ELECTRONIC EVIDENCE IN ADMINISTRATIVE PROCEEDINGS: LEGAL REGULATION, POWERS OF THE JUDGE AND FOREIGN EXPERIENCE

МАЦЕЛИК Тетяна Олександрівна - доктор юридичних наук, професор, професор кафедри фінансового та податкового права Державного податкового університету Міністерства фінансів України
ORCID https://orcid.org/0000-0003-0354-4663
УДК 347.956/958:347.961(477)
DOI: https://doi.org/10.71404/LAW.UA.2024.4.38

The features of the application of electronic evidence in administrative judicial proceedings (legal regulation, judicial powers and foreign experience) are considered. Taking into account the recommendations of the Council of Europe and positive foreign experience regarding electronic evidence in administrative proceedings, for example, the United States of America, the United Kingdom of Great Britain, the Republic of Poland, the French Republic, the Federal Republic of Germany, the Caribbean countries, the Pacific States, Lithuania, and Turkey, the main areas of borrowing positive foreign experience for Ukraine are identified: ensuring compliance of electronic evidence with the right to a fair trial, which is enshrined in Article 6 of the European Convention on Human Rights; creating standards for electronic evidence that will establish requirements for the implementation and functioning of information management systems, including storage and transfer of information; to introduce the use of artificial intelligence in the consideration of administrative cases, which can be based on repetitive models of factual scenarios and legal classification of disputes, or at least for data analysis, regarding the presence or absence of a signature, and consideration of the claim in its absence, i.e. return, since it was filed through the e-judicial system in a manner not foreseen by law; ensuring compliance with the principle of the rule of law and the inadmissibility of accepting electronic evidence that was obtained illegally; to introduce the storage of electronic evidence using the latest methods, namely replacing cybersecurity agencies, timestamp certification with a blockchain system, since printing, blocking cloud or server storage - depend on the actions of the operator or administrator; to adopt model legislation on electronic evidence; to take into account the position set out in the Recommendations of the Committee of Europe that courts should not deny the legal force of electronic evidence only because it does not contain an electronic signature; state bodies must ensure the confidentiality of personal data, and provide measures for their preservation, etc.

Keywords: judicial discretion, judicial judgment, discretionary powers, internal conviction, administrative-legal principles, judge's competence, judge's powers, administrative court, administrative proceedings, judge, judicial power, electronic evidence.

Electronic evidence is a relatively recent addition to the means of evidence in legal proceedings. Indeed, in order to correctly assess the possibility of using electronic evidence, it is necessary to know its features and characteristics. Most electronic gadgets are now permanently or periodically connected to other digital devices or networks (internal or Internet). Traces of created files and history logs can form a large volume of electronic evidence [1, p. 16].

The collection of electronic evidence is relevant in all types of legal proceedings. State authorities have powerful legal capabilities to collect the necessary evidence, including electronic [2, p. 220]. The functioning of the national system of administrative justice has certain features that distinguish it from other types of legal proceedings. The pur-

pose of administrative justice is to effectively protect the rights, freedoms and interests of individuals, the rights and interests of legal entities from violations by subjects of government authority [3]. Therefore, individuals and legal entities are not on equal terms with the state in obtaining and using the necessary electronic evidence to protect their rights and interests.

Samonova V. notes that the issue of the role of electronic communication technologies in the relationship between government and society is acute in the era of their rapid development. At the same time, there is a rapid comprehensive transfer of the results of state activity into electronic form [4, p. 727].

Polishchuk M. notes that the opposing parties in administrative proceedings are state authorities and local government bodies, on the one hand, and individuals and legal entities, on the other. To protect their interests, the parties use a variety of evidence, including electronic evidence. In this regard, public need prompted the legislative consolidation of electronic evidence. It is expected that electronic evidence in legal proceedings will soon become the only type of evidence [5, p. 125].

But in scientific research, the issues of foreign experience of the activities of subjects of authority regarding the use of electronic evidence in administrative proceedings are revealed superficially and require deepening.

Highlighting previously unresolved parts of the general problem, to which the specified article is devoted. The conducted analysis of scientific works allows us to determine that the issues of foreign experience of the activities of subjects of authority regarding the use of electronic evidence in administrative proceedings have not been resolved at a sufficient level and require further research in terms of improving the features of foreign experience of the activities of subjects of authority regarding the use of electronic evidence in administrative proceedings and solving urgent problems in this area of administrative legal relations.

The article is aimed at substantiating the model, generalizing the principles and outlining the main directions of improving the activities of subjects of authority regarding the use of electronic evidence in administrative proceedings.

In many countries, there are no clear existing rules of evidence under which electronic evidence can be authenticated and presented. In the United States, judges make discovery and presentation decisions based on established frameworks. Similarly, in some developing countries, courts have used existing law, practice, and case law to regulate the admissibility of electronic evidence. But in most developing countries, without such a clear framework, courts have been hesitant to do so. In the United States, discovery of electronic evidence is governed by the general provisions of the Federal Rules of Civil Procedure (in federal court) related to discovery and by each state's own rules of civil procedure for cases in state courts. With respect to discovery in civil cases, the FRCP (34) allows one party to search for electronic documents (email, documents on a server, text messages, voicemail, documents stored locally or on a laptop). The admissibility of electronic evidence in federal court is governed by the Federal Rules of Evidence (e.g., regarding authentication/storage), again by the relevant state courts.

In legal proceedings, electronic evidence generally means evidence that is stored in electronic form by or on behalf of a service provider at the time of its request and consists of: signatory data, access data, transaction data, and content data [6, p. 163]. In this regard, the Committee of Ministers of the Council of Europe emphasizes the need for an appropriate and secure method of collecting electronic evidence, since the risk of destruction or loss of this type of evidence is significantly higher than that of non-electronic evidence, and therefore it is necessary to develop a specific procedure for collecting and seizing electronic evidence.

Evidence in electronic or printed form is another type of independent, complete evidence that can be used in administrative proceedings [7, p. 27].

On 30 January 2019, the Council of Europe adopted the first guidelines on elec-

tronic evidence in civil and administrative proceedings.

An essential document to the Guidelines is the Explanatory Memorandum, which explains the provisions of the Guidelines and discloses the sources used in the Recommendations. The purpose of this document is to determine whether the Recommendations need to be revised.

The reason for adopting the guidelines was that courts and administrative authorities deal with electronic evidence submitted by parties and other persons involved in civil or administrative proceedings on a daily basis [8].

The Recommendations state that the Guidelines should be designed in such a way as to enhance the efficiency and quality of justice. This is particularly important since the rules on electronic evidence adopted so far in the member states do not focus sufficiently on procedural guarantees, but rather on the efficient resolution of disputes in a cost-effective manner. This is a challenge to ensure that the rules on electronic evidence are consistent with the right to a fair trial, as set out in Article 6 of the European Convention on Human Rights. It is important that the guidelines contribute to more effective access to justice [9, p. 7].

A new challenge is the rapid emergence of artificial intelligence (AI). AI is a broad area of ICT technology that allows for the automation of reasoning. This allows for automated decision-making. In practice, this means that many civil and administrative processes based on lengthy court work can be automated. It can be based on repeatable models of factual scenarios and legal classification of disputes. AI components are currently being implemented in judicial systems, in particular in relation to data analysis [11].

The guiding principle of the Guidelines is the rule of law and the inadmissibility of electronic evidence that has been obtained unlawfully (e.g. as a result of a breach of confidentiality or data) [12].

An example is the seizure of an electronic device without a court order, as provided for by law, as well as evidence obtained by a party by hacking into an IT system. For example, the case law of the ECtHR has shown that evidence collected as a result of an employer's violation of the principles of protecting the employee's privacy may be inadmissible due to a violation of the principle of proportionality. In the landmark case of Bărbulescu v. Romania, the Grand Chamber of the ECtHR found that the Romanian courts, when reviewing an employer's decision to dismiss an employee after checking his electronic messengers, failed to strike a fair balance between the employee's right to respect for his private life and correspondence and the employer's right to take measures to ensure the smooth operation of the company [8].

However, a complex issue arises when electronic evidence is collected without the knowledge or recognition of the person, but it shows that the person committed a crime. In the case of López Ribalda and Others v. Spain, the Grand Chamber of the ECtHR found that the surveillance of employees using hidden cameras (of which the employees were unaware) was compatible with the right to private life, since the video recording was used only to search for those responsible for the loss of goods from the shop and to apply disciplinary measures to them [9].

Conclusions. It was found that none of the 47 Council of Europe member states has regulatory rules on the procedure for obtaining electronic evidence. Polish law does not provide for the definition of any type of "electronic evidence" in all types of proceedings. In Turkey, the Code of Administrative Procedure also does not provide for separate rules on the procedure for submitting electronic evidence. Croatia, the Czech Republic, Estonia, Greece, Romania and Serbia provide for the obligation to certify electronic evidence with an electronic signature. In France, a party may provide a copy of a website or a screenshot to prove a legal fact, but the court may find it necessary to request information to clarify it. In Lithuania, the court rules require the submission of original documents, and if copies are provided, they must be certified by a notary or lawyer involved in the case. An electronic signature is used to identify the person who signed the electronic document, not its content. Among

the European countries surveyed, the use of modern electronic signatures demonstrates the authenticity of electronic evidence in Belgium and Spain. In England and Wales, as well as in Montenegro, the law on electronic signatures provides for the authenticity of electronic evidence that is duly certified by an electronic signature.

References:

1. Weir, George R. S. Mason, Stephen. (2017). The sources of electronic evidence. Stephen Mason and Daniel Seng (eds.), "Electronic evidence". London, University of London, school of advanced study, institute of advanced legal studies. 1-18.
2. Kasper, Agnes; Laurits, Eneli. (2016). Challenges in collecting digital evidence: a legal perspective. *Tanel Kerikmäe and Addi Rull (eds.), "The future of law and eTechnologies"*. Cham, Springer. 195-233.
3. Kodeks administratyvnoho sudochynstva Ukrainy [Code of Administrative Procedure of Ukraine]. : Zakon vid 06.07.2005 № 2747-IV. Uriadovyi kurier. [Law of Ukraine dated July 6, 2005 No. 2747-IV. Government Courier]. 17.08.2005. №153, №153-154 [in Ukrainian].
4. Samonova V. (2022). Electronic Evidence in Administrative Proceedings. *Cuestiones Políticas*, Vol. 40, Num. 73. 726-740. DOI https://doi.org/10.46398/cuestpol.4073.41
5. Polishchuk M. (2019). Heneza pravovoho rehuliuvannia vykorystannia elektronnykh dokaziv u sudovii systemi Ukrainy. [The genesis of the legal regulation of the use of electronic evidence in the judicial system of Ukraine]. *National Law Journal: Theory and Practice*. № 6, № 28. 124-127.
6. Tosza, Stanislaw. (2020). "All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order." *New Journal of European Criminal Law*. Vol. 11, No. 2. 161-183. DOI: https://doi.org/10.1177%2F2032284420919802
7. Muhammad Alifian, Geraldi Fauzi and Nurmayani, Nurmayani and Syamsu, Syamsir. (2021). The position of electronic documents in the process of evidence in the state administrative jurisdiction in indonesia. *International Journal of Business, Economics and Law*. Vol. 24, No. 2. 25-28.
8. ECtHR judgment of 5 September of 2017 in case Bărbulescu v. Romania, petition No. 61496/08.
9. Biasiotti, M. A. Cannataci, J. A. Mifsud Bonnici, J.P. Turchi, F. (2018). Introduction: Opportunities and Challenges for Electronic Evidence. Handling and Exchanging Electronic Evidence Across Europe. *Law, Governance and Technology Series*; Vol. 39. 3-12. DOI: https://doi.org/10.1007/978-3-319-74872-6_1
10. López Ribalda and others v. Spain: Case of the European Court of Human Rights from 09.12.1994. Retrieved from https://zakon.rada.gov.ua/laws/show/980_348#Text
11. Leheza Ye., Odyntsova I., Dmytrenko N. Teoría y regulación legal del apoyo informativo de los procedimientos administrativos en Ucrania. Ratio Juris Unaula. 2021. Vol. 16, no. 32, pp. 291-306. DOI: https://doi.org/10.24142/raju.v16n32a12.9.
12. Leheza Ye., Len V., Shkuta O., Titarenko O., Cherniak N. Foreign experience and international legal standards of applying artificial intelligence in criminal proceedings. Revista de la universidad del zulia. 2022. Vol. 13, no. 36, 276-287. DOI: https://doi.org/10.46925//rdluz.36.18.8.

ЕЛЕКТРОННІ ДОКАЗИ В АДМІНІСТРАТИВНОМУ СУДОЧИНСТВІ: ПРАВОВЕ РЕГУЛЮВАННЯ, ПОВНОВАЖЕННЯ СУДДІ ТА ЗАРУБІЖНИЙ ДОСВІД

Розглянуто особливості застосування електронних доказів в адміністративному судочинстві (правове регулювання, повноваження судді та зарубіжний досвід). Враховуючи рекомендації Ради Європи та позитивний зарубіжний досвід стосовно електронних доказів в адміністративному судочинстві на прикладі Сполучених Штатів Америки, Сполученого Королівства Великої Британії, Республіки Польща, Французької Республіки, Федеративної Республіки Німеччина, країн Карибського

басейну, Тихоокеанських держав, Литви, Туреччини виокремлено основні напрямки запозичення позитивного зарубіжного досвіду для України:

забезпечення відповідності електронних доказів праву на справедливий суд, яке закріплено у ст. 6 Європейської конвенції з прав людини; створення стандартів електронних доказів, які будуть встановлювати вимоги до впровадження та функціонування систем управління інформацією, включаючи зберігання та передачу інформації; запровадити при розгляді адміністративних справ використовувати штучний інтелект, який може ґрунтуватися на повторювальних моделях фактичних сценаріїв та юридичній класифікації спорів, або якнайменш для аналізу даних, стосовно наявності або відсутності підпису, та розгляду позову за його відсутності, тобто повернення, оскільки був поданий через систему електронного судочинства у непередбачуваний законом спосіб; забезпечення дотримання принципу верховенства права та неприпустимість прийняття електронних доказів, які були отримані незаконним способом; запровадити зберігання електронних доказів із використанням новітніх методів, а саме замінити агентства з кібербезпеки, сертифікацією часових позначок із системою блокчейн, оскільки друк, блокування хмарних або серверних сховищ - залежать від дій оператора чи адміністратора; прийняти типове законодавство стосовно електронних доказів; враховувати судам позицію викладену у Рекомендаціях Комітету Європи стосовно того, що суди не повинні заперечувати юридичну силу електронних доказів лише тому, що вони не містять електронного підпису; державні органі мають забезпечувати зберігання у конфіденційності персональні дані, та забезпечувати заходи для їх збереження тощо.

***Ключові слова**: судова дискреція, судовий розсуд, дискреційні повноваження, внутрішнє переконання, адміністративно-правові засади, компетенція судді, повноваження судді, адміністративний суд, адміністративне судочинство, суддя, судова влада, електронні докази.*