LAW SERIES 2022

OPINIONS and ANALYSES
OF THE INSTITUTE DE REPUBLICA

Recommendations on the evaluation of electronic evidence in civil and administrative proceedings, with particular reference to blockchain and cloud computing

DR HAB. MAREK ŚWIERCZYŃSKI, PROF. UCZ.
DR ZBIGNIEW WIĘCKOWSKI

INSTYTUT
De Republica

PUBLICATION SERIES "OPINIONS AND ANALYSES OF THE IDR" NO. 8 (10)

OPINIONS and ANALYSES
OF THE INSTITUTE DE REPUBLICA

Recommendations on the evaluation of electronic evidence in civil and administrative proceedings, with particular reference to blockchain and cloud computing

DR HAB. MAREK ŚWIERCZYŃSKI, PROF. UCZ.
DR ZBIGNIEW WIĘCKOWSKI

INSTYTUT De Republica

LAW SERIES 2022

Series editors
dr hab. Bogumił Szmulik, university professor
dr Magdalena Maksymiuk, PhD
Łukasz Gołąb, MA

Translation: Dariusz Sala

© Copyright by Instytut De Republica 2022

ISBN 978-83-67253-12-3 (online)

Publisher
Instytut De Republica
ul. Belwederska 23 lok.1
00-761 Warszawa
+48 22 295 07 29
e-mail: instytut@iderepublica.pl
www.iderepublica.pl

Table of contents

Recommendations on the evaluation of electronic evidence in civil and administrative proceedings, with particular reference to blockchain and cloud computing

Marek Świerczyński
Zbigniew Więckowski

Summary:

The Council of Europe guidelines on electronic evidence in civil and administrative proceedings were adopted by the Committee of Ministers of the Council of Europe on 30 January 2019. The draft guidelines were developed by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe. The purpose of the guidelines is to provide practical guidance for the handling of electronic evidence in civil and administrative proceedings to courts and other competent authorities with adjudicative functions; professionals, including legal practitioners; and parties to proceedings. The guidelines concern, inter alia, oral evidence taken by a remote link, the use, collection, storage and archiving of electronic evidence.

Key words:

electronic evidence, metadata, blockchain, cloud computing

1. The subject matter of the opinion

The subject matter of the recommendation is the analysis of the Council of Europe guidelines on electronic evidence in civil and administrative proceedings (CDCJ guidelines) adopted on 30 January 2019 by the Committee of Ministers of the Council of Europe. The purpose of the CDCJ guidelines is to provide Member States with practical guidance on the use of electronic evidence in civil and administrative proceedings.

The document is structured as follows. Preliminary remarks (introduction) have been included in section 4.1. Conclusions and recommendations included in section III serve as the conclusion of the conducted analysis. The particular legal issues concerning electronic evidence are presented in sections 4.2 - 4.10. The particular issues have been discussed taking into account the position of the Council of Europe as presented in the CDCJ guidelines.

The present opinion aims to improve access to justice in the era of intense development of information technologies.

2. Applied abbreviations, sources of law and European documents

2.1. Convention for the Protection of Human Rights and Fundamental Freedoms drawn up in Rome on 4 November 1950 (Journal of Laws 1993 No. 61, item 284, hereinafter: the Convention).

2.2. Convention No. 108 of the Council of Europe on the Protection of Individuals with regard to Automatic Processing of Personal Data, drawn up in Strasbourg on 28 January 1981 (Journal of Laws 2003 No. 3, item 25, hereinafter: the Convention 108; or, in its modernised version, the Convention 108+).

2.3. 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. EU L 257 of 28. 8. 2014, pp. 73 - 114, hereinafter: the eIDAS Regulation).

2.4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ. EU L 119 of 4. 5. 2016, pp. 1-88, hereinafter: RODO).

2.5. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (CM(2018)169-add1final) and their Explanatory Memorandum (CM(2018)169-add2), accessible on: https://www.coe.int/en/web/cdcj/activities/digital-evidence, hereinafter: CDCJ guidelines).

3. Main recommendations

3.1. The CDCJ guidelines organise the legal terminology regarding electronic evidence. The document defines the concept of electronic evidence, metadata and trust services. Considering the continuous technological development, the guidelines adopt a broad definition of "electronic evidence".

3.2. In the forthcoming revision of the CDCJ guidelines, it is advisable to define the terms *blockchain* and *cloud computing*, due to their close relationship with electronic evidence as well as increasing importance in legal transactions.

3.3. The CDCJ guidelines aim to increase the confidence of judges and other legal practitioners in the use of *cloud computing*.

3.4. *Blockchain* technology serves to secure electronic evidence effectively. It prevents the modification of data. *Blockchain* is suitable for evidence purposes, e.g., in disputes related to infringement of intellectual property rights.

3.5. We recommend adopting the following definition of *blockchain* in the revised CDCJ guidelines: "a sequence of blocks containing information on operations performed in a system built on the basis of algorithms recorded in a distributed, decentralised information technology system using cryptographic methods of information protection".

3.6. Three main principles should guide the assessment of electronic evidence as set out in the CDCJ guidelines: a) it is for the court to decide on the relevance of the electronic evidence (in particular this decision should not be passed on to an expert in information technology), b) the principle of neutrality of electronic evidence means lack of both discrimination and preference towards other types of evidence, c) the parties should be equally treated, this includes ensuring that the authenticity of electronic evidence can be challenged.

3.7. The methods used by the courts for hearing witnesses at a remote hearing should protect the video or audio transmission against loss of data, distortion or unauthorised disclosure. As far as technically possible, remote evidence should be given in the same manner as it is given in court.

3.8. In the case where the testimony requires confidentiality, technical means or solutions should be employed to restrict access only to authorised persons. For security

reasons, the communication systems used, whether public or private, should provide for encryption of the video signal to protect it from interception by unauthorised persons.

3.9. Electronic evidence should be presented in its original form. If a printout of electronic evidence is submitted, the court may order, upon request of a party or on its own initiative, the submission of the original of the electronic evidence. The metadata present in the original (digital) version of electronic evidence may provide the necessary context for a proper assessment of the evidence. Courts should be aware of the potential probative value of metadata.

3.10 The CDCJ guidelines refer to the EU acquis, in particular the eIDAS Regulation, in relation to electronic signatures. Courts should take into account the fact that different types of electronic signatures are in use and that they have different probative value.

3.11. Courts should follow the CDCJ guidance on procedures for managing the collection, preservation and archiving of electronic evidence. Electronic evidence requires special precautions because of the ease of it being modified, damaged or destroyed by improper handling.

3.12. Collecting and storing electronic evidence requires Member States of the Council of Europe to adopt specific tools and procedures to ensure its integrity, confidentiality and security.

3.13. In the case of electronic evidence, the risk of generating unnecessary amounts of data increases, due to the ease of obtaining it. The above may hinder the taking of evidence or even prevent its effective conduct. The active management of electronic data by the court should respect the principle of proportionality.

3.14. Courts should take a proactive approach towards protecting the integrity of electronic evidence from cyber threats, including damage or unauthorised access. Unauthorised persons should not have access to electronic evidence. Stored electronic evidence can be linked to standardised metadata. With regard to the archiving of electronic evidence, the Recommendation of the Committee of Ministers of the Council of Europe on the archiving of electronic documents in the legal sector (Rec(2003)15) remains relevant.

3.15 The CDCJ guidelines govern data migration, which involves changing storage media to maintain accessibility to electronic evidence. Neglecting migration may result in unreadable data. The recommended solution is to migrate data using web-based solutions such as *cloud computing*, which are constantly being improved as technology advances.

3.16. It is recommended that, when taking cross-border electronic evidence, the courts should cooperate closely on this issue, taking into account the existing acquis of EU regulations in this field.

3.17. The optimisation of the transmission of electronic evidence by electronic means can be achieved by implementing common technical standards and file formats as well as by digitising national judicial and administrative systems.

3.18. Knowledge of electronic evidence should be promoted among judges as well as other legal practitioners.

4. Legal analysis

4.1. Preliminary remarks (introduction)

4.1.1. The COVID-19 pandemic is an enormous medical and logistical challenge, on an unprecedented scale in modern world history. It represents a turning point of which the consequences are difficult to predict today. Many areas of our lives are being changed. Among the negative consequences of the pandemic period, such as pain and the death of loved ones, loneliness, mental disorders associated with isolation, and restrictions on the freedom to conduct business activities, however, at least one area stands out, the development of which has been exclusively enhanced by the current situation, namely new information technologies in their broadest sense. The requirement of social distance, isolation, and limited social contacts enforces the broader use of digital technologies in society. Remote learning, remote working, and remote use of cultural goods are examples of activities that, although known before the outbreak of the pandemic, were not as widespread as they currently are.

4.1.2. The COVID-19 pandemic forced changes also in the field of justice, when more than ever before it became necessary to use new tools and methods for processing and managing electronic evidence. The Council of Europe guidelines on electronic evidence in civil and administrative proceedings, adopted by the Committee of Ministers of the Council of Europe nearly a year before the outbreak of the pandemic in Europe, i.e., on 30 January 2019, deserve special attention. The purpose of the guidelines is to provide practical guidance on the use of electronic evidence in civil and administrative proceedings, for courts and other competent authorities exercising a judicial function, for professionals, including lawyers, and for parties to proceedings. The guidelines concern the taking of evidence remotely, the rules on the handling of electronic evidence, the collection, seizure and transmission of evidence, the relevance, reliability, storage and preservation, archiving, as well as raising public awareness

of the importance of electronic evidence and the need for training in this field in the Member States.

4.1.3. The guidelines are the first such international instrument prepared with the aim of supporting the 47 Member States of the Council of Europe in adapting the justice system to the issue of electronic evidence in civil and administrative proceedings. The adopted guidelines represent an important stage in the process of adapting the judiciary to the information technology revolution in the administration of justice.

4.1.4. The CDCJ guidelines have the advantage of being adopted as soft-law. Imposing binding solutions on Member States might fail. It is for Member States to decide whether and how the guidelines will be implemented in their legal systems.

4.1.5. The CDCJ has prepared not only the text of the guidelines, but also an *Explanatory Memorandum*, which acts as an official commentary to the guidelines, setting out in more detail the possibilities and conditions for the handling of electronic evidence in civil and administrative proceedings.

4.1.6. Taking into account the specific nature of all types of international acts, which by their very nature require numerous compromises to be made, the adopted text of the guidelines should be assessed positively. The document is not free of flaws and shortcomings, however, it is possible to remove them at the stage of revising the guidelines in the future. For the moment, not only should the adoption of the document by the Council of Europe be regarded as a success of the organisation, but the adopted formula of the instrument (soft law) should also be praised, as it gives Member States the possibility of flexible adaptation. The differences in the legal systems of Member States have been taken into account. The purpose of the guidelines is not to establish binding legal norms (these would appear if the convention were adopted) and to harmonise the laws of Member States, but to provide practical guidance in order to strengthen efficiency and quality of justice in the field of electronic evidence. The guidelines may be applied only to the extent to which they are not inconsistent with national legislation.

4.1.7. As we have mentioned, to date there are few standards at international, European or national law level for electronic evidence. On the other hand, which is also one of the consequences of the pandemic, courts are increasingly confronted with the need to deal with electronic evidence. This type of evidence differs in many respects from previously known types of evidence (the potential probative value of metadata; the ease with which electronic evidence can be manipulated and distorted; the involvement of third parties in the collection and archiving of electronic evidence, e.g., Internet service providers). Consequently, there is a legitimate need not only to raise the awareness of electronic evidence, but also to change the accepted manner of handling it in civil and administrative proceedings.

4.2. Recommendations on the terminology of electronic evidence

4.2.1. The CDCJ guidelines define key concepts such as electronic evidence, metadata and trust services. It should also be considered appropriate to define at least two additional concepts in the revised version of the guidelines: *blockchain* and *cloud computing*, because of their close link to electronic evidence.

4.2.2. In the view of ongoing technological developments, the guidelines adopt a broad definition of "electronic evidence". It may take the form either of text (e-mail, SMS), video, photographs or audio recordings. Data may come from a variety of media or access methods, such as mobile phones, websites, on-board computers or GPS recorders, including data stored in the cloud computing.

4.2.3. Metadata means data of other data (e.g., date and time of creation or modification of a file or document, date and time of sending the data). Metadata is usually not directly available to users and requires additional steps in order to be disclosed.

4.2.4. Trust services play an important role in the identification, authentication and security of electronic exchange. The guidelines adopt the definition of "trust service" as set out in Article 3 para. 16 of the eIDAS Regulation, i.e., an electronic service typically provided in return for remuneration and comprising the creation, verification and validation of electronic signatures, electronic seals or electronic time-stamps, recorded electronic delivery services and certificates related to these services; or the creation, verification and validation of website authentication certificates; or the maintenance of electronic signatures, seals or certificates related to these services.

4.2.5. In the adopted version of the guidelines, definitions of *cloud computing* and *blockchain* did not appear, despite discussions within the CDCJ on the need for their introduction. Ultimately, both concepts are only referred to in the *Explanatory Memorandum*.

4.2.6. As regards *cloud computing*, the issue of data sharing (cloud), i.e., storing certain data on different servers that may be located in different physical locations (a common security technique), has been raised. The global nature of the Internet and the growing importance of cloud computing services make it increasingly difficult to assume that access to data is strictly national. There is the need to increase awareness and trust among judges and other legal professionals for cloud storage of electronic evidence. Direct cooperation between courts and trust service providers should be encouraged. When choosing a provider, factors such as where the service provider is based, where the data is processed and the existence of local legislation governing access to data should be taken into account.

4.2.7. *Blockchain* technology can be defined as a distributed ledger, which refers to a list of records (blocks) that are linked to each other and secured cryptographically, in

a decentralised *peer-to-peer* network. The functionality of the *blockchain* makes the digital record resistant to data modification. The data registered in a particular block cannot be modified retroactively without modifying all subsequent blocks, which requires the approval of the majority of the networks. Thus, *blockchain* is suitable for evidentiary purposes. For instance, § 1913 of the Vermont Rules of Evidence (USA) states that: "(1) any digital record electronically registered in a blockchain is self-authenticating, under 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) an affirmation that the record was maintained in the blockchain as a regular conducted activity". In China, in a judgment of 28 June 2018, the Hangzhou Internet Court ruled that in the case before it (an intellectual property dispute), the data stored on the *blockchain* platform was sufficiently reliable and free from distortion to be relied upon and was accepted by the court as reliable evidence in the case.

4.2.8. Defining *blockchain* in the text of the guidelines proved to be a too difficult challenge for the CDCJ. Therefore, we think that when revising the guidelines, the definition of *blockchain* proposed in the Polish literature by D. Szostek may be used: "a sequence of blocks containing information on operations performed in a system built on the basis of algorithms recorded in a distributed, decentralised information technology system using cryptographic methods of information protection"[1].

4.3. Recommendations on the main principles for handling electronic evidence

4.3.1. Three main principles, set out in the CDCJ guidelines, should guide the formulation of the main principles for dealing with electronic evidence.

1. It should be for courts to decide on the potential probative value of electronic evidence.
2. The principle of neutrality of electronic evidence implies on the one hand no discrimination and on the other hand no favouring of electronic evidence in court proceedings[2].

[1] D. Szostek, *Blockchain a prawo*, Warszawa 2018, p. 42.

[2] "Although Article 6 of the Convention guarantees the right to a fair trial, it does not regulate the admissibility of evidence or its evaluation, which is therefore primarily a matter for domestic law and the national courts" (see García Ruiz v. Spain, no. 30544/96, para 28).

3. The requirement of equal treatment of the parties to proceedings with respect to electronic evidence means, in particular, allowing a party to challenge the authenticity of particular electronic evidence[3].

4.4. Recommendations on remote hearings

4.4.1. Oral evidence taken via a remote link (this does not include pre-recorded oral evidence), is considered electronic evidence under the CDCJ guidelines. This applies to oral evidence taken by means of a videoconferencing platform (which allows the transmission of synchronised video and audio in real time). The guidelines emphasise that not all oral evidence can be taken via a remote link. It may be necessary to take the witness's testimony in person and to observe their behaviour during their hearing. The disadvantage of remote connection is that some of the witness's reactions (in terms of non-verbal communication) cannot be fully observed. It is important that judges, lawyers and supporting staff are aware of the potential differences between in-person and remote testimony.

4.4.2. In the case where the testimony requires confidentiality, it is necessary to use technical means or solutions which restrict access only to authorised persons. Equipment ensuring the integrity of telecommunications transmission will ensure that the court and the parties have adequate opportunity to hear the witness remotely.

4.4.3. The guidelines require that the technology used should allow for questions to be asked during the witness's testimony (if the procedural rules so provide), particularly where the evidence is crucial to the decision of the case. This requirement cannot be met when transmission is distorted due to insufficient connectivity or when the parties' access to technical means is limited. This may result in an unfair advantage for one of the parties. As far as it is technically possible, remote evidence should be taken in the same manner as in court.

4.4.4. Applied methods should provide adequate safeguards against loss, distortion or unauthorised disclosure of the image or sound. The court may verify the identity of the person giving evidence by requiring the person to present a relevant document, such as a valid identity card, passport or driving licence. A solution applied in some countries is to connect with the witness by means of a controlled link, following correct verification of the answers given. Alternatively, the connection could be

[3] "Although Article 6 of the Convention guarantees the right to a fair trial, it does not regulate the admissibility of evidence or its evaluation, which is therefore primarily a matter for domestic law and the national courts" (see García Ruiz v. Spain, no. 30544/96, para 28).

made by verifying the data via the website of the bank, where the person has his/her account.

4.4.5. For security reasons, the communication systems applied, whether public or private, should at least provide video encryption to protect against interception. In accordance with the guidelines, it is possible to receive evidence via a private connection if permitted by national law, provided that the applied solutions ensure sufficient technical security and comply with procedural safeguards. Private connection means a communication system that is not an official governmental system specifically designed for the purpose of taking evidence in court. We recommend that electronic evidence be uploaded to the secure server of the relevant court.

4.5. Recommendations on the format of electronic evidence

4.5.1. Electronic evidence should be submitted to the court by the parties in its original format. In the case of the submission of a printout of electronic evidence, the court may order, upon request of a party or on its own initiative, that the original of the electronic evidence be provided by a competent person. Geolocation data is an example of evidence which may be relevant for the resolution of a case, provided that it is submitted in its original - digital - version. Providing printouts of dynamic websites or voice transcriptions is not compatible with the nature of electronic evidence, which provides, inter alia, such valuable data as metadata. Metadata provides the context necessary to evaluate the evidence (data) and courts should be aware of its potential probative value. They may be used to trace and identify the source as well as the purpose of the communication, the details of the device that generated the electronic evidence, the date, time, duration and type of connection. Metadata can be relevant as either indirect evidence (such as indicating the most appropriate version of a document) or as direct evidence (such as a document in file form).

4.5.2. The demand to accept only files in their original format is justified, inter alia, because printouts of electronic evidence can be easily manipulated. A screen printout from a web browser is not reliable evidence since it is nothing more than a copy of the screen. It can be modified in a very simple way, as no special software or hardware is needed.

4.6. Recommendations on electronic signatures

4.6.1. Regarding the different types of electronic signatures, the guidelines aptly refer to the EU acquis, in particular the eIDAS Regulation. "Advanced electronic signature" means an electronic signature which meets the requirements of Article 26 of the eIDAS Regulation. "Qualified electronic signature" means an advanced electronic signature which has been created by means of a special device designed for that purpose, i.e., having a "qualified electronic signature certificate", i.e., a certificate issued by a natural or legal person who provides one or more qualified trust services ("qualified trust service provider") and who is authorised to provide such services by the competent supervisory authority.

4.6.2. Currently, most electronic evidence lacks an advanced or qualified electronic signature and is not secured otherwise. However, they should be recognised by courts as electronic evidence (with the probative value of such evidence varying depending on the particular case), taking into account, for instance, the various trust services related to electronic document management and signatory identification that are available worldwide. One of the examples is the biometric signature, which is the method of obtaining an electronic version of a handwritten signature, in which a person places his or her signature on an electronic device using a special stylus and pad. Depending on the applicable law, a court may consider such a biometric signature to be equivalent to a handwritten signature.

4.7. Recommendations on the collection, preservation and archiving of electronic evidence

4.7.1. The CDCJ guidelines also address the important issue of managing the collection, preservation and archiving of electronic evidence, particularly in the context of the need to reuse evidence. Electronic evidence requires special precautions, due to its nature and the ease with which it can be modified, damaged or destroyed by improper handling. Otherwise, it will be useless or lead to inaccurate conclusions.

4.7.2. In principle, in civil and administrative proceedings, it is the parties who are responsible for the proper collection of electronic evidence. Different types of data may require appropriate methods of collection (especially in the context of preventing damage to the integrity of evidence). When dealing with significant cases, parties should consider collecting electronic evidence with the assistance of an information technology specialist or a public notary. Authentication of electronic evidence may also be carried out by other legal professionals.

4.7.3. It should be noted that although judges and legal professionals have increased their knowledge and experience in handling with electronic evidence, there is still lack of uniform standards in this field. The collection and storage of electronic evidence requires Member States to adopt special tools and procedures to ensure its integrity, confidentiality and security. However, it is important in the framework of existing or planned procedures to take into account the need to create and archive back-up copies (also in original format) in case one of the storage methods fails.

4.7.4. In the case of the court's acceptance of electronic evidence, the guidance rightly indicates that its acceptance is only justified if it is useful for evidence purposes. There is a risk that the ease with which a party can obtain electronic evidence may result in a large amount of unnecessary evidence. The above may make it difficult or even impossible to handle it effectively. Active data management should respect the principle of proportionality. Each party's request to present electronic evidence should be considered with regard to its substance, in particular its suitability for evidence purposes. Parties should be entitled to challenge such requests.

4.7.5. The reliability of electronic evidence may be challenged due to the separation of digital identity from physical identity. According to the CDCJ guidelines, courts should seek to establish the identity of the creator of the electronic data. It seems reasonable to ask, however, whether it is not for the party relying on the evidence to show who the creator of the relevant content is. The guidelines aptly point to objective ways of establishing identity when the applicable law is silent on the subject (electronic signature, checking the e-mail address from which the document was sent). Trust services can provide support in ensuring the reliability of evidence. The most popular appear to be the certification of electronic signatures[4] and time-stamping[5].

4.7.6. The guidelines encourage, to the extent permitted by applicable law and subject to the discretion of the court, the admission as evidence of all types of electronic evidence. In the case of a dispute, the parties will generally determine the issues relevant to the adjudication of the case and, unless one of the parties raises an objection that the electronic evidence is not authentic, the court is not obliged to raise the issue on its own initiative. A party who intends to rely on electronic evidence may be required to demonstrate its authenticity - for instance, by providing metadata or applying for an appropriate legal order to obtain additional data from another person (e.g., a trust

[4] Electronic signature certificates, sometimes referred to as a person's "digital identifier", may guarantee both the authenticity and integrity of data. In the case where the identity of the person making the electronic signature is in doubt, the court may require the electronic signature service provider to make a statement regarding the matters on which it is competent to provide evidence.

[5] Time-stamping (time attestation) is a mechanism that allows the integrity of data to be proven. It proves that the data existed at a specific point in time as well as that it has not been modified. Time-stamping is a valuable aspect of electronic evidence as it contains important metadata regarding when it was created.

service provider) when the party challenges the electronic evidence. The reliability of electronic data can be proven by any means, for instance by a qualified electronic signature or by other similar identification methods which ensure the integrity of the data. It is for the applicable law to determine the legal effect of electronic signatures, for instance by specifying that only a qualified electronic signature should have the equivalent legal effect of a handwritten (ink) signature, or by requiring that the signature creation device be under the sole control of the signatory. Although the guidelines were created to assist Council of Europe member states (47 countries) to ensure data integrity, the guidelines refer to a register of qualified trust service providers in the EU.

4.7.7. The CDCJ guideline regarding the burden of proof requires further clarification. Vulnerable persons, i.e., consumers, children, persons with disabilities may not be technically or economically able to provide electronic evidence. In such a case, if they benefit from statutory provisions that facilitate or shift the burden of proof to the other party, such provisions take precedence over the guidelines. We entirely agree with the view stated in the guidelines that the courts should play an active role in cases involving vulnerable people. It would be helpful to disseminate remote participation in court proceedings to those in need of support.

4.7.8. The CDCJ guidelines also take into account the increased probative value of public (official) electronic systems that generate electronic evidence. The established European standard is to treat data from electronic public records as official documents.

4.7.9. The CDCJ guidelines also regulate the storage and archiving of electronic evidence. Storage refers to the duration of a particular civil or administrative proceeding, archiving refers to the time following the conclusion of the proceeding. The court may store electronic evidence, for instance, on portable devices (memory cards), servers, backup systems or other data storage (including *cloud computing*). Electronic evidence should be stored and archived in its original format (i.e., not in printed form) in compliance with applicable law.

4.7.10. Courts should take a proactive approach to protecting the integrity of electronic evidence from cyber threats, including damage or unauthorised access. By focusing on prevention, courts can prevent the impact of cyber threats on the integrity of electronic evidence and reduce overall cybersecurity risks. Regardless of the storage method used, unauthorised persons should not have access to electronic evidence.

4.7.11. Stored electronic evidence can be linked to standardised metadata. The implementation of international standards for metadata ensures a certain level of consistency in

the storage of electronic evidence. As creating standardised metadata can be difficult and time-consuming, courts can use tools that help generate standardised metadata[6].

4.7.12. As regards archiving, the Recommendation of the Committee of Ministers of the Council of Europe on the archiving of electronic documents in the legal sector (Rec(2003)15) remains valid. National law usually determines the storage periods and technical conditions for archiving. The electronic data medium, if used, should be accompanied by an identification certificate containing basic data relating to it. Such a medium should be adequately protected, in particular against loss, harmful effects of chemical agents, magnetic or electric fields, heat, light and mechanical damage.

4.7.13. According to the guidelines, archiving services in the courts may verify, possibly by means of an electronic signature or other electronic procedures, that electronic evidence is archived by qualified specialists or competent organisations and that the data has not been modified by them. Member States should ensure that organisations entrusted by law with archiving duties have the necessary means to archive electronic evidence.

4.8. Recommendations on data migration

4.8.1. The CDCJ guidelines also address such an important and sensitive issue as data migration, i.e., changing the storage medium in order to maintain accessibility to electronic evidence. Neglecting migration may result in unreadable data. Electronic documents can be archived by periodically transferring data from one storage medium to another or from one format to another. The migration should also concern the metadata of the archived electronic documents. Migration to a new storage medium should be carried out regularly when it is appropriate due to technological developments.

4.8.2. According to CDCJ guidelines, archiving evidence on CDs, DVDs and other optical discs that become unreadable due to physical or chemical deterioration should be avoided. There are various causes ranging from oxidation of the reflective layer to physical abrasion of the surface or edge of the disc, including visible scratches, to other types of reaction with contaminants.

4.8.3. Migrating data to networked facilities, such as cloud computing, which is constantly improving due to advances in the technology of the storage medium and hardware,

[6] Many tools are available to create standardised metadata. For instance, a metadata management tool can generate an XML (eXtensible Markup Language) file containing metadata associated with electronic evidence. XML files do not require professional software. The tool can simplify both the storage and the retrieval of electronic evidence. In this respect, international standards applicable to metadata, such as those published by the International Organisation for Standardisation (ISO), should be followed.

is also worth considering. Cloud archiving can also provide greater control over costs through the ability to pay only for the required space.

4.9. Recommendations on cross-border evaluation of electronic evidence

4.9.1. Although the use of electronic evidence is frequently strictly national in nature, it is increasingly common that it also involves other countries (cross-border element). The location in another country of the infrastructure used to process or store the data, or of the provider who enables the storage or processing, may be an example.

4.9.2. Moreover, there are significant differences among national procedural rules on the taking of evidence abroad. Courts using such evidence should take the differences into account. It is recommended that, when taking electronic evidence across borders, the courts should cooperate closely on this issue. The requesting court should be informed on the procedural rules applied by the requested court in order to adapt, if necessary, its assessment of the electronic evidence. In particular, taking of evidence abroad should not result in a breach of fundamental principles of procedural law.

4.9.3. The efficiency of proceedings is significantly improved when electronic evidence can be transmitted to other courts (including foreign courts) in its original format (including metadata) instead of being printed and sent. Optimisation of the process of transferring electronic evidence by electronic means may be achieved by implementing common technical standards and file formats as well as by digitising national judicial and administrative systems. Having regard to the higher risk of destruction of electronic evidence, relevant procedures should be adopted at national level that allow for the secure transmission of electronic evidence. Data integrity and security rules should be taken into account when evidence is transmitted (the use of trust services may be useful to ensure proper transmission of electronic evidence). If the transmission of data requires confidentiality, it may be necessary to use technical measures or solutions, such as encryption, that restrict access to secure communication only to authorised persons.

4.10. Recommendations on education regarding electronic evidence

4.10.1 Knowledge of the specifics of electronic evidence, as well as the CDCJ guidelines should be promoted among judges and other legal professionals. The possibility of

the use of electronic evidence in civil and administrative proceedings should also be promoted to the public. Training courses are recommended to discuss specific issues related to electronic evidence, such as the importance of metadata and time-stamping, the use of *cloud computing* or *blockchain* in evidence collection, as well as the need to submit electronic evidence in its original format and not as scanned images or printouts. Instruction on substantive and procedural issues in the context of electronic evidence should be a regular part of legal education.

Dr hab. Marek Świerczyński, university professor, advocate in the Kieszkowska Rutkowska Kolasiński Law Firm, consultant of the Council of Europe on information technology (CDCJ, CEPEJ), associate professor at the Institute of Legal Sciences at UKSW. ORCID: 0000-0002-4079-0487; m.swierczynski@uksw.edu.pl

Dr Zbigniew Więckowski, assistant professor at the Department of Civil Law and Private International Law at INP UKSW, Deputy Director of the Institute of Legal Sciences at Cardinal Stefan Wyszyński University. ORCID: 0000-0001-7753-3743; z.wieckowski@uksw.edu.pl

INSTYTUT
De Republica

Our ambition is to support Polish scientists and promote their achievements. The main tasks of the Institute include unlocking the potential of Polish science by promoting and popularising Polish research thought in the field of the humanities and social sciences, as well as creating mechanisms and social capital to organise around the idea of statehood.

The Institute De Republica is a modern expert, promotional and publishing centre for fields of science which are undervalued in the country and abroad, although being of great importance for proper understanding of history and social phenomena. Another equally important aspect in this respect is the cooperation with universities, research and analysis institutes from Poland and all over the world.