http://dx.doi.org/10.12775/CLR.2019.009

Bartłomiej Oręziak*
Marek Świerczyński**

ELECTRONIC EVIDENCE IN THE LIGHT OF THE COUNCIL OF EUROPE'S NEW GUIDELINES

Abstract

This paper aims to analyse the significance of the "Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings" adopted by the Council of Europe on January 30, 2019. The authors examine the practical aspects of the specific guidelines following from this soft law instrument. They make an in-depth analysis of metadata as an essential element of electronic evidence. The authors also present the fundamental principles of electronic evidence, as presented in the Guidelines, along with an explanation of their meaning, including the principle on the protection of human rights and rule of law. The paper ends with the authors' conclusions regarding treatment of electronic evidence in the courts, the practical significance of the Guidelines and the importance of IT law in legal education.

Keywords

Electronic evidence – guidelines – metadata – cyberlaw – law of new technologies

* Bartłomiej Oręziak, M.A., Doctoral candidate, Faculty of Law and Administration, Cardinal Wyszyński University in Warsaw; e-mail: boreziak@gmail.com.

** Dr hab. Marek Świerczyński, prof. UKSW, Faculty of Law and Administration, Cardinal Wyszyński University in Warsaw; e-mail: m.swierczynski@uksw.edu.pl.

I. Introduction

Today's world is subject to constant changes affecting how legal disputes are resolved. Traditional procedural solutions are transformed by modern technologies. The aim of this process is to increase efficiency, effectiveness, and safety of justice. Procedural laws play an important role in the ongoing technical, technological or civilization progress. The science and practice of law correlates with hitherto unknown possibilities of current development. There are many examples of this state of affairs, such as: artificial intelligence[1], smart contracts[2], cryptocurrencies[3], e-health[4].

---

[1] The literature analyses examples of the use of so-called artificial intelligence in legal practice, e.g.: A. Silverman, *Mind, Machine, and Metaphor. An Essay on Artificial Intelligence and Legal Reasoning*. *Boulder*, Colorado: Westview Press, 1993, p. 1; J. Searle, *Is the Brain's Mind a Computer Program?*, "Scientific American" 1990, vol. 262(1) pp. 26; K. Bowrey, *Ethical Boundaries and Internet Cultures*, [in:] L. Bently, S. Maniatis (ed.), *Intellectual Property and Ethics*, London: Sweet & Maxwell, 1998, p. 36; D. Partridge, *A New Guide to Artificial Intelligence*, New Jersey: Intellect Books 1991, p. 1.

[2] The possibilities and advantages of using smart contracts in legal transactions are presented by: P. Venegas, *Guide to smart contracts. Blockchain examples*, Cambridge: Economy Monitor, 2017, p. 5–7; J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartentein, J. Hierrera-Joancomarti, *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Oslo: Springer, 2017, p. 297–411; J. Alferes, L. Bertossi, G. Governatori, P. Fodor, D. Roman, *Rule Technologies. Research, Tools and Applications*, New York: Springer, 2016, p. 151–199; B. Kelly, *The bitcoin big bang. How alternative currencies are about to change the world*, New Jersey: Wiley, 2015, p. 149–163; Ch. Dennen, *Introducing ethereum and solidity*, New York: Apress, 2017, p. 89–111; I. Bashir, *Mastering Blockchain. Distributed ledgers, decentralization and smart contracts explained*, Birmingham: Packt Publishing, 2017, p. 21–23, 43–44.

[3] Cryptocurrencies are gaining significance not only in the financial market: M. Miller, *The Ultimate Guide to bitcoin*, Indianapolis 2014, s. 12; European Central Bank, *Virtual Currency Schemes*, Frankfurt am Main, 2012, p. 13; The Financial Action Task Force Report, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, Paris, 2014, p. 4; European Banking Authority, *EBA Opinion on „virtual currencies"*, London 2014, p. 11; A. Sieroń, *Czym jest Bitcoin* [*What is Bitcoin*] "Wrocław Economic Reviev" 2013, vol. 19(4), pp. 31.

[4] The issue of digital medicine is widely discussed in the literature, where it is no longer treated in terms of technological innovations, but as a necessity: M. Sosa-Iudicissa, *History of Telemedicine*, [in:] O. Ferrer-Roca, M. Sosa-Iudicissa (ed.), *Handbook of Telemedicine*, Amsterdam-Berlin-Oxford-Tokyo-Washington: IOS Press, 1998, p. 1; K. Lops, *Cross-border telemedicine. Opportunities and barriers from an economical and legal perspective*, Rotterdam: Erasmus University Institute of Health Policy and Management

It also affects changes in the substantive law. Nevertheless, ubiquitous digitization will also lead to changes in procedural law. An example of this is the electronic evidence constituting the research problem in question.

On January 30, 2019, the Council of Europe adopted the "Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings" (hereinafter: the Guidelines).[5]. It showed that contemporarily the use of electronic evidence is a matter of international interest. This is important because at the national level, courts and administrative bodies are increasingly resolving cases based on electronic evidence that have been submitted by the parties and other persons involved in civil or administrative proceedings[6]. Furthermore, electronic evidence also is gaining importance in criminal proceedings owing to the phenomenon and the forms of prevention of cybercrime[7].

Master Health Economics Policy and Law, 2008, p. 7; M. Maheu, P. Whitten, A. Allen, *E-Health, Telehealth, and Telemedicine: A Guide to Startup and Success*, San Francisco: Jossey--Bass, 2001, p. 2–4; M. Äärimaa, *Telemedicine Contribution of ICT to Health*, [in:] I. Lakovidis, P. Wilson, J. C. Healy (ed.), *E-Health Current Situation and Examples of Implemented and Beneficial E-Health Applications*, Amsterdam-Berlin-Oxford-Tokyo-Washington: IOS Press, 2004, p. 112.

[5] The Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies), 30 January 2019, CM (2018)169-add1final.

[6] M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi, *Introduction: Opportunities and Challenges for Electronic Evidence*, [in:] M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi (ed.), *Handling and Exchanging Electronic Evidence Across Europe*, Cham: Springer, 2018, p. 4.

[7] It should be noted that the issue of criminal procedural law and cybercrime correlation is widely analysed in the literature: A. Kigerl, *CAN SPAM Act: An Empirical analysis*, "International Journal of Cyber Criminology" 2009, vol. 3/2, pp. 566–589; B. Wible, *A Site Where Hackers are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime*, "The Yale Law Journal" 2003, vol. 112/6, pp. 1577–1623; C. Coleman, *Security Cyberspace – New Laws and Developing Strategies*, "Computer Law and Security Report" 2003, vol. 19/2, pp. 131–136; I. Walden, *Harmonising Computer Crime Laws in Europe*, "European Journal of Crime, Criminal Law and Criminal Justice" 2004, vol. 12/4, pp. 321–336; J. Reidenberg, *Technology and Internet Jurisdiction*, "University of Pennsylvania Law Review" 2005, vol. 153/6, pp. 1951–1974; M. Gercke, *Europe's Legal Approaches to Cyber crime*, "ERA Forum" 2009, vol. 10, pp. 409–420; M. Nuth, *Taking Advantage of New*

There are already established broad standards in this area[8]. The title of the Guidelines explicitly explains that they apply only to civil and administrative proceedings. Nevertheless, the adopted standards of electronic evidence have been defined in a general way. Therefore, their

Technologies: For and Against Crime Computer Law and Security Report, "Computer Law & Security Review" 2008, vol. 24, pp. 437–446; P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, "University of Pennsylvania Law Review" 2005, vol. 153/6, pp. 1975–2001; S. Brenner, J. Schwerha, *Introduction-Cyber crime: A Note on International Issues*, "Information Systems Frontiers" 2004, vol. 6/2, pp. 111–114; S. Hilley, *Pressure Mounts on US Senate to Pass Cyber crime Treaty*, "Digital Investigation" 2005, vol. 2, pp. 171––174; S. Moitra, *Developing Policies for Cyber crime*, "European Journal of Crime, Criminal Law and Criminal Justice" 2005, vol. 13/3, pp. 435–464; S. Wang, *Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crimes*, "Computer Standards and Interfaces" 2007, vol. 29, pp. 216–223; W. Chung, H. Chen, W. Chang, S. Chou, *Fighting cyber crime: a review and the Taiwan Experience*, "Decision Support Systems" 2006, vol. 41, pp. 669–682.

[8] For example: A Simplified Guide to Digital Evidence, available on the site: http://www.forensicsciencesimplified.org/digital/Digital Evidence.pdf [last access: 2.06.2019]; Défense et sécurité des systèmes d'information. Stratégie de la France, available on the site: https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_str ategie_de_la_France.pdf [last access: 2.06.2019]; DOD Dictionary of Military and Associated Terms 2017, available on the site: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf [last access: 2.06.2019]; Draft Convention on Electronic Evidence, "Digital Evidence and Electronic Signature Law Review" 2016, vol. 13, available on the site: http://journals.sas.ac.uk/deeslr/article/viewFile/2321/2245 [last access: 2.06.2019]; Electronic evidence – a basic guide for First Responders: Good practice material for CERT first responders, available on the site: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders [last access: 2.06.2019]; European Competition Network Recommendation on The Power to Collect Digital Evidence, Including by Forensic Means, available on the site: http://ec.europa.eu/competition/ecn /ecn_recommendation_09122013_digital_evidence_en.pdf [last access: 2.06.2019]; Explanatory Report to the Convention on Cybercrime, available on the site: https://rm.coe.int/16800cce5b [last access: 2.06.2019]; Good Practice Guide for Computer-Based Electronic Evidence, available on the site: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf [last access: 2.06.2019]; P. Grimm, *In the United States District Court for the District of Maryland. Memorandum opinion*, 2007, available on the site: https://www.gpo.gov/fdsys/pkg/USCOURTS-mdd-1_06-cv-01893/pdf/USCOURTS-mdd-1_06-cv-01893-0.pdf [last access: 2.06.2019]; Forensic Examination of Digital Evidence: A Guide for Law Enforcement, available on the site: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf [last access: 2.06.2019].

implementation in the field of the criminal process is methodologically possible. This remark is important because it shows the authority of the Guidelines that can be considered as a general international principle of electronic evidence. This is because there are few provisions on the international, European, and national levels that facilitate proceedings with the use of electronic evidence in this area[9]. Both in law and in court practice there is a legal loophole concerning the key technological rules of dealing with electronic evidence[10]. For this reason, the adoption of the Guidelines is important. Their aim is not to establish binding legal standards. They provide a practical toolbox for Member States to adapt judicial and other dispute resolution mechanisms using electronic evidence. The Guidelines aim to facilitate the use and management of electronic evidence within legal systems and in court practices. It is necessary to pay attention to the specificity of electronic evidence.

The Guidelines deal with number of specific issues, such as oral evidence taken by a remote link, use of electronic evidence, collection, seizure and transmission of evidence, relevance, reliability, storage and preservation, archiving, awareness-raising, review, training and education. They contain definitions, fundamental principles and detailed guidelines. The guidelines cannot be interpreted as prescribing a specific probative value for certain types of electronic evidence. They can be applied only insofar as they are not in conflict with national legislation.

As regards the applicability of the Guidelines to Polish court practice taking into account the current provisions of the Code of Civil Procedure, it should be clarified that the Guidelines are fully aligned with the Code.

---

[9] For example, the UNCITRAL Model Laws: The Model Law on Electronic Commerce adopted on June 12, 1996, at its 85th meeting plenary meeting December 16, 1996, including an additional article 5 as modeled on July 31, 2001. The Model Law on Electronic Signatures was adopted by the Commission on 7 July 2001.

[10] The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis. Report prepared by Stephen Mason assisted by Uwe Rasmussen. Strasbourg, 27 July 2016, CDCJ (2015)14 final; J. Albert, Study on possible national legal obstacles to full recognition of electronic processing of performance information on construction products (under the construction products regulation), notably within the regimes of civil liability and evidentiary value, Final General Report, 30-CE-0517177/00-3630-CE-0517177/00-36.

Moreover, as both the authors of this paper have supported the Council of Europe in the preparation of the guidelines, a number of the Guidelines are directly inspired by the Polish provisions of the Code of Civil Procedure and its decrees (e.g. regarding video- and teleconferences). We are of the opinion that the Polish Code does not require any legislative changes or specific interpretation with respect to the new forms of evidence discussed in the Guidelines.

II. Definitions of electronic evidence, trust services, and court adopted in the Guidelines

For the purpose of the Guidelines, the definition of specific terms was adopted. However, the proposed meanings go far beyond this document. They have a wide range of objectives and correctly reflect the specificity of cyberlaw. In the law of new technologies, narrow, closed, or casuistic definitions should not be created. The point is that technology changes quickly. For example, what we consider electronic evidence tomorrow may cease to exist, and the day after tomorrow a new type of electronic evidence will be created. It is important that the Guidelines do not just concentrate on the technology. They are technology neutral. For this reason, the inclusion of these definitions in the Guidelines should be assessed positively.

The guidelines have adopted a broad definition of "electronic evidence" (also called "digital evidence"[11]). According to this, electronic evidence means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network. Thus, they can have a different form. It may be the content of the

[11] Z. C. Schreuders, T. W. Cockcroft, E. M. Butterfield, J. R. Elliott, A. R. Soobhany, *Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force*, 2018, p. 34, available on the site: http://eprints.leedsbeckett.ac.uk/5076/1/Needs%20Assessment%20of%20Cybercrime%20and%20Digital%20Evidence%20in%20a%20UK%20Police%20Force.pdf [last access: 11.06.2019].

message or conversation and related metadata[12]. Most often, these will be messages sent via e-mail boxes, mobile phones (SMS/MMS messages) or messaging applications. Electronic evidence can also be stored in the system or on electronic data carriers. So, electronic evidence includes, for instance: 1) registry files (they contain data collected by computer system monitoring devices, which may take the form of: Internet Protocol, Universal Resource Locator, user ID, connection acquisition and end time, warning about unsuccessful attempts to obtain access or list of operations carried out, including running programs, downloaded or sent files, and referenced documents); 2) electronic documents (digital version of traditional documents); 3) billing data (they contain information on the subscriber's station number, subscriber's address, number of billing units counted for a given station in the adopted billing period, numbers with which the subscriber has received the call, date of obtaining and duration of the call and its type (internet, international, national or local)); 4) records of devices recording payment transactions (they contain data on the numbers of payment cards used (both physical and digital) as well as information on the date, place and size of transactions made); 5) recordings of service cameras (e.g. this technique allows recognizing a person's face and comparing it with data contained in the system, e.g. photographs of criminals)[13]. In conclusion, electronic evidence can be in the form of text, video files, photos, or sound recordings[14]. Data can come from various sources, such as mobile phones, websites, computers, or GPS recorders[15]. This also includes data stored remotely within cloud computing. Electronic messages are a typical example of electronic

---

[12] E. Caseya, *Digital Evidence and Computer Crime*, Amsterdam-Boston-Heidelberg-London-New York-Oxford-Paris-San Diego-San Francisco-Singapore-Sydney-Tokyo: Elsevier, 2011, p. 49–81.

[13] A. Lach, *Dowody elektroniczne* [*Electronic evidence*], Toruń: Dom Organizatora, 2004, p. 41–51.

[14] J. Bonnici, M. Tudorica, J. Cannataci, *The European Legal Framework on Electronic Evidence: Complex and in Need of Reform*, [in:] M. Biasiotti, J. Bonnici, J. Cannataci, F. Turchi (ed.), *Handling and Exchanging Electronic Evidence Across Europe*, Cham: Springer, 2018, p. 189–234.

[15] G. Weir, S. Mason, *The sources of electronic evidence*, [in:] S. Mason, D. Seng (ed.), *Electronic Evidence*, London: University of London School of Advanced Study Institute of Advanced Legal Studies, 2017, p. 14–17.

evidence. This is evidence from an electronic device (computer or similar computing device) that contains the appropriate metadata[16].

Another defined concept is trust services that play a key role in the identification, authentication, and security of online transactions. Trust service means an electronic service which consists of: a) the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, and certificates related to those services or, b) the creation, verification, and validation of certificates for website authentication or, c) the preservation of electronic signatures, seals or certificates related to those services. It should be noted, that this definition of "trust service" adopted in the Guidelines was based on Article 3 (16) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS regulation)[17]. In addition, the Guidelines also address individual trust services related to ordinary, advanced, or qualified electronic signatures and certificates[18]. This means that it is possible to use other definitions adopted in eIDAS regulation when applying the Guidelines.

The concept of court used in the Guidelines includes any competent authority with adjudicative functions in the performance of which it handles electronic evidence. This includes all authorities with competences to adjudicate legal disputes between parties to civil and administrative proceedings. It is about courts and tribunals and even administrative authorities.

The definitions of cloud computing and blockchain have not been introduced into the final version of the Guidelines, despite the fact that the final draft included them. In the case of the first concept, the proposed definition has been deleted, because this term does not appear in the final version of the Guidelines (it is used only in the Explanatory

---

[16] Supra note 15.

[17] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73–114).

[18] S. Mason, *Electronic Signatures in Law: Fourth Edition*, London: University of London School of Advanced Study Institute of Advanced Legal Studies, 2017, p. 149–167.

memorandum to the Guidelines[19]). Regarding the second concept, the attempt to define it proved to be too much of a challenge. It is possible that this will change with the future update of the Guidelines related to technological development. Especially, that prepared definitions reflect the sense of new technologies, have a wide range, and are technologically neutral.

The Guidelines also refer to terms such as "simple" or "qualified" electronic signature, which means that it is possible to apply other definitions adopted in eIDAS regulation. According to these principles, an electronic signature is defined data that is inserted, connected, or logically linked with other data for the authentication of the latter and/or identification of the signatory. The certificate is an electronic certificate that links the signature verification data with the signatory and confirms or allows the identification of the signatory. A secure electronic signature, created using a secure signature-creation device and certified by an important, qualified certificate, has the same legal effect as a signature

---

[19] According to The Explanatory Memorandum: Blockchain is an emerging technology which has the potential to provide increased trust and security in electronic evidence. It can be defined as a distributed ledger that refers to the list of records (blocks), which are linked and secured using cryptography and are recorded in a decentralized peer-to-peer network. By design, a blockchain is inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. This makes blockchain suitable for evidencing purposes. In USA, § 1913 of the Vermont Rules of Evidence reads: (1) A digital record electronically registered in a blockchain shall be self-authenticating pursuant to the Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and: (a) the date and time the record entered the blockchain; (b) the date and time the record was received from the blockchain; (c) that the record was maintained in the blockchain as a regular conducted activity; and (d) that the record was made by the regularly conducted activity as a regular practice. In China, the Hangzhou Internet Court confirmed on June 28, 2018 that blockchain-based electronic data can be used as evidence in legal disputes. The usage of a third-party blockchain platform that is reliable without conflict of interests provided the legal ground for proving an intellectual infringement; According to The Explanatory Memorandum: Data sharing (clouds) is the storage of different parts of a database across various servers that might be located in different physical locations. It has become a common security technique. The global nature of the internet and the growing use of cloud services make it increasingly difficult to assume that access to data is strictly domestic in nature.

in written documents and is an admissible means of evidence in court. The electronic signature administration functions are performed by an appointed governmental institution.

As we see there are no fundamental discrepancies between the definitions adopted in the Guidelines and the Polish legislation. Both the Guidelines and Polish legal acts use definitions developed in international practice, which were then introduced to EU law (e.g. in the eIDAS or GDPR Regulations). The fact that this fact is not clearly explained in the Guidelines is owing to the simple fact that the Council of Europe wants to avoid the accusation of extending EU law to the Member States of the Council of Europe that are not EU members.

III. The importance of metadata

The concept of metadata and related standards is the key to the Guidelines[20]. For this reason, considerations regarding metadata must be presented separately. According to the adopted definition, metadata refers to electronic information about other electronic data, which may reveal the identification, origin, or history of the evidence, as well as relevant dates and times. In other words, metadata are structured or semi-structured information that enables the creation, registration, classification, access, preservation, and disposition of records through time and within and across domains (ISO 23081–1)[21]. In practice, they are called the "digital fingerprint" of electronic evidence. Metadata are usually not directly available. For example, they are of key importance to judicial investigations, including criminal cases, regardless of the accepted divisions of cybercrime[22]

---

[20] B. Schafer, S. Mason, *The characteristics of electronic evidence*, [in:] S. Mason, D. Seng, *Electronic Evidence*, London: University of London School of Advanced Study Institute of Advanced Legal Studies, 2017, p. 28.

[21] ISO 23081–1, available on the site: https://www.sis.se/api/document/preview/906833/ [last access: 07.06.2019].

[22] K. Bremer, *Strafbare Internet-Inhalte in internationaler Hinsicht, Ist der Nationalstaat wirklich uberholt?* [*Punishable internet content internationally, is the nation state really outdated*?], Frankfurt am Main: Peter Lang GmbH, Internationaler Verlag der Wissenschaften, 2000, p. 60–64; I. Vassilaki, *Multimediale Kriminalität, Entstehung, Formen und rechtspolitische Fragen der Post-Computerkriminalität* [*Multimedia crime, origins, forms and legal issues of post-*

(e.g. illegal access[23], system interference[24] or offences related to child pornography[25]), because the perpetrators want to hide all traces of their crime.

The term "record" is directly related to the metadata (there are many Guidelines regarding only metadata[26]). Records are a special

---

computer crime], "Computer und Recht" 1997, vol. 5, pp. 296–300; A. Płaza, *Przestępstwa komputerowe* [*Computer crimes*], Rzeszów, 2000, p. 6–9, available on the site: http://vagla.pl/skrypts/mgr_a_plaza.pdf [last access: 11.06.2019]; U. Sieber, *Computerkriminalität und Informationsstrafrecht* [*Computer Crime and Information Criminal Law*], „Computer und Recht" 1995, vol. 2, pp. 100–101; U. Sieber, *Der strafrechtliche Schutz der Information* [*The criminal protection of information*], "Zeitschrift fur die Gesamte Strafrechtswissenschaft" 1991, vol. 103, pp. 778–788; S. Hoeren, *Trapattoni und das Ende des Computerrechts* [*Trapattoni and the end of computer law*], „MultiMedia und Recht" 1998 vol. 4, pp. 169–171.

[23] S. McQuade, *Encyclopedia of crime*, London: Greenwood 2009, p. 46; J. Clough, *Principles of cybercrime*, New York: Cambridge University Press 2010, p. 50; O. Kerr, *The problem of perspective in Internet law*, "Georgetown Law Journal" 2003, vol. 91, pp. 60.

[24] M. Jakobsson, Z. Ramzan, *Crimeware. Understanding new attacks and* defenses, Boston: Addison-Wesley Professional, 2008, p. 3; I. Walden, *Computer Crimes and Digital Investigations*, New York: Oxford University Press, 2007, p. 19

[25] J. Steward, *International Policing of Child Pornography on the Internet*, "Houston Journal of International Law" 1997, vol. 20 pp. 205.

A. Gillespie, *Child protection on the Internet – challenges for criminal* law, "Child and family Law Quarterly" 2002, vol. 14, pp. 410–413.

[26] For example: UMass Amherst Libraries Metadata Guidelines, available on the site: https://www.library.umass.edu/assets/Digital-Strategies-Group/Guidelines-Policies/Metadata-Guidelines-v4.pdf [last access: 4.06.2019]; Guidelines for Statistical Metadata on the Internet, available on the site: https://www.unece.org/fileadmin/DAM/stats/publications/metadata.pdf [last access: 4.06.2019]; Descriptive Metadata Guidelines for RLG Cultural Materials, available on the site: https://www.oclc.org/content/dam/research/activities/culturalmaterials/RLG_desc_metadata.pdf [last access: 4.06.2019]; INSPIRE Metadata Implementing Rules: Technical Guidelines based on EN ISO 19115 and EN ISO 19119, available on the site: https://inspire.ec.europa.eu/documents/Metadata/INSPIRE_MD_IR_and_ISO_v1_2_20100616.pdf [last access: 4.06.2019]; Guidance on the Structure, Content, and Application of Metadata Records for Digital Resources and Collections, available on the site: https://archive.ifla.org/VII/s13/guide/metaguide03.pdf [last access: 4.06.2019]; State Records Guideline No 5 Recordkeeping Metadata, available on the site: https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Guideline%2005%20Recordkeeping%20Metadata.pdf [last access: 04.06.2019]; U.S. National Archives and Records Administration (NARA) Technical Guidelines for Digitizing Archival Materials for Electronic Access: Creation of Production Master Files – Raster Images, available on the site: https://www.archives.

form of recorded information. According to the definition included in the international standard ISO 15489–1, record is information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business[27]. Its primary role is to document decisions, actions, activities, and communication to tell the whole story. It means that record is real information about data, but metadata are significant in supporting record management[28]. It is often claimed that metadata are data about data[29]. However, from a technical point of view, metadata are data or information about the records, for example, the context of creating records, systems, and processes that generate and manage them, and the actions supported by records. Metadata are an adhesive that combines various record components and link the record to other records that are relevant to their understanding and use. According to the international standard ISO 23081–1 metadata support records management processes by: protecting records as evidence and ensuring their accessibility and usability through time; facilitating the ability to understand records; supporting and ensuring the evidential value of records; helping to

gov/files/preservation/technical/guidelines.pdf [last access: 04.06.2019]; Basic Guidelines for Minimal Descriptive Embedded Metadata in Digital Images, available on the site: http://www.digitizationguidelines.gov/guidelines/GuidelinesEmbeddedMetadata.pdf [last access: 04.06.2019]; Composition Metadata Guidelines, available on the site: https://isdcf.com/papers/ISDCF-Doc6-Composition-Metadata-Guidelines.pdf [last access: 04.06.2019]; Queensland Recordkeeping Metadata Standard and Guideline, available on the site: https://www.forgov.qld.gov.au/glossary/recordkeeping-metadata [last access: 04.06.2019].

[27] ISO 15489–1, available on the site: https://www.sis.se/api/document/preview/920396/ [last access: 05.06.2019].

[28] Digital Preservation in Lower Resource Environments: A Core Curriculum, available on the site: https://www.ica.org/sites/default/files/Metadata%20Module.pdf [last access: 07.06.2019].

[29] Z. Ambrus, *Applied Technology in Litigation Proceedings (The Electronic Discovery Reference Model)*, [in:] M. Kengyel, Z. Nemessányi, Electronic Technology and Civil Procedure. New Pats to Justice from Around the World, Dordrecht-Heidelberg-New York-London: Springer, 2012, p. 288; W. Lawrence Wescott II, *The increasing importance of metadata in electronic discovery*, "Richmond Journal of Law & Technology" 2008, Vol. 14(3), pp. 1; R. Gartner, *Metadata Shaping knowledge from Antiquity and to the Semantic Web*, London: Springer, 2016, p. 2.

ensure the authenticity, reliability, and integrity of records; supporting and managing access, privacy, and rights; supporting efficient retrieval; supporting interoperability strategies by enabling the authoritative capture of records created in diverse technical and business environments and their sustainability for as long as required[30]. Metadata are a powerful tool to help find records, understand them, and use them for many purposes, including evidence. Metadata are needed to track, store, protect, and maintain records and manage them over time. They enable the authentication and verification of information contained in records, as well as capture important technical details that enable the rendering of records. We are dealing with three basic types of metadata, which have significant probative value:

1) Descriptive metadata – data about finding or understanding the resource. They describe the work for the purposes of discovery and identification (e.g. creator, title, and subject);
2) Administrative metadata (include technical metadata, preservation metadata, rights metadata) – data about decoding and rendering files, file management, and intellectual property rights related to content;
3) Structural metadata – Data showing how compound objects are structured[31].

The Guidelines do not address all the problems that courts may face when dealing with electronic evidence (metadata). Instead, it has been emphasized that courts should be aware of the probative value of metadata and of the potential consequences of not using it (guideline No. 8). Courts should not always demand metadata when dealing with electronic evidence, because metadata can be important, but they are not necessary in every case. The Guidelines contain a recommendation to take care of metadata by storing them in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy (guideline No. 25). For example, from the metadata point of view, the paper version of the document is

---

[30] Supra note 21.

[31] Understanding Metadata What is Metadata, and What is it for?, available on the site: https://groups.niso.org/apps/group_public/download.php/17443/understanding-metadata [last access: 07.06.2019].

not equal to the digital copy of the document. Printouts of documents (web browser screens) do not contain metadata. Printing an electronic document may eliminate some or all of the metadata associated with the electronic version of the document. Threats related to the printouts of electronic documents have been discussed in US case law[32]. Additionally, electronic evidence should be stored with standardised metadata so that the context of its creation is clear (guideline No. 26).

The above does not mean that an amendment to the Polish regulations, including the Code of Civil Procedure, is required in order to regulate the status of metadata in Polish law. The issue of the proper treatment of metadata by courts should be the subject of the proper education of judges and legal professionals in the use of information technology. In other words, this issue belongs rather to the technical area of the handling of evidence, which is part of the judicial practice.

IV. Fundamental principles

The final version of the Guidelines includes just three fundamental principles. However, four such principles were included in the final draft presented to the Council of Ministers for adoption. During the plenary discussion the principle relating to the protection of human rights was removed. It should be underlined that the change is of formal and not substantive significance. The issue of protection of human rights in the context of the use of electronic evidence is too complex to be included in such a short principle.

The deleted principle referred to the rule of law and the admissibility of electronic evidence that was received unlawfully. An example is the confiscation of an electronic device, without a court order as required by law, as well as evidence obtained by the party by hacking the IT

---

[32] C. Ball, *Beyond Data About Data: The Litigator's Guide to Metadata*, 2005, p. 2: "*A hard copy of a document might give one person as the last individual to modify a document and the date of that modification while the metadata attached to the document might give an entirely different person and date for a later modification because the later modifier did not record the later modification on the document itself*", available on the site: http://www.craigball.com/metadata.pdf [last access: 05.06.2019].

system. Another example is well known: the fruit of the poisonous tree doctrine[33]. The fundamental problem in formulating this principle was related to the determination of exceptions. It was proposed that they cover situations in which it is necessary in a democratic society, in the interests of national security, public safety, for the prevention of disorder or crime, for preventing the disclosure of information received in confidence, and for the protection of the reputation or rights of others. For example, the case law of the ECtHR shows that evidence obtained as a result of an employer's violation of the principles of protection of employee privacy may be unacceptable due to violation of the proportionality principle[34]. We are of opinion that the removal of this principle is justified. It is impossible to include the protection of human rights in one short principle. Each Member State of the Council of Europe to which the Guidelines are addressed is also a party to of Convention of Human Rights and Fundamental Freedoms[35]. This act of international law in the case of using electronic evidence is then fully applicable.

The first of three finally adopted principles explains that it is for the courts to decide on the potential probative value of electronic evidence in accordance with national law. This means that although the role of experts in assessing electronic evidence is important, ultimately the courts decide on the potential probative value of electronic evidence. In doing so, courts may be bound by the applicable law (e.g. providing specific probative value for a certain type of electronic evidence). This does not deny the existence of a boundary for the free appraisal of evidence, for example related to the use of qualified electronic signatures. The assessment of the

---

[33] M. S. Bransdorfer, *Miranda Right-to-Counsel Violations and the Fruit of the Poisonous Tree Doctrine*, "Indiana Law Journal" 1986, vol. 62, pp. 1061–1100; R. M. Pitler, *The Fruit of the Poisonous Tree Revisited and Shepardized*, "California Law Review" 1968, vol. 56, pp. 579–651; J. M. Bain, M. K. Kelly, *Fruit of the poisonous tree: recent developments as viewed through its exceptions*, "University of Miami Law Review" 1976, vol. 31, pp. 615–650; V. P. Singh, *Poison Tree Principle: It's Applicability in India*, "International Journal of Advanced Research and Development" 2018, vol. 3(1) pp. 370–375; M. A. Lemley, *The Fruit of the Poisonous Tree in IP Law*, "Iowa Law Review" 2017, vol. 103, pp. 245–269.

[34] *Bărbulescu v. Romania*, Application no, 61496/08, Judgment of 5.09.2017.

[35] Convention of Human Rights and Fundamental Freedoms, available on the site: https://www.echr.coe.int/Documents/Convention_ENG.pdf [last access: 06.06.2019].

credibility and power of electronic evidence is a fundamental task of the court. It constitutes the essence of judgment. This means that disputable issues should be settled on the basis of independence, the judge's own belief, considering all the collected relevant evidence[36]. The situation is complicated when the court analyses the extensive evidence. Therefore, the case law indicates that the conviction of the court about the credibility of some pieces of evidence and the unreliability of others remains under the protection of procedural law. This holds true when the conviction of the court is preceded by the disclosure in the course of the entirety of the circumstances of the act in a way dictated by the duty to seek the truth[37]. This conviction is the result of considering all the circumstances that both favour and disadvantage the party of the proceedings and is comprehensively and logically justified in the justification[38]. In this justification, the court must indicate an analysis of the evidence, showing the premises on the basis of which, out of a wide range of different discrepant evidence, it based its findings and conclusions[39].

The second principle explains that electronic evidence should be evaluated in the same way as other types of evidence, in particular regarding its admissibility, authenticity, accuracy, and integrity. This requires that electronic evidence should not be discriminated against or favoured over other types of evidence. In this respect, courts should adopt a technology-neutral approach. This means that any technology that allows the authenticity, accuracy, and integrity of the data to be established should be accepted: "While Article 6 of the Convention of Human Rights guarantees the right to a fair hearing, it does not lay down

---

[36] The judgment of the Polish Supreme Court of 16 February 1996, II CRN 173/95, LEX No. 1635264.

[37] J. Jackson, *Two methods of proof in criminal procedure*, „The Modern Law Review" 1988, vol. 51, pp. 554; M. S. Nieuwland, A. E. Martin, *If the real world were irrelevant, so to speak: The role of propositional truth-value in counterfactual sentence comprehension*, "Cognition" 2012, vol. 122(1), pp. 102–109; F. P. Ramsey, *Truth and probability*, p. 21–45, available on the site: https://core.ac.uk/download/pdf/7048428.pdf [last access: 11.06.2019].

[38] The judgment of the Polish Supreme Court of 8 November 2005, SNO 52/05, LEX No. 569005; The judgment of the Polish Supreme Court of 3 February 2005, SNO 2/05, LEX No. 471932.

[39] The judgment of the Polish Supreme Court of 3 October 2005, IV KK 190/05, LEX No. 200391.

any rules on the admissibility of evidence or the way it should be assessed, which are therefore primarily matters for regulation by national law and the national courts"[40]. It also means that there is the possibility of using such recognized tests as the Daubert[41] or the Grimm test[42].

The third principle explains that the treatment of electronic evidence should not be disadvantageous to the parties or give unfair advantage to one of them. It refers to the equality of arms and equal treatment of parties to proceedings. A trial with electronic evidence should not be detrimental to the parties of the proceedings. For example, a party should not be denied the opportunity to challenge the authenticity of evidence. If the court requests from the party deliveries of electronic evidence, such party should not be deprived of the opportunity to submit relevant metadata. The case law of the European Court of Human Rights (hereinafter: the ECtHR) remains valid, from which it follows: "The principle of the equality of arms implies that each party must be afforded a reasonable opportunity to present his case – including his evidence – under conditions that do not place him at a substantial disadvantage vis-à-vis his opponent"[43].

In accordance with these principles, the improvement of court proceedings in Poland should be based on: 1) proper use of experts to evaluate electronic evidence, 2) non-discrimination against electronic evidence, as well as the abandonment of unreflective acceptance of such evidence, which unfortunately also could be observed in the Polish judicial practice, 3) equal treatment of parties with regard to the use of electronic evidence, which, in particular, should lead to a gradual departure from the current practice of presenting it in the form of printouts.

---

[40] *García Ruiz v. Spain*, Application no, 30544/96, Judgment of 21.01.1999, at par. 28.

[41] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), available on the site: https://supreme.justia.com/cases/federal /us/509/579/case.pdf [last access: 05.06.2019].

[42] P. Grimm, *In the United States District Court for the District of Maryland. Memorandum opinion*, 2007, available on the site: https://www.gpo.gov/fdsys/pkg/USCOURTS-mdd-1_06-cv-01893/pdf/USCOURTS-mdd-1_06-cv-01893-0.pdf [last access: 05.06.2019]; B. Esler, *Lorraine V Markel: Unnecessarily Raising the Standard for Admissibility of Electronic Evidence*, "Digital Evidence and Electronic Signature Law Review" 2007, vol. 4, pp. 80–82.

[43] *Letinčić v. Croatia*, Application no, 7183/11, Judgment of 03.05.2016, at par. 48.

V. Final remarks

In our opinion, the adoption of the Guidelines by the Council of Europe should be of great importance for improving court proceedings with the use of electronic evidence. Specific examples were presented above. It, however, heavily depends on the correct implementation of the Guidelines. We express hope that the Guidelines will be both recognized and used in practice by attorneys, prosecutors, judges, and IT specialists. We note that IT education in law should be an important part of legal education as such.

To sum up, the whole of the above analysis leads us to the following conclusions:

We are witnessing huge technical, technological, and civilizational progress. Many legal solutions are transformed under the influence of modern technologies. The aim of this process is to increase the efficiency, effectiveness, and safety of traditional tools. Procedural law as a multi-threaded analytical area is a participant in this because it plays an important role in the ongoing progress.

Currently, the use of electronic evidence is a matter of international interest. The main actors impacting international law are beginning to pay attention to the employment of modern technologies for practical use. This applies to artificial intelligence, cryptocurrencies, clever contracts, e-health, and electronic evidence.

The Guidelines can be considered as a general international constitution for electronic evidence. What we see is a lack of legislation at international, European, and national level. Both in law and in judicial practice, there is a legal loophole concerning the key technological principles of proceeding with electronic evidence.

The purpose of the Guidelines is not to establish binding legal standards. They amount to only as much as a practical toolbox for the Member States. The Guidelines are intended to facilitate the use and management of electronic evidence in law.

The proposed definitions of electronic evidence, trust services, and metadata can be used also beyond the scope of the Guidelines. They are technologically neutral and are not narrow, closed, or casuistic.

It is possible to use definitions adopted in the eIDAS regulation when applying the Guidelines. It results from the accepted definition of trusted services, which is synonymous with that in the indicated regulation.

Metadata are fundamentally significant for electronic evidence. The concept of metadata and related standards is the key to the Guidelines. Metadata are a powerful tool to help find records, understand them, and use them for many purposes,. Metadata tell a complete story. They enable the authentication and verification of information contained in records, as well as capture important technical details that enable the rendering of records. Understanding metadata and their proper storage allows for the effective use of electronic evidence capabilities.

Fundamental principles presented in the Guidelines have a different value from detailed guidelines. They show the path that Member States should follow. They can be taken into account as much as possible. In some sense{s?}, it is possible to apply Alexi's concept here[44].

An interdisciplinary approach is required for all professionals, including lawyers and judges working with electronic evidence. This requires practical training. A good example of training documents is the U.S Courts Guidelines for Editing Metadata[45].

In conclusion, we hope that electronic evidence is the future of court proceedings. Only with the help of electronic evidence will it be possible to improve the efficiency of today's justice system. We believe that electronic evidence is an emanation, extension, and fulfilment of such important values as equity, the rule of law, fair trial, and truth.

---

[44] M. Bohlander, *Radbruch redux: the need for revisiting the conversation between common and civil law at root level at the example of international criminal justice*, "Leiden Journal of International Law" 2011, vol. 24(2), pp. 393–410.

[45] U.S Courts Guidelines for Editing Metadata, available on the site: http://www.njd.uscourts.gov/sites/njd/files/EditMetaDataGuidePublic.pdf [last access: 07.06.2019].