Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Antigua Universidad s/n - Apdo. 28
20560 Oñati - Gipuzkoa (Spain)
opo@iisj.es / http://opo.iisj.net

Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure

OÑATI SOCIO-LEGAL SERIES VOLUME 12, ISSUE 3 (2022), 582–613: NORM, NORMAL AND DISRUPTION: THE ROLE OF LAW, KNOWLEDGE AND TECHNOLOGIES IN NORMALISING SOCIAL LIFE
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL/0000-0000-0000-1304
RECEIVED 15 APRIL 2021, ACCEPTED 7 APRIL 2022, VERSION OF RECORD PUBLISHED 1 JUNE 2022

ELENA ALINA ONŢANU*

Abstract

Society is increasingly relying on technology for daily business and activities. This is linked to a rapid update in technology use and digitalisation with courts being called to consider new forms of evidence in an electronic environment and/or rely on technology for the taking of evidence. The normative framework concerning electronic evidence remains fragmented while various legislative projects are ongoing. In this process the global pandemic accelerated attention for technology solutions and their integration in the handling of court claims. In the EU, the recast Taking of Evidence Regulation (Regulation 2020/1783) addresses some of the necessary aspects related to electronic evidence and cooperation between authorities. Other elements are covered by cross-sectorial EU legislation such as regulations concerning data protection or electronic identification and trust services. New regulation proposals concerning the digitalisation of judicial cooperation and communication in cross-border procedures are set to address some of the legislative gaps in the near future as well as support the development of necessary technology. However, the overall existing legislation is only partly sufficient for providing a comprehensive framework and does not provide much guidance in the process of considering metadata or assessing electronic evidence.

Key words

Cross-border litigation; electronic evidence; electronic taking of evidence; Regulation (EU) 2020/1983; eIDAS; GDPR; e-CODEX

Resumen

La sociedad se apoya cada vez más en la tecnología para sus negocios y actividades diarias. Esto está relacionado con la rápida actualización del uso de la tecnología y la digitalización, y los tribunales están llamados a considerar nuevas formas de prueba en un entorno electrónico y/o a confiar en la tecnología para la obtención de

* Dr. Elena Alina Onţanu, Assistant professor of Global and Comparative Private Law, Tilburg University (The Netherlands). Email address: e.ontanu@tilburguniversity.edu

pruebas. El marco normativo relativo a las pruebas electrónicas sigue estando fragmentado, mientras que hay varios proyectos legislativos en curso. En este proceso, la pandemia mundial aceleró la atención sobre las soluciones tecnológicas y su integración en la tramitación de las demandas judiciales. En la UE, el Reglamento revisado sobre la obtención de pruebas (Reglamento 2020/1783) aborda algunos de los aspectos necesarios relacionados con las pruebas electrónicas y la cooperación entre autoridades. Otros elementos están cubiertos por la legislación intersectorial de la UE, como los reglamentos relativos a la protección de datos o la identificación electrónica y los servicios de confianza. Las propuestas de nuevos reglamentos relativos a la digitalización de la cooperación judicial y la comunicación en los procedimientos transfronterizos están destinadas a colmar algunas de las lagunas legislativas en un futuro próximo, así como a respaldar el desarrollo de la tecnología necesaria. Sin embargo, la legislación general existente sólo es parcialmente suficiente para proporcionar un marco global y no ofrece mucha orientación en el proceso de consideración de los metadatos o de evaluación de las pruebas electrónicas.

Palabras clave

Litigios transfronterizos; pruebas electrónicas; obtención electrónica de pruebas; Reglamento (UE) 2020/1983; eIDAS; RGPD; e-CODEX

Table of contents

1. Introduction

The rapid evolution of technology and digitisation of society have acted as accelerators of change in evidence-taking law and practice. The ongoing pandemic has been an additional incentive towards a total shift in electronic handling of claims, hearings, evidence taking, and delivery of justice in several countries (e.g. France, England, Italy, the Netherlands, Norway). Although the COVID-19-determined measures were expected to be temporary, they brought with them an increased openness towards the electronic environment and its use in court proceedings. These changes and their effects are likely to persist beyond this period of crisis (Krans and Nylund 2020, Velicogna 2020, CEPEJ 2020) as more developments are being considered in several Member States and at EU level in terms of digitalisation of court proceedings and use of information and communication technology. These initiatives aim to create a framework that moves away from the ad-hoc technical solutions put in place during the prolonged health emergency to create a stable legislative system. Such framework is set to use technological means to improve access to justice, uphold procedural guarantees in the use of such means, secure data protection, and provide the necessary resilience of communication flows in judicial cooperation including in relation to taking of evidence during usual times as well as in case of lasting disruptive events (Draft Commission Ref.Ares(2022)573182, Proposal for a Regulation on Digitalisation (COM(2021) 759 final, 2021/0394 (COD)).

Overall, electronic evidence is finding its place among the general evidentiary means parties may choose to rely on when disputes arise, and legal and technology developments adopted to facilitate this development. Although the use of some form of electronic evidence such as videotapes and voice recordings are not necessarily new and have been considered as means of evidence for some time, particularly in criminal proceedings, present technology developments require courts and parties to be able to deal with more complex situations where information to be considered is contained in clouds, is accessible via websites, social media, apps, blockchain in various formats (i.e. written, audio or even other forms such as emoticons and emojis; Govender 2017, Janssen 2018, Wharton 2019, Docrat and Kaschula 2020). Together with the content of the evidence we would normally consider when dealing with traditional paper-based formats of evidence, additional information becomes relevant for electronic evidence: its metadata.[1] The normative circle related to these types of evidence – their collection, their value, elements relevant to determine their reliability, their storage and access for parties and the courts – is not consistently developed across the legal fields. Looking at domestic legislations in the area of civil procedural law the approaches chosen regarding electronic evidence are divergent or, in some instances, even lacking across jurisdictions.[2] Attention towards electronic evidence and taking evidence via information and communication technology has been recently gaining ground due to the necessity of securing access to justice and adapting to remote court proceedings,

[1] Sometimes simply defined as data about data. It provides for example information about where the data originates, who created it, whether that is the latest version or an original version of a document, audio- or video-recording, who modified that original data. See Wilson 2015, 1.

[2] Most developments so far address electronic evidence from a criminal law perspective. Also, legislation is much more developed in this area of law in dealing with information and communication technology in its various forms.

especially in urgent matters (e.g. family matters, maintenance, custody hearings). In addition to this, judicial procedures are faced with a growing need to be able to manage and consider an increased amount of *ab initio* digital evidence.

Some dedicated rules and/or guidelines have been adopted nationally across EU Member States in order to allow justice systems to continue functioning during the long period of health emergency (e.g. Belgium,[3] Croatia,[4] England and Wales;[5] see further also Krans and Nylund 2021). However, there are no systematic and clearly regulated processes for civil and commercial litigation when dealing with electronic documents, evidentiary means, and their evaluation. Given the still limited number of norms addressing this type of evidentiary means as well as the various forms of electronic evidence in civil and commercial matters, judges have been often left to their inspiration in evaluating and interpreting the various forms of electronic evidence they receive. In this they have to decide on what are the relevant elements to consider, but this is not generally an aspect covered by their legal education or procedural law courses.[6] Thus, the judges have to decide on what type of electronic evidence to accept, the requirements this type of evidence needs to comply with for its valid use, the methods that are considered to be legally valid for collecting such evidence, the reliability of technology, the ways in which to interpret electronic evidence, etc.[7] without having much training on how to deal with technical considerations. The situation becomes even more complex in cross-border settings not only for the judges but also for parties and their legal representatives. How to decide what type of electronic evidence will be accepted? What is the type of information related to the electronic evidence that is necessary for a valid consideration of the piece? Is electronic evidence taken in one country valid in another, and under what circumstances? Should the judge proceed to an interpretation or a handling by correlation? The process is additionally challenging when the electronic evidence is confused with the device carrying or containing it as the legal framework remains mainly anchored in traditional physical evidence and in person or written forms of evidence taking.

In practice, the use and reliance on electronic evidence can bring with it a series of potential legal issues that judges have to address: individuals' privacy (e.g. General Data Protection Regulation (GDPR) [Regulation (EU) 2016/679], Article 8 ECHR), the preservation of the material, diversity of sources, authenticity and integrity of the evidence, the legality of obtaining the evidence, and several practical aspects (e.g. standards, technical equipment needed for the handling of electronic evidence, costs for obtaining such evidence, collaborations with information technology specialists and/or training for being able to understand and meaningfully use different kinds of electronic evidence). This paper aims to explore the normative gap in dealing with technology-

[3] Recommendations from the Management Committee of the Courts and Tribunals, see Bayard 2020; Act of 20 December 2020.

[4] Minister of Justice Decree of 20 April 2020.

[5] Coronavirus Act 2020, Schedule 25, CPR PD 51Y -*Video or Audio Hearings during Coronavirus*.

[6] For example, during the last years some initiatives in dealing with electronic evidence as part of continuous professional trainings offered to judges and court clerks have been offered by the European Judicial Training Network –the EJTN Civil Justice Seminars.

[7] For example, Article 152 Dutch Code of Civil Procedure states that, unless the law provides otherwise (e.g. for notarial evidence), evidence can be given using any means, and the judge can freely evaluate the evidence; this includes electronic evidence.

based evidence in civil and commercial legal proceedings. The existing EU legislation will be taken as the reference point. Section 2 will look at how electronic evidence is defined by various instruments. Then Section 3 will focus on aspects of the legislative and socio-techno normativity framework. The analysis maps the elements that the legal provisions should provide in order to facilitate the acceptance, use, and evaluation of electronic evidence as well as the changes that will follow at the level of human interactions and technical normativity. This mapping will be transposed in Section 4 to present EU legislative framework concerning taking of evidence in cross-border litigation as well as relevant cross-sectorial legislation referred to in relation to evidence and evidence taking. Section 5 concludes on remaining aspects to be addressed and achievements of present legislative developments in sustaining technology integration as part of the evidentiary process in civil and commercial litigation.

2. Defining electronic evidence

The last decade has seen a process of including electronic evidence in civil proceedings, using them in parallel or even replacing traditional formats of evidence (e.g. paper-based or analogic proofs). Although the extent of relying on digital objects in court proceedings differs across the EU Member states, the switch towards electronic documents or digitalised documents is becoming more visible (Stuerner 2018, 67), and the process has been accelerated by the COVID-19 pandemic (Krans and Nylund 2020, Velicogna 2020, CEPEJ 2020). However, the existing rules of civil procedure have not been traditionally drafted with the characteristics of electronic documents and evidence in mind nor with anticipation of the present developments of technology or of the various protocols that may be used to handle them. This can result in divergence and issues of compatibility when dealing with electronic evidence in a transnational setting. Electronic evidence and evidence taking via information and communication technology require new work practices and tools. For this a coherent and supportive normative framework is necessary. When seeking to achieve this, it is necessary to determine first what should be considered to be electronic evidence for the task.

No unified definition of what is to be considered or accepted as electronic evidence has been established so far (see also Vazquez Maymir 2019, 3). Different types of definitions have been proposed by various projects and international or European organisations in the civil or criminal area (e.g. IBA Evidence Rules [2010],[8] International Organisation of Computer Evidence,[9] Draft Convention on Electronic Evidence,[10] Directive making competition authorities more effective enforcers [Directive (EU) No 2019/1]).[11]

In connection to the definition of electronic evidence the definition of "electronic documents" is relevant and may at times represent a valuable proxy. The eIDAS

[8] Electronic evidence is "a writing, communication, picture, drawing, program or data of any kind, whether recorded or maintained on paper or by electronic, audio, visual or any other means".
[9] "Digital evidence is an information stored or transmitted in binary form that may be relied upon in court."
[10] Private initiative promoted by Mason defines electronic evidence as "evidence derived from data contained in or produced by any device the functioning of which depends of a software program or from data stored on or communicate over a computer system or network".
[11] Referring to electronic documents as "any content stored in electronic form, in particular text or sound, visual or audiovisual recording".

Regulation[12] and the new legislative Proposal for a Regulation on the digitalisation of judicial cooperation and access to justice[13] contain such definition. The proposal refers to "electronic documents" rather than "evidence" most likely in consideration of the exchanges of documents that will be taking place via a decentralised IT system between various authorities and will involve more than just evidentiary means. The definition is coupled in this European legislation with a provision requiring authorities not to deny legal effect to electronic documents or consider them inadmissible on the ground of their electronic format (Article 46 eIDAS, Article 10 Digitalisation of Judicial Cooperation Proposal). A similar provision with regard to the legal effect of electronic documents is included in Article 8 of the new Taking of Evidence Recast Regulation ((EU) 2020/1783).

The national approaches are similarly rich in formats, but when bringing together the two sides both national and international approaches follow two main lines in seeking to define what should be identified and considered as electronic evidence for procedural purposes. One approach relies on a broad wording that aims to give sufficient flexibility to accommodate a rapidly evolving technology. For example, defining electronic evidence as "any content stored in electronic format" together with referencing some generic groups of electronic data that could be used for evidentiary purposes such as text, sound, visual or audio-visual recordings. This is the case of Article 3(35) eIDAS Regulation, Article 2(3) Private Damage in Competition Law Directive (Directive (EU) No 2014/04), or national legislation: 31B PD 5.3 Civil Procedure Rules in England and Wales, and Art. 1(p) Code of digital administration in Italy. The other approach focuses on identifying specific types of electronic evidence that should be considered (e.g. IBA Evidence Rules, Directive making competition authorities more effective enforces (Directive (EU) No 2019/1), or national legislation: Section 26-1 Norway Dispute Act, Articles 245 and 308 Polish Code of Civil Procedure).

For this paper electronic evidence should be understood broadly as not only the evidence that is digitally generated, but also other type of evidence that is converted and stored into a numerical format for a determined reason (e.g. commercial, professional, procedural, etc.) and is suitable for being transmitted and processed by a network or computer system.

3. Normalising electronic evidence acceptance

3.1. A legal normativity

Technology backed developments for justice and court proceedings need to be legalised to produce the procedural effects they are expected to provide – to execute and enforce legal rules. The same is necessary for forms of electronic information that can be used or be retained relevant as evidence in court proceedings. Dedicated rules and/or guidelines need to be adopted in order to support the adducing of electronic evidence into court proceedings, but also in relation to its assessment. As previously underlined by Contini:

[12] Article 3(35) defines electronic document as "any content stored in electronic form, in particular text or sound, visual or audiovisual recording" (Regulation (EU) No 910/2014).

[13] Article 2(3) defines "electronic document" as "a document transmitted as part of electronic communication, including scanned paper documents". Article 10 of the Proposal concerns the legal effects of electronic documents (COM(2021) 759 final).

"technologies affecting proceedings must be made legal to become performative from a legal perspective" (Contini 2020, 5). Steps in this direction are being considered or undertaken by both national and European legislators as technology is gaining a more prominent role in court proceedings in the taking and handling of evidence. In this process of shift towards more detailed rules the wording needs to remain flexible enough to withstand the test of technology developments. Together with this the provisions need to address a series of aspects: their use, their assessment, the technology to be used in relation to their handling, and the human interaction in this process. Rules normalising technology use and electronic information in court proceedings need to be conceptualised and designed in a way that allows a dynamism of adaptation of norms (Canguilhem 1991, 239) to technology developments and evolution.

The fact that the electronic evidence can be easily changed or interfered with means that the digital evidence has to be accompanied by additional documentation or information (e.g. qualified certifications, metadata) indicating when changes where registered, whether the contained information is still up to date, what is its "chain of custody",[14] or whether some form of seal has been applied confirming that the information presented corresponds to the situation it actually seeks to present. Further, the "chain of custody" needs to be able to be validly opened, checked and read across jurisdictions as a general working approach for the courts, not only for electronic documents and information provided by the interested parties, but also for evidence being taken via information and communication technology.

Overall, a series of aspects need to be considered in relation to the generation, use, authenticity, and assessment of electronic evidence, as well as the security of its transmission across jurisdictions. As a general framework, the legislation has to coherently address the following elements:

- Privacy: particularly relevant when it concerns personal data, personal devices, social media communications and accounts, access to electronic forms of evidence acquired for the proceedings, and their transmission between involved authorities in view of the GDPR and Article 8 ECHR;
- Preservation and transmission: chain of custody, spoliation of electronic material (alterable, damageable and destructible electronic data), immaterial form, way of transmission of data, volume of data to be transmitted and stored;
- Diversity of sources to be considered: type of evidence (e.g. paper-based documents transformed in an electronic format, electronically created documents, electronic messages, audio folders, video materials, other forms of communication that can convey a message or information), places where evidence is available (e.g. computers/laptops, other digital devises, USBs, mobile navigation systems, networks, clouds, apps, emails, chatrooms, social media, databases, blockchain);

[14] The chain of custody document is meant to describe in detail what happens to digital evidence from the moment in which it was identified as evidence until its presentation before the judge in the trial phase (e.g. the person who took possession of it to preserve its authenticity, when, where and how, and in what manner). See further on this Biasiotti *et al.* 2018, 5.

- Authenticity and integrity: alterations, manipulation, electronic signatures and seals, metadata (not always immediately available for consultation);
- Legality: equivalence of legally collected evidence cross-border, illegally obtained electronic evidence, fairness of proceedings, processing of data and evidence for the purpose of their collection;
- Evaluation and transparency: software used, processes for collecting the evidence, use of data, assessment means and processes;
- Collection of electronic evidence: queries design when taking of evidence concerns databases or environments containing significant volumes of data, outcomes of evidentiary data following queries used;
- Other practical aspects: software used for the collection of evidence or means of taking evidence via information and communication technology, standards,[15] technical equipment, actors involved, costs.

When considering the above elements existing legislation is fragmented between several European pieces of legislation or existing legislative projects and national legislation of the Member States.[16] For example, the EU legislation leaves a significant number of aspects to national law (e.g. the ways of transmission and preservation of electronic data and evidence, arrangements related to verification of authenticity and integrity of electronic documents, the diversity of sources to consider and devices containing them, and/or the evaluation by the judges of electronic evidence obtained abroad). Aspects such as the safe cross-border transmission of electronic data and evidence are expected to be addressed by e-CODEX and the Digitalisation of Judicial Cooperation Proposals. Other elements such as evaluation of electronic evidence remain part of a legislative gap at EU level and are left at the interpretation of the national courts.

3.2. The socio-technical normativity

The legislative picture shows numerous complexities in itself, and it is certainly difficult to "transfer into digital media practices that are smoothly running in paper-based mode" as previously pointed out by Velicogna (2007), Fabri (2009) and Contini (2020). It is complex to guarantee the identity of a digital signature or the e-identity of a lawyer or a party and even more so in a transnational context. The same situation is relevant for electronic evidence and taking of electronic evidence. Additionally, procedural law and practice diversity need to be "reconciled with the features of digital technology" (Contini 2020) in order to achieve a "maximum manageable complexity" (Lanzara 2014). The interaction between multiple legal and institutional frameworks and national IT systems further increases intricacy (see Velicogna and Steigenga 2016). As electronic systems need to remain manageable, technology has to be "closed from a technological perspective (black-boxed) and certified" for legal compliance (Contini 2020). An example in this direction is the eIDAS Regulation in the EU. The Regulation establishes rules on legal recognition of electronic signatures, seals, time stamp, electronic delivery and web

[15] For example, ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition, and preservation of digital evidence*, ISO/IEC 27042:2015, *Guidelines for the analysis and interpretation of digital evidence*.

[16] On the difficulties and limitations of parties' identification and recognition across national systems and the differences in application of procedures (even in relation to uniform European procedures), see further Onţanu 2017 and 2019 (in particular section 5.4).

authentication with a cross-border setting in mind. The certifications of registered organisations and companies issuing this type of electronic instruments can be verified online via the European Commission dedicated websites.[17] This approach can provide a way for judges themselves to easily verify the credentials without looking into the technical details of the relevant trust service. Technology has the potential of being an "ideal platform for the exchange of documentation submitted during the procedure" (Biasiotti 2018, 18) securing fast communication of digitally generated or converted evidence. However, at the same time the computers, internet connections and different information and communication systems or platforms need to comply with the appropriate inscriptions and security requirements necessary to observe the privacy rules related to judicial proceedings.

Technology integration in providing justice services leads also to a reshape of the human interaction in the proceedings. Technology can accelerate procedural exchanges, but also modify practices and interactions between actors and their tasks (Garapon and Lassègue 2018, 169–193). The actors involved are increasingly executing their tasks interacting with pre-established software interfaces and background routines, while other activities that are traditionally carried out by members of court staff are delegated to technology (e.g. recording of evidence taking, statistical reporting, transcribing) or are shaped by technology (e.g. data exchanges, data checks). Thus, potentially, a decision that on a traditional paper-based procedure would be made on a case-by-case basis by the clerks and/or judges, in case of digitisation could be pre-established at the time of software development, when a certain sequence of activities is inscribed in the technology (Velicogna and Contini 2009, Lanzara 2009). The software code or used platform features would establish and control the execution of the procedure and become "the pre-packed interpretation" of the legal rules. At the same time a procedural step established by the norm can be carried out only if properly "inscribed in the platform" used (Contini 2020).

Additionally, during initial stages, the implementation of technology based routines for hearings and for taking of evidence may result in delays as courts' staff and/or judges may lack sufficient technical skills, the court may suffer from inadequate technological infrastructure, or technology architecture may require further adaptation or fine tuning.[18] This expectation is in line with previous experiences of implementing technology into courtroom proceedings (Lanzara 2016) where traditional means and modern technology come to interact and cooperate in delivering access to justice.

In dealing with digital evidence, judges and lawyers will also need to consider and address the separate reality that surrounds these types of evidentiary means and that are not always visible upfront. Experiences from other areas of law, such as criminal law can be a valuable addition. As Biasiotti, Cannataci, Mifsud Bonnici and Turchi argue, in this it is important not only to rely "on studies and analyses on a theoretical level but also on the experience of those who routinely work with this particular type of evidence in real life, and also managing the variety of actors involved in various capacities in the lifecycle of electronic evidence. Constant and open dialogue with these actors is crucial

[17] EU Trust Services Dashboard: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

[18] See on this the European Economic and Social Committee, COM(2018) 378 final – 2018/203 (COD).

in this area, especially given the continued and rapid evolution of technology" (Biasiotti *et al*. 2018, 5).

Furthermore, these new dynamics of relations and roles bring with them a change of court rituals,[19] the solemnity of acts, certain traditional gestures,[20] and a symbolism of actions and objects[21] (Mohr 2005) that may not fit in an electronic environment and which will tend towards the creation of new highly standardised and repetitive processes (Garapon and Lassègue 2018, 191–193). In the process of adapting to a new digital "normal" that has been speeded up (and in many cases surpassed) by the realities and necessities of the COVID-19 pandemic, the legislators are working towards imagining a new court experience. However, this new reality seems it cannot be imagined without incorporating some of the elements we are familiar with and expect to find in court (Mohr 2005, Velicogna and Ng 2006). As the next Section reveals, even with new legislation accommodating and creating a framework for electronic evidence taking the legislation sought to maintain a certain level of symbolism encountered in the traditional proceedings we associate with features of justice services (e.g. evidence is taken in courtroom, in the presence of the judge, with the use of professional interpretation services) (Velicogna 2020).

4. An EU procedural perspective into normalising electronic evidence use

4.1. EU Competence: A Short Overview

National civil procedural rules establish how claims can be lodged and whether an electronic filing is possible, as well as the way in which submissions have to be filed, how evidence is to be submitted and in what format, whether hearings are to be recorded, if a transcription of some sort is necessary, and how the parties would gain access to all related documents of the proceedings. These procedural norms are country-specific and differ across states even for systems of law that are considered to be part of the same legal family (e.g. civil law, common law).

In the EU, following the Amsterdam Treaty in 1999, Article 65 European Community Treaty (EC Treaty), present Article 81 Treaty on the Functioning of the EU (TFEU) provided the legal grounds for adopting legislation in the area of judicial cooperation in civil and commercial matters having cross-border implications for securing a "well-functioning legal system within the European Union" (Tulibacka 2009, 1527) and the internal market. Around a dozen instruments have been adopted over the years dealing with matters of judicial cooperation in civil and commercial matters such as jurisdiction, recognition and enforcement of judicial decisions among Member States, applicable law to contracts and torts, taking of evidence, service of documents, uniform European procedures for certain types of claims (e.g. uncontested debts, order for payments, small claims, attachment of bank accounts). The European rules have been focusing on supporting judicial cooperation and direct communication between national authorities involved in legal proceedings in the area of civil and commercial law.

[19] Such as the specific dress code and position in the court room of various stakeholders.
[20] Such as the raising of the parties present in the courtroom when the judges enter.
[21] Such as the presence of a Bible, swearing to tell the truth before a witness is being heard.

Taking of evidence in cross-border proceedings has been the object of a dedicated regulation and some references can be found in some cross-border uniform European procedures (e.g. European Small Claims Procedure [Regulation (EC) No 861/2007] European Account Preservation Order [Regulation (EU) No 655/2014]). Initially, the rules concerning evidence have not given much attention to electronic evidence. For example, the European Taking of Evidence Regulation offered only the possibility for the requesting authorities interested in direct taking of evidence abroad to request the use of communication technology, if such means were available with the requested court (Article 10(4) Regulation (EC) 1206/2001, Taking of Evidence Regulation).

As commercial practices are integrating more electronic means and technology has been seen as a way to facilitate access to justice, new rules have been considered at European level to respond to the new digital developments. These rules are set to specifically address this type of evidence as well as to facilitate cooperation between authorities and the exchange of information in cross-border proceedings, securing the legal validity of the evidence collected or transmitted in an electronic format.

Besides the European regulations in the area of judicial cooperation in civil and commercial matters, a number of sectorial instruments address directly or indirectly aspects that are of relevance for taking of evidence, storage, processing (e.g. GDPR, eIDAS) or are set to address in the future matters of judicial cooperation in the communication and exchange of electronic documents and/or objects for evidentiary purpose (e.g. the Proposal Regulation on a Computerised System for Communication in Cross-Border Civil and Criminal Proceedings (COM(2020) 712 final) and the Proposal for a Regulation on Digitalisation of Judicial Cooperation and Access to Justice in Cross-Border Civil, Commercial and Criminal Matters Proposals; COM(2021) 759 final). When globally considered, these rules appear fragmented. The use of the Taking of Evidence Regulation and the Recast is not mandatory in cross-border proceedings. Other regulations have a cross-sectorial importance (e.g. GDPR, Regulation (EU) 2016/679; eIDAS, Regulation (EU) No 910/2014) and have gained a procedural dimension. Further developments of the European legislation are expected with the adoption of the abovementioned legislative proposals. These are of particular importance for organising and supporting the transmission and exchange of electronic documents in court proceedings between authorities of EU Member States – the Proposal for a Regulation on Digitalisation of Judicial Cooperation and Access to Justice in Cross-Border Civil, Commercial and Criminal Matters (Digitalisation of Judicial Cooperation Proposal) and the Proposal Regulation on a Computerised System for Communication in Cross-Border Civil and Criminal Proceedings (e-CODEX Proposal). A much more developed framework as to electronic evidence is available in the area of criminal law, and some interesting developments concern competition law. However, these instruments will not be the focus of the present paper.

4.2. Taking of Evidence Regulation

4.2.1. Overview

The Taking of Evidence Regulation is the instrument dedicated to cooperation in evidence taking in cross-border proceedings (Regulation (EC) 1206/2001). The text of this regulation was amended in 2020 (Regulation (EU) 2020/1783, Taking of Evidence Recast)

and the new provisions will become applicable among EU Member States (with the exception of Denmark) on 1 July 2022 (Article 35 Taking of Evidence Recast). The regulations can be relied on if evidence needs to be taken abroad in relation to civil and commercial court proceedings. However, its use is not mandatory and is left to the choice of the requesting courts and that of the interested parties (*Lippens c.s./Kortekaas c.s, ProRail BV v Xpedys NV e.a.*). Until now, practice indicated a certain tendency to seek to by-pass, if possible, the use of the Taking of Evidence Regulation. This is to avoid what is often seen as a "cumbersome, bureaucratic and time-consuming" solution by practitioners (Gascón Inchausti and Requejo Isidro 2019, 766). The courts handling proceedings seek as much as possible to resort instead on taking evidence in their own country based on their own national procedural rules or via designated experts.

Both the Taking of Evidence Regulation and the Recast provide for two ways of taking evidence abroad: by the requested court in the country where the evidence has to be taken or by the requesting court directly taking the evidence in another country (Sections 3 and 4 of the regulations). The Taking of Evidence Recast regulation extends the provisions concerning technology use for evidence transmission, evidence taking, and effects of electronic documents.

The activities to be undertaken in the taking of evidence cross-border based on the provisions of the Regulation are the hearing and/or examination of witnesses or other persons, taking expert depositions, collecting documents, information and/or samples or undertaking DNA tests, and for preserving evidence (Gascón Inchausti and Requejo Isidro 2019, 51). In carrying out such activities, distance communication like videoconferencing or teleconferencing can be used, resulting in electronic evidence for the proceedings. According to Article 17(4) Evidence Regulation, the use of technology is to be encouraged in direct taking of evidence by the requesting court in the requested Member States. This is possible, if technology is available, and the legal norms allow such process regardless of whether the acts of performing the taking of evidence is to be carried out by a representative of the requested or requesting court. In practice, this did not seem to be extensively used prior to the COVID-19 pandemic (see Krans and Nylund 2021). The taking of evidence with the use of information and communication technology has led to mixed results varying from positive experiences to frequent reports related to various technical problems since not all involved authorities rely on the same type of IT infrastructure (the European project interconnecting national authorities and facilitating the use of European procedural instruments – e-CODEX[22] – is not uniformly implemented, tested, and deployed across Member States; see Gascón Inchausti and Requejo Isidro 2019, 51, 55).

The Recast is seeking to normalise the use of technology. Technology is not used for the moment at "its full potential" from a legal, technical, and institutional point of view. The Taking of Evidence Recast recognises the relevance of modern communication technology as an "important means of simplifying and accelerating the taking of evidence" (Recital 21 Taking of Evidence Recast). Research has shown that practitioners are looking for a better and clearer normative framework in relation to taking of evidence in cross-border procedures and the use of technology for this purpose with "specific and detailed rules" that make explicit the procedural steps to be undertaken to validly

[22] e-Justice Communication via Online Data Exchange (e-CODEX) (https://www.e-codex.eu/).

acquire evidence. These can concern the presence of a judicial officer in the requested Member State (or whether more informal means are acceptable), the use of interpreters, the premises where the evidence taking should be performed (courtroom or other premises and what are the requirements that these premises have to comply with), guarantees with regard to the channels of communication to be used in order to secure data privacy, and professional privileges and software (Gascón Inchausti and Requejo Isidro 2019, 58).

In keeping with this growing need to integrate and legalise technology as well as establish a new normativity that can deal with the particularities of electronic objects and documents, the European Commission was advised to extend the use of technology under the reviewed regulation (Res. P7_TA(2010)0426, para. 18; Res. P6_TA(2009)0089, para. 4; Questionnaire on videoconferencing, para. 5). This has been embraced with some resistance and has been subject to limitations in the legislative process given the various levels of development of electronic justice systems across the EU Member States. Nonetheless, the integration of technology was viewed as a way to attempt to address some of the identified weaknesses, namely: speeding up the process, simplifying it, and making it more efficient to communicate between national authorities by compelling the courts to interact digitally with each other.[23]

The Proposal of the Recast Regulation sought to address these problematics in relation to cross-border taking of evidence via information and communication technology, introducing clarifications as to the place for taking of evidence, the use of qualified interpretation services, the guarantee of professional secrecy and legal professional privacy via the technology system used for taking evidence, the procedure for presenting documents or other materials during the hearing via videoconference or other distance communication technology, delegating to the European Commission the duty to establishing the minimum standards and requirements for the use of videoconferencing (including high quality of communication and real time interaction) in the transmission of the information, a high level of security and the protection of privacy and of personal data (Article 17a of the Proposal). These provisions were expected to remedy access to justice shortcomings, address matters related to the collection and evaluation of electronic evidence, whilst simultaneously limiting the number of cases in which electronic evidence could be potentially rejected due to admissibility issues related to the digital nature of the information and documents provided (see also Jansen 2019, EP legislative resolution COM(2018)0378 – C8-0242/2018 – 2018/0203(COD)). The adopted text of the Recast Regulation lost some of these provisions such as the clarifications regarding the place of taking of evidence by information and communication technologies – although from the wording of Article 20 it could be interpreted as being limited to court premises as the competent authority or a court may be assigned to provide practical assistance in the requested Member State for the direct taking of evidence – and the minimum standards and requirements for the use of videoconference. Some other proposed provisions were shifted to the level of clarifications in recitals (e.g. Recital 23 on court seized with the proceedings instructing the parties and their representatives on the procedure for making available, presenting

[23] Proposal COM(2018) 378 final of 31 May 2018, p. 2, 4, 6, 8. On doubts towards this technology approach solving issues that seem more related to backlog, see Jansen 2019, 767.

and/or relying on documents and other materials necessary in the examination procedure using distance communication technology). Further, Recital 7 and Article 7(1) Taking of Evidence Recast reinforce the call for the use of "any appropriate modern communications technology" in the transmission of requests and communications between Member States for taking of evidence. They also indicate the e-CODEX IT system for "all communication and exchange of documents" as a "secure and reliable decentralised IT system comprising national IT systems" that are to be interconnected based on the e-CODEX platform.

4.2.2. Legal normativity

In looking at the elements identified earlier under the legal normativity framework as desirable to be addressed by legislation in seeking to normalising the acceptance of electronic evidence and broaden its use in a cross-border judicial cooperation only some of the identified aspects are addressed in the new text of the regulation either directly or by reference to other pieces of legislation. The provisions gravitate around aspects related to the forms of taking of evidence, communication among authorities, and the legal value of the evidence not being impaired by its electronic format. No provision offers any basis or guidance towards elements to be considered for their assessment, the forms of electronic evidence, devices containing such evidence, metadata or technical standards and requirements for electronic evidence.

The privacy element is addressed in the rules that establish that the communication and transmission of requests and evidence is to be carried out through "a secured and reliable decentralised IT system with due respect for fundamental rights and freedoms".[24] This system is identified by Recital 7 as the e-CODEX system.[25] Further, the Taking of Evidence Recast acknowledges the need of observing a high level of security in the transmission and the protection of privacy and personal data based on the GDPR (Regulation (EU) 2016/679) and Directive 2002/58/EC requirements. The court requested to take evidence has a duty to secure the confidentiality of information transmitted in accordance with their national law (Article 30 Taking of Evidence Recast). These provisions in Article 30 thus address elements related to privacy that have to be observed also when electronic means are used.

When a seal or handwritten signature is to be used for electronic requests and communication related to taking of evidence, the same definitions as provided by the eIDAS Regulation are applicable for qualified electronic seals or qualified electronic signatures (Article 7(3) Taking of Evidence Recast). Article 3(12) and (27) in conjunction with Article 28-34 and 38-40 eIDAS Regulation define these concepts and the requirements that need to be complied with for their generation, validation, authenticity, and preservation of integrity of the information communicated. The qualified trust services to apply to the requests and communications transmitted through the e-CODEX system will be based on the legal framework provided by the eIDAS Regulation (Article 7(2) Taking of Evidence Recast). For now this is not operational on a large scale as the e-

[24] Article 7(1) in conjunction with Recitals 7 and 12 Taking of Evidence Recast.
[25] This is set to become available at the earlies on 23 March 2025. Article 25(2) in conjunction with Article 35(3) Taking of Evidence Recast.

CODEX system still needs to be deployed in the EU and the Regulation project for its establishment is in the process of being adopted by the European legislator.

The legality aspect is addressed by Article 8 Taking of Evidence Recast. The provisions support an equivalence of the legal effects of electronic documents transmitted through the decentralised system. According to this, electronic documents should not be denied legal effects or considered inadmissible as evidence solely on the grounds of their electronic format. This is a new provision introduced by the Recast seeking to uphold and protect fundamental principles of procedural justice while normalising the use of new objects and practices in cross-border judicial cooperation. Furthermore, its existence is important also because the legal effects of electronic documents and evidence might not always be guaranteed recognition across domestic civil procedure rules due to the electronic format. This principle is to be "without prejudice to the assessment of the legal effects or the admissibility of such documents as evidence in accordance with national law" or "conversion of documents" (Recital 13 Taking of Evidence Recast). The regulation does not provide further guidance with regard to potential ways of gathering evidence that would secure their validity across borders, mutual recognition or their assessment. There may be situations for example in which evidence is legally acquired in one country but deemed illegal according to the legislation of the country where they are intended to be subsequently used. This aspect remains to be assess in relation to the admissibility of the intended electronic evidence and its assessment. Fragmentation of applicable legal provisions remain with regard to the assessment of the validity of electronic evidence and their collection as they are subject to national procedural rules. No unified or coordinated approach at EU level is in place to guarantee their legality, although some elements can be found in the eIDAS Regulation. Further, the new Article 8 gives an impetus for the application of the principle of mutual recognition and mutual trust among Member States also in the area of cross-border taking of evidence (including digital evidence) as in other areas of civil justice (e.g. jurisdiction, recognition and enforcement, European uniform procedures).[26] As pointed out by Biasiotti "only through a shared system of mutual admissibility of evidence can mutual recognition effectively and efficiently improve judicial cooperation, with a view to strengthen the 'Area of freedom, security and justice'" (Biasiotti *et al.* 2018, 16).

In keeping with the requirement of "fair conduct of proceedings", Recital 22 sets out that the requesting court should be provided, if necessary, with assistance by the requested authority in finding an interpreter or qualified interpreter when needing to examine a person that does not speak the official language of the court proceedings. Another practical aspect addressed by the Taking of Evidence Recast Regulation only at the level of recitals and which supports a fair conduct of proceedings concerns the instructions the court seized has a duty to provide to the parties and their legal representatives when examinations are to be held via videoconferencing or other distance communication means (Recital 23 Taking of Evidence Recast). This is to be done in order to properly inform the parties and their representatives on the ways available to present documents or other materials when the examinations are to be carried out using videoconferencing or other appropriate distance communication means. The particularities of how courts

[26] In practice, the admissibility and usability criteria for evidence collected in another country have been entrusted to the interpretation of the judges in the Member States concerned.

will proceed are left to the national applicable rules and is an element that will maintain a diversity of approaches in practice.

The Recast contains provisions also in relation to some of the practical aspects of evidence taking – the means of evidence taking via information and communication technology. Articles 12 and 20 *Taking of Evidence Recast* concern courts using information and communication technology for evidence taking with a particular reference to the use of video- or teleconferencing for this purpose. When taking of evidence is to be carried out by the requested court (Article 12(4)) the requesting court may request the use of specific communication technology. The requested court is expected to use the specified technology unless this would be incompatible with its national law or the court is not able to do so because of major practical difficulties. Although no further clarifications are provided by the recitals as to what could be understood by "major practical difficulties", this may at least cover situations when the technology to be used is not available to the requested court or would be too burdensome to acquire for the purpose of carrying out the request. Article 20 on the direct taking of evidence by videoconferencing and other communication means focuses on the possibility of using such means when evidence is to be collected by the requesting court from a person present in another Member State. This can involve examining a witness, a party to the proceedings or an expert. The requesting court is encouraged to use videoconferencing or other distance communication technology where such technology is available to it and the court considers its use to be appropriate for the circumstances of the case and "the fair conduct of proceedings" (Recital 21 Taking of Evidence Recast). This clarification with regard to the availability of technology is related to the significant differences between courts in Member States on the availability of information and communication technology and the extent to which this is embedded in the daily routine of the courts and made available for carrying out judicial proceedings.

The diversity of sources to be considered as electronic evidence is only indirectly addressed via the references to the technology used for taking of evidence and the value of documents in electronic format. Other aspects for legalising the use of technology in evidence taking are not directly addressed by the Recast but references are made to other cross-sectorial instruments such the GDPR and the eIDAS Regulation. Aspects related to the authenticity and integrity of evidence are covered by the later. The Taking of Evidence Recast makes references in this regard on several occasions. These will be further discussed in Sub-section 4.3. Other aspects such as the preservation of electronic material, diversity of sources carrying out potential electronic evidence, some elements of authenticity and integrity of materials, and evaluation and transparency are left to domestic legislation of the Member States involved in the process of evidence taking. Thus, although the Recast Regulation addresses relevant points of interest in supporting the process of acceptance and normalisation of the use of electronic evidence in cross-border proceedings, normative gaps remain and the diversity of national provisions will maintain an existing fragmentation in dealing with and accepting electronic forms of evidence in court proceedings.

4.2.3. Socio-technical normativity

Together with the legal normativity and in close relation to this, a series of socio-technical elements have to be considered in the process of carrying out evidence taking

in an electronic format and, subsequently, assessing it. For example, in in person court hearings of witnesses, parties or experts are expected to be present in a court room, with some of the participants displaying a specific attire that is symbolic to their professional status, following a certain solemn procedure to initiate the session, identify the participating parties, rendering an oath before initiating evidence taking, occupying a certain predetermined place in the architecture of the courtroom and being in a position that allows the court members, the parties and their representatives, and the members of the public present to follow and observe the person giving evidence. In an online environment, especially when related to evidence taking, some of these elements can be lost given the limited view participants may have on the judges and court staff and vice versa, the number of participants who can be displayed at the same time in an online session, but also in consideration of whether the other participating parties are taking part in the session from their own premises or offices or are present in a court hall equipped with communication technology. Together with this not only individual routines of procedural actions change, but also the dynamic of interactions between various participants in court proceedings. As previously mentioned, the proposal for reviewing the Taking of Evidence Regulation sought to maintain traditional environments as symbolism participants are familiar with as well as means to secure procedural guarantees for the persons giving evidence. Thus, the taking of evidence should take place in court, in the presence of the judge, with the use of professional interpretation services, if necessary, and by referring to a procedure for presenting documents or other materials during the hearing via videoconference or other distance communication technology. In the final adopted text, these provisions are no longer explicit, although it can be argued that this can be interpreted to be the case based on Article 20 Taking of Evidence Recast. At the same time, the text offers some degree of leeway for different arrangements being attempted with the support of the central body, competent authority or court assigned in the requested Member State when the requesting court is seeking to directly take evidence by videoconferencing or other distance communication technology. This may be a handy option in prolonged emergency situations when access to court premises becomes impossible or highly limited as showed by the COVID-19 health emergency. The COVID-19 pandemic has underlined and accelerated the need to normalise reliance and use of technology for evidence taking purposes and dealing with digitalised evidence besides *ab initio* electronic forms of evidence.

The ad-hoc developments in the use of technology for evidence taking during the last couple of years are set to have a long lasting impact on the human interaction in court proceedings. These are likely to become increasingly or completely mediated by software programmes and platforms built in to guarantee resilience for justice services and accelerate procedural exchanges and acts such as the announced e-CODEX system. At the same time this may come to require new skills from practitioners using the new systems although many of the technical requirements are sought to be black-boxed to manage the complexity of the verification task and to achieve ease of use. Such developments will also reshape the human interaction in the proceedings in terms of task carried out, in person performed activities, identification of users, and technical systems users have to rely on to mediate communication between concerned parties.

The process of integrating the use of technology in cross-border evidence taking, transmission of evidence, reliance on electronic documents, and recognising their characteristic value in cross-border court proceedings is being deployed within the EU. This follows a period of two years in which national courts had gone through an ad-hoc experience with technology solutions at various stages of proceedings in order to continue providing justice services. As more legislative and technology based changes to accommodate this paradigm are under way at national level in various EU Member State digitalising judicial proceedings (e.g. the Netherlands, Spain), this will reflect also into the use of technology in cross-border judicial cooperation and deployment of systems such as the expected e-CODEX. The legal framework is being revised in the post-emergency phase and geared towards supporting long-term technology developments to make sure that fundamental procedural guarantees are preserved by the new technology led solutions and the security of transmission and preservation of documents is observed (see also Krans and Nylund 2021, Sorabji 2021, 64 referring to Lord Burnett CJ to House of Lords Select Committee on the Constitution).

The emergency situation has led to a certain degree of acceptance of integrating technology solutions into the justice process and has allowed practitioners and users to become accustomed to a new social order and procedural routine where new rules related to technology have acquired a representation, have been learned, and applied. Remote working arrangements have been in place for various periods since 2020. In this technology has managed to reshape human interaction and working modes in court proceedings and in the practices of handling claims and case files. Although the Taking of Evidence Recast only identifies the decentralised IT system to be used for requests and communications in the taking of evidence, more changes are under way regarding the way of receiving electronic documents, consulting files, interacting with parties, and holding hearings in cross-border litigation. In this the gained national experiences are valuable steppingstones towards embracing further technology developments for justice services. Electronic exchanges and communications between national competent authorities according to Article 7 Taking of Evidence Recast is set to accelerate the procedural exchanges, and subsequently the process of taking of evidence itself.

In handling electronic forms of evidence, the courts need to change some of their assessing formats as electronic evidence may integrate elements that are not or cannot be inscribed in paper formats or the data inscribed have to be handled differently than paper files in order to correctly evaluate the information presented to the court. This is not addressed by the provisions of the Taking of Evidence Recast. The medium in which evidence information is presented can shape the corpus of knowledge based on which the judge can make further inferences and/or take further actions (see also Lanzara 2016, 188–190).

The legal process of formalising the establishment and use of an EU e-Justice Services infrastructure (e-CODEX) for the transmission of requests and other communications between national authorities (Article 7(1) Taking of Evidence Recast) will further push this process of normalisation and general use of technology in evidence taking, transmission, and consideration of new forms of electronic evidence (COM(2020) 712 final). In this transition, practitioners will have to "learn to work with multiple representations" (Lanzara 2016, 190) of reality based on the media in which the evidence

is displayed or contained (e.g. paper written, digitalised paper document, electronic generated evidence, video, personal observation and discussion). The draft Implementation Regulation regarding the Taking of Evidence Recast published by the European Commission on 25 January 2022 is set to establish the rules for the e-CODEX based decentralised interconnected IT system for exchanging data in cross-border taking of evidence. The provisions relate to the technical specifications of communication methods and protocols, the security objectives and technical standards to follow, the minimum availability of services objectives,[27] and the establishing of a steering committee (Ref.Ares(2022)573182). For courts this implementation will secure a friendly interface that will "black-box" several verification and validation steps delivering information and communication between involved authorities situated in different Member States. It will automatise checks such as proof of integrity of the transmitted data and of the origin and receipt of the data, validation of signatures, authentication and authorisation of registered users and verification of their identity. This contributes also to addressing legal requirements concerning the security of the transmission and integrity of the data during this process, digital certification of the origin of the data and proof of data being received, integrity of the data during the transmission process through digital certification, public key infrastructure and digital signatures. When such systems are used judges and court staff do not need to carry out additional specific checks and validation of the IT components as certain characteristics are guaranteed by the technical standards used by the system that has been certified for legal compliance. Although welcomed developments, as with previous technology supported processes adopted by the judicial services, the initial period may involve some undue delays and difficulties of application. This can be the result of the technical characteristics of the system, the interconnection between various national access points and the European gateways of the e-CODEX as well as the knowledge and dynamics of court staff and judges acquiring the technical skills required for a smooth use of the new system, adjusting their procedural practices, and their ease in handling of various forms of electronic evidence.

From a technology perspective as the process of integrating more developments and creating a mediated routine by relying on information and communication technology for accomplishing various procedural steps including evidence taking and handling will further unfold in the coming years, difficulties may also arise in practice in relation to the complexities that have to be tackled. This is due to the fact there are no harmonised technical standards used by the Member States[28] established for securing the quality and security of the transmission such as firewalls in place, passwords use, biometrics for identification of the parties and legal professionals involved, and personal data protection. This remains the domain of national systems and have been developed so far in a piecemeal approach. The e-CODEX project can offer an appropriate infrastructure

[27] This is according to paragraph 6.1 Annex laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1783 of the European Parliament and of the Council 24 hours, seven days a week, with a technical availability rate of at least 98% (excluding scheduled maintenance).

[28] The e-CODEX infrastructure is not going to address this aspect of communication in the process of taking evidence in cross-border proceedings.

for taking of electronic evidence and transmission of such files.[29] The system has the technical capacity to support the transmission of electronic documents and the regulation proposal concerning this communication system is a confirmation of the potential it provides. However, not all Member States have implemented the e-CODEX infrastructure, which at the same time needs to be interoperable with existing national e-justice information systems and practices. Given these circumstances and the fact the Member States may require some time to build in the ability to develop or implement the necessary national IT systems components, a further development of the e-CODEX can be envisaged to combine a centralised and decentralised approach towards national needs in supporting evidence taking while providing the necessary secure connections and technical guarantees to legalise technology solutions in view of legal security requirements (Biasiotti 2018, 21).

4.3. eIDAS Regulation

4.3.1. Overview

Referred earlier as a regulation having a cross-sectorial importance, the eIDAS Regulation establishes unified rules for recognition of national electronic identification across the EU aiming to create a single legal and technical framework that allows interoperability and recognition of national electronic identification schemes for electronic transactions in the internal market (Polański 2015, 775). Its provisions are applicable since 1 July 2016.

In the EU the Regulation provides a legal framework in relation to electronic signatures, seals, time stamps, electronic documents, registered delivery services and certificate services for website authentication. These elements generally differ across Member States legal systems, organisations or activities (e.g. electronic signatures used by professional orders; digital identities, certified emails, iCuria, trust services) and are not directly interconnected outside the national territory. This regulation marked an important step in creating a necessary normative framework and a circle of trust that allows mutual recognition of national identification schemes. Prior to its adoption a legal basis was missing. This meant that projects looking to provide digital solutions for cross-border procedures such as e-CODEX had to develop their own solution between participating parties to secure mutual recognition of identification schemes (Borsari and Velicogna 2011, Velicogna 2014).

Although the eIDAS Regulation establishes rules necessary to facilitate recognition of identities and documents exchanged in an electronic format, the inadequate technical interoperability between existing national systems maintains barriers in the identification and qualification of the parties involved. This is due to the fact specific identification guarantees are required to secure the validity of communication in electronic judicial cooperation between authorities in cross-border procedures. The situation is acknowledged in Recital 9 of the Regulation that recognises that still in most cases today the interconnection of electronic identification is lagging behind. This legal and technical incapacity of the present systems is an important disrupting factor. Mutually recognised electronic identifications enable citizens and businesses to operate

[29] On e-CODEX see further for example, Velicogna 2014, 320–324, Velicogna and Lupo 2017, 197–204.

on a cross-border basis without facing many obstacles in interacting with public authorities. This is a first step in guaranteeing the legal value, integrity, quality, and characteristics of the electronic documents that can be used as evidence.

4.3.2. Legal normativity

For evidence taking, transmission of requests, and communications related to evidence taking via distance communication technology, a secured identification of parties involved is essential. At present, the normative framework provided by the eIDAS Regulation still has little impact and use in judicial cooperation between Member States and more specifically on the taking of electronic evidence. This situation is expected to improve with the coming into application of the Taking of Evidence Recast in July 2022. The regulation will give a further impulse in reaching this interoperability as a legal basis for the recognition of such exchanges as communication is to take place electronically, as well as of the technical systems that have to be interconnected via a system of European connectors.

On a general basis, EU citizens and businesses cannot use their electronic identification to authenticate themselves in other Member States because their national electronic identification scheme is not recognised and interoperable with those of other Member States (Recital 9 eIDAS). The same is true for legal professionals (see Pro-CODEX,[30] Velicogna *et al.* 2017).

The general legal framework for the qualified trust services (i.e. electronic signatures, electronic seals, electronic time marking, electronic documents and certification services for Web authentication) is referred to in the Taking of Evidence Recast regulation in dealing with requests and communication between authorities (Article 7(2)). This reliance on the eIDAS gives the Regulation a procedural law dimension in EU cross-border proceedings and reinforces the calls made by Recital 22 eIDAS to make it possible to use trust services as evidence in legal proceedings in all Member States.

The Taking of Evidence Recast is relying on the provision of the eIDAS Regulation for guaranteeing an electronic environment the security standards that are given to a handwritten signature and seal in paper-based formats. The qualification of relevant data and electronic objects in court proceedings upholds procedural guarantees and standards of certainty associated with paper evidence and documents. These elements that have an importance for requirements of authenticity, integrity, preservation, and evaluation further sustains the legal process and judicial cooperation. In this the eIDAS Regulation provides a valuable part of the necessary legal framework. The solution chosen guarantees certain degrees of certainty and possibility to verify electronic information, and accommodate available information and communication solutions that are generated by systems that are not directly interconnected outside the national territory.

The transmission of requests and electronic documents via a decentralised IT system such as e-CODEX and the forms of the Taking of Evidence Recast will be required to include qualified electronic signatures. The use of such signatures is retained to produce the same legal effects of a handwritten signature (Article 7(3) Taking of Evidence Recast

[30] Technical solutions (https://www.e-codex.eu/technical-solutions), Velicogna *et al.* 2017.

in conjunction with Article 25(2) eIDAS). The qualified electronic seals when used enjoy the presumption of integrity of data and of correctness of origin of the data (Article 35(2) eIDAS).[31] By relying on this legal framework the principle of equivalence reduces the margin of appreciation placed on the judge in the proceedings, unless counterevidence is submitted. Thus, if a qualified electronic signature or seal is used, this is retained to produce equivalent effects to ones in a handwritten-format or to guarantee the integrity of the data and correctness of the origin of the data (Article 25(2) and Article 35(2) eIDAS) without the judge having to carry out additional investigations or assessments. The use of an electronic signature is expected to secure the link between the procedural act or the act to be evaluated as electronic document for evidentiary purposes and the signatory, as well as its identity and the integrity of the document (Jacquemin and Gillard 2018, 565). Pursuant to Article 25(1) eIDAS Regulation, an electronic signature is not to be denied "legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form, or that it does not meet the requirements for qualified electronic signature". Thus, the principle of non-discrimination should guarantee a parallel acceptance of electronic and physical/paper-based evidence provided that the electronic signature "achieves each function fulfilled by the handwritten signature and/or enumerated by the legislator or identified by the judge or any other person that has to give an interpretation" (Jacquemin and Gillard 2018, 565). The same applies pursuant to Article 35(1) eIDAS Regulation for electronic seals.

Furthermore, Article 2(35) eIDAS Regulation defines the concept of "electronic document" as "any content stored in electronic form, in particular text or sound, visual or audiovisual recording". This is of significant importance as the Taking of Evidence Recast does not define the concept, and only addresses the legal effects of electronic documents. With this definition of electronic documents, Article 2(35) eIDAS touches upon the requirement of adopting legal provisions to deal with the diversity of sources that may constitute electronic evidence. Article 46 eIDAS relies on the principle of non-discrimination between electronic and paper-based documents and establishes that an electronic document "shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form". The same wording is relied on by Article 8 Taking of Evidence Recast Regulation. Thus, a court should not and cannot reject such document from provided evidence, just based on its format (Jacquemin and Gillard 2018, 586) being it *ab initio* electronic or being subsequently digitalised for communication purposes.

4.3.3. Socio-technical normativity

For mutual recognition of trust services between Member States, the legal sphere is not sufficient, but this has to be doubled by a technical interoperability. In this, the eIDAS does not extensively deal with socio-technical components besides setting the ground for mutual recognition of electronic identification (Article 6 eIDAS), assurance levels of identification schemes and minimum technical specifications (Article 8 eIDAS), descriptions of electronic identification schemes (Article 9 eIDAS), and cooperation and interoperability (Article 12 eIDAS). The Proposal on the e-CODEX system will provide

[31] Electronic seals serve as evidence that an electronic document was issued by a given legal person, ensuring the document's origin and integrity (Recital 59 eIDAS Regulation).

a framework for the necessary interconnection between national electronic systems (COM(2020) 712 final). However, the handling and storage of the transmitted electronic data will remain within the management of the national justice systems' electronic solutions.

Furthermore, Article 46 eIDAS Regulation on the principle of non-discrimination between electronic and paper-based documents establishes that an electronic document is relevant also from a socio-technical normativity point of view as it impels the reshape of practices of involved authorities and the human interaction in court proceedings. As rightfully pointed out by Polanski, this provision "may revolutionise daily operations of national courts, which either did not recognise or very reluctantly admitted electronic documents" so far, and more so with the Taking of Evidence Recast Regulation becoming applicable in July 2022 (Polański 2008, 776–777, Mason 2008). As previously mentioned, the qualified certifications certainly facilitate the task courts have in ascertaining certain characteristics of the electronic evidence submitted to them and diminish the need to rely on experts in order to be able to deal with such elements in court proceedings.

4.4. GDPR

4.4.1. Overview

Similar to the eIDAS Regulation, the General Data Protection Regulation is a regulation having a cross-sectorial importance. The Regulation is applicable since 25 May 2018 and is considered to be at the "heart of the EU framework guaranteeing the fundamental right to data protection" (COM(2020) 264 final) as set by Article 8 Charter of Fundamental Rights of the European Union and Article 16 Treaty on the Functioning of the European Union. The GDPR aims to strengthen data protection safeguards, protect individual rights, increase transparency and ensure that the personal data falling under its scope of application are handled in a responsible and accountable manner.

When looking at court proceedings, the GDPR applies to the activities of courts and other judicial authorities as processors of personal data. Therefore, in acting in their judicial capacity the members of the judiciary have to comply with the obligations set out by this Regulation (Recital 20). This also concerns electronic data.

4.4.2. Legal normativity

The gathering of electronic documents and data for evidence purposes and the uploading of the data in electronic files can fall under the material scope of the GDPR as structured sets of personal data that are accessible in accordance with certain criteria. These have to address and comply with privacy requirements.[32] The processing of different type of electronic documents may lead to the processing of special categories of personal data (e.g. photographs revealing special characteristics of a person, documents containing personal identification details, property, genetic data, biometric data, health data). Based on the privacy requirement such data should be processed only if necessary, in relation to the handled legal claims or in relation to judicial capacities of

[32] Article 2(1) GDPR. See also Zwenne *et al*. 2018, 65-66.

the members of the court (Articles 9(1)(f) and (2)(f) GDPR).[33] Article 30(1) Taking of Evidence Recast underlines that "any processing of personal data carried out" in relation to the regulation, "including the exchange or transmission of personal data by competent authorities" has to be carried out in conformity with the provisions of the GDPR. Any personal electronic data that is not relevant for the handling of the case or the evidence being taken also when this is carried out via information and communication technology should be immediately deleted. This can be linked to the requirement of legality in the processing of data.

The courts or other national authorities involved in the taking of electronic evidence or their assessment will be regarded as controllers in the sense of the GDPR when processing personal data (Article 30(2) Taking of Evidence Recast in conjunction with Article 4(7) and Articles 24–43 GDPR). Thus, they will have a role in determining the purpose and means of processing the personal data. This means that the provisions of the GDPR are relevant for various elements of the legal normativity framework, namely: privacy, legality, and transparency.

Further, some of the data in electronic files may be automatically processed in accordance with the provision of Article 2(1) GDPR (e.g. via computers, laptops, cloud services, routers part of the e-justice system). Thus, elements of legal normativity should be integrated and developed also for this purpose as such services are put in place or offered to courts in handling proceedings and collecting data that can be used as electronic evidence. This can touch upon rules of privacy, guaranteeing the security of the transmission, legality of the data use, and transparency in relation to the relevant GDPR rules.

4.4.3. Socio-technical normativity

From the requirements set by the GDPR provisions in terms of handling of personal data, processing and controlling activities, electronic evidence may be handled by the members of the court, be subject to an automatic handling, thus entrusting the compliance with privacy of data requirements to a machine based process, or be the result of a mixed handling. In all circumstances the legal requirements and technical development reshape the tasks of the parties involved and the human interaction, their access to specific types of information contained by electronic evidence as well as the followed routines.

5. Concluding remarks

This paper explores the developments brought by electronic realities in a rapidly changing society and how these reflect in the taking of evidence in court proceedings. The shift towards electronic environments and objects comes as a search to deliver efficient justice services and to respond to the needs of a growing digitally mediated reality in our everyday lives and activities (see also Velicogna 2020). These new realities are taking shape and pushing the limits of traditional paper-based approaches that are no longer sufficient to deal with the particularities of information, access to data and evidence brought by technology. The switch towards integrating electronic forms of evidence and their gathering in an electronic format comes with a search for order and

[33] See also Recital 52 GDPR.

re-establishment of legality within the same procedural standards and guarantees of fundamental rights. The process requires new norms that are able to mediate the interaction and joint functioning of traditional paper-based documents and evidence with new electronic objects covering the same function.

The EU legislation concerning cross-border taking of evidence is preparing itself to address more of the identified legal aspects that are relevant when dealing with electronic formats and information and communication technology. This will also influence the processes court staff and judges need to follow, their routine in interacting with each other and with colleagues from other Member States as well as with the parties. The process will also lead to an adaptation in the tasks they have to cover on their own, mediated by technology or delegating them to technology.

In terms of effect, electronic evidence has to be given the same use as other forms of evidence which we have been widely accustomed to. In this process consideration has to be given to their different characteristics and particularities compared to physical or paper-based formats. Although more ambitious developments could not have been considered and agreed upon during the European legislative process, the new text of the Taking of Evidence Recast Regulation adds an additional layer towards further integration and normalisation of technology use in judicial cooperation and evaluation of electronic evidence. The process is ongoing and cannot be ignored or set aside, but further developments remain necessary as guidance in evaluating the characteristics and the correct content of this type of evidence.

The legislative, technical, and institutional framework is not yet complete in cross-border litigation, but the present developments are gaining momentum due to their increase relevance and capabilities of upholding the consolidated values of justice from a procedural and fundamental rights perspective. The Taking of Evidence Recast rules act at different levels in providing a normative framework and normalising the use of technology in the process of taking of evidence in cross-border litigation, namely, it recognises the legal value of electronic documents and/or objects communicated for evidentiary purposes, pushes for a full digital communication between authorities involved in the process of taking of evidence, and supports the use of technological means for participation in the taking of evidence process and direct taking of evidence. Together with these regulations such as the eIDAS or the GDPR are relied on to address matters related to legal normativity such as authenticity, privacy, legality, and transparency. Other elements remain to be further addressed by new proposed regulations such as the e-CODEX Proposal and the Digitalisation of Judicial Cooperation Proposal. Matters related to the evaluation of electronic forms of evidence, assessing related metadata, manipulation and storing of such information are not directly address by the present European framework or related proposal. They remain gaps that have to be filled in my national legislation or practices.

References

Bayard, F., 2020. Aanbevelingen ingevolge corona (College van hoven en rechtbanken). *Legal News* [online], 13 March. Available from: https://legalnews.be/geschillen-procedure/aanbevelingen-ingevolge-corona-college-van-hoven-en-rechtbanken/ [Accessed 8 April 2022].

Biasiotti, M.A., 2018. Present and Future of the Exchange of Electronic Evidence in Europe. *In:* M.A. Biasiotti *et al.*, eds., *Handling and Exchanging Electronic Evidence Across Europe*. Cham: Springer, 13–32.

Biasiotti, M.A., *et al.*, 2018. Introduction: Opportunities and Challenges for Electronic Evidence. *In*: M.A. Biasiotti *et al.*, eds., *Handling and Exchanging Electronic Evidence Across Europe*. Cham: Springer, 3–12.

Borsari, G., and Velicogna, M., 2011. Executive summary. *In:* G. Borsari *et al.*, eds., *e-CODEX deliverable 7.1 governance and guidelines definition* (v. 1), 10–12.

Canguilhem, G., 1991. *The Normal and the Pathological*. New York: Zone Books.

CEPEJ-CoE 2020. *European judicial systems – CEPEJ Evaluation Report – Evaluation cycle 2020. Part 1: Tables, graphs and analysis.* Council of Europe.

Contini, F., 2020. Artificial Intelligence and the Transformation of Humans, Law and Technology Interactions in Judicial Proceedings. *Law, Technology and Humans* [online], 2(1), 4–18. Available from: https://lthj.qut.edu.au/article/view/1478 [Accessed 8 April 2022].

Docrat, Z., and Kaschula, R.H., 2020. Forensic linguists explore how emojis can be used as evidence in court. *The Conversation* [online], 22 March. Available from: https://theconversation.com/forensic-linguists-explore-how-emojis-can-be-used-as-evidence-in-court-133462 [Accessed 8 April 2022].

Fabri, M., 2009. The Italian Style of e-Justice in a Comparative Perspective. *In*: A. Cerrillo i Martínez and P. Fabra i Abat, eds., *Information and Communication Technologies in the Court System*. Hershey: IGI Global, 1–19.

Garapon, A., and Lassègue, J., 2018. *Justice digitale : Révolution graphique et rupture anthropologique*. Paris : PUF.

Gascón Inchausti, F., and Requejo Isidro, M., 2019. Classic Cross-border Case: The Usual Situation in the First Instance. *In*: B. Hess and P. Ortolani, eds., *Impediments of National Procedural Law to the Free Movement of Judgments, Luxembourg Report on European Procedural Law* (*Volume I).* Oxford/Baden-Baden: Beck/Hart/Nomos, 5–85.

Govender, S., 2017. Those smiley face or thumbs up emojis could land you in legal hot water. *Times Live* [online], 1 October. Available from: https://www.timeslive.co.za/news/south-africa/2017-10-01-those-smiley-face-or-thumbs-up-emojis-could-land-you-in-legal-hot-water/# [Accessed 8 April 2022].

Jacquemin, H., and Gillard, N., 2018. Regulation 910/2014/EU – eIDAS Regulation. *In:* S. Gijrath *et al.*, eds., *Concise European Data Protection, E-Commerce and IT Law* 3rd ed. Alphen aan den Rijn: Kluwer Law International, 503–590.

Jansen, R., 2019. Explaining the methods for taking evidence abroad within the EU and some first observations on the proposal for the Evidence Regulation (recast). *Nederlands Internationaal Privaatrecht*, 4, 753–770.

Janssen, E. 2018. Hearsay in the Smiley Face: Analyzing the Use of Emojis as Evidence. *St. Mary's Law Journal* [online], 3, 699–725. Available from:

https://commons.stmarytx.edu/cgi/viewcontent.cgi?article=1012&context=thestmaryslawjournal [Accessed 8 April 2022].

Krans, B., and Nylund, A., eds., 2020. Civil Justice and Covid-19. *Septentrio reports* [online], 5. Available from: https://doi.org/10.7557/sr.2020.5 [Accessed 8 April 2022].

Krans, B., and Nylund, A., eds., 2021. *Civil Courts Coping with COVID-19* [online]. The Hague: Eleven International. Available from: https://boeken.rechtsgebieden.boomportaal.nl/publicaties/9789462362048#5 [Accessed 8 April 2022].

Lanzara, G.F., 2009. Building Digital Institutions: ICT and the Rise of Assemblages in Government. *In:* F. Contini and G.F. Lanzara, eds., *ICT and innovation in the public sector: European studies in the making of e-government.* Basingstoke: Palgrave, 9–48.

Lanzara, G.F., 2014. The Circulation of Agency in Judicial Proceedings: Designing for Interoperability and Complexity. *In:* F. Contini and G.F. Lanzara, eds., *The Circulation of Agency in E-Justice: Interoperability and Infrastructures for European Transborder Judicial Proceedings*. Dordrecht: Springer Netherlands, 3–32.

Lanzara, G.F., 2016. *Shifting Practices: Reflection on Technology, Practice, and Innovation*. Cambridge, MA: The MIT Press, 145–194.

Mason, S., ed., 2008. *International Electronic Evidence*. London: British Institute of International and Comparative Law.

Mohr, R., 2005. Enduring Signs and Obscure Meanings: Contested Coats of Arms in Australian Jurisdictions. *In:* A. Wagner, T. Summerfield and F. Benavides, eds., *Contemporary Issues of the Semiotics of Law*. Oxford: Hart, 180–195.

Onţanu, E.A., 2017, *Cross-Border Debt Recovery in the EU: A Comparative and Empirical Study on the Use of the European Uniform Procedures*. Cambridge/Brussels: Intersentia.

Onţanu, E.A., 2019. Adapting Justice to Technology and Technology to Justice. A Coevolution Process to e-Justice in Cross-Border Litigation. *European Quarterly of Political Attitudes and Mentalities* [online], 8(2), 1–18. Available from: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-62449-5 [Accessed 8 April 2022].

Polański, P.P., 2015. Towards the single digital market for e-identification and trust services. *Computer Law and Security Review*, 31(6), 773–781.

Sorabji, J., 2021. Developing the New Normal for English Civil Procedure Post Covid-19. *In*: B. Krans and A. Nylund, eds., *Civil Courts Coping with COVID-19* [online]. The Hague: Eleven International, 63–72. Available from: https://boeken.rechtsgebieden.boomportaal.nl/publicaties/9789462362048#5 [Accessed 8 April 2022].

Stuerner, R., 2018. Current Developments of the Law of Evidence from a Comparative Point of View. General Report. *In:* Instituto Iberoamericano de Derecho Procesal, ed., *La prueba en el proceso (Evidence in the Process), II Conferencia International & XXVI Jornadas Iberoamericanas de Derecho Procesal, IIDP-IAPL.* Barcelona: Atelier Libros Jurídicos.

Tulibacka, M., 2009. Europeanization of Civil Procedure: In Search of a Coherent Approach. *Common Market Law Review*, 46(5), 1527–1565.

Vazquez Maymir, S., 2019. Anchoring the Need to Revise Cross-Border Access to e-Evidence. *Internet Policy Review* [online], 9(3), 1–243. Available from: https://doi.org/10.14763/2020.3.1495 [Accessed 8 April 2022].

Velicogna, M., 2007. Justice systems and ICT-What can be learned from Europe. *Utrecht Law Review* [online], 3(1), 129–147. Available from: https://doi.org/10.18352/ulr.41 [Accessed 8 April 2022].

Velicogna, M., 2014. Coming to Terms with Complexity Overload in Transborder e-Justice: The e-CODEX Platform. *In:* F. Contini and G.F. Lanzara, eds., *The Circulation of Agency in E-Justice: Interoperability and Infrastructures for European Transborder Judicial Proceedings*. Dordrecht: Springer Netherlands, 309–330.

Velicogna, M., 2020. *Cross-Border Civil Litigation in the EU: What Can We Learn from COVID-19 Emergency National e-Justice Experiences?* [online]. Available from: https://dx.doi.org/10.2139/ssrn.3737648 [Accessed 8 April 2022].

Velicogna, M., and Contini, F., 2009. Assemblage-in-the-making: Developing the e-services for the Justice of the Peace Office in Italy. *In:* F. Contini and G.F. Lanzara, eds., *ICT and innovation in the public sector: European studies in the making of e-government.* Basingstoke: Palgrave, 211–243.

Velicogna, M., and Lupo, G., 2017. From Drafting Common Rules to Implementing Electronic European Civil Procedures: The Rise of e-CODEX. *In:* B. Hess and X.E. Kramer, eds., *From Common Rules to Best Practices in European Civil Procedure*. Oxford/Baden-Baden: Hart/Nomos, 197–204.

Velicogna, M., and Ng, G.Y., 2006. Legitimacy and Internet in the Judiciary: A lesson from the Italian Courts' websites experience. *International Journal of Law and Information Technology*, 14(3), 370–389.

Velicogna, M., and Steigenga, E., 2016. Can Complexity Theory Help Understanding Tomorrow E-Justice? *Conference on Complex Systems, Law and Complexity session, Amsterdam* [online], 20–23. Available from: https://www.e-codex.eu/sites/default/files/2019-08/Velicogna_Steigenga_2016_-_Can_complexity_theory_help_understanding_tomo_0.pdf [Accessed 5 April 2022].

Velicogna, M., *et al*., 2017. *D1.1 The existing context: Assessment report on the current situation to connect legal practitioners to e-CODEX in Pro-CODEX participating countries, Pro-CODEX project deliverable v.1.0.* Bologna: IRSIG.

Wharton, J., 2019, Judges need to know what the aubergine emoji really means. *Metro* [online], 22 February. Available from : https://metro.co.uk/2019/02/22/judges-need-know-aubergine-emoji-really-means-8708867/ [Accessed 8 April 2022].

Wilson, S., 2015, Developing a Metadata Repository for Distributed File Annotation and Sharing, Open Access Theses. p. 1.

Zwenne, G.J., *et al.*, 2018. Regulation 2016/679/EU – General Data Protection Regulation. *In:* S. Gijrath *et al.*, eds., *Concise European Data Protection, E-Commerce and IT Law* 3rd ed. Alphen aan den Rijn: Kluwer Law International, 19–252.

Rules and guidelines

Belgium

Act of 20 December 2020. *Moniteur Belge* [online], 24 December 2020. Available from: http://www.ejustice.just.fgov.be/eli/arrete/2020/12/24/2020044702/moniteur [Accessed 8 April 2022].

Croatia

Minister of Justice Decree of 20 April 2020 [online]. Available from: https://www.hok-cba.hr/obavijesti-zborova/oz-zagreb/odluka-o-ispunjenju-uvjeta-za-elektronicku-komunikaciju-za-sudovima-u-rh/ [Accessed 8 April 2022].

England and Wales

Coronavirus Act 2020, Schedule 25 [online]. Available from: https://www.legislation.gov.uk/ukpga/2020/7/schedule/25/enacted [Accessed 8 April 2022].

CPR PD 51Y -Video or Audio Hearings during Coronavirus [online]. Available from: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part51/practice-direction-51y-video-or-audio-hearings-during-coronavirus-pandemic [Accessed 8 April 2022].

European Union

Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation (COM/2020/264 final) [online]. Brussels, 24 June 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264 [Accessed 8 April 2022].

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. *Official Journal of the European Union* [online], L 201, 31 July 2002, p. 37–47. Available from: http://data.europa.eu/eli/dir/2002/58/oj [Accessed 8 April 2022].

Directive 2014/104/EU on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union. Text with EEA relevance. *Official Journal of the European Union* [online], L 345, 5 December 2014, 1–19. Available from: http://data.europa.eu/eli/dir/2014/104/oj [Accessed 8 April 2022].

Draft Commission Implementing Regulation laying down the technical specifications, measures and other requirements for the implementation of the decentralised IT system referred to in Regulation (EU) 2020/1783 of the European Parliament and

of the Council, Ref.Ares(2022)573182 -25/01/2022 [online]. Available from: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13227-Cross-border-taking-of-evidence-in-civil-commercial-matters-new-IT-system-for-exchanging-data_en [Accessed 8 April 2022].

European Economic and Social Committee, Opinion a) Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters [COM(2018) 378 final – 2018/203 (COD)] (online). Available from: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/taking-evidence-and-service-documents [Accessed 8 April 2022].

European Parliament legislative resolution of 13 February 2019 on the proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (COM(2018)0378 – C8-0242/2018 – 2018/0203(COD)). *Official Journal of the European Union* [online], C 449/537, of 23 December 2020. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019AP0103 [Accessed 8 April 2022].

Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (COM/2018/378 final) [online]. Brussels, 31 May 2018. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2018%3A378%3AFIN [Accessed 8 April 2022].

Proposal for a Regulation on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726 (COM(2020) 712 final) [online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0712 [Accessed 8 April 2022].

Proposal for a Regulation on Digitalisation of Judicial Cooperation and Access to Justice in Cross-Border Civil, Commercial and Criminal Matters, and Amending Certain Acts in the Field of Judicial Cooperation (COM(2021) 759 final) [online]. Available from: https://ec.europa.eu/info/sites/default/files/law/cross-border_cases/documents/1_1_178479_regul_dig_coop_en.pdf.pdf [Accessed 8 April 2022].

Questionnaire on videoconferencing, in Note 15641/07 ADD 2 of 12 December 2007 (referring to 10509/07 JURINFO 23 JAI 301 JUSTCIV 163COPEN 89) [online]. Available from: https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vi7jgt8023zd [Accessed 8 April 2022].

Regulation (EC) 1206/2001 on cooperation between the courts of the Member States in the taking of evidence in civil and commercial matters (Tacking of Evidence

Regulation). *Official Journal of the European Union* [online], L 174, 27.6.2001, p. 1–24. Available from: http://data.europa.eu/eli/reg/2001/1206/oj [Accessed 8 April 2022].

Regulation (EC) No 861/2007 establishing a European Small Claims Procedure. *Official Journal of the European Union* [online], L 199, 31 July 2007, p. 1–22. Available from: http://data.europa.eu/eli/reg/2007/861/oj [Accessed 8 April 2022].

Regulation (EU) 2016/679 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). *Official Journal of the European Union* [online], L 119, of 4 May 2016, p. 1–88. Available from: http://data.europa.eu/eli/reg/2016/679/oj [Accessed 8 April 2022].

Regulation (EU) 2020/1783 on cooperation between the courts of the Member States in the taking of evidence in civil and commercial matters (Taking of Evidence Recast). *Official Journal of the European Union* [online], L 405, 2 December 2020, p. 1–39. Available from: http://data.europa.eu/eli/reg/2020/1783/oj [Accessed 8 April 2022].

Regulation (EU) No 655/2014 establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery in civil and commercial matters. *Official Journal of the European Union* [online], L 189, 27 June 2014, p. 59–92. Available from: http://data.europa.eu/eli/reg/2014/655/oj [Accessed 8 April 2022].

Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive (EC) No 1999/93. *Official Journal of the European Union* [online], L 257, 28 August 2014, p. 73. Available from: http://data.europa.eu/eli/reg/2014/910/oj [Accessed 8 April 2022].

Resolution P6_TA(2009)0089 of 10 March 2009 [online]. Available from: https://www.europarl.europa.eu/doceo/document/TA-6-2009-0089_EN.html?redirect [Accessed 8 April 2022].

Resolution P7_TA(2010)0426 of 23 November 2010 [online]. Available from: https://www.europarl.europa.eu/doceo/document/TA-7-2010-0426_EN.html [Accessed 8 April 2022].

Case law

CJEU 6 September 2012, Case C-170/11 *Lippens c.s./Kortekaas c.s*, ECLI:EU:C:2012:540.

CJEU 21 February 2013, Case C-332/11 *ProRail BV v Xpedys NV e.a.*, ECLI:EU:C:2013:87.