Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 7 (56) No. 2 - 2014

THE ELECTRONIC SIGNATURE - TECHNICAL AND LEGAL IMPLICATIONS

Adrian Constantin MANEA[1]

Abstract: *The end of the twentieth century, known as the Internet bubble period or the dot-com boom was marked by the adoption of regulations regarding the electronic signature and its use in electronic transactions both at the European Union level as well as that of other structures. From the technical point of view, the application of the electronic signature on the documents transmitted online is solved, with the necessary technologies implemented, in terms of practice, the steps taken are small - we are still in an early stage of implementation of the electronic signature on tax returns.*

Key words: *electronic signature, extended electronic signature (advanced), certificate, provider of certification services, non-repudiation.*

1. Introduction

In the context of technological development and the involvement of the information society in day to day life, considering that networks play a growing role in the economic and social life of individuals, transporting increasingly more sensitive data and important economic information, information security has become a priority and a challenge against the attacks that take different forms.

The rapid development of modern information and communication technologies - a prerequisite to building an information society - had a major impact on the society as a whole, marking true mutations in the operating philosophy of economics, politics and the cultural field, but also on the everyday life of the individual, so that currently, the use of internet and computer networks is omnipresent in our lives, in any daily activity, from job-related duties, programming our vacations and leisure time, from making daily or luxury purchases, to the enrolment in education and attending courses on online platforms, from communicating with those who are far from us via social networks or the internet, to organizing online conferences and events even broadcast online.

The interception of electronic communications and copying the data sent, even changing them and generating material damage (e.g. stealing passwords or bank card details by third parties, unauthorised by the cardholder) or the moral damage by affecting the right to privacy and personal data of network users, up to the infliction of security incidents due to natural disasters or disasters affecting communication networks, all are threats to networks and

[1] PhD. Student on Computer and Information Technology, *Transilvania* University of Braşov.

information systems, with serious consequences for the individual and for the community as a whole, for which protecting computer networks has become a political and legislative priority.

The interest for a public policy in the information security domain at national level, but also of the international structures and bodies is due to, on the one hand, the need to protect individual data / economic operators / public authorities in order to ensure a functional economy but, on the other hand, there is also the need to ensure national security and economic stimulation by promoting electronic commerce at international level, among users from different countries.

2. The need for a public security policy

The cyberspace is characterized by the absence of borders between users, dynamism and anonymity, creating both opportunities to develop the knowledge-based information society, but also risks to its operation (at individual, state and even cross-border level).

Regarding the benefits that computerization brings to the modern society, they are undeniable, as real as the vulnerabilities of the information system, which they speculate and which some individuals use for their own advantage, so that ensuring the security of the cyberspace is acknowledged at the level of political, administrative and legislative actors in view of developing and implementing a coherent policy in this area.

Part of the information security policy are also the legal texts regulating the security of the communication networks and information systems, with reference to the internet and electronic commerce (Law no.365 / 2002 on electronic commerce [6]) as well as the regulatory documents that protect the data export via computer networks, the use of the electronic signature in the transactions concluded on-line or the texts of criminal laws on the prevention and punishment of cyber crime.

In the current context where access to information resources is a remote one, when contracts are concluded at a distance, between people who do not see each other face to face, but that legally oblige each other to certain economic operations, when the electronic systems of payment are used and implemented by more and more providers in order to facilitate the access of their own clients, including the transfers of funds from bank accounts can be ordered via the internet, and the electronic commerce is growing, the element of safety and mutual trust between the partners of the legal relationships with economic overtones set at a distance is a prerequisite, ensuring the identification of the parties, the data transmission and the security of the methods of payment in the legal framework implemented.

In the context of increasing the volume of transactions on the internet, both numerically as well as in terms of traded value, given that the entities of the legal relations concluded at a distance had not known each other beforehand, and most likely will have no contact after the completion of the contractual operations to which they have undertaken through the information system, together with the fact that, in most cases, these entities are under different jurisdictions, the basis of the development of electronic commerce and online transactions under high security conditions depends on the electronic signature.

Thus, the electronic signature associated to the online transactions is the manner in which the authentication of the electronic documents' content is done, thus guaranteeing the authenticity of the documents submitted through the information systems.

3. The enactment of the electronic signature in agreement or disagreement with the cryptographic technology

The concern regarding the enactment of the electronic signature and the creation of a legal framework to support the use of this technology is currently embodied by the existence of a national and international legal framework regarding the legal status of electronic signatures that provides the non-repudiation of the electronic documents generating obligations, while minimizing the risk of forgery of electronic documents.

The year 1995 represents the debut of electronic signature enactment, together with the publication by the American Bar Association of the guidelines regarding electronic signatures, the document which actually refers to digital signatures, the conditions they must meet in order to have legal consequences and be implemented in practice.

The initiators of the electronic signature enactment established a legal principle on the reporting of the legal norm to the functional technology of the electronic signature, thus making a distinction between the digital signature and the electronic signature, in the sense that when elaborating a law, the definition of the signature as being electronic or digital is based on the dependence on the technology concerned.

The signature applied to a document in electronic format shall be defined by the law as digital signature if the legal standard is dependent on the cryptographic technology with public keys used, and if the legislature's approach does not require the contact with a particular technology, we refer to a neutral legislation in which the electronic signature term is used with predilection.

Thus, the US legislation in the domain uses the concept of digital signature, based on digital technologies (public key cryptography), while the European regulatory framework and the legislation of the EU Member States use the concept of electronic signature, digital technologies being assimilated to it, as well as other electronic authentication methods such as the capture of the signature in electronic format with biometric data.

The advantage of a legislation dependent on the digital signature technology, by strict reference to the legal rule regarding encryption technology consists in the comprehensive determination of the capabilities and limitations of the respective technology, with strict legal implications that cannot be applied by analogy, thus also representing a downside in regard to the legislation addressing the electronic signature, because the free circulation of products and services based on different technologies is limited.

From the practical perspective of proving in court, with respect to which the legal requirements must be met in order for an electronic signature to be equated in terms of legal consequences to a handwritten signature, the regulations depending on the technology used do not have a very powerful impact, because currently the only technology available that provides verification is the technology based on cryptographic algorithms with public keys and digital certificates that provide user authentication from whom an electronic document comes, but the user identification cannot be established.

3.1. The regulation of the electronic signature by the United Nations Commission on International Trade Law

On 12 June 1996, the United Nations Commission on International Trade Legislation (United Nations Commission on International Trade Law - UNICTRAL) adopted the Law on electronic commerce -

The Model Law on Electronic Commerce (MLEC) - at which point they first addressed a problem regarding the enactment of the electronic signature required in international commercial transactions, namely establishing uniform rules to facilitate the use and recognition of electronic signatures [4].

This was the beginning, thus in 2001 the United Nations Commission adopted the model law on electronic signatures, respectively UNICTRAL - The Model Law on Electronic Signatures (MLES) [5], which in its 12 articles establishes a set of rules that can be used by the United Nations member states in their own legislations without the obligation to notify the adoption of these rules.

By establishing in article 1 MLES [5] that the scope of the rules on the electronic signature relates to e-commerce activities, according to the United Nations Commission on International Trade Law, the electronic signature represents data in electronic format, attached to or logically associated to a data message that can be used to identify the signatory in relation to the data message, indicating the approval of the signatory for the information contained in the data message transmitted (art.2 MLES [5]).

In the opinion of The Model Law on Electronic Signatures, the signatory of a document, by applying the digital signature, is either the person holding the signature creation data, who acts on their own behalf or the person who, having access to the certificate signature acts on behalf of the certificate holder as representative, implicitly with the consent of the holder for the operation confirmed by the electronic signature.

The electronic signature applied to a data message / transaction is recognized as being legal and gives legal effects to the act / operation to which it is associated if it is safe in relation to the purpose for which it was created, in the sense that the signature creation data belongs exclusively to the signatory, ensuring his/her authentication, and at the time of signing, the creation data of the signature are under the exclusive control of the signatory (art.6MLES [5]).

Also, the electronic signature is considered safe if the amendments subsequent to its application, either on the data message confirmed by signature, or on the signature itself can be detected (art.6 MLES [5]).

3.2. The electronic signature legislation at EU level.

Setting July 2001 as a deadline for the EU member states to implement the EU rules on the electronic signature, after the European Commission admitted, in April 1997, that the digital signature represents the key instrument in ensuring the security of electronic transactions, on 13 December 1999, the Parliament and the European Council approved the Directive on Electronic Signatures (Directive 1999/93 / EC [7]).

Without insisting on the technology procedure associated to the electronic signature, Directive 1999/93 / EC [7] uses the concept of electronic signature and aims mainly to ensure the use and legal recognition of electronic signatures within the Community, with e-commerce applications when using the electronic signature in the public sector, within the national and community administrations, in the communications between the respective administrations, but also between the administrations and the citizens and / or businesses in electronic applications with fiscal implications (submitting certain tax returns online), within the scope of social security, health and in the legal area.

Defining the electronic signature as *data in electronic format attached to or logically associated with other electronic data and which serves as a means of authentication,* Directive 1999/93 / EC [7] stipulates (Article 5 Directive) that only the advanced electronic signature based on a certificate qualified and generated using a secure signature creation device is legally equivalent to the handwritten signature, generating the same legal effect and having the same probative value.

The advanced electronic signature is defined by Article 2 of Directive 1999/93 / EC [7] as the electronic signature which meets the following conditions:

a) refers uniquely to the signatory
b) is capable of leading to the identification of the signatory
c) was created using means that the signatory can maintain under his/her control
d) is linked to the data to which it relates so that any subsequent amendment thereto can be detected.

Regarding the compulsory legal effects to be recognized with reference to the advanced electronic signatures proposed by the laws of the EU Member States, namely the acknowledgement of the legal force of an act / operation confirmed by electronic signature similar to acts under private signature, as well as their admissibility as evidence in court, Directive 1999 / 93 / EC [7] imperatively rules in Article 5 that the other forms of electronic signature are not limited in the possibility of acknowledging their legal effect and / or the admissibility as evidence in legal proceedings by the national legislations, this freedom of enactment being left to the Member States.

Defining the electronic signature creation device as configured software or hardware units used to implement the signature creation data, Directive 1999/93 / EC [7] lays down in Annex III the requirements for the signature verification devices to qualify as secure devices.

Also, the identification of signatories by applying an electronic signature requires the use of certificates defined by Article 2 of Directive 1999/93 / EC [7] as the procedure for electronic attesting which relates the verification data of the signatures to a person and confirms the identity of that person, and in Appendix I lists the technical characteristics that a qualified certificate must meet, certificate issued by a certification service provider, which must also meet no less than 12 conditions listed in Annex II of the Directive.

All these precautions and normative conditionings are justified by the fact that according to Directive 1999/93/ EC[7] the certification service providers are liable for the damages caused to users to whom they have issued these qualified certificates, if such damage is caused by the proper use of the certificates, including the compliance by the user to the limitations specified by the certification service provider at the time of issuing the qualified certificate in terms of purposes of use (type and value of transactions).

3.3. The Romanian Law regarding the Electronic Signature and the Implementing Rules.

Developed in line with the neutral form of Directive 1999/93/EC [7], the legislation in Romania regarding the electronic signature includes Law no.455 / 2001 [8] and the Technical and Procedural Rules regarding the enforcement of the law adopted by Government Decision no.1259 / 2001 [9].

Starting from the list contained in Article 4 of the law [8] regarding the definitions used, we understand that the data in electronic format are representations of information in a conventional form,

suitable for creating, processing, sending, receiving or storing it electronically, and the document in electronic format is a collection of data in electronic format among which there are logical and functional relationships and which render letters, numbers or any other characters with intelligible meaning, intended to be read by a computer program or another similar process.

Hence, the information contained in an electronic document bearing an electronic signature is not encrypted, is not protected against reading and can be accessed by anyone.

Since they do not contain the original signature of the issuer, prior to the adoption of Law no.455 / 2001[8] some authors [1] believed that electronic records can only be considered an initial form of written evidence, as they can provide evidence on the legal relationship contained by them only corroborated with other evidence.

Since the adoption of the Law no.455 / 2001[8], the document in electronic format, which had been incorporated, attached or logically associated an electronic signature based on a qualified certificate unsuspected or unrepelled at the time and generated using a secured device which creates the electronic signature is assimilated, in terms of conditions and effects, to the document under private signature (article 5 of the Law).

Using, as a Community rule, two concepts distinctly defined: the electronic signature *(data in electronic format which are attached to or logically associated with other data in electronic format and which serve as a method of identification)* and the advanced electronic signature *(the electronic signature which fulfils cumulatively the following conditions:*

a) it is uniquely linked to the signatory;

b) ensures the identification of the signatory;

c) it is created using means controlled exclusively by the signatory; and

d) it is linked to the data in electronic format, to which it relates in such a manner that any subsequent amendment affecting them is identifiable) the Romanian legal standard confirms the fact that the signatory of the electronic message agrees upon its content, therefore having the role of certification of consent, so that the other three characteristics of the advanced electronic signature are justified in terms of identifying the author of the message transmitted electronically, which determines its being assimilated only to the handwritten signature [3].

Law no.455 / 2001 [8] defines the secured electronic device which creates the electronic signature (that device creating the electronic signature) that meets the following conditions:

a) the signature creation data used to generate it can appear only one time and their confidentiality can be assured;

b) the signature creation data used to generate it cannot be deduced;

c) the signature is protected against forgery by technical means available at the time of its generation;

d) the signature creation data can be effectively protected by the signatory against the use of unauthorized people;

e) the data in electronic format which must be signed are not to be modified, nor prevented from being presented to the signatory prior to the completion of the signing process and the same is valid for the signature-verification device (that software and / or hardware configured, used in order to implement the signature-verification data).

In order for the electronic document to which an electronic signature is associated to have the same probative force as the document under private signature, it is

required that the electronic signature be based on a qualified certificate.

The qualified certificate is a collection of data in electronic format certifying the link between the electronic signature verification data and a person, confirming the identity of that person, which also fulfils the requirements of art. 18 and which is issued by a certification service provider that meets the requirements of article 20 of the Law [8].

Each signatory using an electronic signature is assigned by the certification service provider a personal code that provides his/her unique identification, and which is also the core of the qualified certificate.

Guaranteeing the association of the signatory's name or pseudonym with its serial number so as to be able to register clients with the same initials, records are held by the provider of certification services (Article 17 of the law [8]), the qualified certificate contains the private key - public key pair meant to identify the signatory.

At the request of the holder of the qualified certificate, the certification service provider can include other information on the qualified certificate issued, after a preliminary verification of the accuracy of this information, in this sense the certificate holder must provide the appropriate means to prove the respective additional information.

At the time of issuing the qualified certificates, certification service providers are required to verify the identity of the applicants solely on the basis of identity documents, and shall also issue two copies of this paper, one copy being made available to the holder and the other one being kept by the supplier for 10 years, according to article 19 of the Law [8].

In order to check the digital signature in the sense of authenticating the certificate holder concerned, the Romanian legislation, as well as the EU rules, uses the private key-public key cryptographic system, therefore publishes two different cryptographic keys, but logically and functionally related to each other (as defined in art. 2 paragraph 1 of Government Decision no. 1259/2001 [9]).

The public key is made available to anyone wishing to visualize the transmitted data, but usually, the public key is known by a limited number of people, namely those involved in the legal relationship and are in possession of a qualified certificate issued by the certification services provider [2].

The document to which the electronic signature is attached is signed with the private key, which proves the holder's consent to the text, thus avoiding further challenges regarding the terms of the document. This function, which allows verifying the consent of the electronic signature holder to the content of the document by applying the electronic signature, is called non-repudiation, thereby producing legal effects of the confirmation report of the document bearing the electronic signature.

Article 2 paragraph 1 letter e of the Methodological Norms for the enforcement of Law no. 455/2001 [9] describes in technical terms the mechanism of creating the electronic signature on a document, a mechanism consisting of applying a *hash-code* function, obtaining the document print, and through an algorithm, the "private key" is applied on the document print, thus resulting the electronic signature.

However, the private key is defined as a unique digital code generated by a *specialised hardware* and / or *software.*

The document in electronic format, into which it has been included, attached to or logically associated with an electronic signature, recognized by the party to whom it is opposable, has the same effect as an

authentic document between those who have subscribed to it and those who represent their rights (according to article 6 of the law [8]) and if any of the parties of the legal report confirmed on the basis of a document bearing the electronic signature does not recognize the writing or signature, the court is always bound to rule that the examination be done by specialized technical expertise on the certificates.

The expertise cannot ignore the real possibility of falsification of electronic documents (e.g. stealing the necessary data and instruments in order to generate the electronic signature).

One of the characteristics of the extended electronic signature, commonly referred to when it is described, is "non-repudiation" (along with the assurance regarding the authenticity and integrity of the message). Non-repudiation consists in the technical inability to support the fact that a signature was not generated using a specific digital certificate [10].

4. Technological principles regarding the electronic signature operation

Given the purpose of the electronic signature related to remote contracts, using computer networks, the signature mechanism must provide proof of authorship of an electronic document, the identification and authentication of its author.

The identification is done by using the digital certificate which contains the private key-public key cryptographic system.

A cryptographic key is actually a file, while the encryption algorithms are based on complex mathematical operations with huge integer numbers - hundreds of decimal digits or thousands of bits (for example, according to article 35 of Government Decision no. 1259/2001 [9] the minimum length of the private key used by a signatory in order to create an extended electronic signature must be a minimum of 1024 bits for the RSA algorithm, and 300 decimal digits, an algorithm established for the electronic signature under article 34 of Government Decision no. 1259/2001 [9].

The public key cryptography promoted by R.Rivest, A.Shamir and L.Adleman - the authors of the RSA algorithm (after the initials of the authors, and the most widely used cryptographic algorithm with public keys) – ensures the confidentiality of an encrypted message with the public key of the recipient so that only the latter should be able to decrypt the message with his/her own private key. If there is an answer, the recipient will use the sender's public key in such a way as the decryption be performed solely by the sender (with his/her pair private key).

Public key cryptography works on the principle that each entity has access to the public keys of the entities with whom s/he corresponds, as there is one public key for each entity.

The public key infrastructure (Public Key Infrastructure -PKI) allows users to obtain the authentic public keys under the form of digital certificates.

The certificate allows the dissemination of information regarding the identity of the signatory, each third party being able to verify the integrity of the certificate due to the issuer's public key, the distribution of the public key by the issuer being the fundamental element for the proper functioning of the electronic signature authentication system.

5. Conclusions

In the Romanian literature [3], it was stated that although the law is based on the

principle according to which the holder of the private key is the author of the document in electronic format, it can be considered that it does not confer an absolute presumption on the identity of the signatory, as a third party in possession of the private key can sign the electronic message instead of the legitimate holder.

The legislature stated that the identity of the person is included in the qualified certificate through the secure electronic code, so that the distribution by the holder of the certificate in itself and at the same time of the public key is assimilated with the manifestation of the will that a third party be able to use that certificate in the name and on behalf of the proprietor, the latter being unable to repudiate the document to which the electronic signature is attached.

In conclusion, the fulfilment of the legal security conditions by the electronic signature, having the same role as in the case of a handwritten signature, will lead to the assimilation of the electronic document bearing the electronic signature to the document under private signature, their identical probative force being acknowledged.

There is no general definition of the handwritten signature in the Civil Code and in the Romanian Code of Civil Procedure (the only explanation assimilated to the concept of holographic is encountered in art.1041 Civil Code regarding the definition of the holographic will), the definition belonging to the doctrine and indirectly stating what its specific effects consist in.

In order for the advanced electronic signature to have the same legal effect as the handwritten signature, the security conditions must be met, for only thus the verification and authentication of the signatory's identity is ensured.

Acknowledgements

This paper is supported by the Sectorial Operational Programme Human Resources Development (SOP HRD), ID134378 financed from the European Social Fund and by the Romanian Government.

References

1. Cărpenaru, S.D.: *Romanian Commercial Law (Drept comercial roman)*. Bucharest. All Beck Publishing, 2000.
2. Elisei, C., Andon, A.V.: *New implications of the computerization of society on the law: Law no.455 / 2001 on electronic signature. (Noi implicații ale informatizării societății asupra dreptului: Legea nr.455/2001 privind semnătura electronică).* In: Law Journal, No.12 / 2001, p.18-29.
3. Savu, T.G.: *The legal consecration of the electronic signature. (Consacrarea legală a semnăturii electronice).* In: The Commercial Law Journal, no.7-8 / 2002. Bucharest. Lumina Lex Publishing, 2002, p.222-235.
4. http://www.uncitral.org/ uncitral / uncitral_texts / electronic_commerce / 2001Model_signatures.html. Accessed: 25-09-2014.
5. http://www.uncitral.org/ pdf / english / texts/electcom/ml-elecsig-e.pdf. Accessed: 25-09-2014.
6. *** *Law no.365 / 2002 on electronic commerce*, published in the Official Gazette no.483 from 05.07.2002, republished in the Official Gazette no.959 from 29.11.2006.
7. *** *Directive 1999/93 / EC of the European Parliament and of the Council of 13.12.1999 regarding a Community framework for the electronic signatures*, published in the Official Journal of the

European Union no. L13/12 of 19.01.2000.
8. *** *Law no.455 / 2001 on electronic signature*, published in the Official Gazette no.429 from 31.07.2001, republished in the Official Gazette no. 316 from 30.04.2014.
9. *** *Government Decision no.1259/ 2001 on the approval of the technical and methodological norms for the enforcement of Law no.455 / 2001 on electronic signature*, published in Official Gazette no.847 of 28.12.2001.
10. http://novit.ro/2011/03/29/cateva-probleme-juridice-legate-de-semnatura-electronica. Accessed: 25-09-2014.