1 2 9 0

INSTITVTO IVRIDICO
FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

fct Fundação para a Ciência e a Tecnologia
UID04643

Digital Transformation and Governance in the Judiciary

COORDENAÇÃO:
Fabrício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell

Ficha Técnica

TÍTULO
Digital Transformation and Governance in the Judiciary

COORDENAÇÃO:
Fabrício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell

EDIÇÃO
Instituto Jurídico
Faculdade de Direito da Universidade de Coimbra
geral@ij.uc.pt • www.uc.pt/fduc/ij
Colégio da Trindade • 3000-018 Coimbra

CONCEPÇÃO GRÁFICA
Pedro Bandeira

CAPA
Dalldesign

ISBN: 978-989-9075-92-4
e-ISBN: 978-989-9075-85-6

DOI: 10.47907/DigitalTransformationAndGovernance/livro

julho de 2025

A publicação do presente trabalho inscreve-se nas atividades do IJ/UCILeR (Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra), no contexto do projeto estratégico UID 04643 – Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra (financiado pela FCT – Fundação para a Ciência e a Tecnologia).

Fabrício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell
Editors

Digital Transformation and Governance in the Judiciary

Authors

Ana Carla Werneck
Audrey Kramy Araruna Gonçalves
David Soto
Fabrício Castagna Lunardi
Federico Bueno de Mata
Fernando Martín Diz
Francesco Contini
Inês Oliveira
Irene González Pulido
Irene Yáñez García-Bernalt
Lorenzo-Mateo Bujosa Vadell
Pedro Miguel Alves Ribeiro Correia
Ricardo Pedro
Salomão Akhnaton Z. S. Elesbon

1 2 9 0

INSTITVTO IVRIDICO
FACULDADE DE DIREITO
UNIVERSIDADE D
COIMBRA

University Of Coimbra
National School For Training And Improvement Of Judges (Enfam)

ACADEMIC AND SCIENTIFIC COOPERATION BETWEEN THE FACULTY OF LAW OF THE UNIVERSITY OF COIMBRA (FDUC) AND THE BRAZILIAN NATIONAL SCHOOL FOR TRAINING AND IMPROVEMENT OF JUDGES (ENFAM)

On August 31, 2022, FDUC (Portugal) and ENFAM (Brazil) signed, through their top representatives, an Academic and Scientific Cooperation Agreement aimed at implementing joint and effective actions that would ensure the performance of academic activities related to teaching and research, by of their Research Centers and Institutes. The cooperation has involved the implementation of projects, research groups, international seminars, scientific publications, data sharing and exchange of experiences, among other products.

This book is another important product of the Scientific and Academic Cooperation Agreement between the two renowned higher education institutions, of the partnership between research groups, as well as of the collaboration of professors and researchers from the University of Salamanca.

ACKNOWLEDGEMENTS

This work is the result of research developed by renowned researchers on technological transformation and digital governance in the justice system, in their research centers. This connection between researchers has been important for the production of knowledge, as it allows knowledge to be developed from a global perspective.

In this sense, we would like to thank all the authors who contributed to this work based on their research, materialized in the chapters: Ana Carla Werneck, Inês Oliveira, Audrey Kramy Araruna Gonçalves, Irene González Pulido, David Soto, Irene Yáñez García-Bernalt, Fabrício Castagna Lunardi, Lorenzo-Mateo Bujosa Vadell, Federico Bueno de Mata, Pedro Miguel Alves Ribeiro Correia, Fernando Martín Diz, Ricardo Pedro, Francesco Contini, and Salomão Akhnaton Z. S. Elesbon.

We would also like to thank our institutions, which supported us in the research and production of this book: National School for the Training and Improvement of Magistrates – ENFAM (Brazil), University of Coimbra (Portugal) and University of Salamanca (Spain).

We would also like to thank the ENFAM team of librarians, who helped us standardize the text, especially the bibliographical references, in accordance with the Publisher's standards.

We would also like to give special thanks to the Press of the Legal Institute of the Faculty of Law of the University of Coimbra, which edited this work.

Finally, we would like to thank our readers, professors, researchers and students, who are the reason for this book.

Have a great read!

Brasília/Coimbra/Salamanca, March 2025.

Fabrício Castagna Lunardi
Pedro Miguel Alves Ribeiro Correia
Lorenzo-Mateo Bujosa Vadell
Editors

Contents

PART III – PEOPLE MANAGEMENT IN DIGITAL JUSTICE

PART IV – DATA MANAGEMENT: JUDICIAL TRANSPARENCY, LITIGANCE AND PROTECTION OF PERSONAL DATA

CHAPTER 1 – EVIDENTIARY ASPECTS OF THE BLOCKCHAIN: ANALYSIS OF THE LEGAL REALITY IN EUROPE AND SPAIN

(DOI: 10.47907/DigitalTransformationAndGovernance/09)

Federico Bueno de Mata[1]

Summary: 1. Genesis of a revolution at the evidentiary level. 2. A legal regulatory framework for the use of blockchain technology at the evidentiary level. 3. Procedural treatment of the blockchain. 4. Final reflections: looking at the Web3. Bibliography.

Abstract: This research analyzes the impact of blockchain technology in the field of electronic evidence. It starts from a hypothesis of assuming that blockchain technology will have a significant impact on both public administrations and society in general, which will mean changing the way personal electronic information is managed by putting control in the hands of individual citizens rather than centralized servers or platforms. The article also analyzes regulatory efforts in the European Union to adapt to the changing landscape of electronic evidence, including the proposed eIDAS 2 regulation, which seeks to establish autonomous digital identities based on blockchain technology and then focuses on the procedural treatment of blockchain as a means and source of evidence and differentiates between this technology as a means of storing electronic evidence and as a mechanism to preserve and secure this type of evidence. Likewise, the text concludes by emphasizing the potential of blockchain technology in the context of Web3, where decentralized and interoperable systems are expected to play a fundamental role in the Spanish and European administration of justice.

Keywords: Blockchain, electronic, evidence, identity.

1. Genesis of a revolution at the evidentiary level

We must be aware that blockchain technology is here to stay, understanding that it will not only have an impact on Public Administrations, but will also have an important impact at a social level that is still difficult to imagine and project at a legal level. Its application would imply changing the way in which we handle information through the Net, since its use would mean that the ownership and control of personal electronic data would cease to be in the possession of specific servers or electronic platforms and would be managed directly by each citizen. In this sense, a further step could be taken in the near future if this type of technology were applied by default in the use of the Internet by individuals, since we would avoid not only the problem of prior manipulation of the electronic evidence, but also the information would no longer depend on servers and would reside in each individual citizen. Undoubtedly, we are facing a situation that will mean a real change in the international paradigm at the evidentiary level.

[1] Catedrático de Derecho Procesal. Universidad de Salamanca. Full Professor of Procedural Law. University of Salamanca.

That is, we are currently facing an Internet where the information is requested from the judicial or police authorities to the information servers and, once we have that information collected, we propose to apply this type of technology to secure and encrypt it through blockchain and that it is not altered in view of its proposal and practice in court, but what would happen if that information did not reside properly in the servers and depended properly on each citizen? Undoubtedly, this question would change the parameters we currently know regarding the treatment of obtaining and preserving electronic evidence within a context of international procedural cooperation. This question in turn connects with two specific issues that will have to be reflected at the international regulatory level in the coming years: on the one hand, the regulation of the Internet with the new Web model3 and, on the other, the concept of self-sovereign digital identity (Allende López, 2020), based on blockchain technology pointed out by the Eidas 2 draft Regulation, in which we would not depend on intermediaries or digital platforms that store our information and would be responsible for the processing of our personal data. We believe that this technology will eventually find its true potential in this scenario and will have its impact at the regulatory level with the effective implementation of this draft Regulation (Pérez Bes, 2018).

On the one hand, we are faced with the current phenomenon of Web3, which is booming at the normative level because it involves everything related to the metaverse phenomenon. We thus start from an evolution of the Internet in three phases: Web1, Web2 and Web3 (Barrio Andrés, 2022). On the one hand, Web1 was the Internet in reading format through the hosting of static pages where users could read contents and information of various kinds; Web2 is conceived as the evolution towards a format in which users feed their own virtual content and profile their pages according to their own tastes and interests, which gave rise to the boom of social networks and an evolution in the use of the Internet, and Web3 where the user is no longer limited only to reading or creating content, but goes further and relies on what is offered on the Web to interact and take their activities from the offline world to the online world, i.e. extrapolate the physical world to the virtual world through different centralized technologies where the metaverse will gain prominence in the coming years (Bueno de Mata, 2022).

Within Web3, one of the technologies used to manage personal data is the blockchain, based on an interoperability of systems that would affect the metaverse. A priori, having a multiverse configured through platforms is not the same as talking about Metaverse as an evolution of the Network of Networks and with decentralized technological patterns. In other words, the aim is really to decentralize the service through blockchain technology, by having a purely decentralized architecture, but through various platforms that must be interoperable with each other. We will try to explain it in a less technical way: the avatar we create in a metaverse service should be valid for another metaverse created by another platform, and the particular information of each avatar will not be registered or subject to the processing of personal data, but will depend on each user through what is known as "self-sovereign digital identity" (Alamillo Domingo, 2020).

We are thus talking about decentralized infrastructures for users to create and manage their digital assets, without depending on communication service providers for their storage and

conservation. Undoubtedly, all this would mean a revolution at the level of international procedural cooperation in the field of electronic evidence. At the regulatory level, this issue has a first legal basis through Regulation (EU) No. 910/2014 of July 23, 2014, known as the eIDAS Regulation (known by its acronym eIDAS, electronic IDentification, Authentication and trust Services), entering into force on July 1, 2016 for the entire European Union and aimed at ensuring secure electronic transactions through user identification technologies in various electronic services and with agreed technical parameters. Here the data is still hosted on different electronic platforms, but all this seems to be changing thanks to the qualities of blockchain technology.

Specifically, on July 3, 2021, the European Commission presented a proposal to amend the eIDAS Regulation, called eIDAS 2, in order to regulate cross-border digital identification within the European Union, which calls for the creation of a secure interoperable European electronic identity by means of what has been called "European digital identity wallet" and which is finally approved in June 2023. This will allow all European citizens to identify themselves digitally, store and manage personal data and official documents in electronic format, while having full control over their data, without them being stored by computer servers. In this way, the new self-sovereign digital identity managed through blockchain technology would be legally recognized, so its application would entail a paradigm shift in our judicial system by impacting on various legal institutions, having a clear impact on international procedural cooperation in the field of electronic evidence within the EU.

2. A legal regulatory framework for the use of blockchain technology at the evidentiary level

During 2018, the European Commission of Justice is aware that the European Investigation Order should be strengthened through complementary mechanisms that would take into account the particularities of the commission of crimes on the Internet aimed at obtaining electronic evidence by the various authorities. Thus, the Commission spoke of creating new rules to facilitate and expedite this type of evidence "such as emails or documents located in the cloud, which are needed to investigate, prosecute and convict criminals and terrorists" while framing this action as a milestone to achieve greater security for European citizens. The measures that are proposed by the Commission, through a communication of April 17, 2018, to be developed through a Regulation and a Directive three initiatives: the European Electronic Evidence Warrant, the European Electronic Evidence Assurance Order and a proposal for a Regulation by which all service providers would be obliged to appoint a legal representative in the EU.

All these initiatives did not name any type of technology, but it is clear that blockchain could fit into many of the issues raised. Of all the proposals, blockchain technology could be accommodated in the second of these, as its own assurance mechanism and technology aimed at preserving and crystallizing proof of data that would have its transcendence at the level of international procedural cooperation. Although years ago this matter was a clear priority for the EU, no one could have imagined that in the years 2020 to 2022 Covid would burst into our lives and thus

also disrupt European regulatory plans for at least three years. However, the Covid-19 disease has served as the ultimate reason to force us to update the incorporation of ICTs into the process and put us in a position to take advantage of the benefits of these electronic media, as well as to be on guard against possible risks, among which the flow of electronic data and its possible implications in criminal disputes has become a clear protagonist.

The EU is gradually deflating its expectations on these texts while the problem persists and worsens. Undoubtedly, the legislative technique is not advancing at the pace originally envisaged. As of today, the proposal made by the European Commission in April 2018 consisting of proposing European orders for the collection and preservation of electronic evidence, and on the other hand, a proposal for a Regulation by which all service providers would be obliged to appoint a legal representative in the EU, in connection with the last General Data Protection Regulation, are still latent. With these regulations, analyzed in the article preceding this one, we saw how the EU intended to articulate instruments so that a judicial authority of a Member State could request data of an electronic nature directly from a service provider and deliver it to the legal representative of another Member State within 10 days, or in the case of cyberterrorism within six hours; It also provided that the requested State should retain the data for two years with a view to presenting this evidence in future investigations through a European Investigation Order (EIO), so we could be talking about a kind of "pre-orders", or a series of instruments that would complement the EIO.

However, later we saw how the Council bet on a "Regulation on cross-border access to electronic evidence", which includes European orders for delivery and preservation in order to reach an agreement with the European Parliament and that it ratifies the position that is raised, in order to make it a clearly differentiated instrument of the EIO. Subsequently, during 2019 the processing begins to be paralyzed because the EU did not reach an agreement on data transfer with the US and mutual collaboration was maintained without an agreement ratified by both parties and finally, after a turbulent year of negotiations, the pandemic breaks out in 2020 paralyzing these legislative plans and altering the priorities on this matter that were held at international level and where blockchain technology could have counted on legislative support at international level (Mirashi, 2017).

Specifically, the issue is paralyzed until April 2022, when the EU Council issues a communiqué authorizing all Member States to sign the Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention), aimed at improving cross-border access to electronic evidence for use in criminal proceedings. We must start from the global scope of the protocol, since being linked to the Budapest Convention, it would be applicable to 66 countries and 26 Member States, so we would practically be dealing with a standard that would affect data traffic around the globe and that would blur the principle of jurisdictional exclusivity inherent to each country. Ultimately, this will serve to achieve direct cooperation between States and communication providers so that they can share data through international procedural tools.

However, finally the two European Directives on the collection and preservation of evidence in criminal matters have been approved in June 2023, so they can be implemented next year, and

further development will be needed to implement proposals on the preservation of data and the techniques proposed for it, a crucial issue where blockchain technology could fit in.

To find a reference to the storage of electronic evidence, we must go to the last points of the Protocol, which deals with data classified as "sensitive", i.e., personal data revealing racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, genetic data or biometric data. It is at this point where an allusion to the conservation periods is indicated, leaving it open to an individual and not unified interpretation, something that seems to us to be ill-advised, since it is not really asking for anything specific or unifying criteria or techniques on a subject that is crucial to us. Thus, the Protocol textually states, with respect to retention periods, that: "each party shall retain personal data only for such time as is necessary and appropriate for the purposes of the processing of the data. In order to comply with this obligation, it shall provide in its domestic legal system for specific retention periods or for a periodic review of the need for continued retention of the data". Despite this, nothing is stated about decentralized blockchain technology.

At the European level, only Italy directly regulates Blockchain technology by means of an amendment to Article 8 of the Law of Conversion of the Simplification Decree-Law (D. I. n. 135/2018) introducing the definitions of DLT (distributed log technology) and "Smart Contracts" accompanied by the evidentiary value of a document stamped in Blockchain (art. 41), i.e., establishing an evidentiary treatment of this technology for the first time.

For our part, in Spain, and more specifically in Barcelona, through a research group led by Magistrate Yolanda Ríos, blockchain technology is being used in the commercial courts through a pilot experience aimed at crystallizing information relating to trade secrets by means of a Protocol for the Protection of Business Secrecy of the Commercial Courts of Barcelona since November 2019. So far, these are isolated initiatives that hopefully will soon transcend to a national and international level.

Specifically at the EU level we can see how in December 2021 the Presidency of the European Council and the European Parliament signed an interim agreement with the aim of digitizing cross-border digital communication. This project, called e-CODEX is composed of various software that connects the various systems of each of the European nations. Thanks to blockchain technology, the disruptive technology of 2022, communications are decentralized, interoperable and secure among them, so it would be applicable to private companies and public administrations alike, in order to serve to perform secure data exchange and that they are recognized in computer programs, regardless of the country in which they are located. It is also committed to working towards greater semantic interoperability, through the harmonization of the terms used in metadata and standards; we are therefore talking about a dual approach connected through legal interoperability and technical interoperability.

As a final noteworthy novelty, the Plan contemplates the possibility of developing software that allows the automatic transcription and translation of the interventions in oral proceedings of different judicial processes, even incorporating co-official languages and dialects and their technical peculiarities in reference to legal technicalities.

In conclusion, the EU continues to seek full interoperability with new measures and in a technological and social moment much more conducive to advance and end up fulfilling this highly complicated goal thanks to blockchain technology as the main ally. In this sense, and focusing properly on criminal procedural matters, perhaps it would be the time for this model to be replicated in a future and desirable third additional protocol to the Budapest Convention, which focuses on models of preservation of electronic evidence derived from criminal investigations and trials in cybercrime, where the blockchain technique is directly consolidated as a priority technical.

3. Procedural treatment of the blockchain

In the following, we analyze the procedural fit that blockchain could have, starting from the Spanish legislation but applying concepts linked to the general theory of evidence but that could find a place in the different European legislations in a global way.

We think that the treatment can be twofold, on the one hand as a means of proof and on the other as a mechanism of authentication or evidentiary assurance.

Attention should be paid to what evidentiary value the data or information recorded in the blockchain should have in the process, as well as the cryptographic system itself that produced the blockchain. Blockchain makes it possible to verify information at three related ends, namely the facts, actions or conditions that make up the record, the identity of the grantor and the time stamp or timestamp of each transaction in its true and immutable form. In short, two visions of blockchain as evidence must be separated, as they will be treated differently (Ríos, 2022):

– The electronic data that is included within the blockchain as a data storage system. Here we are talking about the procedural treatment of electronic evidence as an electronic medium in which to store data.
– The proper mechanism for preserving and securing electronic evidence. Here we speak of a technique of time-stamping the evidence to ensure its chain of custody. It is thus indicated that notes such as the integrity and immutability of the sealed data in each block is inherent to this technology, which allows, from the use of public and private cryptographic keys, to record in real time certain information in an authentic, integral and unmodifiable way.

The right to evidence, whether electronic or not, is guaranteed as a fundamental right in the Spanish Constitution (specifically in article 24.2) and consists, as the Constitutional Court has reiterated, in the right to have evidence admitted and practiced. This same vision can be extrapolated to the different Latin American Constitutions. But it is not an unlimited right; its exercise must be accommodated to the requirements imposed by the procedural rules themselves. This fundamental right corresponds to both procedural parties, the plaintiff and the defendant or accused.

The wording of art. 24.2 itself highlights its relationship with the right of defense. In order to understand that the right to evidence has been violated, it is required that the injured party has been left defenseless by the inadmissibility of evidence (for this reason it is necessary to motivate or reason the decisions that inadmit a means of evidence) or the non-execution of a means of

evidence that has been admitted. In short, if we relate this issue to the proposition of electronic evidence linked to blockchain, we will never be able to make it impossible to provide this type of evidence, although it will be a different matter if, within the evidentiary procedure, the admission or not is subsequently decided by the judge through the so-called admissibility trial.

In order to analyze the evidentiary value that the blockchain could have in a possible proceeding, it is necessary to determine to what extent the logbook that constitutes the blockchain can be a source of evidence, and by what means the recorded data can be introduced in the process as a means of evidence. At the procedural level, the distinction between source and means of evidence is clear. We speak of source of evidence as an extraprocedural and extrajudicial concept, unlimited and existing in reality; while the means of evidence would be the channel through which these sources of evidence access the process.

In the case of a data contained in blockchain, the source is the blockchain itself, so it is necessary to attend to its container and its content. Regarding the means of evidence, it is necessary to take into account the provisions of Article 299 LECiv that admits public and private documents, opinions and means of reproduction of the word, sound or image when the same can be introduced by means of an electronic or computer support.

We think that we are faced with a new source of electronic evidence that can be incorporated into the process through different means of evidence, depending on the litigation strategy to be followed. In this sense, for example, if we refer to an e-mail as a source of evidence, we could incorporate it into the process through different means. For example, we could use a documentary but also an expert opinion if what we want is to prove its authenticity, we could also choose to apply a judicial recognition to the device from which it was sent or from which it was received or bet on a testimonial or a party statement to corroborate its content. As can be seen, the options are multiple and therefore we would have a single source of electronic evidence that could be incorporated into the process through different means depending on the procedural strategy to be developed. However, the legislator has not clarified whether we are dealing with a new means of evidence or only with electronic sources of evidence. It would be very convenient that this option is thought and publicized at a regulatory level to offer a plus of legal certainty to all citizens.

So, in what ways or through what means of proof could blockchain technology have a place?

In the first place, we could speak of the blockchain as an electronic support, which would be framed in the means of reproduction of words, sound or images, as well as in arts. 382 and 384 LECiv. That is to say, we would speak of blockchain as a book-record, or support suitable to contain information, is its electronic nature, since all the computers or nodes that make up the blockchain network are interconnected with each other from the download of the same program. Therefore, it is electronic elements that make up the virtual database.

Secondly, as public or private documentary evidence. As private documentary evidence. Article 326.1 LEC provides that private documents will be full proof in the process as long as their authenticity is not challenged by the injured party. Therefore, the rule is that, in case the authenticity is not contested, the blockchain record printed on a private document displays full probative force.

As a public documentary, the information recorded in the blockchain, such as the data or transaction recorded, or the time stamp, cannot legally constitute full proof from the contribution by documentary means in a process, since the document by definition lacks the character of public, that is, we cannot yet equate the certification provided by the registry with the value derived from the public faith provided by the intervention of a notary, but it would be a way to grant judicial public faith to the document generated with this technology (Perea González, 2020).

Thirdly, through an expert opinion. We would speak here of providing an expert opinion from a computer expert analyzing the blockchain to attest to the authenticity of the document provided by analyzing the time stamps, the hash and the other cryptographic aspects involved. However, the convenience of providing such an opinion does not exclude the possibility of assessing the means of documentary evidence on its own, at the whim of Article 326.2 of the LECiv without the need to accompany it with expert examinations whose claim is none other than to illustrate to the judge about aspects that, by themselves, already result from the information reflected in the blockchain. All roads lead to Rome, just as all considerations about the final authentication of an electronic evidence lead to being advised by an electronic expert. The rulings of the Spanish Supreme Court make it clear that we are dealing with an extremely volatile evidence that must be treated with the greatest possible caution and, in case of any doubt about its authenticity, it will eventually have to resort to an electronic expert so that he himself dictates the veracity in the authorship of the same, as well as its possible or not manipulation.

This is based on the fact that the vast majority of legal operators do not have sufficient computer skills to assess whether an electronic evidence has been previously manipulated or whether it is authentic. As a result, both individuals and legal personnel will end up resorting to this figure as a last resort. We wonder whether it might be a good time to reformulate the catalog of auxiliary personnel that make up the jurisdictional bodies of our country. That is to say, we would not be talking about judicial computer experts, but that in each court there would be a de facto expert who would be in charge of the work of accrediting the authenticity of the evidentiary materials of computer nature that are provided by any of the parties in a given process. This challenge would be a revolution in the composition of the jurisdictional organs, since the idea is that, just as there is, for example, an LAJ, there would also be an expert of this nature, something that would be in keeping with a Judicial Administration that promotes itself as computerized.

Undoubtedly, this challenge would entail a high economic budget that would have to be faced by the Executive that would take on this task. On the other hand, this would avoid a possible conception of privatized justice, since what we are transferring to the citizen is that he would always need to pay a computer expert to authenticate electronic evidence with all the guarantees within the framework of a judicial process. We believe that it is necessary for the public administration to offer a solution to this endemic problem that has been with us from the very beginning.

Apart from the means of evidence, blockchain technology could be used as a mechanism for preserving and securing electronic evidence. At the national level, we have the answer in our two laws of prosecution, both in the LECiv, as a norm where the general evidentiary procedure

in matters of evidence is regulated, and in the LECrim, because thanks to the reform operated through the LO 13/2015, a mechanism is established to protect and preserve electronic evidence with the help of communication service providers. Firstly, art. 283 bis speaks of the procedure for access to sources of evidence and specifically in its second point indicates that "The request for measures of access to sources of evidence may also include the request for measures to secure evidence, if they proceed according to articles 297 and 298 of this law. In such a case, the procedure provided for in this article shall be followed".

In this way, articles 297 and 298 LECiv offer a regulation about the preservation of the sources of evidence that are presented and provided in previous periods or in exceptional situations by the judicial authority, in order to ensure its practice in the procedural moment that originally corresponds, basing its application on the protection of the right to evidence, in order that it has effects in a certain process; but constituting in our opinion an extra mechanism of protection for evidence that present certain risk, as is the case of electronic evidence (Muñoz Sabaté, 2001).

Thus, art. 297 of our LECiv indicates that the jurisdictional organ can be asked for useful security measures to avoid that, due to human conducts or natural events, which can destroy or alter material objects or states of things, it is impossible to practice a relevant evidence at the time, consisting in actions that allow the preservation of the material provided or to make a reliable record of its reality and characteristics of the proposed evidence.

Similarly, art. 298 LECiv indicates that the court may take appropriate measures to secure evidence whenever there are reasons for it, including the court must take into consideration and may accept the possible offer made by the applicant of the measure to provide security for damages that the measure may cause. This means that here we would be talking about judicial securing of evidence, or in other words, the use of blockchain by the appropriate judicial authorities. A different matter would be the use of blockchain by individuals, a situation that can also be dealt with, but which is not the subject of this study.

Secondly, the blockchain could also fit in our art. 588 octies LECrim, indicating that the police authorities "may require any natural or legal person the conservation and protection of data or specific information included in a computer storage system that is at their disposal until the corresponding judicial authorization is obtained for its transfer in accordance with the provisions of the preceding articles".

Preservation measures are undoubtedly an ideal mechanism to guarantee the chain of custody in the face of such volatile evidence as electronic evidence, so encouraging and clarifying its use is a new challenge to be faced by the Spanish legislator; we particularly believe that blockchain technology will be a great ally to achieve that goal.

4. Final reflections: looking at the Web3

At the level of international procedural cooperation, we believe that it is time to face a third addendum to the Budapest Convention so that not only the technique for obtaining cross-border electronic evidence is agreed upon, but also to incorporate blockchain technology for securing

and sealing it and thus preserving the chain of custody. We are faced with a tool that is decentralized, open source and interoperable, which means that it can be promoted by all States in order to obtain legal recognition globally through a formula of minimums such as the aforementioned proposal.

All this, together with the data management model based on self-sovereign identity, where the users of electronic services themselves hold the data through an "electronic wallet" or e-wallet, where they store their own certificates, would turn the criminal procedural cooperation system and the fight against cybercrime upside down. In other words, users would store their own personal data, could transit different electronic services through interoperable digital platforms and, if necessary, validate the information of each citizen, but without storing or possessing it.

All this is envisioned with the development of technologies such as blockchain and artificial intelligence, which will play an absolute role in the so-called Web3. In this sense, it would be logical to move towards a Network based on blockchain technology that provides multiple access with the same credentials to different people, since, as García Mexía (2022) points out, this technology "whose decentralized DNA fits perfectly with a metaverse called to facilitate "horizontal" or direct relationships between its users, beyond intermediaries", should be clearly taken into account (García Mexía, 2022).

That is to say, one's avatar could go from one platform to another and the agreements, transactions or relationships made in one would be valid in the others. As Bonmatí Pérez (2022) points out, web3 is initially conceived as an Internet in which "the community acquires even more strength because it is committed to an absolute dissociation from proprietary platforms, such as those of web 2.0 mentioned above" (Bonmantí Pérez, 2022).

All this will make the user himself acquire much more power over the management and ownership of his own data regardless of the platform on which he interacts; so they themselves will have tools to govern their data and their digital assets, which opens up a new world of e-government and e-participation through this new version of the Internet. In short, there will be an important qualitative leap from Web2 to Web3 in which the citizen will once again have a dominant position over his own information and, therefore, over the control of his own rights and of the electronic evidence derived from the latter.

References

Barrio Andrés, M., "Metaverso: origen, concepto y aplicaciones", *Derecho Digital e Innovación*, Nº 12, Sección Doctrina, Segundo trimestre de 2022, Wolters Kluwer LA LEY 6042/2022.

Alamillo Domingo, Ignacio, «La identidad descentralizada como garantía de la privacidad en la vida digital», *La Ley Privacidad*, 5, Sección El Foro de la Privacidad: Ejemplar dedicado a: COVID-19 ¿Hacia un rediseño de la privacidad? (2020).

Allende López, Marcos, *Identidad digital autosoberana: el futuro de la identidad digital: auto-soberanía, billeteras digitales y blockchain* [em linha], org. Marcelo da Silva; Alejandro Pardo Vegezzi, [S.l.]: Inter-American Development Bank (BID), 2020, 112 p, [consult. 12 Jun. 2024]. Disponível em: <https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/IDENTIDADDIGITAL.pdf>.

Barrio Andrés, Moisés, «Metaverso: origen, concepto y aplicaciones», *Derecho Digital e Innovación. Digital Law and Innovation Review*, 12, Sección Doctrina: abril-junho (2022).

Bonmatí Pérez, Marga, «¿Metaverso? Cuidado con lo que se desea, que puede cumplirse», *Consultor de los Ayuntamientos y de los Juzgados: Revista Técnica Especializada en Administración Local y Justicia Municipal*, Extra 1: abril, Ejemplar dedicado a: La Gobernanza Inteligente (2022).

Bueno de Mata, Federico, «Del metaverso a la metajurisdicción: desafíos legales y métodos para la resolución de conflictos generados en realidades virtuales inmersivas», *Revista de Privacidad y Derecho Digital*, 7/27 (julio-septiembre) (2022) 19-59.

García Mexía, Pablo, «Metaverso: ¿ruido o nueces? ¿Y en materia legal?» [em linha], 15 Mar. 2022, [consult. 11 Maio 2022]. Disponível em: <https://www.expansion.com/juridico/opinion/2022/03/15/6230c55fe5fdea8b7c8b465f.html>.

Mirashi, Eltjon, «Protección de datos: escudo de privacidad y el decreto ejecutivo de Trump», in Federico Bueno de Mata, ed., *FODERTICS 6.0: los nuevos retos del derecho ante la era digital*, Salamanca: Comares, 2017, 53-62.

Perea González, Álvaro, «Blockchain y proceso civil: más allá de la jurisdicción y la fe pública judicial», *Actualidad Civil* 6 (2020).

Pérez Bes, Francisco, «Identidad y blockchain», in Beatriz Aranda Briones; Francisco Alcaide Soler; Pablo Luis García Mexía, ed., *Criptoderecho: la regulación de Blockchain*, [S.l.]: Wolters Kluwer España, 2018, 143-168.

Ríos López, Yolanda, «Blockchain, Smart contracts y administración de justicia», *Blockchain Intelligence*, 2021.