Impact of the Council of Europe Guidelines on Electronic Evidence in Civil and Administrative Law

Remigijus Jokubauskas
Mykolas Romeris University, Lithuania
remigijus@jokubauskas.org

Marek Świerczyński
Uniwersytet Kardynała Stefana Wyszyńskiego, Warszawa, Poland
m.swierczynski@uksw.edu.pl

Abstract

On 30 January 2019 the Council of Europe adopted guidelines on electronic evidence in civil and administrative law (hereinafter “the Guidelines”). The article summarizes and analyses this soft law instrument and explains why its creation is important for the proper administration of justice and how it addresses and reflects technological developments, new business models and evolving case-law. Several conclusions have been identified regarding how use of the Guidelines will address current practical problems for courts and attorneys while maintaining full compliance with important principles like the right to a fair trial, protection of private life and national laws of the member states.

Keywords

1 Introduction

Court practice shows that guidelines on electronic evidence in areas of civil and administrative law are highly needed.1 Stephen Mason’s 2016 report commissioned by the Council of Europe reached the same conclusion.2 A number of such guidelines exist for criminal proceedings.3 In case of civil and administrative proceedings, however, there is almost no practical guidance at the international, European or national levels.4 Gaps remain both in law and in

2 “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” (Stephen Mason, assisted by Uwe Rasmussen) (European Committee on Legal Co-operation, Strasbourg, 27 July 2016, CDCEJ(2015)14 final). The aim of the study was to identify the problems that the different legal systems in the CoE member states are faced with in this field and in respect of which they are in need of remedies or in respect of which they have put in place solutions.
4 For example, the E-Commerce Directive contains only general non-discriminatory principle. There are some non-European documents, such as Commonwealth Draft Model Law on Electronic Evidence and Electronic Evidence: Model Policy Guidelines & Legislative Texts (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013). Comp. also general soft law instruments such as the Model Law on Electronic Commerce adopted by the Commission on 12 June 1996, following its 605th meeting and adopted by the General Assembly in Resolution 51/162 at its 85th plenary meeting 16 December 1996, including an additional article 5 bis as adopted by the Commission at its 31st meeting in June 1998. The Model Law on Electronic Signatures was adopted by the Commission at its 727th
practice. For example, in some countries submission of electronic evidence is not addressed by the law in sufficient detail. As a result, courts and administrative bodies with adjudicative functions working with electronic evidence are requesting practical guidance.

The Guidelines also reflect the development of the ECHR’s case law based on Article 6 and Article 8 of the European Convention on Human Rights (the Convention). The Convention does not lay down rules on evidence, the admissibility or probative value of evidence or on the burden of proof in civil in administrative cases. Also, it does not regulate relevance of evidence. However, the fundamental principles of equality of arms and respect of private life should be considered with due care when dealing with electronic evidence.

What is particularly new and fundamental about the finally adopted document is the attempt to propose practical genuinely advice to the courts and administrative bodies. It consists of a catalogue of the best national practice. The development of the Guidelines also promotes confidence in and acceptance of electronic evidence obtained in other jurisdictions. Also noteworthy, adoption of an international convention instead of the Guidelines would not serve such purposes due to the general legal nature of such legal instrument, the complicated process of adoption and the fact that technology is advancing at a very rapid rate.

The main part of the document consists of 35 detailed guidelines contained in separate sections. It is not possible to discuss them all in this paper. Also, the Explanatory memorandum was adopted together with the Guidelines. The Explanatory memorandum explains the Guidelines in detail and provides examples of the relevant case law, national laws and legal teachings. To illustrate the

___


5 ECHR judgment Mantovanelli v. France, petition No. 21497/93, para. 34: “Moreover, the Convention does not lay down rules on evidence as such”.

6 ECHR judgment Tiemann v. France and Germany, petitions No. 47457/99 47458/99, para. 2: “In addition, Article 6 § 1 of the Convention does not lay down any rules on the admissibility or probative value of evidence or on the burden of proof, which are essentially a matter for domestic law”.

7 ECHR judgment Centro Europa 7 S.R.L. and Di Stefano v. Italy, petition No. 38433/09, para. 198: “...that it is for the national courts to assess the relevance of proposed evidence”.


careful crafting and value of the Guidelines, we will draw attention to select guidelines, explaining the context of their creation, problems and discussion related to their preparation. The following sections will address why regulation of electronic evidence is necessary, the assumptions, sources and preparatory work supporting the Guidelines, the relevance of electronic evidence, and metadata.

2 Why Regulate Electronic Evidence?

Electronic evidence may come into play in any civil or administrative case. Obviously, electronic evidence is different from other types of evidence and specific challenges arise from dealing with it.\(^9\) Examples of current challenges include evidence collected from smartphone applications, cloud computing services\(^9\) or using other services of trusted third parties.\(^10\) Though electronic evidence is already known for decades there is no common knowledge on the differences between different types of such evidence. However, this may have direct impact on their reliability. Also, adoption of General Data Protection Regulation (GDPR)\(^12\) and Electronic Identification and Trust Services Regulation (eIDAS)\(^13\) in the EU leads to paperless data management and thus makes the original electronic evidence even more important in practice.

An example of a practical problem is identification of the source of evidence and its author, e.g. user of an e-mail account. Failure to follow proper procedures may result in lost or damaged evidence. What’s more, there are rising doubts regarding significance of evidence derived from the use of such

---


10 Comp. the Council of Bars and Law Societies of Europe (CCBE) that have produced a set of guidelines dealing specifically with ‘cloud computing’ in the legal profession.


new technologies like cloud computing\textsuperscript{14} or blockchain. The development of digital technology is dynamic and the judges and administrative staff may well face significant challenges. In every case it is necessary to assess the possibility of modification, manipulation or distortion of the data. Among other issues, the Guidelines underline awareness of potential probative value of metadata (see section 8 of this paper).

It goes without saying that professionals collecting, seizing and analysing electronic evidence should be properly educated and trained. As rightly pointed out by Stephen Mason, this is in the interests of justice and fairness between the parties, and because evidence in electronic form is now ubiquitous and an every-day part of legal proceedings.\textsuperscript{15}

For these reasons, adoption of international guidelines is important and necessary. The treatment of electronic evidence in civil and administrative proceedings has to be improved in order to ensure the good administration of justice. It is important to raise both knowledge and awareness of professionals working with electronic evidence in such proceedings.

\section{Assumptions for the Guidelines}

Essentially, the Guidelines are not aimed at harmonization of the national legislation of member states. It is not a legal mandate or policy directive. It does not represent the only correct course of action. Also, it should be general enough to accommodate different legal systems. Therefore, the Guidelines are fully in line with the principles recognized by the member states’ laws.\textsuperscript{16} For example, it underlines equivalence between written and electronic evidence. This should result in non–discrimination of electronic evidence versus other types of evidence (see second principle of the Guidelines). It is based on the

\begin{itemize}
  \item As pointed out in the proposed Draft Convention on Electronic Evidence, see Digital Evidence and Electronic Signature Law Review 13/2016.
  \item For example on December 15, 2017, the Law of Ukraine of October 3, 2017, No. 2147-VIII «On Amendments to the Commercial Procedural Code of Ukraine, the Civil Procedural Code of Ukraine, the Code of Administrative Court Procedure of Ukraine and other legislative acts» came into force, which, in particular, sets out in the new edition the Civil Procedural Code of Ukraine (hereinafter referred to as \textit{cpc}) and the Code of Administrative Court Procedure of Ukraine (hereinafter referred to as \textit{cacp}). The \textit{cpc} and \textit{cacp}, among others, regulate the issue on determining, the procedure for the provision and investigation of electronic evidence.
\end{itemize}
universally acknowledged principle that electronic evidence should have the same value as any other evidence (in particular paper evidence). The principle of assessing the probative value of electronic evidence by courts under national procedural law is also recalled.

It goes without saying that the Guidelines are not to be interpreted as prescribing a specific legal value for certain evidence. This is a matter reserved for the national law. In this respect, the Guidelines are fully compatible with the national laws, even if not drafted in exactly the same terms. On the one hand, international guidelines negotiated by representatives with different legal traditions may be drafted in different terms than is the case for national legislation. On the other hand, the flexibility of Guidelines allows member states to take into account different legal traditions and different levels of development with regard to use of electronic evidence in the courts. The Guidelines also fully respect fundamental rights, like the rule of law, right to a fair trial and right to a private life.

Out of necessity, the Guidelines aim to ensure that specific challenges related to electronic evidence are addressed, such as probative value of metadata, ease of manipulation, distortion and erasure of the electronic evidence, involvement of a third party, such as cloud or trusted services providers in the collection and seizure of electronic evidence. Undoubtedly, a differentiated approach is needed with regard to different categories of electronic evidence.

The Guidelines apply to civil and administrative proceedings (criminal proceedings are excluded) and aim to ensure that all specific aspects of electronic evidence in such proceedings are fully addressed. The Explanatory memorandum to the Guidelines explains how electronic evidence is different from other types of evidence and causes specific challenges for the courts. It gives full context to specific challenges and needs. Noteworthy, the concept of court used in the Guidelines covers all bodies with competence to settle legal disputes between parties in civil and administrative proceedings. These include courts, tribunals and even administrative bodies with adjudicatory powers.

Obviously, the Guidelines, to be useful, need to be kept under review and adapted as required. But at the same time judges and legal practitioners should be also aware of the evolution of information technology, which may impact on the value of electronic evidence. An example is emerging blockchain technology. Although no specific guideline on blockchain has been adopted yet in


18 Comp. R. Neisse, G. Steri, I. Fovino, A blockchain-based approach for data accountability and provenance tracking. In: Proceedings of the 12th International Conference on
the Guidelines, it is specifically addressed in the Explanatory memorandum to the Guidelines. More research on blockchain is necessary to determine how to legally treat blockchain and increase its compatibility with existing evidentiary rules.

4 Sources for the Guidelines

The drafters of the Guidelines explored a vast amount of literature. The full list of the relevant case law and legal teachings is provided in the Explanatory memorandum. The drafters analyzed and discussed a large number of existing national legal provisions, guidelines, jurisprudence and standards (most of them relate to criminal proceedings) to reflect the reality of electronic evidence on the rules of evidence and modes of proof. The drafting group relied particularly on the multi-jurisdictional survey conducted for CDCJ by Stephen Mason in 2016 and an excellent report on use of electronic evidence administrative proceedings presented by J. Albert in 2014. The complete set of sources and documents used in the preparatory works are listed at the end of the paper.

As there is no legal and internationally accepted definition of the definition of “blockchain” different sources were taken into consideration. Authors of this paper are in opinion that blockchain can make a real breakthrough in the field of the collection and seizure of electronic evidence in the civil and administrative proceedings. 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 blockchains suitable for the evidencing purposes.


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.
the official explanatory memorandum to the Guidelines. A number of international monographs relating to electronic evidence served as inspiration.22

Existing EU regulations and ongoing work at the Hague Conference were also used as a source of inspiration for the preparation of the Guidelines. This includes in particular the eIDAS Regulation, with focus on the legal effects of electronic signatures.23 For example, the Explanatory Memorandum makes clear that qualified electronic signatures ensuring data integrity do not require a special analysis by the court of the technology used to create them.24 It is enough to check the register of qualified trust service providers in the EU. We also have deliberately indicated a biometric signature as an electronic replacement for a handwritten signature. This is a case when a person writes his or her own signature directly on an electronic device. Depending on the applicable law, the court may consider such a biometric signature equivalent to a handwritten signature on paper.

An important regulation on the taking of evidence25 is currently undergoing an amendment process. Indeed, the formulation of specific guidelines on cross-border evidence collection has proved to be an extremely difficult task. Although the collection of data is national in nature, it is increasingly likely that it will have a cross-border character.26 An example is the location in a foreign country of the infrastructure used for processing or storage of data, or the location of a provider that allows the storage or processing of data. The Explanatory Memorandum encourage direct cooperation between courts and providers of trust or cloud services (cloud computing) in cross-border cases.

---


24 Indeed, on January 2019 Polish administrative bodies tried to invalidate legal effect of the qualified electronic signature based on SHA-1 algorithm in the public tenders. Such interpretation was overruled by the subsequent opinion of the Polish Ministry of Digitalisation dated 15.02.2019 (see https://www.gov.pl/web/cyfryzacja/algorytm-funkcji-skrotu-sha-1-nierekomendowany-co-nie-znaczy-wycofany).


As we see the Guidelines were not created in a complete legislative vacuum. Some issues have already been raised in the Council of Europe itself. In particular, for the archiving sections the Council of Ministers have decided to refer to the Recommendation on archiving of electronic documents in the legal sector,\textsuperscript{27} taking into account the technological progress that has taken place in recent years.

To this end, the drafting group took into consideration experience rising from the operation of electronic justice mechanisms already implemented in the member states. The Guidelines are also a very valuable source of information for anyone who wants to be comprehensively informed about the experience of different member states courts that were dealing so far with the electronic evidence. For example, the Explanatory Memorandum refers to the electronic justice system set up in Lithuania and Croatia.

5 Preparatory Works

The Guidelines were prepared in full coordination and with the participation of the competent representative of the CoE member states. Preparatory works were supervised by the European Committee on Legal Co-operation (CDCJ), which is the intergovernmental body responsible for the standard-setting activities of the Council of Europe in the field of civil and administrative law.

Since 1963 CDCJ has been responsible for the standard-setting activities of the Council of Europe in the field of public and private law. The achievements of the CDCJ are to be found, in particular, in the large number of binding or non-binding international legal instruments it has prepared for the Committee of Ministers (mainly treaties and recommendations).\textsuperscript{28}

It was decided that the scope of the Guidelines should include the following sections: 1) collection and seizure (of electronic evidence); 2) submission of evidence; 3) procedure to establish identity; 4) classification (of electronic evidence); 5) admissibility (use) of electronic evidence (quality, integrity and authenticity); 6) storage and preservation (of electronic evidence); 7) transmission of electronic evidence between judicial authorities. The final version of the Guidelines reflects this structure (with some variations).

\textsuperscript{27} Recommendation Rec(2003) 15 of the Committee of Ministers to member states on archiving of electronic documents in the legal sector.

The Guidelines were drawn up by an ad-hoc drafting group composed of six CDCJ members and designated experts over a period of one year (three two-day meetings were organized in Strasbourg). Mr. Seamus Carroll from Ireland was appointed as the President of the drafting group. The meetings also involved the relevant Council of Europe bodies with expertise and responsibilities in this field. The CEPEJ, the CCJE, and the European Association of Court Clerks were also invited to participate in the drafting process. The ad-hoc group also kept the CDCJ fully informed at all stages of the evolution of the guidelines drafts. The member states replied to the questionnaire of national procedures, e.g. on use of metadata in their jurisprudence which were considered by the drafting group.

6 Definitions

The Guidelines provide a small number of definitions. It is important that the Guidelines do not just concentrate on the technology. They are technology neutral.

A broad definition of “electronic evidence” is adopted in order to include all forms of electronic evidence. “Electronic evidence” means any evidence derived from any data contained in or produced by any device which functioning depends on a software program or from data stored on or communicated over a computer system or network (point (a) in the definitions section). The notion of electronic evidence is the subject of numerous elaborations in the doctrine. Therefore, the general considerations may be omitted, referring the readers in this respect to the rich literature of the subject, and instead, a few specific issues in the context of the evidence will be focused on. Noteworthy, this definition was formulated in accordance with different sources, such as the Draft Convention on Electronic Evidence.

Depending on the typology applied by a local jurisdiction, electronic evidence may take various forms, types and relate to different access methods. For example: (i) it may take form of movies, photos or sounds, (ii) the type of such evidence can be text messages or billings, (iii) data may originate from carriers or access methods, such as mobile phones, webpages, on-board computers or GPS recorders. An example is evidence obtained from websites, such as uploaded images. The types and categories of electronic evidence are not closed.

---

Examples of information that can be gathered from electronic devices are text documents, emails, text and instant messages, images and metadata, such as Internet histories. They can be used very effectively as evidence. Physical evidence is not to be considered as electronic evidence, although it may be further digitized (e.g. a digital photograph).

An electronic message is a typical example of electronic evidence, as it is originally created in electronic form by an electronic device (computer or computer like-device) and includes metadata that may be important for the trial outcome.\(^{32}\) It contains information such as text, voice, video, sound or image sent over an electronic communications network which can be stored in the network or in related computing facilities, or in the terminal equipment of its recipient. Another example is an electronic document that means any document held in electronic form. It includes, for example, email and other electronic communications such as text messages and voicemail, word-processed documents and databases, and documents stored on portable devices such as memory sticks and mobile phones.

In the Guidelines, reference is also made to concepts such as “simple” or “qualified” electronic signature, which implies possible application of other definitions adopted in the eIDAS Regulation. According to these rules, an electronic signature is defined as data that is inserted, connected, or logically linked with other data for the authentication of the latter and/or identification of the signatory. A 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 by a secure signature-creation device and certified by a valid, qualified certificate, has the same legal validity as a signature in written documents and is an admissible mean of proof in court. The functions of the administration of electronic signature are performed by the appointed governmental institution.

7 Relevance of Electronic Evidence

In a civil law system, judges enjoy authority of “free assessment of evidence” meaning that relevance of evidence is assessed in each case.\(^ {33}\) Though relevance of evidence may vary within national legal systems, the main goal of

---

adjudication is always a prompt settlement of the dispute.\textsuperscript{34} One of the main features of electronic evidence is its relevance. For instance, Stephen Mason includes relevance in the definition of electronic evidence.\textsuperscript{35} Thus, electronic evidence is coupled only with data, which has potential evidentiary value for the parties to make factual circumstances more or less probable. The notion of “relevance” should not be confused with admissibility of evidence. The evidence may be admissible, but it may completely lack relevance in the fact-finding process.\textsuperscript{36}

The Guidelines do not aim to harmonize the rules on relevance of electronic evidence, but rather suggest which peculiarities of electronic evidence courts should consider when dealing with it. The Guidelines recognize the obstacles in the effective management of electronic evidence and suggests that courts should engage in active management of electronic evidence (Guideline 17). The rationale behind this rule is to encourage courts to assess the need of electronic evidence and avoid excessive and (or) speculative provision or demand for electronic evidence.

Nowadays, parties in the proceedings may provide a large amount of electronic data and/or demand the court to collect electronic data, which they do not possess. Courts should assess difficulties of demanding electronic data, which is under control of the third parties. In general, the court has the authority to demand third parties to produce data, which is under their control.\textsuperscript{37} Such requests may significantly burden the effective case management: provision of metadata, collection of evidence controlled by a third person (for instance, cloud computing, trust service), its transfer to the court by electronic means of communication. The Explanatory memorandum of the Guidelines also recognizes the principle of proportionality regarding the collection of electronic evidence (see para. 35 of the Explanatory memorandum).

\textsuperscript{34} J. Sladic, A. Uzelac, Assessment..., p. 111.
\textsuperscript{35} B. Schafer, S. Mason, The characteristics..., p. 19: “Electronic evidence: data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence”.
\textsuperscript{36} B. Schafer, S. Mason, The characteristics..., p. 20: “Third, the definition restricts the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is decided by an adjudicator, whatever the form and level the adjudication takes. This part of the definition includes one aspect of admissibility–relevance only–but does not use ‘admissibility’ in itself as a defining criterion, because some evidence will be admissible but excluded by the adjudicator within the remit of his authority, or inadmissible for reasons that have nothing to do with the nature of the evidence”.
\textsuperscript{37} For instance, Art. 142(1) of the Code of Civil Procedure of Germany; Article 199(1) of the Code of Civil Procedure the Republic of Lithuania.
The Guidelines also recognize the need for technical expertise for the analysis of electronic evidence (Guideline 18). In general, judges enjoy discretion to require the analysis of certain evidence by experts. Such need may particularly arise when complex evidentiary issues are raised or where manipulation of electronic evidence is alleged. However, technical expertise may take quite long and increase litigation costs.

Therefore, the Guidelines recognize relevance of electronic evidence and encourage courts to evaluate the need of electronic evidence in each case and consider how collection of electronic data may affect the active management of the case.

8 Metadata

Although the prevalence of metadata has triggered scholars' attention and challenged courts already, it remains a rather obscure concept in law. Due to the increasing use of metadata in civil and administrative cases and its practical importance, the Guidelines and particularly the Explanatory memorandum address important questions relating to metadata. Noteworthy, the term metadata stems from two words: meta and data. Meta is an ancient Greek word, which means “about”.[38] Thus, legal scholars have notoriously defined metadata as “data about data”. The Guidelines follow this path and define metadata as electronic information about other electronic data.[40] The definition of metadata was scrutinized during the drafting stage. Though there is no internationally accepted definition of this concept, the working group sought to include the major traits of metadata.

Metadata can be described by the analogy of an envelope and a letter. The envelope of the letter reveals some basic information: who is the author and the addressee, when it was served to the post service and when and where it was received. Thus, it may not necessarily give a chance to see the content of the letter, but rather provides some information. Similarly, metadata provides a sort of information about digital record.

---


[40] “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.
Since metadata is indispensable from all documents in a digital form, the Explanatory memorandum picturesquely describes metadata as the “digital fingerprint” of electronic evidence. Metadata can assist in establishing the content of electronic documents and the context in which it was created, allow identification of the structural links within the electronic document (versions and drafts). It is also relevant as indirect evidence in relation to the document or serves as direct evidence itself. One of the main peculiarities of metadata is the fact that it is automatically created, without any specific actions of the user and even without his or her knowledge. In practice, courts should be cautious, that some metadata may be wrongfully altered. For instance, a person can easily manipulate metadata of the file simply by changing a date-time stamp.

A hard copy version of a document is not equal to the digital copy of document. The Explanatory memorandum emphasizes that printouts of documents (web browser screens) miss metadata. Printing of an electronic document may eliminate some or all the metadata associated with the electronic version of the document. The perils of printouts of electronic documents have been addressed in American case law.

Metadata is hidden in the digital document and it is not visible when the document is printed out into a hard copy. Metadata is often viewed only when the file is viewed in its native form. Some forms of metadata can only be viewed when the file is opened by a special program or software. Some metadata, such as file dates and size, can easily be seen by users. Other metadata may be hidden or embedded and unavailable to computer users who are not technically adept. Thus, courts should consider whether special expertise is needed to handle metadata properly.

Since metadata is indispensable from electronic evidence, courts should know what information it can provide. Of course, the amount of metadata

41 B. Schafer, S. Mason, The characteristics..., p. 27.
42 M. A. Shields, Discoverability..., p. 5.
43 B. Schafer, S. Mason, The characteristics..., p. 38.
44 M. A. Shields, Discoverability..., p. 5.
45 C. Ball, Beyond Data About Data: The Litigator’s Guide to Metadata, at p. 2 (2005): “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 at http://www.craigball.com/metadata.pdf (Access: 25.02.2019).
depends on the digital document itself. Metadata of a digital photo can differ from metadata of a MS word file or other programs. Nevertheless, metadata usually reveals various information about digital record: when and how a document was created (purported time and date), the file type, the name of the purported author (although this will not necessarily be reliable), the location from which the file was opened or where it was stored, when the file was last opened (purported time and date), when it was last modified and possibly other information.\textsuperscript{48} It also does not mean that all this information can be easily retrieved and readable, depending on the type of a digital file. For instance, metadata of an e-mail may include information address and/or names of the send and recipients, the subject line, the data and time the letter was sent.\textsuperscript{49}

The Guidelines do not address all issues with which courts may encounter when dealing with metadata. Instead, it highlights the importance of metadata and emphasizes that courts should be aware of the probative value of metadata and potential consequences of not using it (Guideline 8). Courts should not always request metadata when dealing with electronic evidence since metadata may be important, but not necessary in each case. Also, the Guidelines encourage to take care of metadata for a proper storage of electronic evidence (Guideline 25). Electronic evidence should be stored with standardized metadata so that the context of its creation is clear (Guideline 26).

To sum up, the Guidelines establish that courts should be aware of collection and submission of metadata. Metadata is usually not directly accessible. Thus, it may be difficult to collect metadata. Legal rules usually do not specify how electronic evidence should be collected, instead relying on the general rules on taking of evidence. Metadata can be found as part of the electronic evidence itself or linked to it from a separate system. Often metadata can be viewed from the “properties” section of the electronic file, but it may also be possible that it can be viewed only by specific software programs.

9 Conclusions

We believe that awareness of the wider digital context and the use of technologies such as cloud computing, trust services or blockchain are important for both judges, lawyers and administrative staff. Knowledge of electronic evidence should be an important part of initial and continuing legal education.

\textsuperscript{48} B. Schafer, S. Mason, \textit{The characteristics ...}, p. 27.

The following conclusions result from our analysis of the Guidelines presented in this paper:

1) The Guidelines do not aim to harmonize the national laws on electronic evidence, but rather reflect the current practical problems and propose guidance how courts should deal with them;

2) The Guidelines were drafted in full compliance with the right to a fair trial, protection of private life and national laws of the member states. Courts are not obliged to follow the Guidelines. They can rely on it as a soft law document or fill national legal omissions;

3) Metadata of electronic evidence is a particularly significant aspect of electronic evidence. The Guidelines emphasize that courts should address metadata with due care and assess the practical difficulties in obtaining it. Metadata is important, but not necessary in each case and courts should assess the practical problems in collecting metadata;

4) Court should engage in the active management of case when dealing with electronic evidence. In contrast to “traditional” paper documents, electronic evidence may be difficult to collect and submit to the court. Electronic evidence should be submitted in the original (electronic form) and not printed out;

5) Awareness-raising among lawyers, training and education are key to the proper implementation of the Guidelines among the member states. These include broad dissemination of Guidelines for courts and practitioners, its translation into local languages, organisation of seminars and conferences on electronic evidence. A review of technical standards related to electronic evidence may include, for example, recommended methods of storage, preservation and archiving;

6) Interdisciplinary training is necessary for all professionals, including lawyers and judges working with electronic evidence. The training may include specific challenges related to electronic evidence, such as the importance of metadata, the importance of time stamping and the use of cloud or blockchain in the collection of electronic evidence.