Information Technology Applications In The Judiciary Evidence System

Florea MĂGUREANU
and
George Poptean MĂGUREANU
Faculty of Law, Romanian-American University, Bucharest, Romania

ABSTRACT

The unprecedented evolution of IT system, could not help marking its stamp on the evidence system, by using some new opportunities and possibilities of evidence, for supporting the parties' statements in the civil lawsuit.
The pre-drawn written documents reflect the truth, to a larger extent, being drawn up before the appearance of the conflict between the subjects of the legal report under judgment, whether they are on paper or on electronic support.
The written documents under private signature can be made up using any way, but, in exchange, the signature of the one who has obligations must be oleograph; it cannot be typed or lithographed or replaced by a stamp, seal etc.
Commercial contracts, which are concluded online today, meant establishing a system which could be used, with the same safety elements as the signature or writings on paper as a writing support, and thus eliminating forgery.

Evidence- the action through which a certain fact is stated to exist, the way to establish a fact which must be proved, or the result reached by using the means of evidence, the extent to which all this managed to convince the judge.

The written document- any statement on a legal document or legal fact, hand written, through typing, lithographing or printing it on paper or on any kind of material.
The electronically written document- an electronic data collection between which there are logical and functional relations and which provide letters, figures or any other characters with intelligible significance, meant to be read through a soft, or any other similar procedure;
The electronic signature- the electronically made signature, which is attached or logically associated with electronic data, and which serves as a means of identification.

CONTENTS

By using some new opportunities and possibilities of evidence, for supporting the parties' statements in the civil lawsuit, the IT system by its unprecedented evolution, marked its stamp on the legal evidence system as well.
Among the means of evidence which make up the evidence system the written documents have a special importance[1].

It is an unquestionable fact the practical utility of making up the pre-drawn written documents, the fact that theses reflect the truth, to a larger extent, being drawn before the appearance of the

[1] For a detailed examination on the written documents, see: F. Măgureanu, The Written Documents Means of Evidence in the Civil Lawsuit, the 2nd revised and improved edition, ALL-BECK publishing house, Bucharest, 2003

conflict between the subjects of the legal report under judgment.

According to the traditional norms, the written document under private signature does not require a special form, in exchange, the signature of the one who has obligations must be oleograph, not being able to be typed or lithographed, or replaced by a stamp, seal etc.

The numerous commercial transactions, public service operations which happen today online have implied establishing a system which could be used, with the same safety elements as the signature or the written documents made on paper as a writing support.

On the communitarian level, there is a diversity of juridical norms, which regulate the electronic signature, fact which led to the European Commission's initiative to homogenize the incidental dispositions in the member states' legislation in order to eliminate all legislation[2] differences. In this context, the European Parliament and Ministers Council adopted, on 13th December 1999, the directive no. 1999/93/CE regarding a communitarian framework for the electronic signature[3].

The directive has the goal to create a homogenous juridical framework for using electronic signatures in the European Community, the guarantee of a good functioning of the internal market in the domain of the respective signatures, also establishing the criteria which constitute the basis of juridical identification of the electronic signature and its certifying services, as well as the assimilation of the electronic signature with the oleograph signature.

The homogenization of the Romanian legislation with that of the European Union, dictated the adoption of a new law in our country as well, law which should establish the juridical regime of the electronic signature and the electronic written documents, as well as the conditions of providing certifying service of the electronic signatures[4].

The respective law comprises:

[1] the electronic data are information representations under a conventional form proper to creating, processing, sending, receiving or stocking it through electronic means;

[2] an electronic written document represents a collection of electronic data between which there are logical and functional relationships and which provide letters, figures or any other characters with intelligible significance, meant to be read through a soft or any other similar procedure;

- the electronic signature represents electronic data, which are attached or logically associated with other electronic data and which serve as a means of identification.

According to the provisions of art. 5 of Law 455/2001, the electronic written document, to which they incorporated, attached or logically associated an extended electronic signature, based on a certificate classified as non-adjourned or irrevocable at the moment, and generated with the help of a safety device of creating the electronic signature, it is assimilated, regarding its conditions and effects, with the written document under private signature.

In the juridical literature they have raised the issue of the value and effects of these written documents as compared to the classical written documents. However, the respective law provided for art. 6 that the electronic written document to which they incorporated, attached or logically associated an electronic signature, certified by the one which it opposes, has the same effect as the authentic document between the ones who sign it and between the ones who represent

[2] See the European Commission Proposal regarding the communitarian framework for electronic signatures, published in the European Community Official Journal, series C, no. 325 of 23th October 1998, p. 5-12.

[3] The directive was published in the European Community Official Journal, series L, no. 13 of 19 January 2000, p. 12-20.

[4] See Law no. 455/2001 regarding the electronic signature, published in the Romanian Official Monitor, Part I, no. 429 of 31st July 2001 and the Technical and Methodological Norms for the application of Law no. 455/2001, , published in the Romanian Official Monitor, Part I, no. 847 of 28th December 2001.

their rights and, of course, it goes without saying, the same value as well.

In the cases where, according to law, the written form is required as a term of evidence or validity of a juridical document, an electronic written document meets this requirement if they incorporated, attached or logically associated an extended electronic signature, based on a qualified certificate and generated through a safety device of creating a signature.

The electronic written documents, as compared to the traditional written documents, do not have a visual representation except the moment the receiver checks them, using specific methods, the conformity of the signature, respectively the authenticity, integrity and confidentiality of the document contents as well as the identity of the signer. Also a great advantage represents the fact that the digital support (diskette, CD, etc.), is much more durable than paper, the accountancy and the possibilities to archive are totally superior, and the electronic language became universal, eliminating the difficulties of speech, translation and interpretation.

However, the signature represents a basic element used as a means of evidence, the evidence of its authenticity, the guarantee that it comes from the one who states that the facts mentioned in writing belong to him/her.

According to the provisions of art. 4 point 3 and 4 of the law "the electronic signature represents electronic data, which are attached or logically associated with other electronic data and which serve as a method of identification", and "the extended electronic signature represents that electronic signature which cumulatively meets the following terms:

a) it is uniquely related to the signer;
b) it ensures the signer's identity
c) it is created through means exclusively controlled by the signer;
d) it is related to the electronic data, to which they refer to so any subsequent alteration of these data can be identified.

The main objective of the respective law represents the identification and certification of the consent of the author of the electronic written document and the insurance of all the reliability terms and of the security system based on the electronic signature.

For ensuring the viability terms of the electronic signature, they need secured devices of creating and checking a signature and a valid certificate from the certifying services provider, the lack of the provider leading to the impossibility of assimilating the electronic written document under private signature (art. 5 of the law)[5].

Art. 4 point 7 of the law stipulates the necessity of using a secured device (configured hardware and/or software) of data implementation for creating the electronic signature, and in point 8 they mention the terms that the electronic signature should meet:

a) the data for creating a signature, used for generating a signature, so that these data could appear only once and their confidentiality could be secured;
b) the data for creating a signature, used for generating the signature so that these data could not be deduced;
c) the signature should be really secured against forgery through technical means available at the moment of generating it;
d) the data for creating a signature could be protected against using them by unauthorized persons;
e) they should not alter the electronic data, which must be signed, and not to make their presentation difficult to the signer before finishing the signing process.

According to law, the data for checking an electronic signature represent the electronic

[5] Also see F. Măgureanu, The Electronic Signature. Its Confirmation as a Means of Evidence, The Commercial Law Magazine no. 11/2003, p. 137-141.

data, such as public cryptographic codes or keys, which are used to check an electronic signature.

To establish the identity of the person who the electronic signature belongs to, they need a certificate which represents an electronic data collection, which certifies the connection between the data for checking an electronic signature and a person, validating the identity of that person and which is issued by a certifying service. According to law, any person, Romanian or foreign, who issues certificates or who provides other services regarding the electronic signature must keep the information provided secret (art 15 of the law)[6].

Consequently, the process of creating an electronic signature implies using a "hash-code function", getting the document stamp and the application of a private key over the respective stamp, "the private key" being a unique digital code, created through specialized hardware and/or software devices.

The certificate represents a collection of electronic data which certify the relationship between the data for checking an electronic signature and a person, confirming the identity of that person (art. 4 point 11 of the law), and it must contain the following technical elements:

a) mentioning the fact that the certificate was delivered with the title of qualified certificate;
b) the identification data of the certifying service provider, as well as his/her citizenship, in case of natural persons, respectively their nationality, in case of legal persons;
c) the name of the signer or his/her pseudonym, identified as such, as well as other specific attributes of the signer, if they are relevant, depending on the purpose for the issue of the qualified certificate;
d) the identification personal code of the signer;
e) the data of checking a signature, which correspond to the data of creating a signature under the exclusive control of the signer;
f) mentioning the beginning and the ending of the validity period of the qualified certificate;
g) the identification code of the qualified certificate;
h) the extended electronic signature of the certifying service provider who issues the qualified certificate;
i) if the case, the limits of using the qualified certificate or the value limits of the operations for which it can be used;
j) any other information established by the regulating and specialized surveillance in this domain (art. 18 of the law).

To ensure the unique identification, each signer is provided with a personal code by the certifying service provider.

In case there are circumstances which imply discussing the certificate validity, according to the provisions of art. 43 of the law, the certificate holders are at once obliged to ask for their revocation, when:

a) they have lost the data for creating an electronic signature;
b) they have reasons to believe that the data for creating an electronic signature are available to an unauthorized third person;
c) the essential information in the certificate are no longer valid.

In the juridical literature they suggested that although law starts from a principle according to which the private key holder is the author of the electronic written document, it can be considered that he/she does not provide value to an absolute hypothesis on the signer[7]'s identity, a third person holding "the private key", who can sign the electronic message instead of its legal holder, through confirmation of the extended electronic signature. Thus it was

[6] Also see Law no. 676/2001 regarding processing confidential data and private life protection in telecommunication, published in the Romanian Official Monitor, Part I no. 800 of 14 December 2001 and Law no. 677/2001 for persons' protection regarding personal data processing and the free traffic of these data, published in the Romanian Official Monitor, Part I no. 790 of 12 December 2001.

[7] T.G. SAVA- The Legal Trust of the Electronic Signature, The Commercial Law Magazine, no. 7-8/2002, p. 226-230.

concluded that a trustee can sign within the limits of the trust awarded, instead of "the private key holder".

They searched for and, to a large extent, they succeeded that the person's identity be included in a digital certificate, a secured electronic code, which can be identified only by the holder of a decoding key and which can offer sufficient security elements, which could ensure the certification of the message origin, integrity and confidentiality.

According to the general principal that the value of the means of evidence must be freely judged by the court, the electronic signature does not have a pre-established value, either, there is the possibility of using "the private key" without permission, either by the certifying service provider or any persons who can illegally hold it. To fight forgery and to give the electronic signature a high value, according to the provisions of art. 23 letter d) of the Methodological Norms, the signer has the obligation to protect "the private key" against theft, damages, alterations of the content or compromise.

Until confirmation of the electronic signature law, in the juridical literature, it was justly stated that the electronic recordings can be considered the beginning of the written evidence, being able to be used as means of evidence only corroborated with other means of evidence, because these do not contain the original signature of the issuer[8].

Although we also had a similar opinion, considering this aspect, because "Civil procedure code does not offer a legal framework for these (electronic) means of evidence, the judge would consider them very carefully…"[9], today in terms of Law no. 455/2001, of the international regulations and of the practice in the domain, we believe that if the electronic signature meets the security terms, it can be assimilated to the oleograph signature, the electronic written document can be, in its turn, assimilated to that under private signature and as a result, the acknowledgement of a similar force of evidence.

The electronic written document, to which they incorporated or associated an electronic signature, but this is not an extended electronic signature or is not based on a qualified certificate or it is not made up with the help of a secured device of generating a signature, it can be assimilated, as far as its terms and effects are concerned, with the beginning of the written evidence (art. 5 of Law no. 455/2001) and it can be completed with other means of evidence to make the proof of the respective legal report.

Including the electronic written document among the other means of evidence does not automatically lead to assimilating the two categories of signatures- oleograph and electronic; the electronic signature will produce its effect only when it has sufficient guarantees able to certify the integrity of the transmitted message and its author's consent.

In the end of our approach, we believe that the problem they raise regarding the electronic signature, is not whether it can be received as a means of evidence in the civil or criminal process or nor, but establishing a legal framework, so it cannot be questioned by the one it opposes, so it could be used under a form which could enable automatic reading and processing by the interested subjects.

It is also required that juridical and technical norms should be completed, norms that are necessary to the good functioning of the entire set regarding the electronic signature and to the insurance of the information security for eliminating forgery and for a high confidence of the people in the judiciary system in this technical and efficient means of evidence.

REFERENCES

[1] The European Commission Proposal regarding a communitarian framework for electronic signatures, published in the Official Journal of the European Communities, series C, no. 325 of 23 October 1998.

8 In this respect see ST.D.CĂRPENARU-Romanian Commercial Law, 2nd edition, ALL-BECK publishing house, Bucharest, 2000, p. 377.

9 See F. MĂGUREANU-The Written Documents, Means of Evidence in the Civil Lawsuit, 2nd ed. ALL-BECK publishing house, Bucharest, 1998, p. 147.

[2] Law no. 455/2001 regarding the electronic signature, published in the Romanian Official Monitor, Part I, no. 429 of 31st July 2001 and the Technical and Methodological Norms for the application of Law no. 455/2001, published in the Romanian Official Monitor, Part I, no. 847 of 28th December 2001.
[3] Law no. 676/2001 regarding the processing of personal data and private life protection in the telecommunications sector, published in the Romanian Official Monitor, Part I, no. 800 of 14th December 2001.
[4] Law no. 677/2001 for the protection of persons regarding the processing of personal data and the free traffic of these data, published in the Romanian Official Monitor, Part I, no. 790 of 12th December 2001.
[5] ST.D.CĂRPENARU-Romanian Commercial Law, 2nd edition, ALL-BECK publishing house, Bucharest, 2000.
[6] F. MĂGUREANU-The Written Documents, Means of Evidence in the Civil Lawsuit, 2nd ed. ALL-BECK publishing house, Bucharest, 1998.
[7] F. Măgureanu, The Electronic Signature. Its Confirmation as a Means of Evidence, The Commercial Law Magazine no. 11/2003
[8] T.G. SAVA- The Legal Trust of the Electronic Signature, The Commercial Law Magazine, no. 7-8/2002.