

The law on electronic signatures. Application in practice of e-signing and its importance in electronic commerce

Msc. Dorina NDREKA

Department of Law, UAMD, Durrës-ALBANIA
dorinandreka@uamd.edu.al

ABSTRACT

People who do business on the Internet require security and trust. In electronic commerce and communication, you cannot be sure regarding the identity of the person with whom you are speaking. The legal framework regarding electronic commerce has created in Albania the premises for a real revolution, regarding the way in which the business is organized. The problem is that this revolution has yet to come. The focus of this article will be the electronic signature, one of the most important innovations regarding the electronic commerce. The electronic signatures are electronic data, attained through specific informatics procedures that are used for security and trust in electronic business and communications.

This article deals with the legal importance of signed documents and the debate regarding the relevance of the electronic signature, with a specific focus on the law and its practical application. The law recognizes three kinds of e-signatures: the simple electronic signature, the advanced electronic signature, and the qualified electronic signature, but only the last one is regulated by the law.

From the information attained at the National Authority on Electronic Certification, after almost three years from the approval of the law, the use of qualified electronic signature is in its first steps. This is not an astonishing fact if we take in consideration the public knowledge in Albania regarding the e-signature. Considering the electronic signature a very effective tool in the improvement of electronic commerce in Albania, but also in the development of e-government, the article makes recommendations regarding the best practical uses of e-signature in public and private sector.

INTRODUCTION

Globalization and informatization are transforming our world. In response to the relationships constructed through the computer and that, appear on them, communications and business without borders require high legal and technical standards. The stipulation of distance contracts without the physical presence of the

parties should be accompanied with security measures that produce confidence that the data sent or received are not altered, forged, copied or misused by unauthorized persons. The development of information technology and the speed of information exchange it makes possible, have determined considerable changes in the development of international trade. The economic and legal system, which was built for classical trade and cash, cannot meet the demands of today's on-line transactions. [1]

The new, digital era and the informational economics are the main causes that influence the redefinition of business strategies and the transfer from traditional economy to e-business. One of the main direct profits from the use of technology innovations is the saving of time, and time in business, is money. The increase of capital flowing through these channels of communication ought to be regulated into a legal framework, otherwise these economical transactions risked not to be considered as juridical acts. The main objective of this legal framework would be the creation of a trust environment in the society. Electronic communication includes the lack of physical presence of the parties, and the absence of a handshake, the symbol of business agreement, posing the need for alternative means in order to attain the same trust. This increasingly frequent use of new technologies for the formation, transmission, reproduction and storage of documents has prompted several states to recognize the legal validity of electronic documents and their value as evidence before the court law. With the proper legislation, e-commerce would be enforceable just like any other form of commerce. This is the reason why in the last years e-commerce legislation is expanding all over the world.

The national laws on electronic signatures are one of the ways in which this trend is reflected. At the beginning of 1999, most of the world's major industrialized nations began to adopt electronic commerce and electronic signature legislation with the goal of spreading commerce through the internet. The first law to do this was the Utah Digital Signature Act, of 1995. Similar laws were adopted in Italy and Germany in 1997. [2]

In 1999, was adopted the Framework Directive (EU Directive 1999/EC). The Albanian law no 9880, dated 25.02.2008, was based specifically on this directive, considering the aspiration of the country to become an EU Member State. All the laws have given to electronic signatures the same legal standing as the handwritten signatures, despite the fact that each country has taken its own legislative approach, regarding the signature specifications and their implementation. In e-commerce it is crucially important that internal rules be in some sort of way compatible with international rules, or other countries rules, because given the freedom of communication, most of the electronic transactions are between parties of different nationalities.

In distance contracts or other forms of juridical acts, where the parties are not present, the computer becomes an instrument that takes part directly in the process of will expression. The use of electronic signature permits to send an electronic document with e-mail, instead of faxing signed documents, scan it or even post it. The time consumed is incomparable, because electronically it is possible to finish the stipulation of the contract in just a few minutes. In the global

world, there is a greater need for guarantees on commercial transactions. The electronic signature responds to this need by providing a clear answer about the origin of electronic documents. Considering this technological and legal innovation crucial for the future development, of e-commerce, e-government and e-communication in general, this article takes, an in depth look at the legal aspects of the electronic signature.

ELECTRONIC DOCUMENTS AND THE NEW WAY OF SINGING

Every document has the scope of making something known, from Latin “docere” – ‘to let know, to teach’. It has two important components: the immaterial one, which is the intellectual component, and the material one, which is the physical support. Document in the broad sense, is every material apparition of the thought. Given that the most common tool used to carry this material presentation is the letter, usually the term, which refers to the document, is precisely the paper document.[3] The author of the document in order to give its name and authorship to the document puts his signature. The signature (from Latin: signare - to sign) is a handwritten depiction of someone's name, nickname, or initials that a person writes on documents as a proof of his identity and intent, being so the element in which is based the security and the relevance of the documents. A signed document gives full confidentiality that the declarations made in it are of the signatory, if he acknowledges the signature, because no one signs a document, which expresses the material thought of another person.

Before proceeding with other aspects of electronic signature, it is necessary to clarify the terminology used from the Albanian legislation. The Albanian dictionary defines the signature as, ‘*the name, surname, or the shortening, placed in a paper work*’. In fact, the law uses the term ‘*electronic subscription*’, which bears incongruence in terminology, comparing to its use in the traditional way. In the electronic document cannot exist any kind of scription (scripture – Latin, writing), and this scripture cannot be placed sub (sub- Latin, under). Using the same term for these two very different tools refers to their same utilization and mission that they fulfill.

Electronic documents are part of a special kind of document, which differ from paper documents. They are data in electronic form so the parties send to each other only bits (0s and 1s). The electronic document can be copied an infinite number of times, making their reliability very difficult, because individuals or businesses will think twice before entering a contract, making a payment, sending a confidential message, which can be altered or copied. The need to arrange even in cyberspace an instrument capable of performing functions, similar to those traditionally accomplished by the subscriptions attached to a paper document is the foundation of the research made for the electronic signature.

Electronic signatures are present in all aspects of our everyday life. Multitudes of our actions are related to some kind of numerical code, or other forms of identifications. You need a PIN code to use a Bank ATM, e-banking services, personal computer, e-mail, electronic declaration of taxes, etc. The problem that

emerges in these cases is if the actions we have performed during these activities are part of a juridical act and if they legally implicate us. Common law jurisdictions have recognized telegraph signatures since at the mid of the 19th century and faxed signatures since the 1980s. [4-5] A signed electronic document has the same legal validity as the equivalent paper document. [6]

The persons who signs electronically a document has full responsibility of everything it is intended in it. This is one of the main objectives of the signature, to relate the physical person with its thoughts materialized in some sort of electronic data. The signature can also serve other purposes. One of the most important is to assure the immutability of the document and to make possible the detection of every possible unauthorized alteration. In traditional contracts, this is done mainly by putting the initials in the bottom of all the pages, beside the signature at the final page. The electronic signature does not create immutable documents, because the electronic document is in essence alterable and has the ability to be duplicated infinite times. Its purpose is to make noticeable every manipulation, even with a single bit, compared with the original one signed electronically. This control is made possible without the need of complicated calligraphic expertise. In electronic transactions, this function is essential given the changeability of the electronic document. Electronic signature also identifies the signatory. In the paper world, the person who signs a document is already identified by its Identification documents.

Thus, while handwritten signatures in most cases serve merely to indicate the signer's intent, signatures in an electronic environment typically serve three critical purposes for the parties engaged in an e-commerce transaction –to identify the sender, to indicate the sender's intent, and to ensure the integrity of the document signed.[7]

The Albanian legislation on e-commerce has indirectly embraced the principle of technology neutrality, leaving space to all technologies that are capable to satisfy all the standards set by the law. In the time of speaking, the only technology capable is the PKI (Public Key Infrastructure), but in the future new technologies can be explored or invented. States should anticipate that authentication methods would change over time and avoid legislation that might impede the use of innovation or new applications. Any rules should neither demand nor prohibit the use or development of innovative authentication technologies.

The only form of electronic signature that nowadays can fulfill all the legal criteria is the one based on applied cryptography with asymmetrical keys. The cryptography refers to the study of concealing information with the use of mathematical transformations. [8] The concept of securing messages through cryptography has a long history. The Spartans and later Julius Caesar are credited with creating one of the earliest cryptographic systems. The earliest cryptography methods involved a person carving messages into wood or stone, which was then delivered to the intended individual who had the necessary means to decipher the message. [9] The cryptographic system works out through the key, which is a numerical value used by an algorithm to alter information, making that

information secure and visible only to individuals who have the corresponding key to recover the information. [10]

A major advance in cryptography occurred with the invention of asymmetrical cryptography, with the use of public-key. They are based on industry standard known as Public Key Infrastructure (PKI), which guarantees data integrity and non-repudiation of documents and transactions. The primary feature of public-key cryptography is that it removes the needs to use the same key for encryption and decryption. With public-key cryptography, keys come in pairs of matched “public” and “private” keys. The public key can be distributed in a public manner without compromising the private portion, which must be kept secret by its owner.[11] The private key used to create the signature and the public key, used to verify it, both different from each other.

If a user wants to create a signature for a document, proceeds in the following way: with the use of the hash function obtains the digital mark of the document, a file of relatively small dimensions (160 bit); afterwards this private key or *signature code* is used to encipher the digital mark, the result of this codification is the signature. Furthermore, it is one-way, not invertible, that means that from the same private key it is impossible to obtain again the original text without the signature. The electronic signature obtained depends from the digital mark of the document therefore, it depends on the document in question, meaning that the electronic signature is different every time. With the sender's public key, or *signature controlling code*, it is possible to decrypt the document and verify its authenticity and if the document has been submitted to changes after the addition of the signature. The signature device is the electronic mechanism, programmed to guard the private keys and to generate electronic signature. This could be a smart card protected by a secret code, like a PIN. To all this it can be added biometric identification devices, which are capable of ensuring even more the correspondence between the keys owner and different users of the system.[12]

ELECTRONIC SIGNATURE LEGAL AND PRACTICAL BOUNDARIES

The laws that regulate in Albania the framework for the development of electronic commerce are the law on Electronic Signature (2008); the law on Electronic Communication (2008); the law on Electronic Commerce (2009) and the law on Electronic Documents (2010).

The law defines electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. In order to fulfill the legal criteria the electronic signature must meet the following requirements:

To be uniquely linked to the signatory;

To be capable of identifying the signatory;

To be created using means that the signatory can maintain under his sole control;

To be linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[13]

Qualified electronic signatures are advanced signatures, which are based on qualified certificates, provided by Certification Service Provider, legally known as such. This is the kind of electronic signature which is regulated by the law and which is supervised and controlled by the National Authority for Electronic Certification. The other kinds of electronic signatures can be traded and used, by anyone without the need to register or to have a legal control on their usage. Electronic signatures involve the use of certificates to establish identity, and certificates are issued by a trusted third party. A qualified certificate links the data used to verify the signature to a certain person. It has to contain certain information and has to be issued by a certification service provider. [13] The law on Electronic Signature, regulates the way in which Certification Service Providers operate.

Another specific feature of the advanced signature is that it is safe only during its validity period, and when this period is finished the digital signature is no longer safe and the Certification Authority will not warrant it any longer. The users have to be careful regarding the period in which the signature is safe, afterward the documents signed with it are not legally validated and have no juridical value. The electronic signature must be updated which means the receipt of a completely new key. It is important to emphasize that the signature continues to be an electronic signature, but it is not regulated by the law.

To form a contract electronically is as easy as just a click, and an electronic contract may be formed in a variety of ways. The fundamental principle in contractual law is that contracts can be stipulated with every free will demonstration, but for some specific contracts, the law requires that the will of the parties must be expressed in writing. Some of the contracts, which according to the Albanian Civil Code must be in writing, are, - pawn, bail, franchising, security contract, etc. Electronic signatures make possible that the same electronic document is signed by more than one person. Every party participating in the legal act signs the electronic message and then sends it to the other parties.

The problem with the stipulation of the contracts electronically is the difficulty to prove the existence of an electronic contract in the event of a dispute between the parties. They need to have some level of comfort that they can prevent the sender from denying that he sent the communication, or claim that the contents of the communication is altered. The existence of insecurity regarding the forgery of documents is foremost related to paper documents. The number of contracts, wills, certificates, authorizations, proxies, etc, that are object of forgery is vast. In order to solve this problem one of the main objectives of the law was precisely to establish proper authentication techniques in accordance with the risk of unenforceability. This was the reason why the EU directive determines that one of the obligations of the Member States is to ensure that advanced electronic signatures: a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature; and b) are admissible as evidence in legal proceedings. [14] This legal ability is known as nonrepudiation and it is guaranteed even by the Albanian legislation. [6]

The signatory is not the person who creates the electronic signature. He is the owner of the device that creates the signature. This feature of the electronic

signature can result problematic. Being just an electronic device, the signature can be used by unauthorized persons to sign documents without the knowledge of the owner. In the case of qualified electronic signature, the proof of the counterfeiting of the signature is virtually impossible. The signature lives the same mark regardless of who uses it. In order to prove illegal usage, the owner of the signature certification must present other indirect proofs. Furthermore, the signatory has the obligation to keep the device of the electronic signature safe to avoid unauthorized use otherwise, he will be responsible for all the damages that may come.

The actual Code of Civil Procedure differently from the previous Code speaks of paperwork and not of documents. [15-16] In fact, the documents are only one of the ways in which may appear a document. Other forms are parchment, papyrus, boards, leatherwork, etc, legally speaking these all are documents, but not paperwork. In the future, there might be problems regarding the ways in which the electronic documents will be treated as proofs before the courts. The authentication of the paper copy of the electronic document is done by the authorized persons in public institutions, or by the public notary. The rules and procedures will be determined with a Directive of the Ministry of Justice. This Directive has not been issued yet.

The law on electronic signature, article 7, determines the exceptions from the use of electronic signature. The first group of juridical acts in which it cannot be used e-signing, consists of familiar and heritage law acts. Another important group excluded, includes all those juridical acts, which according to the law are performed with the inclusion of the public notary or authorization from the court law. The last reserve is related with the bail probation in criminal procedure. These exceptions are easily understood when we look through all juridical acts in which the parties must be physically present. Even if this article in the first glance restricts the use of electronic signature, it helps the up growth of the public trust in this legal institution.

CONCLUSION

It is impossible to foresee what the future holds for the development of humanity in the years to come. This is especially true regarding the development of new technologies and communication. Despite the difficulties that electronic documents and signatures are having in being accepted by the society and the business, in the near future they will certainly have a wide usage. The increase of the persons that use Internet and those who comprehend technology communication and the Web, are some of the reasons that will influence this development. Within the next decades e-business will transform into a necessary and integral part of handling business and no company will be able to imagine doing their business, and no man their everyday life. [1]

One of the main objectives of the electronic signature legislation is to help the growth of electronic commerce. This becomes even more obvious if we scrutinize all the legislation regarding to electronic communication and commerce. The law has given a wide space to the usage of electronic signature. The practical

application will play a key role in highlighting the positive contributions and the negative ones.

As it is shown above, the most practical advantage of electronic signature is that it can be used everywhere and anywhere. Digital and electronic developments gives us the possibilities to enable people to get involved more easily in the activities of democratic institutions and the governance in general. Their implementation in the communication with the public administration will manage office to stay open 24 hours, during all week. This helps the public to get more information, increases the administration efficiency, productivity, and the public satisfaction. It also helps in cutting costs in government institutions. It is important to emphasize that the use of electronic documents and signatures is *voluntarily*. The fact that the law regulates and allows the use of electronic signature does not signify that its use is imposed by the law.

Electronic signature systems are easy to use and do not require new software or hardware. To get a certification for the electronic signature in Albania costs 15 Euro consisting in code number. The only Certification Service Provider is the Albanian Post. The validity of the signature is guaranteed for a year, and then it has to be updated. This means that the CSP will send another code for the year to follow, with the same price. Actually only Albanian Post, itself and one Business has chosen to use the certificated electronic signature. This is done only for the internal communication, between the employees. The electronic signature can be used as a tool to verify the electronic data in electronic contracts, e-banking, online procurement, electronic taxing, and in all communications with public administration. Recently in Albanian it has been discussed the option of on-line voting. It is possible to implement this innovative way of voting only with the use of electronic signature.

Often, businesses rely on other means to attempt to ensure an electronic signature is correct, including talking with the signatory directly or over the phone, before an electronic signing occurred. This is good business practice even in the paper world, as forgeries have been common there since time immemorial, but it is possible only when the parties have an ongoing business relationship. Fraud is a common issue in all signature situations, and neither type of signature (paper or electronic) provides fully effective anti-fraud protections. Biometrics data, like fingerprints, DNA, or iris scan, can provide a degree of authentication well beyond that offered by numerical or word codes. In Albania with ID cards and biometrics passports, it has been made a great progress in this direction.

Electronic legislation has guided Albania in a real revolution. In order to avoid the risk that the revolution remains only on paper, it is necessary to take immediate measures, because for the moment, the usage is very limited. At the time of speaking, the most important objective should be the diffusion of the electronic signature. Albania has to learn from other countries experience. Estonia is a story of success regarding the spreading of electronic signature. In Estonia, the tools for digital signatures have been released to the public for free. The certification validation is done at the moment the document is signed. The signer should be online and after signing the document, the system automatically gets a validity

confirmation from the competent authority. The confirmation is saved with the signed file. [17]

Informatization and electronic communication will define the future of the whole world. It will not be possible to opt-out of the new technologies, because it will mean to close ourselves to the world. Therefore, the issue in question is not if our country will be part of the future, but how will it do that. The proper implementation and enforcement in practice of the innovations of the electronic communication, including electronic signature, will help Albania in this interesting journey.

REFERENCES

- [1] Golubi , D., Golubi , Z., Simec, A. and Antoni , T., A development of e-business in Croatia, 1-8.
- [2] Laborde, C.M. and Lang, P., (2010), Electronic Signatures in International Contracts, 57,62, 69, 72.
- [3] Lamani,A.,(1962), E drejta procedurale civile e RPSH-së, Botim i Universitetit Shtetëror të Tiranës, Tiranë, 135-136, 144-152.
- [4] An early validation of electronic signatures came from the New Hampshire Supreme Court in 1869 [Howley v. Whipple, 48 N.H. 487]. Jones, S.W., (1916) A treatise on the law of telegraph and telephone companies: including electric law, Vernon Law Book, 947.
- [5] Third annual Internet Law Institute, Volume 2, (2002), 138.
- [6] Law no.10273, dated 29.04.2010, “On Electronic Documents”, article 11,12.
- [7] Smedinghoff, T.J. and Bro, R.H., Moving with change as a vehicle for advancing e-commerce, Originally published in *The John Marshall Journal of Computer and Information Law*, Vol. XVII, No.3, Spring 1999 at 723. A copy of this article is also available at: www.wildman.com/resources/articlespdf/movingwithchange.pdf.
- [8] Bishop, D., (2003), Introduction to cryptography, Jones & Bartlett Learning, 2,3.
- [9]Harris, S., (2007), Certified Information Systems Security Professional (CISSP) exam., McGraw-Hill Professional, 660.
- [10] Stewart, J.M., Tittel, E. and Chapple, M., (2008), CISSP: Certified Information Systems Security Professional Study Guide, John Wiley and Sons, 334.
- [11] Curry, I., (2001), An introduction to cryptography and digital signature, Entrust, 1-6.
- [12] Fantin, M., (2000) La firma digitale, Università degli studi di Parma.
- [13] Law no.9880, dated 25.02.2008, “On Electronic Signature”, article 3/2, 3/3, 3/4.
- [14]EU Directive 1999/93/EC, Article 5.
- [15]Law no.8116, dated 29.03.1996, “*The Code on Civil Procedure of the Republic of Albania*”, article 246-277.
- [16]Law no.6343, dated 27.06.1981, “*The Code on Civil Procedure of the Socialist Republic of Albania*”, article 28-34.
- [17]Henderson, A., “Smart Cards, Smart Identities”, in “Digital Identity Management”, Ed. Birch, D.,21.

“1st International Symposium on Computing in Informatics and Mathematics (ISCIM 2011)”

in Collaboration between EPOKA University and “Aleksandër Moisiu” University of Durrës

on June 2-4 2011, Tirana-Durrës, ALBANIA

[18]Kuner, C., Miedbrodt, A., Written Signature Requirements and Electronic Authentication: A comparative perspective, Morrison & Foerster, University of Frankfurt-am-Main.

[19] Ennis, D.P., (2004), The impact of the internet and e-commerce on international law: Jurisdiction, consumer protection & commercial arbitration.

[20] LAW NO.7850, DATED 29.07.1994, ALBANIAN CIVIL CODE.