THE ADVANTAGES OF WRITS AND ELECTRONIC SIGNATURE IN NATIONAL AND INTERNATIONAL TRANSACTIONS

Florea Măgureanu[1]
George Măgureanu[2]

Abstract

Ever increased use of the PC has engendered a series of issues in commercial and civil matters, in general, because many legal provisions imply the existence of writs, of copies signed and authenticated. It is undoubtedly obvious the practical use of drawing up pre-conflict writs, fact which reflects the truth, to a great extent, being drawn up before the conflict between the subjects of the legal report under judgment might arise. Given the major importance of the evidence in clarifying the factual data, the law regulates in detail the procedure of managing the evidence. This represents a guarantee of the right to parties 'defense. The international system has also influenced the evidentiary system, by using new opportunities and possibilities of giving evidence for supporting the parties' allegations in the civil lawsuit.

Keywords: Evidence, means of giving evidence, evidentiary system, informational system, possibilities of giving evidence, writ, electronic writ, electronic signature, national commercial transactions, international commercial transactions, secured device for creating digital signature, certification elements.

Contents

Electronic writ, to which they incorporated, attached or logically assigned an electronic signature, based on an unsuspended or irrevocable certificate at that time and created with the help of a secured device for creating a digital signature, has become a frequently used method in international relations, so that the legal regime of the electronic signature and the electronic writs as well as the terms of providing services of certifying digital signatures, was to be regulated by domestic legal norms[3].

The multitude of national or international commercial transactions could not be performed nowadays with such a great efficiency without the help of informatics technical tools, without an electronic signature confirming the agreement of the parties, which may enable the parties to certify the conventions concluded even if they are not present and the negotiations also take place with the help of electronic devices.

The actions in the area of public services which take place nowadays through the cyberspace have triggered the issue of setting up a system which may be used, with the same elements of certification as the signature or writs drawn up on paper as a writing support by the person who writes or signs being present at the place where these actions occur.

---

[1] Ph.D., professor at the Romanian American University, Bucharest, Romania
[2] Ph.D., lect. at the Romanian American University, Bucharest, Romania

[3] Also see Law no. 455/2001 regarding the electronic signature, published in Official Journal of Romania, Part I, no. 429 of 31st July 2001 and Technical and methodological norms for the application of Law no. 455/2001, published in the Official Journal of Romania, Part I, no. 847 of 28th December 2001.

The rapid development of the informational system could not help influencing the evidentiary system, by using new opportunities and possibilities of giving evidence, for supporting the allegations made by the parties when there occur conflicts which may be solved amiably and the partners are forced to prove their allegations before the court of before the arbitration panel.
It is undoubtedly obvious the practical use of drawing up pre-conflict writs, fact which reflects the truth, to a great extent, being drawn up before the conflict between the subjects of the legal report under judgment might arise.

According to traditional norms, the writ under private signature does not require a specific form, but the signature of the obligor shall be holographic, as it cannot be typewritten or lithographic or replaceable with a stamp or a seal etc.
On the communitarian level there is a diversity of legal norms which regulate digital signature, fact which has led to the initiative of the European Commission for complying with the incidental dispositions in the legislation of member states to level all legislative differences[1]. Within this context, the European Parliament and the Council of Ministers, on 13rd December 1999, direction no. 1999/93/CE regarding a communitarian framework for the electronic signature[2].
The direction focuses on creating a legal harmonized framework for using electronic signatures within European Community, the guarantee of a functioning domestic market in the area of digital signatures, establishing the criteria which underlie the legal validity of the electronic signature and its certification services as well as its equivalence with the holographic signature.
The signature represents a basic element of the writ used as a means of giving evidence[3], the proof of its authenticity, the guarantee that it comes from the person who states that the allegations in the writ are made by him/her.
The electronic writs, unlike traditional writs, have just a visual representation only when the consignee checks them up, using specific methods, conformity of the signature, i.e. its authenticity, the integrity and confidentiality of the document contents as well as the identity of the signee. A great advantage also represents the fact that the digital support (floppy disk, CD, DVD etc.), is far more resilient than paper, the archiving accountability and possibilities are obviously better and the electronic language has become universal, eliminating the difficulties of speech, translation and interpretation.
According to article 4 point 3 and 4 of the law „digital signature represents electronic data, which are attached or logically associated with other digital data and which serve as method of identification", and „extended digital signature represents the digital signature which fulfils, on the whole, the following terms:

---

[1] See 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 23rd October 1998, p. 5-12.
[2] The Direction was published in the Official Journal of the European Communities, series L, no. 13 of 19th January 2000, p. 12-20.
[3] For a detailed examination concerning the evidence, see: M. Eliescu, Curs de drept civil, Teoria generală a probelor, Bucharest Universit, 1950-1951,y A. Ionaşcu, Probele în procesul civil, Ed. Ştiinţifică, Bucharest, 1969; E. Mihuleac, Sistemul probator în procesul civil, Ed. Academiei, Bucharest, 1970.

a) it is uniquely attributed to the signee;
b) it ensures the identity of the signee;
c) it is created by means exclusively monitored by the signee;
d) it is related to the digital data, to which it refers to so that any subsequent change to these data may be identified.

The main objective of the above-mentioned law represents the identification and conformity of the agreement of the electronic writ author and ensuring all the conditions of feasibility and of the security system based on the electronic signature.

In order to ensure the validity requirements of the digital signature, special secured devices are needed for creating and checking the signature and a valid certificate from the certification services provider, otherwise its absence might lead to the impossibility of authenticating the electronic writ with the writ under private signature (art. 5 of the law).

Article 4 point 7 of the law provides the necessity of using a secured device (configured hardware and/or software) for implementing data with a view to creating a digital signature, and in point 8 there are provided the terms this device has to fulfill:
a) data for creating this signature, which might appear just one time and its confidentiality might be ensured;
b) data for creating this signature, which cannot be duplicated;
c) this signature should be protected against forgery through the available technical means at the time of it being created;
d) data for creating this signature might be effectively protected by the signee against these data being used by unauthorized persons;
e) electronic data should not be modified, the data which have to be signed and these data should not prevent from their being presented to the signee before finalizing the signatory process;

On the basis of this law, the data for checking the electronic signature represent electronic data, like codes of public encrypted keys, which are used to check the digital signature.

In order to establish the identity of the person the electronic signature comes from, there has to be a certificate representing a collection of electronic data which may certify the connection between the data for checking the digital signature and the person, certifying the identity of that person and which is delivered by a certification service. According to the law, the provider of the certification service represents any person, Romanian or foreign, who deliver certificates or provide other services related to the electronic signature, this respective person being obliged to keep the information entrusted secret (article 15 of the law)[1].

[1] Also see Law no. 676/2001 regarding personal data processing and private life protection within the telecommunication area, published in the Official Journal of Romania, Part I no. 800 of 14th December 2001 and Law no. 677/2001 for the protection of persons concerning personal data processing and the free circulation of these data, published in the Official Journal of Romania, Part I no. 790 of 12th December 2001.

As a result, the mechanism of creating the electronic signature consists in applying a „hash-code" function, obtaining the print of the document and applying a private key over the respective print, „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 connection between the data of checking up the digital signature and a person, authenticating the identity of this person (art. 4 point 11 of the law) and which should contain the following technical elements:
a) mentioning the fact that the certificate was delivered as a qualified certificate;
b) the data for identifying the provider of the certification services, as well as his/her citizenship, in case of natural persons, respectively his/her nationality, in case of legal persons;
c) the name of the signee and his/her pseudonym, identified as such, as well as other specific characteristics of the signee, if relevant, according to the purpose for which the qualified certificate is delivered;
d) personal identification code of the signee;
e) data for checking up the signature, which correspond to the data of creating the signature exclusively under the control of the signee;
f) specifying the beginning and the ending of the validity period for the qualified certificate;
g) the identification code of the qualified certificate;
h) the extended electronic signature of the certification service provider who deliver the qualified certificate;
i) if necessary, the limits of using the qualified certificate or the value limits of the operations for which is used;
j) any other information established by the authority for regulation and specialized surveillance in the area (article 18 of the law).

In order to ensure unique identification, each signee will be assigned a personal code by the certification service provider.

In the legal literature of the area, it was considered that although law starts from the principle according to which the owner of the private key is the author of the electronic writ, he/she may be considered not to confer, by authenticating the validity of the extended electronic signature, value to an absolute allegation on the identity of the signee[1], a third party owner of the „private key" being able to sign the electronic message on behalf of its legitimate owner. It was thus concluded that a assignee can sign, within the limit of the mandate entrusted, on behalf of the holder of the „private key".

They have tried to achieve and, to a great extent, they have succeeded to include the identity of the person in a digital certificate, a secured electronic code, which may be authenticated only by the holder of the deciphering key and which might provide

[1] T.G. SAVA – Consacrarea legală a semnăturii electronice, Revista de Drept Comercial, nr. 7-8/2002, p. 226-230.

sufficient secured elements to ensure the certification of the message origin, its integrity and its confidentiality.

According to the general principal that value of the means of giving evidence should be up to the free decision of the court[1], the electronic signature does not have pre-established value either, there is the possibility of using without any right „the private key", either by the cirtification service provider fie or other persons who can illegally possess it. In order to prevent forgery and confer the electronic signature an increased value, according to the provisions of the article 23 letter d) of the Methodological Norms, the signee shall protect the „private key" from being stolen, deteriorated, modified in contents or compromised.

By the enactment of the law on the electronic signature, in the legal literature of the area, it was justly stated that electronic recordings can be considered beginnings of written evidence, being used as means of giving evidence only when used combined with other means of giving evidence, as they do not contain the original signature of the issuer[2].

Although we also shared the same opinion, considering that „the Code of civil procedure does not provide a legal framework for these (electronic) means of giving evidence, the judge is to weigh them very carefully .."[3], today, under the terms of Law no. 455/2001, of the international regulations and the practice in the field, we believe that in case the electronic signature meets the security requirements, it may be assimilated to the holographic signature, the electronic writ being assimilated to the writ under private signature and, as a result, acknowledging a similar evidentiary force.

The electronic writ to which an electronic signature was incorporated or associated, but this is not an extended electronic signature or it is not based on a qualified certificate or it is not drawn up by means of a secured mechanism of creating the signature, may be assimilated, as far as its conditions and effects, to the beginning of the written evidence (article 5 of the Law no. 455/2001) and may be combined with other means of giving evidence in order to prove the respective legal report.

According to the provisions of article 6 of the law regarding the electronic signature, „the electronic writ, to which it was incorporated, attached or logically associated an electronic signature, acknowledged by the one which it opposes, has the same effect as the authentic document between the ones who subscribed it and between the ones who represent their rights", and if according to the law, written form is required as a condition of evidence and validity of a legal document, an electronic writ meets this requirement if it was incorporated, attached or logically associated an extended electronic signature, based on a qualified certificate and created through a secured device for creating a signature.

---

[1] For more details regarding the evidentiary system in the civil lawsuit and establishing the values of the means for giving evidence, see: Fl. Măgureanu, Drept procesual civil, the 12th edition, Universul Juridic Publishing House, Bucharest, p. 466 and the next.

[2] See in this respect ST.D. CĂRPENARU – Drept comercial român, 2nd edition, ALL-BECK Publishing House, Bucharest, 2000, p. 377.

[3] See: FL. MĂGUREANU – Înscrisurile mijloace de probă în procesul civil, 2nd edition, ALL-BECK Publishing House, Bucharest, 1998, p. 147

Including the electronic writ in the other means of giving evidence, does not lead automatically to the assimilation of the two categories of holographic and electronic signatures, the electronic signature producing thus its effects only when this signature presents sufficient guarantees so as to certify the integrity of the message transmitted and the consent of its author.

The issue which arises regarding the electronic signature is not it that can be received as a means of giving evidence in the civil lawsuit and criminal trial but it is about establishing the legal framework, so as it cannot be contested by the one it opposes, so it can be used under a form which may enable being automatically read and processed by the subjects interested in it.

It also requires completing the legal and technical norms necessary for the whole system regarding the electronic signature to function well and for ensuring the security of information in order to prevent forgery and increased trust of the judiciary system in this technical and efficient means of giving evidence.

Bibliography

- Law no. 455/2001 regarding the electronic signature.
- Law no. 676/2001 regarding personal data processing and private life protection in the telecommunication area.
- Law no. 677/2001 on people's protection regarding personal data processing and free circulation of these data.
- Technical and methodological norms for the application of Law no. 455/2001.
- 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 23rd October 1998.
- M. Eliescu, Curs de drept civil, Teoria generală a probelor, Bucharest University, 1950-1951.
- A. Ionaşcu, Probele în procesul civil, the Scientific Publishing House, Bucharest, 1969.
- E. Mihuleac, Sistemul probator în procesul civil, the Academy Publishing House, Bucharest, 1970.
- ST.D. CĂRPENARU – Drept comercial român, 2nd edition, ALL-BECK Publishing House, Bucharest, 2000.
- Fl. Măgureanu, Drept procesual civil, 12th edition, Universul Juridic Publishing House, Bucharest, 2010.
- FL. MĂGUREANU – Înscrisurile mijloace de probă în procesul civil, 2nd edition, ALL-BECK Publishing House, Bucharest, 1998
- T.G. Sava – Consacrarea legală a semnăturii electronice, Revista de Drept Comercial (Magazine on Commercial Law), no. 7-8/2002.