THE ELECTRONIC SIGNATURE: A CONTEMPORARY TOOL FOR CERTIFICATION OF IDENTITY AND INFORMATION CONTENT?

Sandra Sophie-Elise OLĂNESCU[*]
Alexandru Vladimir OLĂNESCU[**]

Abstract

The accelerated and continued development of information technology and telecommunications led to an unprecedented growth of the possibilities to conduct activities in any field, especially in the economic, financial, administrative and legal areas.

Currently, we can remotely access information resources, conclude contracts, we have and use electronic payment methods, we use systems to electronically transfer money and trade and many of the like. Thus, development of a trusted context is a prerequisite, given the potential risks, which may occur when we perform activities using on-line electronic systems: party identification, data transfer, securing payments, also taking into account the legal framework still insufficiently clear about consumer protection.

Any economic activity is prone to fraud, so issues arise when it is found that resolving these conflicts requires increased attention, especially in the field of electronic trade.

At European Union level, these issues have been and are being hotly debated, with the Union aiming to provide a common basis for secure electronic interactions between citizens, businesses and public authorities, in order to increase the efficiency of online public and private sector services, e-business and e-commerce in the Union.

This paper proposes a brief foray into the Union and national legislative framework governing the use of electronic signature and an overview of the most important risks that its use may raise, especially from the perspective of cybercrime.

Keywords: *electronic signature, digitization, trust services, signatory, electronic identification..*

1. Introduction

1.1. What is the theme of this paper?

Given the difficulties that the contemporary society faces in the fight against the SARS -CoV2 virus and the need to adapt the activities carried out in all areas to the strict rules on social distancing and quarantine or self-isolation, as the case may be, teleworking has become a key point in the process of adapting to the new living conditions.

Thus, to ensure continuity of economic activities and the exercise of legislative and executive state power in the context of the current pandemic, it was imperative to focus the efforts to create the technical and legal conditions required to work remotely, in order to observe the rules on isolation or quarantine.

A problem exacerbated when working remotely / teleworking is therefore represented by the ways in which the identity of the parties and the content of the sent

[*] Attorney-at-law, Ph.D. Candidate, "Nicolae Titulescu" University (e-mail: sandra.olanescu@cliza.ro).
[**] Attorney-at-law, Ph.D. Candidate, "Nicolae Titulescu" University (e-mail: alexandru.olanescu@cliza.ro).

documents could be certified, so that electronic documents could have the same value as the documents submitted in original/transmitted by hand.

The solution to this problem is not new, because we are talking about a tool that has been used for more than two decades, especially at international and European level, and that is: the electronic signature. However, as the world was gripped by the COVID -19 pandemic, even the most " *traditionalist* " activities carried out, especially by the institutions of the administrative and judicial apparatus in Romania, where personal presence and submission of documents by hand was mandatory, have adapted and started using the electronic signature in their work, perhaps more intensely than ever.

Thus, it is the context of the current pandemic that has brought back into the " *spotlight* " the electronic signature, in the situations when it is required the submission / transmission / communication of official/original documents in electronic format, reason why an in-depth research of the new regulations concerning it and an analysis of the risks involved in its use are necessary and timely, and also represent the subject of this paper.

1.2. What is the importance of the topic under discussion?

The topic under discussion in this paper is of special importance, in relation to the risks that each user of an electronic signature, be it the staff of an institution or public authority, or a private company, a self-employed person or a freelancer must be aware of, especially if the use of this mean of identification was caused by the COVID-19 pandemic, in other words it was a necessity and not an option for the user.

Why, though, would there be issues raised by the understanding and proper use of an electronic signature by a new user in the current global context? Firstly, it is because, in some cases, there was not enough time available to the new user to understand how to properly use an electronic signature, which could increase the risk of use. Secondly, with the increase in frequency of the use of electronic signatures and of the number of users of such signatures, it also increases the risk of spreading of the phenomenon of cyber-crime concerning data theft, unlawful access of databases, etc. Thirdly, the electronic signature must not be confused with an infallible means of identification, in the sense of ensuring the certainty or, at least, an increased degree of confidence in the veracity of the signatory's identity.

1.3. How do the authors intend to respond to the issues raised by the theme addressed?

This paper presents the analysis of the legal framework applicable in the field of electronic signatures, both from the perspective of the European Union and from national perspective, and then it explains by comparison certain technical issues in order to understand how different types of electronic signatures work, and the degree of risk the use of each of them involves.

Finally, the paper relates the detailed information present in its content to the offenses set forth by the national law that may be committed through the use of or in connection with the use of the electronic signature, in order to highlight the highest risk issues faced by both the certification service providers and by their beneficiaries (regardless of their capacity or the category to which they belong) which they should pay increased attention to.

1.4. How does this paper relate to the existing literature?

In the current pandemic context, the regulation of the electronic signature has changed in terms of legislation, at least nationally. In addition, given the exponential increase in the use of this method of identification, we deem that this paper, by its structure, differs from other specialized articles published on this topic precisely by presenting the legislative and practical aspects, in relation to current events regarding the health crisis the society has been through (and still goes through today) and, equally to the risks of criminal nature that improper use of it could pose.

2. National and European law regarding the use of electronic signature

2.1. Regulation (EU) no. 910/2014

In the general world context of digitalization of most of the activities in society, which is a tendency caused by the spread of the phenomenon of " *Internet of things* " (IoT), the European Union has set a number of targets in this respect, which it has conceptualized since 2010, through the Communication from the Commission of 26 August entitled " *The Digital Agenda for Europe* "[1]. This document claims, amongst others, "*to achieve 'smart growth' – that is, a European economy based on knowledge and innovation. The production and consumption of digital ICTs are deeply implicated in this*"[2].

Throughout the Communication, the Commission has identified a number of issues that prevent European citizens from benefiting from a digital single market and from cross-border digital services. Among these problems, the following were identified as major obstacles to the implementation of a digital single economy: fragmentation of the digital market, lack of interoperability and increasing cybercrime.

At the present, a number of legislative instruments have been adopted at European level to mitigate and even eliminate the problems highlighted, at least at the level at which they have been identified and analysed so far.

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 singlr market and repealing Directive 1999/93 / EC[3] [*Regulation (EU) no. 910/2014* " or" *Regulation*"] is among the instruments aimed at achieving the objectives of development and implementation of the digital single market in the European Union, especially in terms of mutual cross-border recognition of electronic identification means , which involves a high level of security of electronic identification systems .

It can therefore be synthesized to that, the Regulation, by its provisions, aims to remove barriers to the use of electronic identification systems in the Union European in the broader context of the creation and implementation of the digital single market. In addition, it establishes the

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe, available at: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri = CELEX: 52010DC0245, accessed on 5th of November 2020.

[2] Robin Mansell, *Here Comes the Revolution — the European Digital Agenda*, The Palgrave Handbook of European Media Policy, Macmillan Publishers Limited, 2014, p. 203.

[3] 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 Directive 1999/93 / EC, available at: https://eur-lex.europa.eu / legal-content / RO / TXT /? uri = celex: 32014R0910 , accessed on 6th of November 2020.

obligation for the Member States of the European Union to cooperate, thus establishing an interoperability framework. This framework requires that the programs of national electronic identification be interoperable, in a technologically neutral system, which does not favour any specific national technical solution for electronic identification.

In addition, Regulation (EU) no. 910/2014 aims to improve confidence in electronic transactions at Union level, in order to achieve its objective of increasing the efficiency of online services in the public and private sector, as well as e-commerce.

With regard to its regulatory object and addressees, it is noteworthy that the Regulation applies, on the one hand, to electronic identification systems (IDEs) notified to the European Commission by Member States and, on the other hand, to trust service providers from the Union.

Overall, the European legislative act defines and establishes the scope of coverage of the notions and basic concepts used in regulating the use of electronic signatures in a clear and comprehensive way, in order to eliminate, as far as possible, any disagreement or misunderstandings. By way of example, for all types of electronic signatures are defined the notions of: authentication, trust services, product, electronic seal, signatory, means of electronic identification, beneficiary, electronic identification data and the like.

Thus, the electronic signature represents *"data in electronic format, attached to or logically associated with other data in electronic format and which is used by the signatory to sign"*. Basically, the electronic signature is nothing more than " *data* " attached to the content of a document in electronic format, with the role of attaching the respective collection of data to a specific identity, namely that of the signatory of the document.

To narrow the circle of persons to whom the Regulation grants legitimacy to use an electronic signature, we must analyse the term "beneficiary ". According to art. 3 point 6 of the Regulation, the beneficiary is any " *natural or legal person benefiting from a service of electronic identification or a trust service* " , meaning they do not require a certain qualification in order to become user of an electronic signature , thus benefiting both people working in the public and private sectors .

However, the Regulation sets strict trust services, stating that they are paid services that include activities of creation, verification and validation of the various categories of objects of certification, namely: electronic signatures, electronic seals or electronic time stamps, registered e-delivery services and certificates relating to such services or certificates for the authentication of a website.

Trust services may also include the storing of electronic signatures, seals or certificates for those services.

In other words, trust services are services involving, *inter alia*, personal data operation, regardless of how that is performed, reason why it applies the provisions of Regulation (EU) 679/2016 of the European Parliament and the Decision of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC[4] ["Regulation *(EU) no. 679/2016"*or " *General Data Protection Regulation "*] . Moreover, trust services providers are, as a

[4] Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC available on: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679, accessed on 9th of November 2020.

rule, personal data operators in the sense established by the provisions of art. 4 point 7 of Regulation (EU) 679/2016. In connexion to the beneficiaries, targeted persons are, in the sense of the provisions of art. 4 point 1 of the General Data Protection Regulation, the identified or identifiable natural persons that benefit from an electronic identification service or a trust service[5].

Going back to the trust service providers in the European Union, the Regulation states that are "qualified " those providers that meet the applicable requirements therein. They have the legal right to provide qualified trust services (e.g. qualified electronic signatures, seals or certificates) in all Member States .However, if the provider of trust service is located in a country outside the European Union, in order for its services to be considered " *qualified* " , there must be an agreement between the European Union and third party State third party state or " *an international organization in accordance with Article 218*"[6] of the Treaty on the Functioning of the European Union (" *TFEU* ").

The Regulation also sets out a number of key aspects on electronic identification. In this regard, it is noteworthy that it establishes the obligation of mutual recognition of electronic identification by and between Member States from 28 September 2018, in particular to facilitate secure electronic transactions at union level. At the same time, it is mandatory to mention the level of assurance of the electronic identification system (i.e. low, substantial or high) for the form of electronic identification issued within that system, with the mention that the mutual recognition is mandatory only when, in the relevant public sectors, one of the ' *substantial* ' or ' *high* ' levels is used to access that online service.

States are required to provide the Commission, when it notifies them, with a series of information concerning the levels of assurance and the electronic identification issuer within that system; surveillance systems and the liability applicable and the bodies that manage the registration of unique personally identifiable information.

Moreover, in case of system or authentication security breach, Member States are under the obligation to immediately suspend or revoke authentication or compromised parts of the system throughout the Union and to inform other Member States and the Commission.

The regulation also states the contractual liability in case of transactions between Member States where the obligations set in the Regulation are violated. Thus, they shall be held liable for any damage caused to any person or body, whether intentional or negligent, as follows: a notifying Member State; the party issuing the electronic identification or the party managing the authentication procedure.

From the perspective of supervision, all trust service providers are subject to supervision and risk management and notification obligations in case of security breach, according to art. 17-19 of the Regulation, but in a differentiated way, depending on their qualification category. Thus, unqualified trust service providers are subject to loose supervision loose, meaning that the surveillance body only reacts if the provider is suspected of improper behaviour. Instead, qualified trust service providers established in the Union are strictly supervised and in that, they must obtain prior authorization from a supervisory body and must be audited at least every two years by

[5] Ciprian Săraru, *Processing of personal data A matter of principle*, in *General Data Protection Regulation. Comments and explanations*, Hamangiu, Bucharest, 2018, p. 12.

[6] See, in this regard, art. 14 para. (1), final thesis of the Regulation (EU) 910/2014.

an organization to assess whether they meet the requirements of Regulation (EU) 910/2014.

In connexion with the legal effects of the electronic signature, the Regulation states that it takes effect *ad probationem* , and can be used as evidence in litigations, regardless if we are talking about a qualified electronic signature qualified or not . At the same time, the Regulation expressly provides for the equivalence of the qualified electronic signature with that of the holograph signature, within the provisions of art. 25 para. (2).

It also established the recognition in all the other Member States of qualified electronic signatures based on a qualified certificate issued by a Member State.

Art. 26 of the Regulation sets out the requirements that an advanced electronic signature must meet, namely: to refer exclusively to the signatory; to allow his/her/their/its identification; be made using electronic signature creation data that the signatory can use, with a high level of trust, which is exclusively under his/her/their/its control; and to be connected with data used for signature such a way that any subsequent change of data could be detected.

For online services provided by a public body, the Regulation provides that advanced electronic signature based on a qualified certificate and qualified electronic signature used in these services is acknowledged, if it uses at least formats or technical methods provided in the Regulation. Also, for these online services provided by public sector bodies, it will not be required an electronic signature at a level of security higher than the level of security of the qualified electronic signature employed for cross-border use of an online service rendered by a public service body, as per the provisions of art. 27 para. (2).

From the perspective of the categories of electronic signatures, it should be noted that there are currently three types of electronic signatures, according to the legislation in force, namely: simple signature; advanced signature and qualified signature.

In practice, they provide different levels of security and recognition for the person who uses them in his/her/their/its relations with other persons or entities (companies or public institutions). For this reason, the three types of electronic signatures cannot be considered identical and must be used depending on the risk associated with the documents to be signed.

It is appropriate to reiterate that electronic signatures are currently regulated by Regulation (EU) 910/2014. This normative act applies, directly[7], in all member states of the European Union, therefore also in Romania. In other words, all persons and entities using electronic signatures must comply with the provisions of this single European legal framework.

In essence, the three types of electronic signatures have different levels of security. Thus, the simple electronic signature has a low level of trust, the advanced electronic signature has a medium level of trust, and the qualified electronic signature has a high level of trust.

Therefore, it can be deduced that the qualified signature is the only one that can be considered the same as the holograph signature.

It should also be noted that electronic signatures are closely linked to the context in which they are used, in order to ensure a certain level of trust and recognition.

European legislation allows the use and recognition of the three types of electronic signatures and regulates that only the qualified electronic signature, issued by

[7] Augustin Fuerea, *The European Union Handbook, 6th Edition*, Universul Juridic, Bucharest, 2016, p. 235.

a qualified trust service provider accredited under Regulation (EU) 910/2014, is equivalent to the holograph signature.

In detail, it can be seen that electronic signatures can be used, depending on the context of their use and the type of signature, as follows:

- **simple electronic signature** (low level of trust): contact details entered in the email signature, biometric signature (made on a tablet). This type of signature can be used to sign e-mails or low-risk electronic documents, such as receipts or acknowledgements;
- **advanced electronic signature,** which requires a simple digital certificate (medium level of trust): e-mails, medium-risk electronic documents (for example, leave applications, expenses reimbursement sheets or other forms can be signed inside a company), enclosed documents (endorsements, estimates or minutes). Usually, the advanced signature is used in a context that involves other actions that can confirm the existence of the will of the parties (for example, the signing of a lease and the related payment);
- **qualified electronic signature**, which requires a qualified digital certificate (high level of trust): signing high-risk e-mails or documents, such as credit agreements, commercial or service contracts, employment contracts and addendums, power of attorneys, mediation contracts, tax invoices, medical documents (analysis bulletins, hospital admission or discharge forms) or documents relating individuals and companies with the state.

Therefore, it is recommended that the first two types of electronic signatures be used in relationships that involve a low risk for the parties (in other words, in those cases where a minimum guarantee is needed that the signatory is who he/she/they/it claims to be).

Usually simple or advanced electronic signatures, can be used in operations with low risk, *i.e.* where potential disputes or the applicable law do not require taking actions through mechanisms binding the parties (handwritten signature or its equivalent).

Thus, a series of internal document flows are identified that can be issued with these types of signatures or in relation to third parties to whom the information transmitted does not require binding, but only a minimal guarantee that they are transmitted by the issuer.

This confirms that a qualified electronic signature is required in high-risk relationships, where the identity of the signatory must be beyond doubt. For example, when applying for a loan or submitting, within the legal deadline, a tax return, the qualified electronic signature ensures that it is the real person using the electronic signature in question. In other words, the real identity of the signatory is closely linked to his/her/their/its electronic identity.

In the case of the qualified signature, we are of the opinion that, in the case of operations that present a higher risk of disputes or litigations, this type of signature is the optimal choice, given the fact that the qualified signature has the value of the holograph signature. Thus, the financial-banking area (loans especially), employment procedures, commercial relations (*business to business*, *business to consumer*, *consumer to business*), forms, applications in relation to state institutions (*business to government* , *citizen to government)*) are areas of practice that generate volumes of documents , in which the rate of incidence of disputes is high .

Therefore, the qualified electronic signature is at the highest level of recognition and trust and is presumed to be binding to the parties.

In order to clearly highlight the differences between the three types of electronic signature, it is appropriate to detail the essential elements for each type of signature, so that the assessment of the areas in which they can be used, depending on the degree of risk, is easier.

On the one hand, the simple electronic signature is essentially data in electronic format, attached to or logically associated with other data in electronic format and used by the signatory to sign, according to Regulation (EU) no. 910/2014.

On the other hand, the advanced electronic signature is an electronic signature that meets the following requirements[8]:

- refers exclusively to the signatory;
- allows the identification of the signatory;
- it is created using electronic signature creation data that the signatory can use, with a high level of trust, exclusively under his/her/their/its control; and
- is linked to the data used for signing, so that any subsequent changes to the data can be detected.

Last, but not least, the qualified electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device and is based on a qualified certificate for electronic signatures.

Consequently, it is the qualified device and the qualified certificate that make up the difference between the advanced signature and the qualified signature. These two additional tools provide a direct and undoubted link between a person's real identity and electronic identity.

Therefore, the qualified electronic signature is considered, according to the Union regulations currently in force, as the only one that is equivalent to the holograph signature.

2.2. Law no. 455/2001

In Romania, the use of electronic signatures has been regulated by law since 2001, so that the adoption of Regulation (EU) no. 910/2014 determined the amendment and supplement of the existing legal framework , to align them with and put the European norm into correct and complete application.

In this regard, Law no. 455/2001 on the electronic signature[9] (" *Law No. 455/2001"*) is the main normative act establishing the legal regime of electronic signatures and electronic documents, including the conditions for the provision of electronic signature certification services. It entered into force on 31 July 2001, republished on 30 April 2014, with the necessary amendments and completions for the application of the aforementioned Regulation.

Thus, Law no. 455/2001 establishes the legal regime of the electronic signatures and of the documents in electronic format as well as the criteria for providing electronic signature certification services, the law

[8] George Hari Popescu, *What you need to know about the electronic signature, given that the new bulletins will contain one - legal value, recognition in other states and technical issues*, published on 14th of August 2020, available on: https://www.avocatnet.ro/articol_55547/Ce-trebuie-s%C4%83-%C8%99tii-despre-semn%C4%83tura-electronic%C4%83-avand-in-vedere-c%C4%83-noile-buletine-vor-con%C8%9Bine-una-valoarea-juridic%C4%83-recunoa%C8%99terea-in-alte-state-%C8%99i-aspecte-tehnice.html, accessed on 6th of November 2020.

[9] Law no. 455/2001 regarding the electronic signature, in the version republished in the Official Gazette, Part I, no. 316 of April 30, 2014, with subsequent amendments and completions, available on: https://lege5.ro/App/Document/gm4tmnjuha/legea-nr-455-2001-privind-semnatura-electronica, accessed on 6th of November 2020.

being completed with the national legal provisions
regarding the conclusion, validity and effects of legal acts.

This has been amended and supplemented, the current version being republished on April 30, 2014, in order to align with the provisions of EU Regulation no. 910/2014. In addition, the changes introduced by the urgent measures adopted, at governmental level, due to the COVID-19 pandemic have led to the additional amendment and completion of Law no. 455/2001, by: Emergency Ordinance no. 39/2020 for the completion of Law no. 455/2001 on the electronic signature[10] („*OUG 39/2020*").

Thus, given the need to move the country to work from home or teleworking, including for civil servants, it was necessary to adopt a set of rules specifically devoted to this purpose, regulating a new authority for certification services destined exclusively to this type of personnel.

In this sense, art. 3^1 newly introduced establishes in para. (1) that the Special Telecommunications Service is designated to provide qualified certification services destined exclusively to the authorized personnel of the institutions and public authorities in Romania, in order to carry out their duties. These services will be provided free of charge both to institutions and public authorities in Romania.

In addition, para. 2 of art . 3^1 provides that the Regulatory and supervision authority will have to update the register of certification services providers by adding the Special Telecommunications Service as qualified certification services provider destined exclusively to the personnel of the institutions and authorities public .

However, unlike other providers, in the case of the Special Telecommunications Service, the information will not refer to fees, contract conditions for the issue of the certificate, including limitations of the liability of the certification service provider and the ways of resolving disputes.

Also, in the case of the Special Telecommunications Service, the provisions of art. 22 setting, *in substance*, that qualified certification service providers should have financial resources to cover the damages that could cause during the performance of the activities relating to electronic signature certification.

Last, but not least, the Special T telecommunications Service shall notify the Regulatory and supervisory authority specialized in this field about the commencement of activities related certification of electronic signatures 3 days before the start thereof, which is an exception to the deadline for other providers, who have a deadline of 30 days.

Section II of Law no. 455/2001 introduces the definitions given by the legislator to certain expressions and terms for a better understanding of the law. Thus, the following notions are defined, among others:

- **the electronic document** is a collection of data in electronic format between which there are logical and functional relationships and which render letters, numbers or any other characters of intelligible meaning, intended to be read by means of a computer program or other similar procedure;
- **Electronic signature** means data in electronic format which is attached to or logically associated with other electronic data and which serve as a method of identification;

[10] Published in the Official Gazette, Part I no. 281 of 03 April 2020, available on: Ordonanța de urgență nr. 39/2020 pentru completarea Legii nr. 455/2001 privind semnătura electronică (lege5.ro) accessed on 10th of November 2020.

•**Extended electronic signature** is the electronic signature which meets all the following conditions :

a) is uniquely related to the signatory;
b) ensures the identification of the signatory;
c) is created by means controlled exclusively by the signatory;
d) it is linked to data in electronic form, to which it relates in such a way that any subsequent modification thereof is identifiable;

• **Signatory** is the person holding a signature-creation device, who acts either personally or on behalf of a third party .

Regarding the legal regime of documents in electronic form, art. 5 of Law no. 455/2001 expressly provides that the electronic document, to which an extended electronic signature has been incorporated, attached or logically associated, based on a qualified certificate, not suspended or revoked at that time and generated by means of a secure electronic signature creation device, is assimilated, in terms of its conditions and effects, with a document under private signature.

The electronic document, with an electronic signature incorporated, attached or logically associated, and which the opposing party acknowledges, has the same effect as the authentic instrument between those who signed it and those who represent their rights.

Also, in cases where, according to the law, the written form is required as a condition of proof or validity of a legal act, an electronic document fulfils this requirement if has an extended electronic signature incorporated, attached or logically associated with it, based on a qualified certificate and generated by a secure signature-creation device.

If one of the parties does not acknowledge the document or the signature, the Court shall always order that the verification be made by specialized technical expertise and an expert or specialist appointed to the case shall request qualified certificates as well as any other documents necessary, according to the law, to identify the author of the document, the signatory or the holder of the certificate.

In addition, the party invoking before the court an extended electronic signature must prove that it meets the following conditions:

•is uniquely related to the signatory;

•ensures the identification of the signatory;

•it is created by means controlled exclusively by the signatory;

•it is linked to data in electronic form, to which it relates in such a way that any subsequent changes to them are identifiable.

It is important to emphasize that it establishes a legal presumption that the extended electronic signature based on a qualified certificate issued by an accredited certification service provider meets the conditions mentioned above.

Moreover, with reference to the burden of proof in case of disputes, the Romanian legislator has established that the party invoking before the court a qualified certificate must prove that the certification service provider that issued the certificate meets the legal conditions provided in art. 20. Also, in this case, there is a legal presumption that concerns the accredited certification service provider, in the sense that it meets the conditions provided in art. 20 of Law no. 455/2001.

It is noteworthy that one of the most important advantages of the electronic signature, especially in the current pandemic, is the fact that the electronic signature can be used for signing documents both in relation to some state institutions and authorities (ANAF, ONRC, ANCPI, CNAS, ITM , ANOFM, SEAP, CSSP, M. Of., BVB,

UAT, etc.), as well as in relation to persons under private law (natural or legal persons in office or in insolvency). Additionally, as the specialized literature claims, the electronic signature ensures the authenticity of the person who signed the document, respectively the integrity of the document, *ie* the fact that it was not modified after signing. The signature can only be used by its owner, being forbidden to borrow and alienate the kit [containing 3 components: a device (token) that has an associated PIN code to be accessed, a qualified digital certificate and an application / software program)] to another person[11].

Signing documents (contracts, tax returns, invoices, etc.) is done safely [5], remotely, efficiently, quickly, saving time and money.

As far as offences are concerned, the provisions of art. 44 of Law no. 455/2001 provide that it is an offence, if, according to the law, it is not a crime , and is sanctioned with a fine from 500 lei to 10,000 lei, the act of the certification service provider, who:

- omits to make the notification provided in art. 13 para. (1) , *i.e.* it is the obligation of the persons who intend to provide certification services to notify the regulatory and supervisory authority specialized in this field 30 days before the start of activities related to the certification of electronic signatures ;
- omits to inform the regulatory and supervisory authority specialized in the field on the security and certification procedures used, under the conditions and in compliance with the terms provided in art. 13;
- fails to fulfil with its obligation to facilitate the exercise of control by the staff of the regulatory and supervisory authority in the field, especially designated for this purpose;
- performs the transfer of activities related to the certification of electronic signatures without complying with the applicable legal provisions .

It is also an offence and is sanctioned with a fine from 1,000 lei to 25,000 lei, the act of the certification service provider who, *inter alia*:

- does not provide to the persons requesting a certificate or, as the case may be, to a third party who holds such certificate, the obligatory information provided in art. 14 para. (3) or does not provide all such information or provides inaccurate information ;
- breaches the obligations regarding the processing of personal data;
- issue certificates, presented to holders as qualified, which do not contain all mandatory particulars ;
- issues qualified certificates that contain inaccurate information , information that is contrary to law, morals or public order, or information whose accuracy has not been verified under the law or issues qualified certificates without verifying the identity of the applicant, under the law ;
- fails to take measures to ensure confidentiality during the process of generating signature-creation data, if the certification-service-provider generates such data;
- does not keep all the information regarding a qualified certificate for a period of at least 5 years from the date of expiry of the certificate;
- stores, reproduces or discloses to third parties the data used to create an electronic signature, except for when the signatory so requests, if the provider issues qualified certificates;

[11] Andreea-Maria Maxim, *Brief considerations on electronic signature*, published on 16th of Aprilie 2020, available on: https://www.juridice.ro/680239/scurte-consideratii-privind-semnatura-electronica.html, accessed 6th of November 2020.

- stores qualified certificates in a form that does not comply with legal requirements;
- uses electronic signature creation devices which do not meet the conditions provided by law , if the certification service provider issues qualified certificates;
- does not suspend or revoke the certificates issued, in cases where suspension or revocation is mandatory, or revokes them in violation of the legal deadline;
- continues to carry out activities related to the certification of electronic signatures in the event that the specialized regulatory and supervisory authority in the field has ordered the suspension or cessation of the activity of the certification service provider;
- issues certificates or carries out other activities related to the certification of electronic signatures, using, without being entitled, the status of accredited certification service provider, by presenting a distinctive mention referring to this quality or by any other means.

Finally , the violation, by the approval agency, of the obligation to facilitate the exercise of powers of control by the staff of the regulatory and supervisory authority in the field, especially designated for this purpose, constitutes an offense and is punishable by a fine of 1,500 lei to 25,000 lei.

2.3. The technical and methodological norms for the application of Law no. 455/2001

The technical and methodological norms for the application of Law no. 455/2001 on the electronic signature of December 13, 2001 ("*Norms for the application of Law no. 455/2001* " or " *Technical norms* ") were published in the Official Gazette, Part I no. 847 of December 28, 2001, the variant currently in force including the amendments brought by Decision no. 2303/2004 on the amendment of normative acts in the field of information technology (" *HG no. 2303/2004* ").

The technical norms establish, *ab initio* , their recipients, namely: any person, natural or legal, located in Romania, in relation to the fact that this category can benefit from certification services in order to use the electronic signature in the sense of art. 4 of Law no. 455/2001 regarding the electronic signature.

From the beginning, the technical norms establish and expressly defines the meaning of certain terms used, in order to avoid potential misunderstandings.

With regard to the legal mechanism for regulation and supervision, the Technical Rules provide that the regulatory and supervisory authority generates or acquires a functional pair of private key-public key pair and must protect its private key, using a reliable system and taking the necessary precautions to prevent the loss, disclosure, alteration or unauthorized use of its private key. In this respect, it is noteworthy that in no way can the private key be deducted from its paired public key.

The same authority has the obligation to manage the Register of certification service providers (hereinafter referred to as the "*Register*") , which Law no. 455/2001 refers to.

Reporting to the Registry, the authority has the exclusive task of updating it, this update having as object all changes in the status of the provider, namely: accreditation, end of the accreditation period, suspension, additions to the types of certificates offered.

With regard to voluntary accreditation, the Technical Rules expressly provide that providers wishing to operate as accredited providers must apply for accreditation from the authority, meaning that the applicant provider must meet all the conditions necessary for the issuance of qualified

certificates and use secure electronic signature-generating devices approved by an approval agency agreed by the Authority.

Verifications are made both on the statements contained in the documentation submitted to the authority and on the concordance between the systems, procedures and practices stated and those that actually exist.

The duration of the accreditation is 3 years and can be renewed, through a procedure similar to the one provided for obtaining the accreditation.

At the same time, it is important to note that, from the perspective of speed, the Technical Rules expressly provide that the duration of verification of the information present in the application and the issuance of the certificate may not exceed, as appropriate: one working day for simple certificates; respectively 5 working days for qualified certificates. These time limits shall be calculated from the time the concerned provider receives all the information required for this purpose.

It is particularly important that the certification service provider cannot issue a certificate without the express consent of the one on whose behalf it is issued. The validity period of a certificate is maximum 1 year from the date of communication to the customer.

3. Conclusions

The development of a trustworthy context is a mandatory condition taking into account the possible risks that may arise when conducting online electronic activities: identification of parties, data transmission, security of payment methods, legislation still insufficiently clear on consumer protection.

Any economic activity is prone to fraud, therefore issues arise when it is found that resolving these conflicts requires increased attention in the field of electronic trade.

It is about, first of all, the huge volume of transactions that take place every day on the Internet, but also the fact that most transactions take place between entities that do not know each other beforehand and probably will not have contacts after completing the contractual obligations in which they are currently involved.

Moreover, these are transactions between entities under different jurisdictions. Here is the most important issue that needs to be resolved legally. The confidence and future of e-commerce in high security conditions depends on the evolution of the electronic signature.

For these reasons, the electronic signature is a way of authenticating the content of electronic documents and will play a decisive role in e-commerce-specific transactions.

In recent years, in developed countries, paper has become only a medium for presenting information and not for archiving or transport. These last two functions have been taken over by computers and their interconnection networks.

That is why a series of solutions were needed to replace the seals, stamps and holograph signatures from the classic documents with their digital variants, based on the classical cryptography and using public keys.

Improving the security of information systems must be an important goal of any organization. However, it must be taken into account the assurance of a good balance between the related costs and the actual advantages obtained.

The measures must discourage attempts at unauthorized access, make them more expensive than legally gaining access to these programs and data.

To ensure information security that are critical for businesses or business

organizations, each company must develop an IT security policy, to ensure that when something happens, there are processes to resolve the situation.

This is an endless process, a process for the development of an IT security policy is like a circle, which always returns to the starting point to increase security: new technologies and ideas call for a continuous update of the IT security policy.

Information security is an issue that is becoming more stringent and current with the development of networks and computer systems industry. One of the basic methods of ensuring information security is the cryptographic method.

Therefore, there are, theoretically, multitudes of types of concrete advanced signatures, as many technologies that meet the four conditions of art. 26 of Regulation (EU) no. 910/2014 could be identified.

Therefore, an organization that aims to accept / use the "*advanced signature*" without specifying the technology / technologies with which it is created, which it accepts / uses, will have big problems both in terms of creating electronic signatures and especially in terms of their verification.

However, Regulation (EU) no. 910/2014, regarding electronic signatures in public services, recommends the use of technology based on public keys, or, if other technologies are used, imposes clear conditions that must be met by those technologies, as we will show when we detail the formats of electronic signature.

In conclusion, the electronic signature is a personal attribute, being used to recognize the identity of a person in certain operations. Also, the electronic signature solves the problem of the person's identity and of the authenticity of the document better than the holograph signature. On the other hand, the costs and potential consequences of inaction or delayed action can be significant.

References

- Augustin Fuerea, PhD, *The European Union Handbook*, 6th Edition, Universul Juridic, Bucharest, 2016;
- Robin Mansell, *Here Comes the Revolution — the European Digital Agenda*, The Palgrave Handbook of European Media Policy, Macmillan Publishers Limited, 2014;
- Andreea-Maria Maxim, *Brief considerations on electronic signature*, published on 16th of Aprilie 2020, available on: https://www.juridice.ro/680239/scurte-consideratii-privind-semnatura-electronica.html;
- George Hari Popescu, What you need to know about the electronic signature, given that the new bulletins will contain one - legal value, recognition in other states and technical issues, published on 14th of August 2020, available on: https://www.avocatnet.ro/articol_55547/Ce-trebuie-s%C4%83-%C8%99tii-despre-semn%C4%83tura-electronic%C4%83-avand-in-vedere-c%C4%83-noile-buletine-vor-con%C8%9Bine-una-valoarea-juridic%C4%83-recunoa%C8%99terea-in-alte-state-%C8%99i-aspecte-tehnice.html;
- Ciprian Săraru, Processing of personal data A matter of principle, in General Data Protection Regulation. Comments and explanations, Hamangiu, Bucharest, 2018;
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Agenda for Europe, available at: https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX: 52010DC0245;
- Guide of good practices and legal aspects regarding the use of electronic signature in organizations, certSIGN , available on : www.certsign.ro/ghid;

- Law no. 455/2001 regarding the electronic signature, in the version republished in the Official Gazette, Part I, no. 316 of April 30, 2014, with subsequent amendments and completions, available on: https://lege5.ro/App/Document/gm4tmnjuha/legea-nr-455-2001-privind-semnatura-electronica;
- The technical and methodological norms for the application of Law no. 455/2001 regarding the electronic signature of December 13, 2001 , published in the Official Gazette, Part I no. 847 of December 28, 2001 , available on: Technical and methodological norms for the application of Law no. 455/2001 regarding the electronic signature from 13.12.2001 (lege5.ro);
- Emergency Ordinance no. 39/2020 for the completion of Law no. 455/2001 on electronic signatures , public in the Official Gazette, Part I no. 281 of April 3, 2020, available on: Emergency Ordinance no. 39/2020 for the completion of Law no. 455/2001 regarding the electronic signature (lege5.ro);
- Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC available on: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679;
- 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 Directive 1999/93 / EC, available at: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32014R0910.