ELECTRONIC EVIDENCE IN INTELLECTUAL PROPERTY DISPUTES UNDER THE COUNCIL OF EUROPE’S GUIDELINES

by

MAREK SWIERCZYNSKI*, REMIGIJUS JOKUBAUSKAS”

On 30 January 2019 the Council of Europe adopted guidelines on electronic evidence in civil and administrative law accompanied by the Explanatory Memorandum. The authors summarize and analyse this soft law instrument with respect to intellectual property (hereinafter “IP”) disputes. They explain 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 in IP disputes. Both authors took active part in the preparatory works and believe it is in the interest of justice and effective IP protection that these guidelines are publicly available in the member states and widely disseminated among professionals dealing with electronic evidence.

KEY WORDS
Council of Europe, Electronic Evidence, Intellectual Property Enforcement, Metadata

* m.swierczynski@uksw.edu.pl, Professor of Law at the Department of Civil Law and Private International Law of the Faculty of Law and Administration of the Cardinal Stefan Wyszyński University in Warsaw, Poland. He is the author of numerous scientific publications in the field of private international law, civil law, health law and IT law.

” remigijus@jokubauskas.org, PhD in Law candidate at Mykolas Romeris university, Lithuania. His principal areas of interests are civil proceedings, corporate insolvency law. He was selected to the Fulbright Foreign Student Program for the 2018–2019 academic year to undertake research in Law at the University of Missouri, Columbia, USA.
1. INTRODUCTION

Effective enforcement of intellectual property rights requires proper handling of electronic evidence in courts. In this respect EU Members States should adapt their court practice to the latest *Guidelines of the Council of Europe on electronic evidence in civil and administrative proceedings* dated 30 January 2019 (hereinafter the “CoE Guidelines”). This is particularly important due to the new rules on IP protection in the digital single market, but also the factual considerations, such as digitalisation of the court proceedings accelerated due to coronavirus pandemic in 2020. We would like to canvass the difficult issues related to electronic evidence in IP disputes and the CoE Guidelines are in the centre of our concerns. *The Council of Europe* (hereinafter “the CoE”) has, among other duties, the task of continuing the on-going reflexion about the development of the new information technologies (IT) to improve the efficiency of justice. The regulatory efforts of the CoE could lead to higher quality standards of civil procedures.

The objectives and principles set out in the rules for protection of IP rights in national systems remain still valid, but there is an urgent need to adapt the procedural standards to the new technological reality. It is necessary to eliminate obstacles to effective management of electronic evidence in the national justice systems. The shortcomings are due to the lack of common standards and the diversity and complexity of the taking of evidence procedures. The correct handling of electronic evidence in courts triggers practical difficulties.

Certain aspects may be emphasized. For example, the European courts tend to request printouts of the electronic evidence from the parties and ignore the significance of the metadata. Some courts reject or ignore upfront

---


evidence presented in electronic form. Other courts take very liberal approach and fail to test reliability of electronic evidence. There is also a question if the credibility of evidence would be better judged in a physical courtroom.

The case laws illustrates the difficulties with which the IP right holders encounter in practice. The court typically requires the plaintiff to submit appropriate evidence stating that the defendant used protected goods to which the plaintiff has copyright. A general statement of the plaintiff on the use of the goods by the defendant seems not to be considered by the court as sufficient to prove the infringement of copyright. The plaintiff had to submit actual evidence to prove his claims.

There are good reasons to assume that electronic evidence become an increasingly common mean of proving the facts in IP disputes. In the past, it was predominantly concerned with conflicts arising from the use of the Internet, such as disputes over e-commerce transactions. Today, with accelerating digitalisation of courts it becomes a common practice. Therefore, we need to learn more about electronic evidence and establish effective ways how to prevent its destruction, manipulation or alteration. Such risks in IP disputes are particularly high due to intangible nature of protected goods.

As a result of the development of digital technologies, the role of the Internet increases as a major market for the distribution of and access to IP protected goods. Nevertheless, many significant differences remain with regard the treatment of electronic evidence in IP cases under national laws. These differences do not merely reflect technical divergences between national legal systems. However, in recent years the digital market has become even more complex. This is due to a mixture of concurrent factors such as the globalization of business and commerce, the increasing role of international providers of IP protected content (e.g. Google, Netflix, Microsoft), and the never-ending expansion of the Internet and other communication technologies.

---

The CoE Guidelines can be treated as an important supplement to international and regional rules on enforcing IP rights. In the EU the applicable rules can be found in the Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights (hereinafter “the Enforcement Directive”) adopted on 29 April 2004, that contains a comprehensive regulation on issues related to evidence, including its gathering and securing (protection). On international level this is the TRIPS Agreement that also contains provisions for the enforcement of intellectual property rights, including procedural measures for the protection of intellectual property rights in part III is entitled “Enforcement of rights intellectual property”.

The aim of this paper is to answer the question how current national regulations on civil proceedings can be further adapted to the needs of the practice in the light of the CoE Guidelines. It should be noted that procedural frameworks differ between the member states, even when they regulate similar issues of electronic evidence. The structure of this paper is as follows. We plan to answer this research question by presenting the solutions provided by the CoE Guidelines and recommending how it can be implemented to the national court practices. A major issue is the used normative framework (or more specifically lack thereof) as regards to the electronic evidence. The CoE Guidelines do not require the member states to amend the national law but we recommend to go step further and make such change.

2. WHAT CAN BE TREATED AS ELECTRONIC EVIDENCE IN IP DISPUTES?

The CoE Guidelines provide definitions of the key terms, including electronic evidence. Certainly, the definition of electronic evidence should be broad enough to cover all types of evidence, regardless of their origin. For the purposes of the CoE Guidelines, “electronic evidence” means any evidence of data contained in or generated by any device whose operation

---


depends on software or data stored in a computer system or in a network or transmitted over a computer system or over a network.\textsuperscript{12} We recommend adopting this definition in the national regulation on evidence.

There is no doubt that it is a broader concept than a document, a typical evidence submitted by the parties in IP disputes so far and explicitly defined in the national laws. This approach undergoes a change now as the new types of evidence are collected by the parties. Protected goods often include not only text but also visual images or sound for computer reading that are converted into bits in order to be transmitted over computer networks. An example is a website. From the technical point of view, it includes the source, result and database codes, and from the visual point of view: texts, graphic materials, animations, videos, sound sequences, etc.

What is even more important for the national regulator, under the CoE Guidelines electronic evidence relates to any method of data sharing. Whether online or stored on a computer, smartphone, separate hard drive, USB stick or stored using cloud computing services. There should be no distinction between data created in analogue or digital form and data created digitally. Therefore, scanned images or documents are also included in this definition.

In court practice, however, it happens that courts of lower instance fail to assess or even admit non-standard evidence presented by the claimant. In one of such cases \textit{Polish Supreme Court} rightly pointed out that the \textit{Polish Code of Civil Procedure} does not contain a closed catalogue of evidence and it is permissible to use any source of information on facts relevant to the decision on the case, as long as it is not contrary to the provisions of law.\textsuperscript{13}

Undoubtedly, electronic evidence become more complex. Most of what we consider now as evidence in the courts is static. Such examples are documents or e-mails. However, more often courts deal with complex evidence, such as a multimedia, a record of an Internet session or the sophisticated system of linking. This new type of dynamic evidence requires much more experience and knowledge from both the parties’ representatives and the courts. An example of technology used to secure

\textsuperscript{12} This definition of electronic evidence is included in the “Definitions” section of the CoE Guidelines.

\textsuperscript{13} The Supreme Court of Poland. (2008) I CSK 138/08, LEX No. 548795.

electronic evidence in intellectual property cases, that requires such knowledge, is blockchain\textsuperscript{14} or evidence generated with use of artificial intelligence.

3. PECULIARITIES OF IP DISPUTES
The CoE Guidelines do not establish separate rules for electronic evidence in IP disputes. However, these disputes often involve electronic data and require specific legal and technical knowledge. The Enforcement Directive establishes specific rules for protection of IP holders in civil proceedings and recognizes that measures, procedures and remedies which ensure enforcement of intellectual property rights shall be effective, proportionate and dissuasive. A. Kur and T. Dreier underline that it lays down two specific provisions concerning evidence in IP disputes:

"access to evidence which is in the hands of the infringer (Article 6) and preservation of evidence (Article 7)."\textsuperscript{15}

It is however disputable whether the measures established in the Enforcement Directive are applicable to all IP disputes. For instance, whether it is applicable in case of peer-to-peer file sharing infringements and whether it is applicable to acts carried out on a commercial scale. Interestingly, in some legal traditions such “exploratory evidence” as established in Article 6 of the Enforcement directive is disputable. For instance, German civil law prohibits exploratory evidence (Verbot des Ausforschungsbeweises) since the underlying principle is that each party must plead and prove the facts (Beibringungsgrundsatz).\textsuperscript{16} In Lithuania the plaintiff can ask the court to recover written evidence from participants in the proceedings or from other persons if they possess such evidence.\textsuperscript{17} If the court’s request to submit written evidence is not fulfilled and no substantial reasons for inability to submit evidence are presented or the court declare the reasons poor, the culprit persons may be imposed a fine within three hundred Euro.\textsuperscript{18}

\textsuperscript{17} Article 199(1) of the Code of Civil Procedure of the Republic of Lithuania.
\textsuperscript{18} Article 199(6) of the Code of Civil Procedure of the Republic of Lithuania.
One of the peculiarities of IP disputes is that the infringer is often in control of the relevant data and it may be difficult for the plaintiff to produce *prima facie* evidence of the infringement. The Enforcement Directive employs the term “control” in Article 6 which itself raises some practical dilemmas. For instance, how the word “control” should be interpreted? Does it cover evidence which is only in possession of the opposing party and (or) also evidence which are controlled by the third party? Even if the opposing party has the evidence, does it have to exercise any request which would require substantial costs? It seems that in such cases a clear answer is impossible. The European Commission suggests that in IP disputes the opposing party should carry out a diligent search for the evidence within its organization and it should be proportionate and not abusive.\(^\text{19}\)

Furthermore, IP disputes are generally complex, involving difficult legal and factual questions and multiple parties. In practice it can be difficult for the plaintiff to specify evidence which are in possession of the opposing party or a third person and satisfy court’s request to specify the exact nature, location, reference numbers or contents of the requested documents.\(^\text{20}\) The “excessive level of detail” which the plaintiff has to specify what evidence the court should demand from other persons may hinder effectiveness of civil proceedings and “fair and equitable” nature of such requirements.\(^\text{21}\) Therefore, though the plaintiff should specify certain evidence which the court should request as specific as possible, this duty shall be interpreted within the reasonable limits, in light of the specifics of the case at hand.\(^\text{22}\) The national laws establish that court may order to present evidence upon a reasonable request from a party.\(^\text{23}\) Also, in some member states the national regulation imposes an obligation

---


\(^{20}\) Ibid.

\(^{21}\) Ibid.

\(^{22}\) Ibid.

to preserve electronic data when as soon as the litigation is commenced in order to avoid spoliation of relevant data.24

Particularly complex are disputes when infringements are committed online. For instance, infringements committed by using peer-to-peer file sharing protocols which involve a number of infringers. In such disputes the use of electronic evidence is almost inevitable and the types of electronic evidence in IP disputes may be ubiquitous: IP addresses, information on websites and, information possessed in the respondent’s and (or) third parties’ servers (“cloud computing”), software programs. Moreover, electronic evidence may be possessed by the opposing party or a third person, likely in another jurisdiction.26

The CoE Guidelines recommend the member states to consider the peculiarities of electronic documents and amend the national laws on evidence accordingly. Also, the guidelines emphasize the importance of effective case management from the courts. The effective case management requires consideration whether certain proves of the validity of electronic evidence is required (for instance, shall be party submit the relevant metadata or a printout of the document is sufficient). The guidelines also recommend considering the practical issues of collection of electronic evidence which are in possession on the third party, such as the provider of trust services.

4. METADATA IN IP DISPUTES

Metadata is indispensable from electronic evidence.27 The CoE Guidelines establish that metadata is significant for the courts when dealing with

24 Practice direction 31b relating to disclosure of electronic documents in civil proceedings prepared for UK courts. [online] Available from: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b) [Accessed 7 February 2020]. “As soon as litigation is contemplated, the parties’ legal representatives must notify their clients of the need to preserve disclosable documents. The documents to be preserved include Electronic Documents which would otherwise be deleted in accordance with a document retention policy or otherwise deleted in the ordinary course of business.”

25 In a P2P network, the “peers” are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client. While P2P networking makes file sharing easy and convenient, is also has led to a lot of software piracy and illegal music downloads. See The Computer Dictionary. [online] Available from: https://techterms.com/definition/p2p [Accessed 23 February 2020].


Generally speaking, metadata is electronic information about other electronic information (data about data). Metadata is usually created automatically by the software and without user’s knowledge. The Explanatory memorandum recognizes that metadata contains some evidentiary value of electronic data (the date and time of creation or modification of a file or document, or the author and the date and time of sending the data) and it is usually not directly accessible. We recommend that member states adopt such definition of the metadata in national regulation.

A practical dilemma is not only what information metadata may reveal, but also how it can be retrieved. Metadata is often hidden in the electronic file and is viewed only when the file is viewed in its native form. In some cases, special software may be necessary to retrieve metadata and courts may need technological expertise.

One of the common blunders in civil proceedings is submission of the content of a webpage (so-called “screenshots”) to the court. It may be particularly tempting to present printouts of the screenshots as evidence in IP disputes when the infringement is committed online. Though it might me a rather easy task from the technological point of view, the credibility of such information is doubtful since “screenshots” do not guarantee that information is correct and precise. Courts usually rely on electronic data presented in a human-readable format, e.g. printed on paper. Printing out “screenshots” means a loss of valuable metadata. The printout is merely a copy of the screen display and it can be modified in a very simple manner without special software or hardware requirements. Therefore, it could hardly be recognized as reliable electronic evidence or the basis for the expert’s verification of authenticity and equal treatment of the parties to the dispute.

S. Mason is correct in his argument that even if we correctly...
identify the carrier of original evidence carrier and rely on physical objects only, such as printouts, they may have no value at all or limited value unless a party to the dispute confirms their significance and the features that make them relevant. Unsurprisingly, some national courts find that screenshots are not trustworthy. Under the CoE Guidelines, the printouts are to be recognised as a secondary proof (copy) in the sense that originally they exist in electronic form.

Nevertheless, evidence in civil proceedings should be defined in a broad sense, encompassing virtually any information. Due to the widespread use and easy collection of “screenshots” the parties can submit them as evidence in civil proceedings. Depending on the national laws, “screenshots” may be accepted, if it is sufficiently visible and precise and comply with certain procedural safeguards. Also, it should not raise difficulties, if the other party does not dispute such evidence and it complies with the general rules for admissibility and legitimacy of evidence in civil proceedings. The Explanatory Memorandum establishes that in case a printout of electronic evidence is filed, the court may order, at the request of a party or on its own initiative, provision of the original of the electronic evidence by the relevant person. The court should also consider the principles of proportionality and economy of litigation and should not demand excessive metadata.

To conclude, we recommend that the member states should adopt these principles regarding the significance of metadata for evidentiary purposes in the national regulations. In particular this refers to Article 8 of the CoE Guidelines that reads:

“Courts should be aware of the probative value of metadata and of the potential consequences of not using it”.

---

36 See Articles 8 and 9 of the Explanatory Memorandum.
38 Article 23 of the Explanatory Memorandum.
5. TAKING OF EVIDENCE IN IP DISPUTES AND ITS RELIABILITY

Taking of electronic evidence is a challenging task which may significantly impact the course of the civil proceedings. The Enforcement Directive lays down no practical rules how electronic evidence in IP disputes should be collected, meaning that the national rules for taking of evidence in civil proceedings are applicable. The recent report reveals that the courts of the EU Member States collect electronic evidence in IP disputes in three forms:

1. establishment of the infringement and appointment of an expert;
2. description;
3. seizure.\(^{39}\)

Thus, courts rely either on the submission of electronic evidence by the parties or appoint an expert to collect such data.

The major difficulties in taking of evidence in IP disputes are:

1. taking evidence in cross-border cases;
2. excessive costs among the member states for production of evidence;
3. inconsistency of information among the member states;
4. different national legislation for production and preservation of evidence.\(^{40}\)

Obtaining and securing electronic evidence, as well as using evidence in the cross-border context, has proved to particularly challenge the effectiveness of the Enforcement Directive.\(^{41}\) In the digital environment, cross-border use of intellectual property is becoming increasingly common. The dissemination of IP protected goods on the Internet is inherently cross-border in nature. Only mechanisms adopted at the international level, such


as Council of Europe, can ensure the proper functioning of the market of digital goods.\textsuperscript{42} The solutions to these issues are not simple. The existing rules of the Regulation on taking of evidence\textsuperscript{43} establishes a model for the co-operation among the courts of the EU Member States in taking of evidence in cross-border civil cases. Nevertheless, it seems that practical issues in taking evidence in cross-border cases are hardly avoidable. Also, the recognition of electronic evidence collected in one member state may be disputable in another. The CoE Guidelines recognize that courts should co-operate in the cross-border taking of evidence.\textsuperscript{44} Therefore, taking of evidence in IP disputes may be particularly complicated due to the complexity of the disputes, but also involvement of “a cross-border element” which almost inevitably require a close co-operation between the national courts.

We recommend that member states should adopt in particular the following principles in the national regulations in accordance with the CoE Guidelines:\textsuperscript{45}

1. Electronic evidence should be collected in an appropriate and secure manner, and submitted to the courts using reliable services, such as trust services.\textsuperscript{46}

2. Having regard to the higher risk of the potential destruction or loss of electronic evidence compared to non-electronic evidence, member states should establish procedures for the secure seizure and collection of electronic evidence.


\textsuperscript{44} Article 13 of the CoE Guidelines

\textsuperscript{45} Articles 10–16 of the CoE Guidelines.

\textsuperscript{46} Trust services play a critical role in the identification, authentication and security of online transactions. The definition of “trust service” can be found in Article 3(16) of the Regulation (EU) No 910/2014 of the European Parliament and Council of 23 July 2014. \textit{Official Journal of the European Union} (L 257). Available from: https://eur-lex.europa.eu/eli/reg/2014/910/oj [Accessed 3 March 2020]. In the CoE guidelines, reference is also made to specific trust services related to “simple”, “advanced” or “qualified” electronic signatures and certificates, which implies possible application of other definitions adopted in the eIDAS Regulation. Secure mechanisms include, in particular: i) certificates to electronic signatures; ii) confirmations by the payment system operator; iii) public trust services providing technological mechanisms that ensure proper authentication of the data source.
3. Courts should be aware of the specific issues that arise when dealing with the seizure and collection of electronic evidence abroad, including in cross-border cases.  
4. Courts should co-operate in the cross-border taking of evidence. The court receiving the request should inform the requesting court of all the conditions, including restrictions, under which evidence can be taken by the requested court. 
5. Electronic evidence should be collected, structured and managed in a manner that facilitates its transmission to other courts, in particular to an appellate court. 
6. Transmission of electronic evidence by electronic means should be encouraged and facilitated in order to improve efficiency in court proceedings. 
7. Systems and devices used for transmitting electronic evidence should be capable of maintaining its integrity. 

Electronic evidence has unique properties that distinguish it from traditional paper evidence. The method of storage and the type of information relevant to evidence are subject to changes due to the use of different electronic devices. The collection and presentation of evidence in its original electronic form in court requires necessary expertise. Still, electronic evidence retains the general characteristics of the evidence. Therefore, the general rules on evidence should continue to be applied. The general principles of the law of evidence should not be ignored, but applied to electronic evidence, taking into consideration the uniqueness and technical aspects of electronic evidence bearing in mind the discretionary power of the judge. 

Another complicated issue regarding taking of evidence in IP cases is protection of personal data. This issue is complex and deserves a separate analysis. In this paper we would like only to state that IP rights are not absolute and protection of the fundamental right to property, which

---

47 Good example in case of IP dispute is use of data sharing (clouds) technology. 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.

48 As further explained in Article 33 of the Explanatory Memorandum. Encouragement and facilitation of the transmission of electronic evidence by electronic means can be achieved through implementation of common technical standards, files formats and digitisation of domestic judicial and administrative systems. Having regard to the higher risk of destruction of electronic evidence, local procedures should be adopted which permit secure transmission of electronic evidence.
includes the rights linked to intellectual property, must be balanced against
the protection of other fundamental rights. Thus, a fair balance between
protection of IP and protection of the fundamental rights of individuals
who are affected by the measures which protect IP holders should be
found.

6. CONCLUSIONS
IP right owners are entitled to effective legal protection. In the case
of exploitation of IP protected goods in the digital environment, it becomes
more difficult. Online transmission of books, music, films and computer
programs enable the use of goods at any time and without geographical
limitations. It is becoming increasingly problematic for IP rights holders
to assert their rights. There is a high risk that rights holders give up their
claims at all. Those who bring an action with little evidence to support their
claims are not able to win the case because it is impossible to prove the real
extent of the damage without all the evidence available. That is why courts
must exercise caution when dealing with electronic evidence in such cases.

Due process is determined not only by legal but also by technological
aspects. Therefore, a more technological approach and practical
to the regulation of electronic evidence is necessary. For example,
regulations should safeguard the reliability of electronic evidence.
A solution to these shortcomings could be seen in uniform application
of the CoE Guidelines. These standards specify both the legal and
the technological requirements for the electronic evidence and serve
as a complementary regulatory tool.

Our recommendations for the member states are following. Due
to the relevance and nature of electronic evidence the national legislation
should define electronic evidence and thus separate it from the other types
of evidence. Such definition should encompass the major traits of electronic
evidence as established in the CoE Guidelines. Also, because

---
of the increasing importance of metadata and technical problems associated with it, we suggest that the national regulation should adopt definition of metadata. Moreover, the courts should be aware that the content of a webpage may not be sufficient to prove certain facts since they lack metadata. It is particularly important in IP disputes in which the parties often present various screenshots. The court should be aware how metadata collected and stored.

The treatment of electronic evidence shall be different from other types of evidence. The effective case management and enforcement of IP rights are particularly important since the information related to electronic evidence may be abroad in possession of the third party.

Also, the national law should specify taking of electronic evidence since their collection and submission to the court. In many cases the IP disputes involve various countries and the cooperation between national institutions may be inevitable. The practical issue is storage of electronic evidence in courts. In countries in which electronic case management systems are not used all evidence shall be printed out meaning that crucial elements such as metadata may be lost. The adoption in national law of a common and comprehensive regulation of proceedings concerning the handling of electronic evidence in IP disputes on the basis of the CoE Guidelines would facilitate the application of the procedural rules and specify the differences between these proceedings and the general principles.

LIST OF REFERENCES


