Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


Cross-border Interoperability and Digital Identity Management in the EU Digital Single Market

Lusambo J. Lwanzo[a]*
University of Chieti-Pescara, Italy

Abstract

This paper pursues the main objective of analyzing the implications of cross-border interoperability as laid down by the article 12 of the eIDAS regulation, on the requirement for secure and trusted pan-European digital identity management system. Both doctrinal and economic legal reasoning methods are mobilized in a complementary approach. Findings suggest that at some cost of cyberspace sovereignty of each Member States, cross-border interoperability need to be in compliance with mutual recognition, personal data protection, net neutrality and functional equivalence principles to faster a more trustworthy, secure and lawful pan-European ID ecosystem. However to incite and emulate other stakeholders aside of Member States, to adopt behaviors that enhance interoperability and make more social welfare effects of digital single market, the EU has to find an optimal trade-off between available interoperable standards and requirement of privacy of personal data ownership and intellectual property of electronic ID software.

Keywords: Cross-Border Interoperability, Digital Identity, Mutual Recognition Principle, Principle of Functional Equivalence, Legal interoperability, Economic analysis of Digital ID interoperability

1. Introduction

The interoperability of digital contents in general, and electronic identity systems in particular, are the crucial requirement for the success of the EU Digital Single Market[1]. As

*Correspondin author: Lusambo J. Lwanzo, E-mail: lusambo.lwanzo@unch.it.

[1] See DIRECTIVE (EU) 2019/770 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, p. 18) and

it was mentioned earlier[2], one of force at play in the making of an interoperable digital ID system, is the role of law. Moreover, in the context of European Union, the interoperability is of paramount importance[3].

Four years after the starting of the XXI[st] Century, the ancestor of the Digital Single Market, the European Information Society, a project of European Commission ordered an interdisciplinary research on electronic identity issues. A research consortium named the 'Future of Identity in the Information Society' evidenced that identity is changing. Indeed, with the digitization of information process, issues regarding the complexity of data transfer, the security and reliability of electronic identification schemes, become more preponderant.

Recently at the International level, concerns about digital Identity had been emphasized by the 2019 World Economic Forum, as both frontier for economic growth and a corn-stone for a regulated, secured, well-functional and sustainable digital economy, digital ecosystem and information and/or knowledge society.

Since the international awareness to go digital and to enhance internet economy, issues about the cross-border legal recognition of IdM and trust services between interconnected economies, cultures and societies are growing. Following recommendations from the 58[th] session of the UNCITRAL's working group IV (Electronic Commerce), the 59[th] session of 8-12 April 2019 in New-York have drafted Provisions on the Cross-border Recognition of IdM and Trust Services[4].

This intention demonstrates an international willingness and strategy from the UNCITRAL to propose to Member State a Model Law in order to fill some legal vacuum regarding interoperability and mutual recognition of electronic identity and trust services, data portability and privacy in the faster and changing digital Economy and knowledge society.

Unlike, intentions from UNCITRAL Working Group IV on electronic commerce, the Parliament and the Council of European Union anticipated since 1999, the legal issues related to IdM and trust service. Indeed, with the repeal of the Directive 1999/93/EC, the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services (eIDAS) for electronic transactions in the internal market, entered into force on all the EU cyberspace by the 1[st] July 2016. The main reason for this change in legislation at both the

---

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive1999/93/EC (OJ L 257, 28.8.2014, p. 90-92).

[2] John Palfrey and Urs Gasser (2007) Digital Digital Identity Interoperability and eInnovation, 33-34. Retrieved on 20 may 2020 from https://cyber.harvard.edu/pubrelease/interop/pdfs/interop-digital-id.pdf.

[3] Norberto Nuno Gomes de Andrade, Legal Aspects in Norberto Nuno Gomes de Andrade et al. Electronic Identity, (Springer 2014) 7

[4] UNICITRAL, Draft Provisions on the Cross-border Recognition of IdM and Trust Services (2019).

Retrieved on 26 May 2019, available on https://undocs.org/en/A/CN.9/WG.IV/WP.157

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


level of competence and scope of power, and the innovation, is to facilitate the promotion and faster development of cross-border online trust services.

Besides, this target, it is expected to lead to more transparency, less or ideally no-fragmentation and security inside the EU Digital Single Market, and to enhance the EU competitiveness in the globalized world. In fact, to get most out of the digital technologies, and therefore to build an effective, efficient, sufficient and secured Digital Single Market (DSM)[5], the eIDAS regulation could be seen as one of crucial tools against obstacles such as the fragmentation of the digital market, the lack of interoperability [6] and the rise in cybercrime in the European Union[7].

The lack of interoperability is a corn-stone issue of digitization in the EU Single Market. The European Commission illustrated its extent in the following quotes: "The Digital Agenda can only take off if its different parts and applications are interoperable and based on standards and open platforms"[8] Although, one of the recommendations from the guidance on the New European Interoperability Framework stressed the same issue. According to the European Commission, a useful framework has to ensure that both existing and new legislations don't compromise interoperability efforts[9]. Unless, its advantages[10], to made interoperable systems and devices within the EU DSM remain a puzzling case. Indeed, the interoperability is not suitable for everybody all the time[11]. It

[5] See European Commission, A Digital Agenda for Europe (2010).

Retrieved on 3 July 2018, available on https://ccdcoe.org/sites/default/files/documents/EU-100519-DigitalAgenda.pdf.

[6] "… interoperability denotes a system, product or service to communicate and function with other (technically different) systems, products or services" see Wolfgang Kerber and Heike Schweitzer, Interoperability in the Digital Economy, (2017) 8 JIPITEC 39-40.

[7] OJ L257, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, 73-114 Recital 4.

[8] European Commission, Idem, 2010, p. 10.

[9] European Commission, New European Interoperability Framework, Luxembourg, Publication Office of the European Union, 2017.

[10]Such as the promotion of innovation, the widening of consumer choice or ease-of-use and the enhancement of competition (See Martina Barbero, Diana Cocoru, Hans Graux, Annette Hillebrand, Florian Linz, David Osimo, Anna Siede and Patrick Wauters, Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, European Union, 2018).

Retrieved on 28 June 2018 from https://publications.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en

[11] See Urs GRASSER and John Palfrey, Breaking Down Digital Barriers: How and When ICT Interoperability Drives Innovation (Bearkman Center Publication Series 2007) Retrieved on 28 June 2018 from http://nrs.harvard.edu/urn-3:HUL.InstRepos:2710237.

can open to several issues linked to Cyberspace Sovereignty[12], to the no one-size-fits-all way to achieve it in the Information and Communication Technology (ICT) context[13], to the existence of two levels (primary and secondary) of intertwined barriers characterized in tree obstacles[14] [15].

In the same line, the declaration of the Vice-President in charge of Digital Single Market reported by the European Commission on 28 September 2018 pointed the issues in cross-border interoperability as follow: *'Europe needs to speed up on eID. Using eIDs increases trust and cuts cost. Now only people and companies from the two countries can access and use online services everywhere in Europe. The sooner the remaining EU countries notify their eID schemes, the quicker it will help all Europeans. I would like to see SMEs, in particular, make more use of eID and electronic signatures, to protect and improve their activities across Europe'*[16].

These wishes demonstrate that the cross-border interoperability which was supposed to be compulsory by the end of September 2018, took time to be effective. Only, Germany and Italy had fulfilled with the notification of their identification schemes for mutual recognition in due time. Indeed, the article 12 of eIDAS regulation establishes that national electronic identification schemes shall be interoperable between the Member States. However, even if recitals 5, 12 and 54 recognize the necessity of cross-border interoperability and mutual recognition to make useful and secure identification, authentication and qualified electronic signature, it leaves an unclear provision on other kind of trust services and electronic documents. Is there any ambiguity in the regulation or does it remain coherent with its broad objective to enhance electronic transactions in EU Digital Single Market? Do legal provisions as stated in Article 12 (cooperation and interoperability) ensure less-risky management of information processes in the environment of pan-European Identity Systems in the EU Digital Single Market?

Unlike the Directive 1999/93/EC, the regulation has a self-executing power on all pan-European identity cyberspace. This change in legislation from minimal harmonization toward a unification of national legal systems in Europe, evidences and raises the question of legal interoperability.

---

[12] "Cyberspace sovereignty is a natural extension of state sovereignty in the cyberspace hosted by the ICT infrastructure located in the territory of a state; namely, a state has jurisdiction (right to interfere in data operation) over ICT activities (in respect of cyber roles and operations) present in cyberspace, ICT systems per se (in respect of facilities), and data carried by the ICT systems (virtual assets)." see Binxing Fang, Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace (Springer-Science Press 2018) 83.

[13] See Urs Grasser and John Palfrey, Idem, ii.

[14] Technical: interoperability and portability, legal (contractual: data ownership, access to and re-use data, etc. and non-contractual: extra-contract liability) others (skills, competition, pricing)] (See Martina Barbero, Diana Cocoru, Hans Graux, Annette Hillebrand, Florian Linz, David Osimo, Anna Siede and Patrick Wauters, Idem, 15).

[16] European Commission, Cross-border digital identification for EU countries: Major step for a trusted digital single Market, (Published online 28 September 2018)

Retrieved on 10 October 2018 from https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


Beyond the issues of trust and security of pan-European Identity and legal interoperability, the legal reform drained by the eIDAS aims also to incite behaviors of all stakeholders of the European Digital Single Market toward an efficient and worthy digital integration. Therefore, it is questionable to understand the probable schema of impact of the article 12 on social welfare.

This research aims to conduct a legal analysis of issues raised by cross-border interoperability in the environment of digital identity management in Europe. The relevance of this exercise is evident since, without an optimal level of cross-border interoperability of different identity systems involved in Europe, promises of both digital market single strategy in particular and the 2020 digital agenda for Europe will be impossible to fulfil.

The second section tries to clarify the main concepts related to this research. The third section presents the analysis of article 12 on interoperability in link with article 6 to 9 on electronic identification. The fourth section presents a tentative of comparative analysis of legal interoperability between three closer legal system of EU, Italy, France and Spain. The fifth section made a tentative of criteria on which an economic analysis could rely on. And the last section contains some conclusive remarks.

2. Terminology: meaning and clarifications

As elements of information process in the digital identity ecosystem, concepts such as electronic identification and electronic authentication, validity, long term preservation (or conservation) and cross-border interoperability don't cover the same technical signification. They are differently conceptualized according to a legal point of view, compared to its complementary and intertwined ones: economic, sociological or computer sciences meanings[17].

In the frame of the Regulation eIDAS, 'electronic identification means the process of using person identification data in an electronic form uniquely representing either a natural or legal person or a natural person representing a legal person'[18].

Sullivan[19], perceives the digital identity as context specific and linked to transaction identity. From this perspective, digital or electronic identification supposes a legal or

[17] On the economic, sociological and IT treatment and conceptualisation of the Digital Identity see Patrick Waelbroeck, Julie Denouël and Maryline Laurent, Digital Identity in Maryline Laurent and Samia Bouzefrane (Eds) Digital Identity Management (ISTE Press and Elsevier Ltd, London-Oxford, 2015) 1-45

[18] OJ L257, Idem, 83

commercial transaction where the key-element is digital identity. Sullivan and Stalla-Bourdillon consider the 'digital identity '… (as) an identity which is composed of information stored and transmitted in digital form'[20].

Unlike Sullivan, Finocchiaro[21] conceptualizes electronic identity as expressed in the eIDAS. First of all, she recalls the double perspective of identity from the legal point of view. Identity has a subjective and objective sense. The electronic identity as defined in the eIDAS belongs to the objective view. Data related to such identity is objectively gathered for identifying a person in his social relations and his transactions with public administration. Beyond that, this choice of conceptualization helps to preserve the public interest by allowing third-party to verify with certainty the identity of other subjects.

E. Netter[22] went a bit far and mentioned that the trend of digital, is blurring barriers between the two traditional functions[23] of identity in private law. In such a context digital identity doesn't refer only to *steady* or *stable identity* (identification elements owned by a subject at his birth) but more to a *built identity* (accumulated personal information of a subject through his digital activities).

Authentication is located in the continuity of electronic identification. It 'means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed'[24]. For Smedinghoff, Authentication of identity comes down to addresses the question 'What can you do?' Therefore, 'Authentication of identity (or selected identity attributes) is not just an end in itself, but rather a process often used to authorize some grant of rights or privileges, to facilitate a transaction or decision, or to satisfy an evidentiary obligation'[25].

Contrary to Smedinghoff, Mik based his arguments on the multidimensional[26] conception of authentication. Thus 'authentication involves the presentation of authentication information that confirms the association between a person and an identifier.

---

[19] Clare Sullivan, 'Digital identity –From emergent legal concept to new reality' (2018) 34 Computer Law & Security Review 723–731.

[20] Clare Sullivan and Sophie Stalla-Bourdillon, 'Digital identity and French personality rights Away forward in recognising and protecting an individual's rights in his/her digital identity' (2015) 31 Computer Law & Security Review 268.

[21] Giusella Finocchiaro, 'Una Prima Lettura Del Reg. ue n. 910/2014 (c.d. eidas): identificazione on line, firme elettroniche e servizi fiduciari (reg. UE n. 910/2014)' (2015) 3 *Le nuove leggi civ. comm.* 420-421.

[22] Emmanuel Netter, Numérique et grandes notions du droit privé, (CEPAS, Paris, 2019), 47.

[23] (1) Identify a moral or naturel person in the legal system for liabilities and claiming and (2) Deliver a social representation to a natural person vis-à-vis of others (see Emmanuel Netter, Op cit, p. 51)

[24] OJ L257, Idem, p. 84.

[25] Thomas Smedinghoff, 'Solving the legal challenges of trustworthy online identity' (2012) 28 Computer Law & Security Review 534.

[26] "Authentication" has multiple meanings: to "establish as genuine" or to "associate oneself" with a document, as in "to sign from Oxford English Dictionary; Stephen Mason, 'Validating Identity for the Electronic Environment', 20 CLSR 3 at 166 (2004) quoted by Eliza Mik, 'Mistaken identity, identity theft and problems of remote authentication' in e-commerce' (2012) 28 Computer Law & Security Review 397.

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


Authentication information consists of something a person knows (password, PIN), possesses (token, smartcard, passport) or is (biometric data)'[27].

However to make the EU Digital Single Market working, digital identity systems of different Member Stata should be interoperable. Nevertheless, interoperability is not also defined by the eIDAS Regulation. The position of European Commission on its meaning was however broadly defined in the DIRECTIVE 2009/24/EC '… as the ability to exchange information and mutually to use the information which has been exchanged'[28]. It is recently the DIRECTIVE (EU) 2019/770, which laid down its meaning**.** **"**Interoperability' means the ability of the digital content or digital service to function with hardware or software different from those with which digital content or digital services of the same type are normally used"[29].

By mentioning the means or instruments by which information have to be exchanged or used, Palfrey and Grasser, make it a bit clear. Interoperability is '… the ability to transfer and render useful data and other information *across systems, applications, or components*'[30].

Nevertheless, there is no one-size-fits-all definition of it'[31] and a broader definition of interoperability can hide some different facets of its multidimensional nature. Interoperability can be understood using four layers: technologies, data, human beings and institutions[32].

Unlike the precedent broader definition, the digital identity management[33]-focused perspective refers to Digital ID interoperability "…as a constantly shifting interconnection among ID users, ID providers, and ID consumers that permits the transmission of Digital ID information between them via a secure, privacy-protected channel"[34].

---

[27] Eliza Mik, Ibidem, 397

[28] EC,

[29] OJ L 136,Idem., p. 18

[30] John Palfrey and Urs Grasser(a), Idem, p.5

[31]John Palfrey and Urs Grasser (b), Interop: The Promise and Perils of Highly Interconnected Systems (Basic Books 2012) 5

[32] J. Palfrey and U. Grasser (b), Op.cit, p. 6

[33] Digital Identity management is a system which allows '…to maintain the integrity of identities through their life cycles in order to make the identities and their related data (e.g., authentication results) available to services in a secure and privacy-protected manner' Elisa Bertino and Kenji Takahashi, Identity Management (Artech House 2011) 23

[34] John Palfrey and Urs Grasser(a), Op. cit.,

retrieved on 18 january 2020 from https://cyber.harvard.edu/pubrelease/interop/pdfs/interop-digital-id.pdf

The previous definition clarifies that technologies and data layers are linked. In this frame, interoperability refers to its syntactic and semantic dimension[35]. It means the feature of systems to connect each other in an agreed-upon interface with the possibility to render data useful on different devices (cellular, computer, tablets,) and meaningful according to information exchange[36].

Besides this information technology view, interoperability requires otherwise human and institutional[37] interaction as well in order to be effective[38]. To be successful, human being are willing to put effort into working together. An example of a human layer is communication through a common language. The human layer can be considered as the most abstract element of interoperability but the more intelligible.

Unlike the human layer, the institutional aspect of interoperability is also considered as the highest and most abstract layer which allows the society system to engage effectively[39]. At this stage, the legal system plays the role of collaboration and exchange of data for example without making parties involved identical. For instance, if we consider, two companies located in two different countries, for example, Namirial SPA in Italy and Cryptolog International SAS in France, they are not obliged to be under a same jurisdiction to allow their respective clients to conclude a contract by signing electronically. One thing is only needed at this stage, to make the French and Italian jurisdictions, able to interoperate legally speaking for providing a non-attackable electronic signature.

The legal interoperability is, therefore, '…the process of making legal norms work together across jurisdictions'[40]. Unlike, the Palfrey and Users's definition, Santosuosso and Malerba explore an in-depth and ontological approach to legal interoperability which raises some issues. Their proposition emerges from the concept of cultural interoperability (ex. European Union)[41]. This shift is based on the conception of law as a sort of word-made world, on the multilingualism drained by the phenomena of globalization, and the Philip Jessup's idea of transnational law. Three situations can be distinguished from these perspectives:

1. 'Same legal system (or State)/ Same language
2. Same language/ Different legal systems
3. Different legal systems/ Different languages'[42]

[35] Wolfgang Kerber and Heike Schweitzer, Idem, 41

[36] Reconstructed upon John Palfrey and Urs Grasser, Ibidem, 6 and Wolfgang Kerber and Heike Schweitzer, Idem, 41

[37] Where legal system played a strategic position among others social systems

[38] John Palfrey and Urs Grasser (b), Idem, 5 and Wolfgang Kerber and Heike, Ibidem, 41

[39] John Palfrey and Urs Grasser (b), Ibidem, p.6

[40] John Palfrey and Urs Grasser, Idem, (b) Op. cit, p.178

[41] Amedeo Santosuosso and Alessandra Malerba, 'Legal Interoperability as a Comprehensive Concept in Transnational Law' 6 Law, Innovation and Technology 57

[42] Amedeo Santosuosso and Alessandra Malerba, Idem, p. 59

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


The third situation refers to the case of the European Union with legal provisions drafted in 23 different languages. With a challenge like this, the linguistic issue has first to be solved in order to minimize as possible as it can a misinterpretation. However, when a case law raises or a tort is consumed between two states members or two citizens of different Member States, both penal and civil procedures can be non-homogenized between jurisdictions. The legal interoperability will be solved by international public law for torts between Member states and international private law for torts between two different national legislations. The eIDAS works as a transnational law, tries to solve issues raised by electronic identification and trust services between Member states of the European Union. Nevertheless, the eIDAS regulates trust services such as electronic signatures, electronic seals, and certified websites which are supposed to be provided by private business. Therefore, a conflict between eIDAS and two particular national legal systems could raise.

The transnational law idea of Jessup, but more the legal features[43] of cross-border effects of digital information identified by Johnson and Post[44], open the path to the central concept of this research, cross-border interoperability.

Recently, Silveira and Covelo de Abreu argued in the same line to support the transnational aspect of law which made a change in the policy of European Union to faster digital agenda by softening gaps between national legislation and actions[45].

The eIDAS regulation establishes principles of the internal market, neutral technology and mutual recognition between Member States to overcome issues linked to barriers and fragmentations in the EU area of Digital Single Market (DSM). The market even digital is based on transactions. In this sense, cross-border interoperability is expected to play a corn-stone role without which at this stage of technology information development it could be impossible to build the EU DSM.

Cross-border interoperability is not just a matter of technical standardization but also of legal interoperability[46]. For the case, 'An electronic document is a dual technical and legal

[43] Johnson and Post mentioned that since the cyberspace is bounded by screens and password rather than physical markers and undermined therefore the feasibility and legitimacy of law based on geographic boundaries, it required a new perspective of law and its institutions.

[44] David Johnson and David Post, 'Law and Borders. The Rise of Law in Cyberspace' (1996) 48 Standford Law Review 1367-1402. .

[45] Joana Abreu and Alessandra Silveira 'Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Government paradigm' (2018) 9 European Journal of Law and Technology .

artefact that depends on a national legislation system and "lives" within a national platform of electronic documents'[47]. For example, in the paper environment system, to conclude a contract between two legal persons located in remote countries, documents were elaborated and then printed to be empowered by signature and then sent by post to other part involving in the contract to sign also. Otherwise, the two legal persons have to meet physically to sign. The other alternative is to scan the document pre-signed by the first party, and send it to the second party and so and so on. However, the legal value of such digitized document can be contested but also the digitization process in such way can be costly for a firm or a citizen to complete such a transaction and not efficient for the paperless environment of modern business. To solve this issue, trust service providers developed documents made digital first-in-a full electronic environment. Nonetheless, to be empowered and therefore to acquire a legal validity, electronic signature has to be putting on them by both two parts involving in two different jurisdictions. Indeed, electronic documents are not created for private use but exchange purposes between various entities participating in the contract.

In this sense, Cross-border interoperability can be envisaged as both technical and legal interoperability which permit an easy exchange and mutual recognition of electronic documents or data with diverse format processor between different national legal systems in the strict respect of the principle of functional equivalence and net neutral technology, regarding their legal power.

3. Cross-border Interoperability and electronic identification and authentication

In response to the recommendation made under the recital 6 of eIDAS, unlike its proposal form adopted by the European Commission which treats the issue of interoperability as a simple point of coordination (see Article 8)[48] between the Member States, the final version of eIDAS published at the official journal devotes a half part of the article 12[49] to interoperability.

As a crucial point for DSM strategy and innovative dispositions comparing to the e-signature directive, the provisions on interoperability at the article 12 paragraph 3 is embedded in the general principles adopted under the eIDAS regulation. Those principles are neutral technology (Article 12, 3, a, and one of key principle of UNCITRAL Model Law on electronic commerce), internal market (Article 12, 3, b and Article 4), mutual recognition (Article 12, 1) and protection and privacy data principle (Article 12, 3, c and d).

---

[46] Jeremy Besson, Adomas Birstunas , Antanas Mitasiunas and Arunas Stockus, 'SignaTM – Towards Electronic Document Cross-Border Interoperability' (2015) 17 Applied Computer System 46

[47] Jeremy Besson, Adomas Birstunas , Antanas Mitasiunas and Arunas Stockus, Ibidem,

[48] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market, 2012

[49] OJ L257, Idem, p. 90

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


Talking about the level of coherence with legal system and standards of Europe, Gomes de Andrade tried to find a 'legal anchor' to the idea of a pan-European electronic identity within the Lisbon Treaty[50]. After evocated some doubts on the Article 77 (3) of the TFEU to all-encompass the legal basis for an interoperable European electronic identity due to the peculiarities of data movement freedom within the European Internal market comparing to persons and goods, he argued that a new regulation to replace the e-signature directive is needed to propose a legal framework for cross-border recognition and interoperability of secure e-Authentication systems[51].

Beyond, the reason above highlight something interesting for our analysis. The principle of mutual recognition is a fundamental basis to ensure that the legal framework will provide interoperable and secured e-identification, e-authentication and cross-border recognition. Indeed, the Principle of mutual recognition supposed that Member states should cooperate and collaborate by exchanging information, experience, good practice, and technical requirement related to interoperability and assurance level (see article 12 paragraph 6 a, b, c, d). It can be deduced that if the principle of mutual recognition is applying each time a member state notifies its electronic identification schemes, as it the case for only 13 countries out of 27 Member State[52], by this act, it is obliged to collaborate with the other member states for their common operational security standards, and therefore to trust each other. The positive consequence could be to make electronic identification schemes secured and for a high level of trust and assurance within the pan-European electronic identification for both public services but also private trust service providers.

However, the mutual character of electronic identification process at the level of Europe by a member state results in the loss of a part of its cyberspace sovereignty for the profit of the European Community. Indeed, the notification of the electronic identification schemes have to be done without undue delay (Article 9, 1)[53] but the request to remove, is with a delay of one month at least (Article 9, 4)[54].

[50] Nuno Gomes de Andrade 'Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID', (2012) 28 Computer Law & Security Review 153

[51] Nuno Gomes de Andrade, Idem, pp.158

[52] See https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS (last update on Jan 02, 2019)

[53] OJ L257, Idem, p. 89

[54] OJ L257, Idem, p. 90

Thus, the principle of mutual recognition ensures in the context of the provision of article 12 that Member States should care about assurance level, security and enhancement of trust within the pan-European electronic identity system. Instead of that, Member states or a third party involving in the notification process are liable for any damage as set by article 11.

When we back to article 12 paragraph 1, the interoperability is about national electronic identification schemes. This provision is in coherence with the technological approach to interoperability as defined previously. Since it is a system, then it can interoperate with another system regardless of the mean and devices of electronic identification. The later can be material or immaterial and contains person identification data which is used for an online service[55].

The interoperability between electronic identification schemes is about personal data. Thus, the process of cross-border identification and authentication should care enough about the principle of data protection. The article 12 paragraph 3, points c and d on criteria to be met by the interoperability framework is coherent with this vision on privacy. By the way, the legislator at the point d of the evocated article refers to the Directive 95/46/EC. The later was understandable at the moment of adoption. However, the directive was repealed and replaced by the REGULATION (EU) 2016/679 on the protection of natural persons about the processing of personal data and the free movement of such data (General Data Protection Regulation-GDPR). The GDPR is effective since 25 April 2018. To avoid misinterpretation, the legislator may at the occasion of new amendment of the eIDAS to update this disposition[56].

At its recital 4 of the GDPR, the legislator indicates that the right to the protection of personal data is not an absolute right and has to balance with its social functions and other rights in coherence with the principle of proportionality. The following recital No 5 and even 6 evidence that the cross-border flows of data within the Union due to the social and economic integration resulting from the functioning of the Internal Market, obligates the Member States to cooperate. This cooperation aims to ensure that personal data will flow freely, and the Member States have to keep their protection at a high level.

The vision of privacy as expressed through the principle of personal data protection have more legal certainty and stability. It guarantees that when systems are interoperated, personal data used for identification process will be highly protected and used lawfully, transparently and fairly for evocated purposes. Therefore, it understandable that the non-legislative act[57] which accompanied the eIDAS, to implement the interoperability framework, sets the security of personal data as primordial.

---

[55] OJ L257, Idem, p. 83

[56] See Giusella Finocchiaro, Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali (Zanichelli 2017)

[57] See OJL235, II COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


As it is evidenced at its article 6[58] paragraph 1, in implementing the technical framework, the European Commission will stay up on the effective application of personal data protection principles which flow through nodes. In fact, 'Nodes play a central role in the interconnection of Member States' electronic identification schemes'[59]. There are not supposed to store personal data. Here again, the European Commission intends to take all precaution about some abuses related to the reuse of personal data and others. However, technically this will increase the cost of data portability if the digital users, trust services providers and public services have to manage that in an approach closer to just in time philosophy.

Otherwise, by adopting the conception of Custers and Ursic, from the legal viewpoint, De Hert, Papakonstantino, Malgieri, Beslay and Sanchez, considered the right to data portability as the notion linked to the ability of people to reuse data across devices and services[60]. Therefore, since 'the role of European Commission in incentivizing interoperability has been removed from the first proposal of the GDPR' and the object of data portability still unclear [61], the non-storage of personal data of the nodes could restrain transparency and right to interoperability for a party involving in cross-border identification process and authentication.

The exception expressed at the paragraph 2 of the same article 6 regarding the article 9 (3) of eIDAS implies that if a Member State notified after the expiry of the period, one year from the date of the implementing acts, the commission would store data within 2 months from the date of receipt of notification[62].

The compliance of the interoperability of electronic identification schemes with both principles of mutual recognition, and of protection of data and privacy, offers two guarantees for the pan-European electronic identity environment. Firstly, Member states could only collaborate if they trust each other and trust within the level of assurance and

[58] OJ L235, Idem, pp.3

[59] OJ L235, Idem, pp.1

[60] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri,Laurent Beslay and Ignacio Sanchez, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) Computer Law & Security Review 203

[61] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri,Laurent Beslay and Ignacio Sanchez, Ibidem, 203

[62] OJ L257, Idem, p. 89

security of the interoperability building blocks. The fact that they are mutually[63] and individually liable about the well and secured functioning of the Digital Single Market, assure trust in e-public and e-private transactions by European citizens and trust services providers. Secondly, the devotion to data protection by both governments, the European Commission and any third-party operator, provide legal certainty and security about the right on personal data and the transparency and fairness in their uses.

The provision pointed at the article 12 paragraph 3 (a), embodies the neutral technology principle and it is in coherence with the article 7 (f). The legislator intends to promote a liberal policy in the development of technical solutions to speed up interoperability between national electronic identification schemes. However, the legislator is aware of security issues linked to the 'liberal approach'. At paragraph 4 of the same article, the Interoperability framework, clearly indicated boundaries within which this neutrality as to involve. They are the assurance levels (see article 8) and common operational security standards, and arrangements for dispute resolution. Beyond, it seems that the legislator also wants to promote innovation through an increase of technical interoperability[64] and to avoid unilateral solutions to interoperability issues[65]. They result in market failure and conflict with principles of fair competition.

The other aspect of neutral technology is located in the finality of interoperable pan-European electronic identification. From the analysis made above, it occurs that all the process of electronic identification and cross-border authentication within the eIDAS regulation, aim to deliver online services (trust services and others) in a frame respectful of digital freedom values and accountability of users, providers and public actors at the micro level. At the macro level it provides a secured DSM, flexible to manage and to cope with the risk of cybercrimes.

Nevertheless, the eIDAS regulation doesn't define what it means by online services and to which class of services it refers. The principle of mutual recognition may explain this legal vacuum. According to the later, the competence of the regulation is limited to electronic identification and authentication process[66]. Infact, the recital 14 sends back conditions of access and final delivery of online services to the competence of national legislation [67].

Nonetheless, it is clear now that interoperability in the context of the article 12 (1-4) offers legal certainty and security for electronic identification process (identification and authentication) to be undertaken and managed in a secured, reliable, fairly and technology

[63] See Article 4 (3) of OJ L 53, COMMISSION IMPLEMENTING DECISION (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, pp. 16

[64] See John Palfrey and Urs Grasser, Idem, pp. 111-112

[65] See Wolfgang Kerber and Heike Schzeitzer, Idem, 39 and 42-44

[66] OJ L257, Idem, p. 75

[67] OJ L257, Idem, p. 75

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


flexible (open to technology) pan-European cyberspace. This assurance of cross-border interoperability is impossible to be achieved without cooperation between Member States (Article 12 (5-9)).

However, what about trust services? Are they the online service what the legislator refers?

From the conventional sense, an online service is an information, or a service provided through the internet. According, to Cardoso and Fromm, an electronic service is a 'service system (with elements, a structure, a behavior, and a purpose) for which the implementation of many of its elements and behaviors is done using automation and programming techniques'[68]. For these authors, online services are just electronic services which are performed through communication technologies by an online connection between the two sides (customer and supplier)[69].

A 'trust service means an electronic service normally provided for remuneration which consists of:

(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;'[70]

It can be deduced from this eIDAS's definition that if a trust service is an electronic service and covered by the eIDAS (see article 1 (b and c)) for all the European cyberspace, then it should use communication technology to perform and, therefore it is understanding as an online service. However, there are other class of online services (e-tax payment, internet banking, e-justice, etc.) which are concerned by interoperable pan-European electronic identification without belonging to trust service classification.

It resorts that trust services regulated by the eIDAS are candidates to cross-border interoperability using the notified identification scheme agreed mutually by the European Union for only identification and cross-authentication steps. Conditions of access and

[68] Jorge Cardoso and Hansjörg Fromm, Electronic Services, in Jorge Cardoso et al. (eds) *Fundamentals of Service Systems*, (Springer 2015) 42

[69] Jorge Cardoso and Hansjörg Fromm, Idem, 2015, p. 42

[70] OJ L257, Idem, p. 84

final delivery are from the competence of national legislation. It could raise some issue of legal interoperability. As the recital 54 aware about it[71].

4. Legal interoperability in Europe (Cases of France, Spain and Italy)

The problem of legal interoperability was already mentioned in 2012 in the proposal of eIDAS. The experience learned from the enforcement of Directive 1999/93/EC evidenced that "…national measures have de facto created barriers to the EU-wide interoperability of electronic signatures, and that they are currently having the same effect on electronic identification, electronic authentication and related trust services. It is therefore necessary for the EU to create an enabling framework to address cross-border interoperability and to improve the coordination of national supervision schemes'[72].

Compared to France and Spain, Italy is in advanced about interoperability issues related to electronic identification. Through the 'Sistema Pubblico di Identità Digitale' (SPID), it is possible to get access to online public service with only one digital identity regardless of the device (computer, tablet or smartphones). Furthermore, it was the first with Germany to notify their electronic identification schemes to the European Commission.

The modification of legislation in 2016 has changed the DLGS 7.3.2005, N. 82 to incorporate interoperability principle within the process (see article 41), the institution of the 'Sistema pubblico di connetività' (SPC) (article 73) the management of its costs (see article 76-Bis), and clarifying its meaning[73].

Paradoxically, French equivalent legislation in vigour don't respectively, even use or reserve any legal treatment to the word 'interoperabilité'. However, this is not alarming since the eIDAS regulation has a self-executing power in all pan-European cyberspace and jurisdiction.

The other issue raised by such a legal uncertainty within the two legislations is about the management of costs. The new article 76 bis of the CAD[74] fixes the accountability about the supporting expenses. Face to a legal vacuum in the French and Spanish legislation, one could asks how technologies, material and humans needed to support a notification scheme and to participate in collaboration and cooperation European team will be managed?

Those peculiarities revealed the consequences of the choice made by the legislator in the EU building process. In fact, according to Palfrey and Grasser, the EU form of legal interoperability is a hybrid approach or medium level, neither pure harmonization nor pure

[71] OJ L257, Idem, p. 80

[72] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market, Brussels, Unpublished pp. 4

[73] **DECRETO LEGISLATIVO 26 agosto 2016, n. 179 Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche Retrieved on 15 November 2018 from**

http://www.gazzettaufficiale.it/eli/id/2016/09/13/16G00192/sg

[74] Codice dell'amministrazione Digitale

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


fragmentation[75]. It is visible through the eIDAS regulation about legal competences delegated to the Member States.

The French legislation on the electronic signature is based on the long tradition of the probative value of proof in Contract Law [76]. Although, the law was codified under the following name: 'LOI n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique'. According to this law, the electronic signature is treated in rigorous attention to integrity and validity of proof in article 4 paragraph 3[77].

It is interesting to mention that the legislator in the French case intended to adopt the recommendation from the directive prudently. By reading only this law, one may see a confusion because the type of electronic signatures is not specified. Nonetheless, the 'Décret n°2001-272 du 30 mars 2001[78] precise clearly at its Article 1. The article 4 paragraph 3 talks about 'la signature électronique' supported by reliable identification process.

The article clarified that the reliability of the 'signature électronique' is presumed until proven otherwise if three conditions are fulfilled. The creation of the electronic signature, the identity of the signatory is ensured or authenticated and the integrity of the act (birth, death, transfer, commercial contract, etc.) is guaranteed. All of these under the conditions fixed by the 'Conseil d'Etat'.

In an earlier comparative law study on electronic signature between France, Germany and Poland, Bierekoven, Bazin and kozlowski, highlighted the paradoxical question of the French perspective on the e-signature Directive when it was in force. The paradoxical question is declined as follow: '… it is possible for one EU jurisdiction or a competent court to recognize the validity of a certified signature, and another one to refuse such

[75] John Palfrey and Urs Grasser, Idem, pp. 185

[76] See **Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations Retrieved from on 15 November 2018** (particularly Art. 1367) https://www.legifrance.gouv.fr/eli/ordonnance/2016/2/10/JUSC1522466R/jo/texte

[77] LOI no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique Retrieved from on 15 Novembre 2018

https://www.legifrance.gouv.fr/eli/loi/2000/3/13/JUSX9900020L/jo/texte/fr

[78] The type of electronic signature and others are fixed in **Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique Retrieved from on the 15 November 2018** https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=20170930

recognition'[79]. A simple answer to this question, according to those authors, is just for France to respect the principle of compatibility and interoperability as stipulated at the fifth recital of the repealed. Indeed, 'Bearing in mind what has been said above, it would have been contradictory for the European legislation on electronic signatures if the same certificate of signature was considered differently in different proceedings. However, a more detailed analysis provides for a more sophisticated answer'[80]. The later required two considerations: the scope of application of the e-signature directive and the two categories of electronic signatures stipulated by the directive.

Before to go far in this analysis on the probable French barrier case to legal interoperability, let us mentioned that in response to the entering into force of the eIDAS regulation in 2016, the 'Décret no 2017-1416 du 28 septembre 2017 relatif à la signature électronique' was signed and directly become applicable. The aims of this 'decret' is to precise and to apply the conditions fixed by the article 1367 of the 'Code civil' fundamentally about the qualified signature and to repeal the 'Décret n°2001-272 du 30 mars 2001'. The 'Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations' at his article 4 modifying the article 1366 of the code civil confirms the principle of functional equivalence of the 'ecrit électronic' as stipulated at the article 3 of la loi 2000-230 and the same modifying the article 1367 of the 'code civile'on electronic signature. At the article 1 of the 'Décret no 2017-1416 du 28 septembre 2017 relatif à la signature électronique' clarifies the type of electronic signature which have a probative legal value[81].

This provision clarifies the type of the electronic signature targeted by the ordonnance mentioned above (Article 4–1367 Code Civile) is the qualified electronic signature which have a substantial probative legal value according to the French 'Droit de la preuve'.

Back to the two dimensions to answer the paradoxical question of the French case. Firstly, it is now evident that by adapting its domestic law system to the eIDAS about qualified electronic signature and qualified electronic certificate, the principle of interoperability seems naturally, to be adopted. The ordonnance has also stipulated and recalled the principles of equivalence functional between the electronic document and paper-based document.

The Italian is quite different and advanced national system than the French case. Indeed, according to Merone, Italy was one of the first countries in the word in 1997[82] to introduce the fundamental principle of (Functional) equivalence between paper and electronic

[79] Christiane Bierekoven, Philip Bazin and Tomasz Kozlowski, 'Electronic signatures in German, French and Polish law perspective' (2004) 7 Digital Evidence and Electronic Signature Law Review 10

[80] Christiane Bierekoven, Philip Bazin and Tomasz Kozlowski, Idem, 2004, 10

[81] Décret no 2017-1416 du 28 septembre 2017 retrieved from https://www.legifrance.gouv.fr/eli/decret/2017/9/28/JUSC1716705D/jo/texte/fr 15 Novembre 2018

[82] Legge 25 marzo 1997, n.59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa
Retrieved on 20 November 2018 from

https://www.gazzettaufficiale.it/eli/id/1997/03/17/097G0099/sg

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


documents[83]. In the same line, Finocchiaro, argued that the eIDAS would not have a significant impact on the CAD because the later is as far as possible well developed.

As the French tradition, the 'Codice dell'amministrazione digitale' (CAD) at his article 20 (1bis) insists on the probative efficiency of the electronic document [84]. Moreover, at paragraph 2 of article 21, it adopts the principles of functional equivalence, the probative value of qualified, advanced electronic signature or digital signature.

Unlike, the LOI 2000-230 which is not explicit about the privacy of personal data, the modified CAD at the same article paragraph 5 forcefully persuade and insists on the strict respect of provisions on personal data.

Article 21 paragraph 1 recognizes the probative value of a digital document signed electronically to be freely assessable in front of a tribunal based on objective quality, security, integrity and immutability. Paragraph 2 completes the precedent provision by reinforcing the accountability of the signatory in the case of an electronic document signed by a qualified electronic signature. The article 28 on the certificate of the qualified electronic signature recall the issues of using the pseudonym (Article 28 paragraph 1 and article 33) and the position of the Italian legislator shows its willingness to interpret and to respect the article 5 paragraph 2 of the eIDAS regulation[85].

Since the French case doesn't precise under which conditions pseudonym will be managed practically, this less legal interoperable can lead to two opposite interpretations from the appreciation of courts and tribunals.

Meanwhile, in general, the French and Italian legal system are interoperable. In fact, their respective systems give the importance on high level of objective quality of signatory (the persons involved in the contracts are objectively identifiable), the probative legal value of qualified electronic signature. It is also agreed on the fundamental principle of functional equivalence between handwritten, the principle of interoperability and the respect of personal data protection principle. Even if, the French legal system doesn't explicitly

[83] Aniello Merone, 'Electronic signatures in Italian law', (2014) 11 Digital Evidence and Electronic Signature Law Review 85

[84] **See DECRETO LEGISLATIVO 26 agosto 2016, n. 179 Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche Retrieved from**

http://www.gazzettaufficiale.it/eli/id/2016/09/13/16G00192/sg on 15 November 2018

[85] OJ L257, Idem, pp. 86

mention the privacy binding, the fact that both eIDAS and GDPR are self-executing on all pan-European cyberspace, oblige the French system directly to apply the principle.

Rooted in the tradition of Civil law System, the 'Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica'[86] lightly modified by the 'Real Decreto 414/2015, de 29 de mayo'[87], provided a legal basis on electronic signature, its legal effectiveness and provision of certification services. Since the eIDAS enters into force, the Kingdom of Spain didn't yet update its regulation. The modification done in 2015 was just on certification. It is understandable why it does not allude explicitly to interoperability principle. Again, since the eIDAS regulation has entered in force the legal vacuum and uncertainty about this issue is fulfilled at the EU level. Only, the coherence of national jurisdiction to make more accessible a legal interoperability with the other Member States remains.

At its article 3 paragraph 4 and 9, the Spanish legislator recognized as in French and Italian case, respectively the fundamental principle of functional equivalence[88] and the principle of non-discrimination[89].

About, the probative legal value of the electronic signature and more the qualified electronic signature, the legislator clarifies it at article 1 paragraph 7 and paragraph 8. The later paragraph specifies that in case of contestation of the qualified electronic signature, IT support in which personal data was used to create and store the signature, can be presented as proof elements. However, the contestation is acknowledged, a penalty between 120 and 360 euro is fixed.

5. Toward an economic analysis of digital ID interoperability

The main principle even implicit of European legal systems is economic efficiency[90]. The repealing of the Directive 1999/93/EC for its lack of incentives toward a less fragmented, interoperable and secured digital single market, evidenced the instrumentalist expectation by the EU through the prelude of the eIDAS regulation.

At the recital 17[91] of the regulation, the legislator strongly recommends Member States to encourage privates a voluntary use of electronic identification and at the article 12 a mandatory notification of their own electronic identification schemes. Nonetheless, to

[86] Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2005-21163 on 15 November 2018

[87] See Reial decret 414/2015, de 29 de maig, pel qual es modifica el Reial decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica. https://boe.es/boe_catalan/dias/2015/05/30/pdfs/BOE-A-2015-5953-C.pdf on 15 Novembre 2018

[88] Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2005-21163 on 15 November 2018

[89] Retrieved from https://boe.es/buscar/act.php?id=BOE-A-2005-21163 on 15 November 2018

[90] Aurelien Portuese, Principe d'efficience économique dans la Jurisprudence Européenne, PhD's Thesis, Unpublished, Université Pathéon Assas, Paris, 2012, 9

[91] OJ L257, Idem, 75

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


predict if the incentive structure framed by the interoperability provisions will impact behaviors of different stakeholders[92] in an economically efficient way, requires presenting some benefit (V.1) and cost (V.2) of a digital ID interoperable system. And beyond that, to put in perspective a plausible social welfare gained by the EU DSM through interoperability in respect of Digital right Management, Intellectual Property law and competition law (V.3).

5.1. Benefits of digital ID interoperability

When an economy is networked, interoperability allows the firm to reduce the transaction or production cost of the internet services (trusted services, e-commerce transaction, digital contents, etc.) owing to the network effect, to make it more competitive, to provide it with an economy of scale.

For the consumer, interoperability in general and more digital ID interoperability provides advantages such as: ease-of-use, privacy, anonymity and low price[93]. It enables also a choice between different digital service with a less switch cost and a non-lock-in system to only one provider.

At the level of the industry and the society, it lowers price of digital services and contents by enhancing competition, promote a more innovative and creative society[94] and increase a privacy control end reduces social and financial risks faced by users online[95].

5.2. Cost and drawbacks of digital ID interoperability

All of these are not without cost and disadvantages. In fact, for the consumer, digital ID interoperability increases the risk of misusing of personal information, data breaching, identity theft, of losing anonymous communication on the web and the risk of more sophisticated phishing[96].

[92] Citizens, businesses, providers of digital services, trust services providers, public administration

[93] John Palvrey and Urs Grasser, Idem, p. 35

[94] Niva Elkin-Koren and Eli Salzberger, The Law and Economics of Intellectual Property in the Digital Age, (Routledge 2011) 205.

[95] John Palvrey and Urs Grasser (a), Idem, p. 36

[96] John Palvrey and Urs Grasser (a), Idem, p. 36-37

In the case of single sign system under digital ID interoperability, firms which depend on consumer lock-in to develop their business can lose their market share due to lower barrier at entries of the industry and the easier poaching of their customer by competitor. Besides, that in a jurisdiction or national legal system where reverse engineering is licit and legal, incentives to develop some platforms can be lower enough to benefit the value added of innovation[97] and break down any effort of fair trade in the competition law.

5.3. Social Welfare Effects of interoperability

The potential benefit, costs and drawback of digital ID interoperability combined to its mandatory nature to deal with both protected digital content (personal information), software (electronic identity system) and mutual liability of European cyberspace security, render its evaluation of social welfare more complicated. The regime of privacy of person data and digital right management over systems developed by trusted service providers have to not be neglected when the pan-European digital identity system goes interoperable. As a consequence, it could result in a development of a non-competitive market structure with some failures related to less incentives to interop to secure trade secret (source code), to avoid the raising of identity theft and other security risk.

Unlike other digital services or contents, electronic identity services are private and protected *sui generis*. The base under which the interoperability has to rely are protected by copyright law as creative things according to the Directive 2009/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2009 on the legal protection of computer programs. This make the choice between protecting or freeing interface of electronic identity systems more delicate. The potential legal impediments of interoperability caused by the Intellectual property regime could result in dominant market structure with monopolistic competitive firm or at least public monopoly which are not in compliance with the principle of internal market and European antitrust and competition law and therefore harmful for the social welfare.

The economic and legal puzzles of digital ID interoperability contrary to other information-based good, lies in the fact that, issue of privacy and intellectual property right really matter. The dilemma of the EU will be to choose between diverse standards[98]: isolated or silo model, centralized model, federated model and user-centric model under the constrain of personal data protection and ownership compliance, and intellectual property (copyright and trade secret) rights. This turn to a traditional problem within Chicago law and economics paradigm of maximization of social welfare resulting from

[97] Pamela Samuelson and Suzanne Scotchmer, 'The Law and Economics of Reverse Engineering' (2002) 3 Yale law Journal 1621-1622, and Niva Elkin-Koren and Eli Salzberger, Idem, 207-208

[98] John Palvrey and Uts Grasser, Idem, p. 12-22 for digital ID interoperability and Patrick Waelbroeck, Julie Denouël and Maryline Laurent, Idem , 33-37 for digital identity management in general

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


interoperability of one of standards under the risk of privacy and infringement of copyright and poaching of trade secret of trusted service providers.

6. Conclusions

The cross-border interoperability for an effective and reliable pan-European electronic identification remains a big legal, technical and operational obstacle between Member States. Since the enforcement of the eIDAS Regulation and the obligation of all public services to be interoperable in European Union, only 13 countries on 27, comply and had fulfilled with the requirement of cross-board interoperability.

Motivated by those facts and some unclear dispositions of eIDAS regarding interoperability, this paper investigated the impact of provisions at article 12 (Cooperation and interoperability) on articles 7 to 9 (Notification and security level of electronic identification schemes) of the eIDAS and economic efficiency of the overall digital identity ecosystem. The objective was to understand if conditions for cross-border interoperability as settled by the legislator comply with principles of functional equivalence, net neutral technology, protection of personal data and mutual recognition to provide secure, reliable, and efficient electronic identification schemes within the EU DSM.

Following the doctrinal view, finding from the textual analysis of article 12, raised the fact that cross-border interoperability will restrain the cyberspace sovereignty of Member States by transferring a share of it at the European Commission. This trade-off between Cyberspace sovereignty and pan-European electronic identification can be functional if the assurance level and mutual liability between the Member States are enhanced. The guarantees of assurance and liability are crucial for cross-border interoperability provisions to impact positively on both security and reliability within electronic identification schemes and protection of personal data flowing the nodes.

The analysis also led to understand that the obligation of interoperable pan-European electronic identification complies with the net neutral technologic principle. It was evidenced that the legislator intends to promote technical solutions to faster interoperability regardless the technology. Nonetheless, they should be conformed to assurance levels, common operational security standards, and arrangements for dispute resolution. Beyond, it seems that the legislator would like to promote innovation and

diversity of solutions to technical interoperability instead of single one. The later could harm the law of free competition.

The comparative analysis between Italy, France and Spain as cases for legal interoperability issues, showed that regarding the similarities between their domestic legislation and the self-executing power of eIDAS, it could not be any barriers. Nevertheless, for some legal vacuum about the probatory issues, the Spanish domestic legislation could result in some barriers with the Italian and French ones.

Regarding the economic efficiency, the puzzle to evaluate if the eIDAS will lead to more positive incentives and therefore adoption and emulated behaviors of stakeholder toward interoperability, if and even if the provision find in his effectiveness, an optimal trade-off between the digital identity standards and the binding of both personal data protection obligations and intellectual property right.

For the novelties of the eIDAS about interoperability, it remain a lot to clarify about which court will be in charge to solve a tort, a dispute, or other legal issues between two or more Member states regarding case of data or electronic documents, since there is an incidence on both European and domestic procedure and laws.

The leave of competence to the Member States about how to promote incentives schemes for interoperability in the private sector is in the straight-line with the willingness of the legislator to keep the share of Cyberspace Sovereignty devoted to the Member States. However, the public-private partnership to give to private business successful access to electronic identification schemes and nodes, have to be carefully thought to avoid a new barrier for cross-border interoperability and de facto for the achievement of the Digital Agenda.

Meanwhile, this work did not cover jurisprudential aspects borrowing by the issues for European case. It could be explained both by the novelties of the Regulation and the compulsory nature of e-public service interoperability which intervened just at the end of September 2018. Besides that, only two countries have completed their notification schemes: Italy and Germany. Nonetheless, an in-depth analysis of case law remains necessary for the understanding of the scope and the effectiveness of eIDAS to solve some practical issues and facts within the EU DSM.

References

Abreu, J., & Silveira , A. (2018). *Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Government paradigm.* Retrieved March 10, 2019, from https://ejlt.org/index.php/ejlt/article/view/590

Barbero, M., Cocoru , D., Graux , H., Hillebrand, A., Linz , F., Osimo , D., . . . Wauters, P. (2018). *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, European Union,.* Retrieved 28 June


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


2018, from https://publications.europa.eu/en/publication-detail/-/publication/74cca30c-4833-11e8-be1d-01aa75ed71a1/language-en

Bertino , E., & Takahashi, K. (2011). *Identity Management.* Boston-London: Artech House.

Besson, J., Birstunas , A., Mitasiun, A., & Stockus, A. (2015). SignaTM – Towards Electronic Document Cross-Border Interoperability'. *Applied Computer System, 17*, pp. 46-52.

Bierekoven, C., Bazin , P., & Kozlowski, T. (2004). Electronic signatures in German, French and Polish law perspective. *Digital Evidence and Electronic Signature Law Review, 7*, pp. 7-13.

Cardoso , J., & Fromm, H. (2015). Electronic Services. In J. Cardoso, H. Fromm, S. Nickel, G. Satzger, R. Studer, & C. Weinhardt, *Fundamentals of Service Systems* (pp. 33-74). London-New Tork: Springer .

COMMISSION IMPLEMENTING DECISION (EU). (2015). *2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014, OJL53/14.*

Commission Implementing Regulation (EU). (2015). *N° 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014, OJL235/1.*

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay , L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, pp. 193-203.

Décret. (2018, November 15). *N°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.* Retrieved from https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=20170930

DECRETO LEGISLATIVO . (2016, Agosto 26). *N° 179 Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione de.*

DECRETO LEGISLATIVO. (2016,, Agosto 26). *n. 179 Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015 n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.* Retrieved November 15 , 2018 , from http://www.gazzettaufficiale.it/eli/id/2016/09/13/16G00192/sg

DIRECTIVE (EC);. (n.d.). *2019/770 of 20 May 2019, on certain aspects concerning contracts for the supply of digital content and digital services, 2019, OJ L 136/1.*

Elkin-Koren , N., & Salzberger, E. (2011). *The Law and Economics of Intellectual Property in the Digital Age,*. London: Routledge.

European Commission (EC). (2018). *Cross-border digital identification for EU countries: Major step for a trusted digital single Market.* Retrieved 10 October 2018, from https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market

European Commission. (2012). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market,*. Retrieved September 6, 2018, from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52012PC0238

European Commission. (2017). *New European Interoperability Framework.* Luxembourg: Publication Office of the European Union .

European Commission. (2018, 28 September). *Cross-border digital identification for EU countries: Major step for a trusted digital single Market.* Retrieved 10 October 2018, from https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market

Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace.* Singapore: Springer-Science Press.


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


Finocchiaro, G. (2015). Una Prima Lettura Del Reg. ue n. 910/2014 (c.d. eidas): identificazione on line, firme elettroniche e servizi fiduciari (reg. UE n. 910/2014). *Le nuove leggi civ. comm., 3* , pp. 419-428.

Finocchiaro, G. (2017). *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali.* Bologna: Zanichelli.

Gomes de Andrade , N. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID', (2012). *Computer Law & Security Review, 28*, pp. 153-162.

Gomes de Andrade, N. N., Chen-Wilson , L., Argles , D., Wills , G., & Schiano di Zenise, M. (2014). *Electronic Identity.* New York: Springer.

Grasser, U., & Palfrey, J. (2007). *Breaking Down Digital Barriers: How and When ICT Interoperability Drives Innovation* . Retrieved 28 June 2018, from http://nrs.harvard.edu/urn-3:HUL.InstRepos:2710237.

Johnson, D., & Post, D. (1996). Law and Borders. The Rise of Law in Cyberspace. *Standford Law Review, 48*, pp. 1367-1402.

Kerber, W., & Schweitzer, H. (2017). Interoperability in the Digital Economy. *JIPITEC , 8* , pp. 39-58.

Legge. (1997, Marzo 25). *N° 59 Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa.* Retrieved November 20, 2018, from https://www.gazzettaufficiale.it/eli/id/1997/03/17/097G0099/sg

LOI. (2018, November 15). *No 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.* Retrieved from https://www.legifrance.gouv.fr/eli/loi/2000/3/13/JUSX9900020L/jo/texte/fr

Merone, A. (2014). Electronic signatures in Italian law. *Digital Evidence and Electronic Signature Law Review, 11*, pp. 85-99.

Mik, E. (2012). Mistaken identity, identity theft and problems of remote authentication' in e-commerce. *Computer Law & Security Review, 28* , pp. 396-402.

Netter , E. (2019). *Numérique et grandes notions du droit privé.* Paris: CEPAS.

Ordonnance. (2016). *N° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.* Retrieved November 15, 2018, from https://www.legifrance.gouv.fr/eli/ordonnance/2016/2/10/JUSC1522466R/jo/texte

Palfrey, J., & Grasser, U. (2007). *Digital Identity Interoperability and eInnovation,.* Retrieved 20 May 2020, from https://dash.harvard.edu/handle/1/2710474

Palfrey, J., & Grasser, U. (2012). *Interop: The Promise and Perils of Highly Interconnected Systems.* New York: Basic Books.

Portuese, A. (2012). *Principe d'efficience économique dans la Jurisprudence Européenne.* PhD's Thesis, Unpublished, Université Pathéon Assas, Paris.

Real Decreto. (2005, diciembre 23). *1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.* Retrieved November 15, 2018, from https://boe.es/buscar/act.php?id=BOE-A-2005-21163

REGULATION (EU). (2014). *No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive1999/93/EC, 2014, OJL 257/73.*

Samuelson , P., & Scotchmer, S. (2002). The Law and Economics of Reverse Engineering. *Yale law Journal, 3*, pp. 1575-1663.

Santosuosso , A., & Malerba, A. (2014). Legal Interoperability as a Comprehensive Concept in Transnational Law. *Law, Innovation and Technology, 6*, pp. 51-73.

Smedinghoff, T. (2012). Solving the legal challenges of trustworthy online identity. *Computer Law & Security Review, 28* , pp. 532-541.

Sullivan, C. (2018). Digital identity –From emergent legal concept to new reality. *Computer Law & Security Review, 34*, pp. 723–731.

Sullivan, C., & Stalla-Bourdillon, S. (2015). Digital identity and French personality rights Away forward in recognising and protecting an individual's rights in his/her digital identity. *Computer Law & Security Review 268, 31*, pp. 268-279.

Criminology and Criminal Law Review
Volume 6 (Issue 1)/2023 | pp. 54-82


DOI: 10.58179/CCLR6104
https://globalresearchpublishing.com/cclr/


UNICITRAL. (2019). *Draft Provisions on the Cross-border Recognition of IdM and Trust Services.* Retrieved 26 May 2019, from https://undocs.org/en/A/CN.9/WG.IV/WP.157

Waelbroeck , P., Denouël , J., & Laurent, M. (2015). Digital Identity. In M. Laurent, & S. Bouzefrane, *Digital Identity Management* (pp. 1-45). London-Oxford: ISTE Press and Elsevier Ltd.

Received 3 November 2022, accepted 11 January 2023.