UNIO - *EU Law Journal*. Vol. 4, No. 2, July 2018, pp 90-98.

School of Law – University of Minho

Electronic Identification, Signature and Trust Services

Francisco C.P. Andrade*

ABSTRACT: The generalization of the use of electronic communications in all spheres of human activities brings along a need for a new legal perspective. This need is particularly felt at European Union level with the assumed aim of building a trustable Digital Single Market. Regulation 910/2014 was set as the main European legal framework aimed at harmonizing the understanding of instruments such as electronic identification, electronic authentication, electronic services, and other trust services of information society, such as electronic seals, electronic time stamps, electronic registered delivery services and website authentication. In the whole, Regulation 910/2014 is intended to establish a common legal framework allowing European citizens to take full advantage of digital services in a technically and legally secure environment.

KEYWORDS: electronic identification – electronic signatures – electronic trust services.

* Professor at the School of Law of the University of Minho. Director of the Master in Law and Informatics of the University of Minho.

I. Introduction

The progressive generalization of electronic procedures, processing, communication and archival of messages brought along an urgent need for a new approach, both from a technical and legal perspective, of a whole new series of issues related to the identification of the intervenients in an electronic communication process. The issue of identifying the user[1] of an informatics system is essential in electronic communication processes, mainly if we consider the written communication from a terminal in an open network.[2] It must be known who is on the other side of the network, in a communicational process in which the parties (usually) will not be facing each other and will not have the vision of one another.[3] Of course, it is technically possible to proceed to a *"logical"* identification of the user in a network – through the respective IP addresses, electronic mail address or domain name.[4] But such an identification process is neither safe nor infallible. The mere logical identification may just establish a presumption of correspondence with certain equipment or with a certain group of users.[5] The problem is that the use of such addresses may, very easily, be abusively undertaken by someone else who is not the legitimate holder of that address. Moreover, this issue becomes more problematic because, in electronic transactions, the participants are not meeting face to face, and they communicate through binary language[6]. The identification of the author of the message and its authentication thus becomes an unavoidable requirement for the viability of electronic commerce and of electronic government.

Regulation 910/2014 of the European Parliament and of the Council of the 23 July 2014, relates to electronic identification and trust services for electronic transactions in the internal market and revoked the former Directive 1999/93/CE[7] . The Regulation seeks to *"enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities"* (point 2 to the Preamble of the Regulation), thus constituting an important pillar of the construction of the European Digital Single Market.[8]

---

[1] "The destinee has very few possibilities of having a certainty on the identity of the sender". See Miguel Pupo Correia, "Assinatura electrónica e certificação digital", *Direito da Sociedade da Informação*, vol. VI (2006): 277 (free translation).

[2] The issues concerning the security and confidentiality of the messages in electronic commerce environments, specially whenever operating in open networks, led to the appearance of special protocols assuring a stronger reliability of commercial transactions. Examples of these are the securitary protocols SET (Secure Electronic Transaction) and SSL (Secure Sockets Layer). See Erica Brandini Barbagalo, *Contratos Eletrônicos* (Rio de Janeiro: Saraiva, 2001), 46.

[3] "Electronic communication is direct and imediate, but becomes impersonal when it does not imply the transmission of the image or voice of the participants". See Miguel Pupo Correia, *Assinatura electrónica e certificação digital*… (free translation).

[4] Erica Brandini Barbagalo, *Contratos Eletrônicos*…

[5] *Ibidem*.

[6] See A.P. Filipov, "Confirmation of the authenticity of authorship (source) of the information transmitted through the Internet", *Legal Aspects of the use of the Internet technologies* (Moscow: Knijni Mir, 2002), 106.

[7] It must meanwhile be remembered that the former Directive was transposed to the Portuguese Legal Order by DL No 62/2003 of 3 April. This DL altered the previously existing DL No 290-D/99 on the use of digital signatures, making it compatible with the Directive. Meanwhile, DL No 290-D/99 still went through further alterations, the last one being that of DL No 88/2009 of 9 April.

[8] As it is stated in point 4 of the preamble of the Regulation, where it is referred that "The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the

II. Personal identification

The issue of the identification of a user of an informatics system is crucial in any electronic communication process, mainly in cases of written communication arising out of a terminal in open network.[9] The identities of the user to a counter party of the network must be known in a communicational process in which the parties will not be facing one another.

Article 3(1) of the Regulation 910/2014 presents a definition of what is to be understood as *"the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"*. But such a definition does not discount the fact that there is a diversity of different means of electronic identification and that different means may be used to build citizen's trust concerning electronic communications and transactions. It is possible to identify someone through something that only the person knows (and such is the case with passwords or Person Identification Numbers), or something that only the person has (such as ATM cards or Smart Cards) or through something that only the person is or that only the person is capable of doing or, at least, of doing in a unique way (such as the tone of the voice or the fingerprint, the image of the eye or the way someone writes on a keyboard or with a pen).[10]

However, it must be recognized that the concept (and means) of electronic identification is much broader than the concept of electronic signature. Among the different available technologies, only two of them have been considered as true means of signature: the digital signatures, operating through a complex system of emission of cryptographic keys and certification procedures, usually referred to as "Infrastructure of Public Keys" ensuring the identification through something that only the person knows or has (Access Code, Secret Key or Smart Card) and a new technology built upon the use of biometric technologies (capable of converting physical characteristics of living beings into digital data)[11] based on something that the person is or that only the person is capable of doing in a certain way. We are referring to the Dynamic Signatures that are based on the digital conversion of the biometric behavior of the written signature.

The fact that we may have different identification methods for different communications and different purposes led the European Legislator to clearly identify two main levels of identification mechanisms associated with the concepts of authentication and electronic signature. Article 3(5) gives us the meaning of authentication as being *"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"*. A

---

virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services."

[9] Erica Brandini Barbagalo, *Contratos Eletrônicos*…

[10] See "Arizona Electronic Signature Infrastructure – Signature Dynamics Electronic Signatures", available on http://www.sos.state.az.us/pa/SigDynamicsCP.pdf.

[11] Technologies for converting "physical phenomena into electronic digital data streams". See Sean O'Connor, "Collected, Tagged, & Archived: The Burgeoning Use of Biometrics in Personal Identification", *Bender's Immigration Bulletin* 1245 (1998): 3; and Francisco Carneiro Pacheco Andrade, *Consideração Jurídica das Assinaturas Dinâmicas no Ordenamento Jurídico Português,* Atas do XVI Congresso IberoAmericano de Derecho e Informática, Tomo II (Quito: Ministerio de Justicia, Derechos Humanos y Cultos, 2012), 57.

different concept is that of electronic signature, now defined as *"data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"* [Article 3(10)].

A good example of a method of authentication which is not considered electronic signature is the Portuguese mechanism for authentication, which is called *"Chaves Móveis Digitais"* (Digital Mobile Keys).[12] It is an alternative and voluntary method for the authentication of citizens in the portals and Internet sites of public administration. It consists mainly of an association of a civil identification number (or passport number for foreigners) to a cellphone number or email address. It is a secure authentication method and brings along a presumption of authorship: the acts associated with the citizen in the portals or sites of the public administration are presumed to have been practiced by him/her.

III. Electronic signature in the Regulation 910/2014

The concept of signature is not defined in the Portuguese general law. In general terms, signature is a way of identifying someone and of showing his/her agreement with a fact, an object, or contents. Signature thus, appears as a symbol that someone uses with the actual intention of authenticating a written document.[13] In classical legal doctrine, it is a distinctive sign by which the person becomes known to others. Hence, the admissibility of a non-written signature must take in consideration a functional analysis of signature.[14] That means that a signature must be a "*strictly personal and distinctive sign that can certify, without margin of doubt, the will of the person who signs*"[15] Vincent Gautrais[16] tells us that a signature contains two main functions: *i*) the identification of the signatory; and *ii*) the manifestation of his/her will.[17]

The European legislator kept the focus on a wide and technological neutral[18] concept of electronic signature[19], understood as a method used by the signatory to sign an electronic document in such a way that allows it to identify the author. In legal doctrine concerning electronic signatures, it is recognized that there is a need for a functional consideration of technological methods in order to comply with the two primordial functions of a signature: *i*) the identification of the person who signs; and *ii*) the manifestation of his/her will. Yet, it is also recognized that electronic signatures must also comply with other main functions: *i*) a function of authentication and verification of the origin of a message or document; *ii*) a function

[12] Law No 37/2014 of 26 June.

[13] "*A traditional signature must be (1) a symbol; (2) executed or adopted; (3) by a party; (4) with present intention; (5) to authenticate; (6) a writing*". See John P. Fischer, "Computers as agents: a proposed approach to revised U.C.C. Article 2", *Indiana Law Journal* 72(2) (1997): 567.

[14] See P. A. Vershinin, *Electronic Document: legal validity and proof value in Court* (Moscow: Gorodiets, 2000), 31.

[15] Alain Bensoussan, *Les Telecommunications et le droit* (Paris: Hermés, 1992): 183.

[16] Vincent Gautrais, "La formation des contrats électroniques", in http://www.droit.umonreal.ca/cours/Ecommerce/_textes/formation2000.rtf.

[17] Vincent Gautrais, *La formation*….

[18] Neutrality of technology is expressly stated in consideration 27 of the Regulation: "*This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met*".

[19] If the wide concept of electronic signature relates to any method used to identify the signatory, the concept of digital signature is a much more restrict one: it relates to the use of cryptographic techniques for the transmission of data and for the identification of the author of the message and for the verification of its integrity.

of integrity or the verification that the message or document was not altered after being signed; *iii*) a function of non-repudiation of the message or document; and, eventually, *iv*) a function of confidentiality. Among the possible technologies used for signing electronically, two have been mainly considered: the digital signature, based on something that only the signatory has (a secret key or smart card) or knows (a special code) and the dynamic signature, based on the something that only the signatory can do in a certain way.[20]

Digital signatures use cryptographic methods. The user has two different keys, a private key (only known by him) and a public key that third parties know or may know.[21] The public key may be directly communicated to the third party or through a trusted third party.[22] The message is encrypted with the private key of the issuer and decrypted with the public key, and third parties have no possibility at all of reversing the encryption functions. Besides that, the digital signature is created with use of a specific algorithm called *"hash"* that allows it to transform the message into a certain mathematical result, in a unique sequence of bits.[23] Once the message is received, the Destinee uses the public key to decrypt the message and to obtain the sequence of bits generated through the *"hash algorithm"*.[24] By submitting the message to the same hash algorithm, he/she may be sure that the message has kept its integrity since it was signed. It is, thus, possible to ensure not only that the message was originated from the sender (and not from a hacker), but also that the message was received exactly as it was sent, without any further modification. Digital signatures can, thus, fulfill all the requirements of a true signature, offering a security level that makes falsifications arduous.[25]

Dynamic signature is based on biometric technologies and uses the behavioural characteristics of the handwritten signature. It uses a digital system and peripherals such as a digital pen and sensitive screen.[26] This signature is thus unique and identifies the person who signs. From the moment when the signature is introduced in the system, it may no longer be altered or copied.[27] But the system does not only capture the digital image of the signature, it also captures the statistical measurements of the signature – meaning the unique behavioural characteristics of the signatory in the precise moment of signing.[28] As a result, this sophisticated system thereby becomes

[20] Dynamics signature is a method derived from the technique of behavioural biometrics. This biometric signature reproduces not only the geometry of someone's signature but also the dynamics characteristics of the process of handwritten signature, such as the speed, acceleration, sequence of scratch, thus making the whole set of data unique.

[21] Lorenc Hughet Rotger and Guillermo Alcover Garau, "Seguridad en la transmisión electrónica: validez jurídica", *Encuentros sobre Informática y Derecho 1994-1995*" (Pamplona: Aranzadi Editorial, 1995), 131-136.

[22] Lorenc Hughet Rotger and Guillermo Alcover Garau, *Seguridad en la transmisión*… . See also "Notariado y Contratación Electrónica" (Madrid: Colegios Notariales de España, 2000).

[23] Erica Brandini Barbagalo, *Contratos eletrônicos*…, 43-44.

[24] Christophe Sorge, "Softwareagenten – Vertragsschluss, Vertragsstraffe, Reugeld" (Karlsruhe: Universitätsverlag Karlsruhe, 2006), 15.

[25] Chris Reed, "Computer Law" (London: Blackstone Press Limited, 1990), 271; and Alain Bensoussan, *L'échange de donnés informatisé*…, 33.

[26] Marc Gaudreau, "On the distinction between biometrics and digital signatures", *CIC Enterprise Solutions*, 1999, disponível em http://www.penop.com/enterprise/whitepapers/whitepaper5.asp.

[27] Francisco Andrade, *Consideração Jurídica*…

[28] Benjamin Wright, "Signing tax returns with a digital pen", *ACM SIGSAC Review – special issues on electronic commerce* 14(4) (1996):17-20.

substantially safe.[29] To be successful in an attack, a hacker would have to get access not only to the source codes but also to the broad set of information on the mode of signing of the author of the signature, which would be a well-nigh impossible task.[30] Besides that, there is still another advantage related to dynamic signatures: it would always be possible for a court to have access to the System of Verification of Signature and, with the assistance of an expert, to produce evidence of whether or not the signature was (or not) produced by the purported author or if the document associated to the signature is (or not) the document used in the moment of signing or if it has (or not) been subject to any further modification. Thus, it can be said that a dynamic signature will have, at least, the same level of certainty as a handwritten signature.[31]

Although the two identified electronic signature's methods are quite reliable and may enhance safe legal relations, it is obvious that not every message or document requires an electronic signature. Therefore, electronic authentication methods and electronic signature methods must co-exist, while ensuring different levels of security and different functions.[32] With electronic signatures, different levels of security and trust must be considered, and that is why the Regulation establishes a distinction between advanced electronic signature[33] and qualified electronic signature.[34]

The advanced electronic signature must comply with the requirements of Article 26 of the Regulation, which are: it must be uniquely linked to the signatory; it must be capable of identifying the signatory; it must be created using electronic signature creation data that the signatory can, with a high level of confidence, use under his/her sole control; it must be linked to the data therewith in such a way that any subsequent change in the data is detectable.

The qualified electronic signature is an "*advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures"* [Article 3(12)].[35] Thus, two complementary set requirements are needed for the electronic signature to be considered as a qualified one: the requirements laid down in Annex II to the Regulation, for electronic signature creation devices (Article 29) and the requirements laid down in Annex I to the Regulation, for qualified certificates for electronic signatures.

The Regulation provides a technologically neutral approach to the use of different methods of electronic signature, understood in a broad sense, allowing the use of both digital signatures and dynamic signatures. Dynamic signature is the result of an electronic processing of data using the same behavioural characteristics of the handwritten signature, thus allowing one to unequivocally identify the signatory of

[29] Benjamin Wright, *Signing tax returns…*

[30] Benjamin Wright, *Signing tax returns…*

[31] Benjamin Wright, *Signing tax returns…*

[32] Although some authors question whether "*the notion of the signature is still relevant in the reliance of the current society on electronic information processes*". See Jos Dumortier and Niels Vandezande, "Critical observations on the proposed Regulation for electronic identification and trust services for electronic transactions in the internal Market", ICRI Research Paper 9 (2013).

[33] Article 3(11).

[34] Article 3(12).

[35] According to Article 3(14) of the Regulation, a certificate for electronic signature is an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. Furthermore, the qualified certificate for electronic signature must be issued by a qualified trust service provider, that is a service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body [Article 3(20)].

a document. The apposition of a dynamic signature to a document is a true act of signature, an act by which the author of a document identifies himself/herself and manifests agreement with the declarative content. The requirements of the *"advanced electronic signature"* (Article 26)[36] do not present special difficulties concerning the consideration of both digital and dynamic signatures.

Advanced electronic signatures and qualified electronic signatures represent two different levels in the provision of electronic signatures and electronic certification services. Given the importance of the supervisory body in the granting of the qualified status, it is important to say that, in Portugal, the supervisory body is the GNS – National Office of Security.[37]

One important clarification of the Regulation concerns the idea that signature is indeed a personal mark or sign used to identify the person who signs and to ascertain his/her agreement to what is signed. Signature must thus be a sign unique to a natural person. This is very clear in Article 3(9)(10), where it says that the electronic signature is *"used by the signatory to sign"*. This is an important clarification since Portuguese law[38], prior to the Regulation, established the possibility of a legal corporation being a holder of an electronic signature.[39] Now, upon the Regulation, it is quite clear that the holders of electronic signatures are only natural persons.[40]

But the main clarification of the Regulation concerns the legal effects and the proof value of electronic signatures. Article 25 of the Regulation is quite clear concerning those aspects. Firstly, it states that *"an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic format or that it does not meet the requirements for qualified electronic signatures"*. In effect, this means that both advanced and qualified electronic signatures are admissible as evidence in court and cannot be denied legal effect. Although, as we already mentioned, different levels of security correspond to advanced and qualified electronic signatures and that difference shall have legal consequences, which the European legislator expressly confirms in Article 25(2): *"A qualified electronic signature shall have the equivalent legal effect of a handwritten signature"*. Although some may see this norm as a follow up of the previous national regimes concerning qualified electronic signatures, the truth is that this norm brings along a very important clarification, concerning both the concept of electronic qualified signature and its legal effects. Mainly, it puts an end to the distinction previously established in Portuguese law[41] between qualified electronic signatures and qualified electronic signatures certified by accredited certification authorities. Now the concept of electronic qualified signature is equally established all over the Member States, and it becomes clear that all electronic qualified signatures have equivalent legal

[36] Being uniquely linked to the signatory, being capable of identifying the signatory, being created using signature creation data that the signatory can, with a high level of confidence, use under his/her sole control and being linked to the data signed in such a way that any subsequent change in the data is detectable.

[37] DL No 116-A/2006. GNS is a central service of the State Administration, administratively autonomous, in the dependence of the Prime Minister or of a Member of the Government designed by the Prime Minister.

[38] DL No 290-D/99 with the latest revision of DL No 88/2009

[39] Article 7(2) of DL No 290-D/99 expressly referred "the legal Corporation holder of the qualified electronic signature".

[40] Although "qualified certificates for electronic signatures may include non-mandatory additional attributes" [Article 28(3) of the Regulation].

[41] Article 3(2) of DL No 290-D/99: "*When it is apposed an electronic qualified signature certified by an accredited certification authority, the document […] shall have the proof value of particular signed document*" (free translation).

effect. Furthermore, the qualified electronic signature *"based on a qualified certificate issued by one Member State shall be recognized as a qualified electronic signature in all other Member States"*.[42] This is important, especially concerning the interoperability of electronic signatures all over the Union, which is a crucial factor for the effective construction of a Digital Single Market in the EU.

IV. Other trust services

Regulation 910/2014 is not just about electronic identification and electronic signatures. It has a broader scope, while considering the need of trust services for electronic transactions in the internal market. To enhance these trustable services along all Member States, the Regulation presents a set of quite relevant services and a legal framework for the provision of such services in the internal market. While reserving electronic signature for natural persons, as we have already seen, the Regulation brings along a new and quite relevant instrument for private and public institutions: the electronic seal, referred as "*data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity*".[43] The electronic seal similarly to what happens with electronic signatures, may also be considered as an advanced electronic seal or a qualified electronic seal[44] according to the certificate associated to the seal. This is an instrument of particular relevance to the certainty of legal relations, particularly in case of electronic contracting and of communication between citizens and the public administration will be the electronic time stamps.[45] The functional equivalence to paper-based services and instruments led the European legislator to introduce in the Regulation the availability of electronic registered delivery services[46] and services of authentication of web sites, thus aiming at making the act of surfing the Internet much safer, at least concerning authenticated websites associated with qualified certificates.[47] All these new instruments must be now used, with both technical and legal certainty, by private and public operators, to build a network of trustable services, allowing citizens to make secure and reliable interactions in the European digital market.

V. Final consideration

Regulation 9110/2014, while revoking Directive 1999/93/CE, aimed at establishing a common legal framework, applied directly in all the Member States, concerning the issues of electronic identification, electronic authentication, electronic signatures, and other trust services of information society. The whole

[42] Article 25(3) of the Regulation.
[43] Article 3(25).
[44] Articles 36 and 38 of the Regulation.
[45] Articles 41 and 42 of the Regulation. Concerning time stamps, see also http://www.antwerpen.be/david/website/teksten/Rapporten/Rapport6.pdf, footnote 7: "*Tijdsstempeldiensten kunnen aan de hand van een tijdsstempel de datum en zelfs het uur van een elektronische transactie vaststellen, of de datum of het uur van het bestaan van bepaalde elektronische informatie, zoals een digitale handtekening*". Free translation: the time-stamping service allows to establish, throughout the appending of the seal, the date and even the hour when a certain electronic operation took place, or the date and time of the existence of a certain electronic information, such as a digital signature. Thus, the date and time of the formation, transmission and reception of an informatic document become certain and may thus be opposed to third parties. See Alessandra Villeco Bettelli, *L'Efficacia delle prove informatiche* (Milano: Giuffrè, 2004), 112.
[46] Articles 43 and 44 of the Regulation
[47] Article 45 of the Regulation.

of the Regulation brings clarification concerning the different ways of identifying natural and legal persons in the networked society, but also concerning who may be the holder of electronic signatures. A common framework of admissibility of electronic documents and signatures in court was also established, as well as a new set of legal instruments, adapted from current technological possibilities, aimed at ensuring certainty and reliability in electronic communications and transactions. An important aspect of the Regulation is the assumed option of the European legislator (in accordance with the spirit of the former European legal framework derived from the now revoked Directive 1999/93/CE) for a technological neutral approach. Thus, regardless the fact that digital signatures still have the lion share in the current European system of electronic certification, it is important to note the possibility of different technologies and methods being considered, such as the digital signatures and the dynamic signatures. It may be also said that technological neutrality and functional equivalence are two important factors in the building up of an innovative, reliable, and secure European digital market of which the Regulation 910/2014 will undoubtedly be the main and common legal instrument.