process, when some participants have advantages due to access to resources or a higher level of technological awareness.

Conclusions and proposals. In view of mentionrd above, it should be noted that the following conditions must be met on the way to introducing digitalisation in criminal process:

1. Improvement of the current regulatory framework in the direction of legislative definition of electronic documents (evidence) in criminal process; a clear list of their mandatory features, details, determination of their status and place in the system of evidence; development of uniform rules and procedures for handling electronic evidence, its seizure and use; as well as amendments to the CPC of Ukraine in terms of disclosure of the content of the main terms of electronic criminal procedure;

2. Readiness of participants of the criminal process relations to use the latest technologies and ensure resource access to digital systems. It is logical to provide for measures to ensure equal access to digital resources for all categories of citizens, including people with disabilities, in order to avoid discrimination in criminal process;

3. High-quality material and information technology support for electronic systems of digital criminal process (digitisation of documents, proper functioning of software, elimination of cyber threats, granting/restricting access rights, etc.) to secure the processing and protection of personal data of participants in criminal process. It is important to develop and implement security standards for judicial systems to protect the data of participants in the process from information loss and cyberattacks;

4. Establishment of independent monitoring bodies to control the observance of the rights of participants in the criminal process in the context of digitalisation, which will monitor the use of digital technologies and ensure the protection of human rights.

The introduction of digital technologies in criminal proceedings should in no way create a threat of possible violation of human rights and freedoms. At the same time, digital technologies are designed to facilitate (and they do facilitate) the detection of events, circumstances of a particular offence and the receipt of possible electronic evidence. In the long run, the use of digital technologies will lead to more efficient and faster implementation of the rights and freedoms guaranteed by law through simplified judicial procedures.

References:

1. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н.В. Глинської; НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса. Нац. акад. прав. наук України. Харків : Право. 2024. 452 с.

2. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 10.07.2025).

3. Мілімко Л.В., Жидовцев Я.В. Електронні докази в кримінальному судочинстві України. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* Випуск 88: частина 3. 2025. С. 302-308. DOI https://doi.org/10.24144/2307-3322.2025.88.3.45.

4. Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування : Закон України від 01.06.2021 р. № 1498-IX. URL: https://zakon.rada.gov.ua/laws/show/1498-20#Text (дата звернення: 10.07.2025).

5. Про інформаційно-телекомунікаційну систему досудового розслідування "іКейс": Наказ Національного антикорупційного бюро України, Офісу Генерального прокурора, Вищого антикорупційного суду, Ради суддів України від 15.12.2021 р. № 175/390/57/72. URL: https://zakon.rada.gov.ua/laws/show/v0390886-21#Text (дата звернення: 10.07.2025).

6. Сенченко Н.М., Чумаченко В.Ю. Електронні докази у кримінальному провадженні: досвід реалізації у зарубіжних країнах. *Академічні візії.* 2025. Випуск 42. С. 1–10. DOI: https://doi.org/10.5281/zenodo.15395747.

7. Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV. URL: https://zakon.rada.gov.ua/laws/show/1618-15?lang=en (дата звернення: 10.07.2025).

8. Шаблистий В.В. Цифрова ера кримінального процесу: можливості іт-систем у досудовому розслідуванні. *Юридичний науковий електронний журнал*. 2025. №1. С. 630-633. DOI https://doi.org/10.32782/2524-0374/2025-1/146.

9. Як працює система електронного кримінального провадження "іКейс". *Укрінформ*. URL: https://www.ukrinform.ua/rubric-polytics/3902652-ak-pracue-sistema-elektronnogo-kriminalnogo-provadzenna-ikejs.html (дата звернення: 10.07.2025).

10. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. *EUR-Lex.* URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:32023L1544 (дата звернення: 10.07.2025).

11. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceeding. *EUR-Lex.* URL: https://eurlex.europa.eu/eli/reg/2023/1543/oj (дата звернення: 10.07.2025).

Дата першого надходження рукопису до видання: 19.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 26.09.2025