DOI https://doi.org/10.51647/kelm.2020.8.2.37

METADANE JAKO ŹRÓDŁO INFORMACJI DOWODOWYCH W POSTĘPOWANIU CYWILNYM

Serhii Chvankin
kandydat nauk prawnych, docent,
Prezes Kijowskiego Sądu Rejonowego miasta Odessy,
Przewodniczący Stowarzyszenia Sędziów Śledczych Ukrainy (Odessa, Ukraina)
ORCID ID: 0000-0002-9800-854X
e-mail: sergey0024@i.ua

W tym artykule naukowym ustalono istotę metadanych jako jednego z ważnych źródeł informacji dowodowych. Udowodniono, że metadane nie są odrębnym rodzajem dowodów elektronicznych, ale składnikiem dowodów elektronicznych, których cechy opisują. Przeanalizowano klasyfikacje metadanych dostępne w literaturze naukowej, zbadano niektóre rodzaje metadanych i zidentyfikowano cechy wykorzystania metadanych w postępowaniu sądowym w sprawach cywilnych.

Słowa kluczowe: sprawiedliwość, postępowanie cywilne, dowód sądowy, przedmiot dowodu, dowody elektroniczne, osadzone metadane.

METADATA AS A SOURCE OF EVIDENTIARY INFORMATION IN THE CIVIL PROCEEDINGS

Serhii Chvankin
PhD in Law, Associate Professor,
Head
Kyiv District Court of the City of Odesa (Odesa, Ukraine),
Head
Investigative Judge Association of Ukraine (Odesa, Ukraine)
ORCID ID: 0000-0002-9800-854X
e-mail: sergey0024@i.ua

Abstract. This research article establishes the essence of metadata as one of the significant sources of evidentiary information. It proves that metadata is not a separate type of electronic evidence, but an integral part of electronic evidence, the characteristics of which it describes. It analyses metadata classifications, presented in the scientific literature, investigates individual types of metadata and determines the peculiar features of utilizing metadata in the process of judicial proof in civil cases.

Key words: justice, civil proceedings, judicial proof, fact in proof, electronic evidence, embedded metadata.

МЕТАДАНІ ЯК ДЖЕРЕЛО ДОКАЗОВОЇ ІНФОРМАЦІЇ В ЦИВІЛЬНОМУ ПРОЦЕСІ

Чванкін Сергій Анатолійович
кандидат юридичних наук, доцент,
голова
Київського районного суду міста Одеси (Одеса, Україна),
голова
Асоціації слідчих суддів України (Одеса, Україна)
ORCID ID: 0000-0002-9800-854X
e-mail: sergey0024@i.ua

Анотація. У цій науковій статті встановлено сутність метаданих як одного з важливих джерел доказової інформації. Доведено, що метадані є не окремим видом електронних доказів, а складовою частиною електронних доказів, характеристики яких вони описують. Проаналізовано наявні в науковій літературі класифікації метаданих, досліджено деякі види метаданих та визначено особливості використання метаданих у процесі судового доказування у цивільних справах.

Ключові слова: правосуддя, цивільний процес, судове доказування, предмет доказування, електронні докази, вбудовані метадані.

Articulation of the issue. From 1986 to 2007, globally, the capacity of computer memory was increasing on the average 23% per year. 2002 was the first year when more information was saved digitally than physically, and in 2007 94% of all information around the world was saved electronically. Every minute daily, people send 200 million emails, download forty-eight hours of video from YouTube, make 2 million requests on Google, and create 571 thousand new web-sites (Rosenberg, 2016: 445).

The increasing amount of electronic information leads to a higher rate of its use in the process of judicial proof. The distinguishing feature and significant advantage of the electronic evidence over the other types of evidence is the considerable volume of metadata, accompanying the data that comprise the main content of the electronic evidence.

Today, the researchers show quite an avid interest in the electronic evidence as a means of proof in civil proceedings. The problematics of utilizing electronic evidence in the process of judicial proof has many times been investigated in the works of such scientists as O.T. Bonner, M.O. Hetmatsev, N.Yy. Holubieva, K.V. Husarov, K.B. Drohoziuk, O.S. Zakharova, A.Yu. Kalamaiko, V.V. Komarov, O.M. Lazko, V.V. Molchanov, Yu.S. Pavlova, V.S. Petrenko, I.V. Reshetnikova, M.K. Treushnikova, D.M. Tsekhan and others. However, the metadata and their relevance in the process of judicial proof were in the spotlight of much fewer works. The judicial practice does not pay enough attention to them either, and it is not justifiable given the benefit this tool may bring in delivering the goal of judicial proof, that is a comprehensive and objective establishing of all the circumstances of a case by the court. The aforementioned makes the topic of this scientific research relevant.

The goal of this research paper is to establish the essence and types of metadata as well as their importance in the process of judicial proof in civil cases.

Statement of the basic material. Metadata are accurately called “digital fingerprints” of the electronic evidence, as they can reveal important evidentiary information, such as the date and time of creation or modification of a file, its author, the time and date when such electronic data were sent, etc.

For instance, MS Word documents hold the metadata that include the name of the author, the name of the computer used to create the file, the time it was last saved, the date of its creation, etc. This type of data is integrated into the file and is updated automatically. Not only computers but most of the modern devices, that operate digital data, can create metadata. For example, the embedded metadata of a digital photograph may hold the information about the time and date of taking the photo, geo-referenced data, original name and type of the file, author or even a person, who holds the copyright for this photo. Having analysed metadata, one can obtain much valuable information about a digital file. It makes metadata critical, yet one of the most controversial types of electronic evidence, specified in Paragraph 1, Article 100 of the Civil Procedure Code of Ukraine (CPC). It relates to several peculiarities that distinguish the metadata from other electronic evidence.

First, the definition of the metadata itself gives the grounds to question whether or not they can be recognized as judicial evidence. According to Par. 1, Article 76 of CPC, the evidence is any data on the ground of which the court determines the presence or absence of circumstances (facts) that establish the denial and claims of the parties, and other circumstances relevant to solving the case (Цивільний процесуальний кодекс України, 2004). It means that the evidence in the civil proceedings is the data about the circumstance of a civil case, while the metadata, according to the generally accepted approach to interpreting this term, are the data about the other data. In the legal literature, metadata are referred to as the evidence that describes the characteristics, origin, use, and relevance of other electronic evidence (Hansen, Pratt, 2020). Therefore, metadata, as a rule, do not contain any direct information about the circumstances of the case, which are the legal fact, but just characterize other electronic evidence. It evokes a logical question about the relevance of metadata as the evidence in the civil proceedings.

The evidence is seen as relevant if it includes information on the fact in proof (Par. 1, Article 77 of CPC) (Цивільний процесуальний кодекс України, 2004). It is possible to assess the ability of metadata to characterise the circumstances that belong to the fact in proof only by determining the scope of these circumstances.

The procedural narrative has two major approaches to defining the scope of the facts in proof: “explicit” and “implicit". According to the “explicit” approach, the fact in proof includes: 1) legal facts of substantive relevance; 2) legal facts of procedural relevance; 3) evidential facts; 4) facts, that should be established for awareness-raising and preventative tasks of justice (Молчанов, 2012: 80; Клейнман, 1967: 284–287). This approach implies that practically all the facts the court finds evidentiary in the process of case consideration that directly or indirectly enable the court to solve the legal dispute in substance, are categorized as the fact in proof. Meanwhile, realizing the fundamental differences in the meaning of individual facts for achieving the final result of the proceedings, major and local facts in proof are distinguished.

According to the “implicit” approach, the fact in proof comprises only legal facts of substantial relevance. O.P. Kleinman argues that judicial activity requires establishing only those legally meaningful factual circumstances of the case, the framework of which are determined by the provisions of substantive law that regulate disputed relationships of the parties (Клейнман, 1967: 54). This point of view is shared by S.V. Kuryliov (Курылев, 2012: 332–333).

The proponents of the “implicit” approach insist on the necessity to distinguish the facts that make a part of the scope of the fact in proof and the facts that are established during the case hearing, with the latter not being related to the correct solution of the issue on the rights and responsibilities of the parties (Курс цивільного процесу, 2011: 486–487).

The legal studies also refer to the "transitional" approaches, where the scholars do not reduce it down to the fact of substantive relevance for the case solution, but speak about a narrower range within the scope of the fact in proof that the "explicit" approach implies (Сахнова, 2008: 376–384).

Without diving deep into the analysis of the aforementioned approaches, it is notable that it is the "explicit" approach that serves best to the goal of determining the relevance of the judicial evidence; it is outlined in the content of Par. 2 Article 77 of the Civil Procedure Code of Ukraine.

Hence, any fact, the establishment of which brings the court closer to the correct solution of the case, can be included into the fact in proof, even if it is a local and not a major fact in proof. Such "transitional" facts, which are also referred to as evidential fact, can be established through the analysis of metadata, so the information contained in the metadata can be seen as those possessing such a crucial feature of judicial evidence as relevance.

At the same time, it should be recognized that the relevance of metadata depends directly on the relevance of major data they describe. If certain electronic data do not relate to the fact in proof in the specific case, the court will not be interested in any metadata associated with it. It means the relevance of metadata for the circumstance that comprise a fact in proof, derives from the relevance of the data they characterize. This is an additional proof to the fact that metadata cannot be seen as a separate type of electronic evidence, as they are just a component of the electronic evidence, the data of which they characterize.

Second, the scientific literature aptly notes a certain conditionality of categorizing this specific information as metadata. The information resources that play a role of metadata in some cases, are the data in the other ones, and vice versa. Indeed, the total of the tags in the hypertext mark-up, the title of an article or its abstract that make a part of its text, can be used as metadata that describe the mentioned resources. Along with that, they are all the integral parts of those resources thus are data (Когаловский, 2012: 7). Therefore, categorizing certain information as metadata is based on the function such information has in this specific situation.

The content of metadata, their functions, and means of their representation depend on the employed information technologies, functionality, and domain applicability of the systems that use them, the nature of the described resources, the context and character of their utilization, as well as many other factors (Когаловский, 2013: 30).

The scientific literature singles out a significant number of metadata types: 1) autonomous and embedded; 2) independent from and dependent on the information resources they describe; 3) static and dynamic; 4) formalized and non-formalized, etc. (Когаловский, 2013: 37–38).

The American legal literature on the problematics of metadata application in the process of judicial proof, outlines three major types of metadata, utilized in the judicial practice: 1) substantive metadata; 2) system metadata; 3) embedded metadata (Isaza, 2010).

Substantive metadata enable the court to track back the history of the changes made to the document content, even if such changes are not shown on the computer display in the final version of the document.

System metadata are the data that are automatically generated by the computer system. As a rule, they show the author, the date and time of creation, and the date of the document modification, etc.

Embedded metadata obtained their name because they are stored in the file, containing the object, described by the metadata. The embedded metadata include text, digits, content, data, or other information that is directly or indirectly inputted by a user to a file and that is, as a rule, not visible for the user who is looking through the input content on the computer screen. The examples of such metadata are the formulas of the electronic tables, hidden columns, externally or internally connected files (such as audio files), hyperlinks, links, and fields, as well as information about a database. This type of metadata often plays a crucial role in understanding an electronic document. For instance, it may be difficult to make sense of a complex electronic table without a possibility to see the formulas that shape a basis of the output data in each section (Isaza, 2010).

The mentioned types do not create any metadata classification but rather name most typical metadata types, observed in the judicial practice, because the embedded metadata can concurrently be system ones, while substantive metadata can also be embedded.

To exploit metadata in the process of the judicial proof, it is important to divide metadata into 1) open and hidden; 2) system and inputted by a user.

Open metadata can be easily observed by any user (for instance, the OS Windows enables the user to see the file name, type, place of storage, date and time of creation, and most recent modification when looking at the file properties). Getting access to the hidden metadata requires special knowledge, and sometimes dedicated software for metadata reading. Meanwhile, it should be borne in mind that by using special knowledge, skills, and dedicated software, one can not only read but also modify metadata in the electronic documents.

So, metadata are not an outright reliable source of credible information and can be intentionally or unintentionally modified. For instance, the modification of date and time on the computer with the following opening or modification of the file on it will change the date and time of the latest file modification, reflected in the metadata. As a rule, an expert can establish that someone was trying to manipulate metadata, however, it is fair to suggest that an experienced professional can get rid of all the signs of such manipulation. Despite metadata are not completely credible, they are often more credible than regular methods of authentication (Rosenberg, 2016: 451).

Hence, if the open metadata can be observed by the court immediately during the examination of the electronic evidence, the hidden metadata, as a rule, require an expert to be considered.

Yet, unlike in the USA that has an established practice of providing electronic evidence together with the metadata in the format, convenient for the court to examine them, the Ukrainian courts rarely analyse the content of not

only hidden but also open metadata of the electronic file, trusting this matter only to the experts. For example, in one of the civil cases, the expert conclusion was the basis for both the Court of First Instance and the Court of Appeal to establish the author of the photographic works. The expert studied the history of creating the photographic works, using metadata and the log data, and discovered the tag that was mapped in the history of file modification. It indicated that the works were created from the original files of the complainant (Рішення Дніпровського районного суду м. Києва від 29.01.2018; Постанова Апеляційного суду м. Києва від 06.06.2018). The other case features the expert conclusion where the file metadata revealed the date when the electronic photographs were taken at the scene.

Sometimes, in the legal literature, the term "metadata" also refers to the files that are deleted by a user but still exist in the "spare" space of the computer memory. Deleting the file from the Recycle Bin does not mean it is completely deleted unless you set up your system differently. What is deleted is the indicator of files or reference data, i.e. the specific metadata of this file. However, the file itself still exists in the "spare space" on the hard drive, even though the computer deleted all the links to it. "Deleted file" is like "an elephant in the room"; the computer acts as if the file does not exist, though it is still where it was before being deleted. The deleted files remain in the "spare space" until they are replaced by new data (Rosenberg, 2016: 448).

In the given example, these are not metadata that are hidden, but the major data of an electronic document, familiarization with the content of which is hampered by the deleted metadata. So, if during the court proceedings, there is a need to explore the content of such an electronic document, it is possible to do that with the help of an expert.

As it was mentioned above, the system metadata include those the pieces of data, automatically formed by the computer system without user's interference. Thanks to the human-factor absence, such metadata are believed to be a more credible source of the evidential information, if their integrity remained intact.

The most significant pieces of metadata that are inputted by a user and often play a critical role in the court when assessing the electronic evidence, are an electronic signature, electronic seal, or electronic time stamp.

Electronic signature refers to the electronic data, added by the signatory to other electronic data or logically associated with them or used by the user as a signature.

Electronic seal refers to the electronic data, added by the creator of the electronic seal to other electronic data or logically associated with them and used for determination of the origin and revision of the integrity of the associated electronic data.

Electronic time stamp refers to the electronic data that link other electronic data with the specific time to certify the existence of such electronic data at that moment (Article 1 of the Law of Ukraine "On Electronic Trust Services" as of 05.10.2017 No. 2155-VIII (Закон України від 05.10.2017)).

The electronic time stamp can also be automatically applied by a dedicated software of a device, in case it is a regular electronic time stamp, or can be consciously added by a user (a qualified provider of the electronic trust services) if there is a qualified electronic time stamp.

A qualified electronic time stamp has a presumption of accuracy of the date and time it refers to, and integrity of the electronic data this date and time are associated with (Article 26 of the Law of Ukraine "On Electronic Trust Services" as of 05.10.2017 No. 2155-VIII (Закон України від 05.10.2017)).

Conclusions. Metadata is a part of the electronic evidence that holds the information about this electronic evidence. Metadata complement the information about the circumstances of the case, held in the electronic evidence, and provide for establishing the authenticity and legal power of the electronic evidence. The relevance of the metadata derives from the relevance of the electronic evidence they describe.

To exploit metadata in the process of judicial proof, it is important to divide metadata into 1) open and hidden; 2) system and inputted by a user.

Open metadata can be examined by the court immediately during the consideration of the electronic evidence, while examination and analysis of the hidden metadata require an expert.

"Human factor" being absent in the system metadata, they are seen as the more credible source of evidential information than those inputted by a user; of course, if their integrity is intact.

An electronic signature is the most significant and widely applicable piece of metadata, inputted by a user, because the lack of it means the electronic document is irrelevant evidence, therefore, it cannot be taken into account by the court in the solution of the case.

Bibliography:

1. Rosenberg Z. Returning to Plato's cave: metadata's shadows in the courtroom. *Arizona state law journal*. 2016. Vol. 48. Issue 2. Pp. 439–480. URL: https://arizonastatelawjournal.org/wp-content/uploads/2016/07/Rosenberg_Final.pdf.
2. Hansen M.D., Pratt T.J. Follow the Audit Trail: The Impact of Metadata in Litigation. *Defense counsel journal*. 2020. Vol. 84. No. 3. URL: https://www.iadclaw.org/defensecounseljournal/follow-the-audit-trail-the-impact-of-metadata-in-litigation.
3. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40–41, 42. Ст. 492.
4. Молчанов В.В. Основы теории доказательств в гражданском процессуальном праве : учебное пособие. Москва : ИКД «Зерцало-М», 2012. 360 с.
5. Штефан М.Й. Цивільне процесуальне право України: Академічний курс : підручник для студентів вищих навчальних закладів. Київ : Концерн «Видавничий дім «Ін Юре», 2005. 624 с.
6. Клейнман А.Ф. Новейшие течения в советской науке гражданского процессуального права (очерки по истории). Москва : Издательство Московского университета, 1967. 119 с.

7. Курылев С.В. Избранные труды. Минск : Редакция журнала «Промышленно-торговое право», 2012. 607 с.
8. Курс цивільного процесу : підручник / В.В. Комаров, В.А. Бігун, В.В. Баранкова та ін.; за ред. В.В. Комарова. Харків : Право, 2011. 1352 с.
9. Сахнова Т.В. Курс гражданского процесса: теоретические начала и основные институты. Москва : Волтерс Клувер, 2008. 696 с.
10. Когаловский М.Р. Метаданные, их свойства, функции, классификация и средства представления. Труды 14-й Всероссийской научной конференции *«Электронные библиотеки: перспективные методы и технологии, электронные коллекции»* – RCDL-2012, Переславль-Залесский, Россия, 15–18 октября 2012 г. С. 3–14.
11. Когаловский М.Р. Метаданные в компьютерных системах. *Программирование*. Москва : МАИК «Наука/ Интерпериодика». 2013. Т. 39. № 4. С. 28–46.
12. Isaza J. Metadata in Court: What RIM, Legal and IT Need to Know. Research Project Underwritten by: The ARMA International Educational Foundation Endowment. Pittsburgh PA 15241 USA, 2010. URL: http://armaedfoundation.org/wp-content/uploads/2016/12/Isaza_Metadata_Final.pdf.
13. Рішення Дніпровського районного суду м. Києва від 29.01.2018 р. у справі № 755/22219/14-ц. URL: https://reyestr.court.gov.ua/Review/71850002.
14. Постанова Апеляційного суду м. Києва від 06.06.2018 року у справі № 755/22219/14ц. URL: https://reyestr.court.gov.ua/Review/74599000.
15. Постанова Апеляційного суду Кіровоградської області від 03.05.2017 року у справі № 389/1189/15-ц. URL: https://reyestr.court.gov.ua/Review/66483026.
16. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 400

References:

1. Rosenberg, Z. (2016). Returning to Plato's cave: metadata's shadows in the courtroom. *Arizona state law journal*. Vol. 48. Issue 2. P. 439–480. Retrieved from: https://arizonastatelawjournal.org/wp-content/uploads/2016/07/Rosenberg_Final.pdf.
2. Hansen, M.D., Pratt T.J. (2020). Follow the Audit Trail: The Impact of Metadata in Litigation. *Defense counsel journal*. Vol. 84. No. 3. Retrieved from: https://www.iadclaw.org/defensecounseljournal/follow-the-audit-trail-the-impact-of-metadata-in-litigation.
3. Civil procedure Code of Ukraine: Law of Ukraine from 18.03.2004 No. 1618-IV. *Information of the Verkhovna Rada of Ukraine.* 2004. No. 40–41, 42. Art. 492.
4. Molchanov, V. (2012). *Osnovy teorii dokazatel'stv v grazhdanskom processual'nom prave* [Foundations of the theory of evidence in civil procedural law]. Moskva: ICD "Zertsalo-M". Pp. 360.
5. Shtefan, M. (2005). *Civil'ne procesual'ne pravo Ukraini: Akademichnij kurs: Pidruch. dlya stud. vishch. navch. zakl* [Civil procedural law of Ukraine: Academic course: Textbook for students of higher educational institutions]. Kyiv: Concern Publishing House "In Yure". Pp. 624.
6. Kleinman, A. (1967). *Novejshie techeniya v sovetskoj nauke grazhdanskogo processual'nogo prava (ocherki po istorii)* [The latest trends in the Soviet science of civil procedural law (essays on history)]. Moscow: Moscow University Press, pp. 119.
7. Kurylev, S. (2012). *Izbrannye Trudy* [Selected Works]. Minsk: Editorial office of the journal *"Industrial and Commercial Law"*. Pp. 607.
8. Komarov, V. (2011). *Kurs civil'nogo procesu* [The course of the civil process]. Kharkiv: Pravo. Pp.1352.
9. Sakhnova, T. (2008). *Kurs grazhdanskogo processa: teoreticheskie nachala i osnovnye instituty* [Civil Procedure Course: Theoretical Principles and Basic Institutions]. Moskva: Walters Kluver. Pp. 696.
10. Kogalovsky, M. (2012). Metadata, their properties, functions, classification and presentation means. *Proceedings of the 14th All-Russian Scientific Conference "Digital Libraries: Advanced Methods and Technologies, Digital Collections"* – RCDL-2012, Pereslavl-Zalessky, Russia, October 15–18. Pp. 3–14.
11. Kogalovsky, M. (2013). Metadata in computer systems. Programming. Moskva: MAIK *"Science/Interperiodica"*. T. 39. No. 4. S. 28–46.
12. Isaza, J. Metadata in Court: What RIM, Legal and IT Need to Know. Research Project Underwritten by: The ARMA International Educational Foundation Endowment. Pittsburgh PA 15241 USA, 2010. Retrieved from: http://armaedfoundation.org/wp-content/uploads/2016/12/Isaza_Metadata_Final.pdf.
13. Decision of the Dniprovsky District Court of Kyiv from 29.01.2018 in case No. 755/22219/14-ts. [online]. Retrieved from: https://reyestr.court.gov.ua/Review/71850002 [[n Ukrainian].
14. Resolution of the Court of Appeal of Kyiv from 06.06.2018 in the case No. 755/22219/14ts. [online]. Retrieved from: https://reyestr.court.gov.ua/Review/74599000.
15. Resolution of the Court of Appeal of the Kirovohrad region from 03.05.2017 in the case No. 389/1189/15-ts. [online]. Retrieved from: https://reyestr.court.gov.ua/Review/66483026.
16. On electronic trust services: Law of Ukraine of 05.10.2017 No. 2155-VIII. *Information of the Verkhovna Rada*. 2017. No. 45. Art. 400.