Journal of Politics and Law; Vol. 11, No. 1; 2018
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Comparative Survey of Various Approaches of the Laws & Regulations in Relation to Electronic Signatures & Security thereof

Ghasem Bakhtiarifar[1] & Parviz Savrai[2]

[1] Department of Private Law, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Department of Private Law and Department of International Commerce Law, Shahid Beheshti University, Tehran, Iran

Correspondance: Parviz Savrai, Department of Private Law and Department of International Commerce Law, Shahid Beheshti University, Tehran, Iran. E-mail: savrai@iran-attorney.com

Received: August 15, 2016 Accepted: August 30, 2016 Online Published: February 2, 2018

doi:10.5539/jpl.v11n1p28 URL: https://doi.org/10.5539/jpl.v11n1p28

Abstract

Signatures are a significant part of the legal, commercial and even artistic personality and credibility of individuals and their existence is essential for validating not only the most important international documents but even a simple greeting card. A signature on a document, is the most significant evidence for attributing its contents to the signatory, indicating the acknowledgement and acceptance of the contents of the document by the parties who signed it with their knowledge and consent. For this reason, security of this process is of utmost importance and entry of such process in the electronic and digital space, makes it twice as much important.

Due to this, without existence of the necessary security infrastructures in the digital space, there is no possibility of providing electronic services, because without availability of the technologies required for validating and regulating the electronic documents, electronic signatures cannot be trusted.

The requirement of legislation along with these technologies for providing this security, is one of the most effective factors for realization of this subject, since in other words, proper application and implementation of such technologies is subject to enactment of some statutes related to this issue.

Therefore, in this research, considering the importance of the part of definitions, recognition of the title and its effect on the most careful study on approaches and differences of legal systems in this regard, we first review and describe the electronic signature in various legal systems. Subsequently, the paper progresses to explain different approaches of such systems towards the issue of security of the electronic signatures. After reviewing relevant laws in different countries including the United States, France and Iran, we designate an appropriate approach regarding the security issue in the electronic signature space.

Keywords: approach, statutes, electronic signature, security, EU Directive, French Civil Code, Electronic Commerce Law of Islamic Republic of Iran

1. Introduction

The common feature in documents, whether official, ordinary, commercial, non-commercial, contracts, unilateral obligations and even friendly letters is the existence of a signature.

Also, due to the progress of science and benefitting from technologies and reforms resulting from the emergence of modern electronic phenomena, signatures were also exposed to reform and are nowadays being issued in modern and electronic forms. Nevertheless, although the enjoyment from the outcomes of the electronic signature is indebted to the efforts of computer, IT and communications specialists, however, like any newly emerged social phenomenon, its legal impacts inevitably require the involvement and presence of lawyers.

Due to this, an ever increasing attention to the concept of this type of signature has reached such an extent that all national and international legislators are persuaded to be particularly sensitive to this concept and to enact, along with enactment of the E-commerce regulations, some special statutes for electronic signature.

Therefore, we firstly review the laws of France, the European Union Directive and the UNCITRAL Arbitration Rules in relation to electronic signatures, so that the definition and concept of each legislation in relation to this process, be specified and in continuation, we will deal with the subject of our research, which is the security of

electronic signature from the viewpoint of the statutes.

One of the most important issues for which some statutes must be enacted while complying with all technical & technological points, is the issue of security of the electronic signatures. The optimum use of this process ensures the highest security and confidence to the users.

The Uniform Law of Transactions and the Electronic Signature of U.S.A, authorizes the use of electronic signatures instead of conventional signature and regarding the role of security, issues of this type of signatures, it has remained silent, but has satisfied the assurance of such security through other means.

Generally, whatever seems more important than assumption in any branch of science, is posing some questions, a response to which will prepare the ground for further study and research and will open a new window in the mind of the researcher. Some of the questions discussed in the context of comparative survey of various approaches under the existing laws & regulations are as follows:

- Which laws currently pertain to the issue of electronic signature and how important is the enactment of statutes particularly in the field of security of electronic signatures?
- What are the different approaches of the existing laws and regulations in relation to electronic signatures?
- What are laws of the countries in the world including U.S.A, France and Iran regarding security of electronic signatures?

This study responds to the questions stated above and performs a comparative review of the various approaches of security laws of electronic signature, so that an approach may be selected that is both appropriate as well as relevant to the particular conditions.

As one of the most important countries in this context, we may refer to the common-law countries including U.S.A. A study of the Law of United States along with the laws of the civil law countries, such as including France and Iran, will shed important light on this aspect.

It should be pointed out that in this research, collection method has not been used and most subjects are the direct result of study of the related laws, therefore, the references are limited.

This study is presented in five parts. In the first part, we will deal with electronic signatures under legal systems and presentation of the related laws in a summarized and general form, because the requirement for security of this process is precise recognition and presentation of a clear and specific definition thereof and the definition provided in international law and laws of different countries are different.

In the second part, we will deal with the security issues, in the third part, we will review the subject of security as a pre-requisite for applicability, then we will focus on the security subject as a means for allocation of liability and finally, we will discuss the most important part of the research and subject of circumstantial evidences and a review of various statutes in this sphere.

2. Electronic Signature under Different Legal Systems

As one of most important foreign legal sources at the international level, regarding electronic signature and electronic documents in general, we may refer to the UNCITRAL Model Law regarding E-commerce. The UNCITRAL Model Law regarding electronic signature, United Nations Convention regarding utilization of electronic communications in international contracts European Union Directive on Electronic Commerce E.U. Directive regarding Electronic Signature and law No. 203 dated 13 Mar., 2000 of France and its subsequent bylaws.

In the next part, we will first describe the UNCITRAL Model Law and EU Directive regarding electronic signatures and we will subsequently review some articles under the said statutes in relation to electronic signature and definition thereof. Further to this, we will briefly review the French legal system and some of its statutes, as one the progressive legal systems in the field of electronic documents and naturally of electronic signatures.

2.1 UNCITRAL Model Law

Section A of Article 2 of the UNCITRAL Model Law of Electronic signature of 2001, provides as follows:

"Electronic signature means a data in electronic form attached to or logically connected to a data message and may be used for recognition of the identity of the signatory in relation to the data message or indicating the signatory's consent as to the information included in the data message"

The same law defines the data message in section C of Article 2 as follows:

"Data message means the information which is sent, received or stored by electronic, optical or similar means including electronic exchange of data, email, telegraph, telex, telecopy, and acts on behalf of the person or his agent."

The most important point in this definition is that the electronic signature has been described as "data" and this definition indicates the technical nature and the real and logical quality of the signature. Furthermore, contrary to the definition of electronic signature under the Iranian law in which there is only a reference to the aspect of recognition of the signatory's identity through issuance of electronic signature, as the only effect and application of the signature. Under UNCITRAL's resolution, two functions of recognition of the signatory's identity and indication of the consent of the signatory as to the information contained in the data message (electronic document or electronic contract), have been enumerated for the electronic signature.

In relation to the electronic signature law from the aspect of UNCITRAL resolutions, it may be stated that according to the Model Law of Electronic Commerce approved in 1996, that group of electronic documents which fulfill the functions of paper documents, are legally valid.

The main functions are: recognition of the signatory, conclusiveness of the involvement of the signatory in creating the signature, establishing connection between the said person and the document content, indication of the signatory's consent regarding the content of the document.

2.2 European Union Directive

The EU Directive of 1999 is considered the most effective document for creating a suitable legal ground for promotion of utilization of the electronic signature and ratification of the necessary regulations in European countries. Although this directive is binding upon the members of the union and only the member states are bound to comply with it in the enactment of their statutes, this document has been the main pattern for research and legislating activities throughout the world. This directive in its clause 1 defines the execution, scope and objectives of the directive, as follows:

"The purpose of this Directive is facilitation of the use of electronic signature and helping to its legal recognition. This directive creates a legal framework for electronic signature and some of electronic certificates for purpose of assurance of their appropriate function in the local market".

Section 1 of Article 2 of this Directive, defines the electronic signature and declares:

"Electronic Signature is a data in electronic form which is attached or connected to other electronic data and is used as a method for proving the identity".

The European Union Directive, in the definitions mentioned in its Article 1, by defining the various aspects and cases related to electronic signature, closed the road to various interpretations and this is itself one of the positive points of the said Directive.

Section 3 of Article 2 of the Directive provides as follows:

"A signatory is a person who has the tool for creating the signature and acts personally or through a real or legal person or an independent unit being his/her agent".

Section (4) of the said Article provides:

"Exclusive data are like private code or keys of secret writing, which are used by the signatory for creation of electronic signature"

It should be pointed out that EU, subsequently in completion of its directive dated 13 Dec., 1999, approved the Directive of 8 June, 2000, the approval purpose of which, was adapting some of the applicable domestic regulations. This made them closer to the services of informative companies in cases such as local market, commercial communications, traffic control laws, electronic contracts, etc.[1]

2.3 French Law

French Law as one of the progressive legal systems in the field of electronic documents, presently has three main reference legal texts as follows:

1) Law No. 2000-230 dated 13 March 2000
2) Bylaw No. 2001 -272 dated 30 March 2001

[1] Kainia, Mohammad, La Signature Electronique, Memoire Pour Le Master 2 de droit notariat, Universite Jean-Moulin Lyon III, 2008, P. 55

3) Bylaw No. 2005-973 dated 10 August 2005,

We will discuss the outcomes of each of the above cases shortly, as follows:[2]

On 13th March 2000, the French Parliament ratified a statute [11] for admission of electronic signature and thereby the electronic signature concept was entered in the French Civil Code.

The said statute is incorporated in the Civil Code under Articles No.1316 to 1316-4. It should be pointed out that the said statute, became enforceable rapidly.

The first part of section 1 of Article 1316-4 of the French Civil Code, regarding the function of signature, provides:

"The signature required for completion of a legal document, identifies the signatory and confirms the authenticity. This signature itself indicates the consent of the contracting parties with respect to the obligations resulting from the deed….".

Article 1316 of the law, without dealing with and considering the definition of electronic signature, deals with the substantial rules of the electronic signature.[3]

Section 3 of the said Article states as follows:

"Upon the proof of issuance of signature by a specific person, the contract (agreement) will have a validity equal to the paper equivalent thereof".

Also, the said statute merely and simply deems the electronic writing similar and equal to a written manuscript and recognizes it as bearing the same legal value of a written instrument.[4]

Article 1316-1 of the French Civil Code, explaining the legal value of electronic signature, provides that:

"Handwriting in electronic form is similar to the written handwriting and will be admitted as evidence with the same degree of validity, provided that it precisely identifies the person from whom such handwriting arises and the written instrument is created and kept in a manner that its entirety be secured".

As mentioned, section 1 of Article 1316-4 of the French Civil Code, explains the function of signature and section 2 of Article 1316-4 of the French Civil Code, has been allocated to the principle of authenticity. This section provides as follows:

"A signature is an electronic signature when it consists of using a safe method for identification and confirmation of authenticity and (also) assuring the connection of such signature with the document to which it is affixed. There is an assumption of validity and authenticity (principle of validity and authenticity) unless it is proved otherwise. When the electronic signature is created, the identity of the signatory will be secured and the entirety of the document, will be guaranteed under the conditions specified by the government council in an order."

Also, the French legislator, in line with the recognition of an electronic official deed, provides in the end of section 1 of Article 1316-4, as follows:

"When the said signature (electronic signature) takes place by a government officer, such signature officialises the document". Therefore, the French legislator is the only and the first legislator who has recognized the electronic official document.

The French Government Council, in implementation of the statute No. 2000-230, approved the Bylaw No. 2001-272 on 30 March, 2001. The first sentence of Article 1 of the said bylaw provides a definition for the electronic signature as follows:

"Electronic signature is a data which arises from the use of a process according to the conditions defined in the first sentence of section 2 of Article 1316-4 of the Civil Code." [5]

The remarkable point in this bylaw is that the French legislator, in the law ratified on 13 Mar., 2000 has only discussed the generalities, substantial rules, results and effects of electronic signature and incredibly refused to provide a definition for electronic signature.[6]

However, as noted, the government council, firstly defines the electronic signature in the beginning of the bylaw,

[2] Kainia, Mohammad, electronic signature according to French Law, Mizan Legal Foundation, 2009,P.30

[3] Kainiya, Mohammad, La dematerialization des acteset conventions, these de doctorat. Universite Jean-moulin Lyon 3, 2011, P.63

[4] Kainiya, op.cit, 2008, p.93.

[5] Kainiya, supra, p.59

[6] Kainiya, op.cit.2011,P.66

first sentence of Article 1 thereof.

3. Comparative Review of the Laws of Iran, France, the European Union Directive, UNCITRAL Rules Regarding Electronic Signatures

The UNCITRAL Model Law, France and EU Directive, by presenting the electronic signature as "data", have acted in a more suitable manner than that of the domestic laws. As pointed out, considering the definition of electronic signatures in the law of Electronic Commerce, using the term "mark" (signage) does not seem much correct.

In most legal systems of the world, two main functions have been discussed for the signature:

1) It identifies the identity of the person by whom the document has been issued.
2) Authenticity of the content of the document and its legal effects, are proved.

The UNCITRAL Model Law also considered two functions for the signature i.e. identity of the signatory and his/her consent with respect to the contents of the document. However, under Iranian Law, the consent of the signatory as to the document contents, has not been taken into consideration and only reference has been made to the identification of the signatory. It would be therefore, more appropriate if the Iranian legislator had referred to the intention of the signatory to be bound by the contents of the deed.

The French legal texts, build a structure based on the validity assumption.

Stipulation of this assumption is itself different from the European Union's system and is regarded as a kind of privilege for the French legislator.

4. Security as an Applicable Pre-Requisite and Means for Risk (Liability) Allocation[7]

Some Laws & regulations, deem a level of security essential for enforceability of the electronic transaction law and some other laws, have considered the existence or lack of security as a criterion for allocation of liability.

4.1 Pre-requisite of Applicability

The UNCITRAL Model Law, regarding electronic signatures, considers the element of reliability[8] , as a requirement for validating the electronic signature and provides as follows:

"In case the signature of a person is deemed necessary under a statute, this condition will be realized in relation to the data message by application of electronic signature, so that considering all circumstances including any agreement existing between the parties, it will be sufficiently reliable proportionate to the purpose for which the data message has been produced or sent".

Section 3 of this Article, defines the criterion of reliability of the electronic signature, explaining it in form of five cases as follows:

(A) Data related to producing the signature, under the conditions of their application, be only connected with the signatory not someone else.

(B) The data related to producing the signature at time of signing, be exclusively under the signatory's control not of somebody else.

(C) Any change resulting in the electronic signature, be recognizable after signing.

(D) In cases where the purpose of the legal condition (existence) of the signature, is securing the whole information with which the signature is connected, any changes in such information, be recognizable after singing.

4.2 Means for Allocation of liability

Article 10 of the Uniform Electronic Transactions Act of the United States[9], in some cases, attributes the liability of the occurred errors, to the party who did not comply with the agreed security formalities. Also, the Uniform Law of Commerce of the United States, allocates the damages resulting from the fraudulent instructions related to electronic payment, on basis of compliance or non-compliance with the agreed security rules.

5. Establishment of Circumstantial Evidence[10]

[7] Risk Allocation

[8] Reliability

[9] Uniform Electronic Transactions Act (UETA)

[10] Legal presumptions

Under some statutes, almost all types of electronic signatures, are qualified for legal effects and may replace the conventional signatures. The relevant statutes have also acknowledged that some electronic signatures are more reliable than the others.

These statutes have established a type of circumstantial evidence in favor of the relying party in respect of the sender's identity or the entirety of such document, for the purpose of creating on incentive in individuals for further use of this group of electronic signatures and for providing a high level of security and confidence in relation to the authenticity or entirety of the electronic documents in which this kind of signature, has been used.

It should be pointed out that this group of statutes are divided into two groups and each group has its own special approach:

5.1 Statutes in Which There Is Reference to a Particular Technology of Electronic Signature [11]

This group of statutes considers the circumstantial evidence of reliability merely applicable in respect of digital signatures.

As an example, the laws ratified in Minnesota, Missouri, Utah and Washington in the United States, Germany, Italy, Malaysia and Singapore, have adopted such an approach.

For the purpose of assuring that the digital signature is sufficiently reliable for enjoyment from such circumstantial evidence, the said laws usually stipulate a special legal framework for activity of the certification authorities, which voluntarily refer to relevant governmental authorities.

On basis of this circumstantial evidence, which considers the certificates issued by approved authorities as reliable, the digital signature produced by a private key connected with a general key presented in the said certificates, will be a reliable signature.[12] The said statutes consider the instruments containing these signatures as reliable.

For example, according to the Digital Signature Law of Utah State[13], whenever a digital signature is recognizable by an approved certification authority through a general key inserted in the issued valid certificate, the courts of the Utah State, will presume that:

A) The digital signature belongs to the subscriber introduced in the said certificate

B) The digital signature by such subscriber, has been attached thereto with the intention of signing the message.

5.2 Statutes in Which There Is no Reference to Any Particular Technology

These statutes primarily and in general, consider the electronic signatures as being valid, but subsequently they provide some rules and criteria which declare that the signatures having such criteria will have a special title and will enjoy the circumstantial evidence of reliability.

Some criteria have been provided without referring to any specific mechanism.

The French Civil Code, The European Union Directive of Electronic Signature and the Electronic Commerce Law of Islamic Republic of Iran, fall under this group.

5.2.1 French Law

As mentioned above, by ratification of the law of 13 March 2000, regarding harmonization of the law of evidences of proof with modern technologies related to the electronic signature, some amendments were made in the French Civil Code. These included presentation of an applied definition for signature and electronic signature.

Also, electronic signature has been defined under Article 1316-4 of the French Civil Code as follows:

'Electronic signature consists of using a reliable process for identification, which guaranties its own connection with the instrument on which it is affixed. The person claiming reliability of such process, must prove it in the court."

However, Article 1316-4 is continued as follows:

"In case creation of electronic signature, assurance of the signatory's identity and entirety of the document, take

[11] Technology-specific statutes

[12] Torrubia, Anders, Mora, Francisco J., Morti, Luis, Cryptography Regulations for E-commerce and Digital Rights Management, Computers & Security Vol. 20, No. 8, 2001, P.P. 730-731

[13] Utah

place under the conditions prescribed by the Government Council, reliability of this process, will be presumed, unless there is a contradictory evidence."

The French Government Council in its decree of 30 March 2001[14] has described those conditions, which are presented as follows:

According to Article 2 of the aforementioned decree, unless there is a contradictory evidence, producing the electronic signature will be presumed to be reliable, subject to the following conditions:

1) In case the process consists of using a secured electronic signature,[15]
2) It has taken place as a result of using a secured instrument for producing the electronic signature.[16]-[17]

According to Article 3 of the said law, the instrument for producing the electronic signature is considered secured when it guaranties the confidentiality of the data required for producing the signature and protection thereof against any change and alteration, inter alia, the following cases may be mentioned:

1) Recognition of this signature has taken place through using a qualified electronic certificate.[18]
2) It must exclusively belong to the signatory, it means that it should not be attributable to another person. A necessary factor for this case is enjoyment from private data (such as private key on the digital signature) for producing the signature.
3) The signatory must have the signature producing instrument under his own control, whether he creates the signature or the others produce the signature upon his responsibility.

   Therefore, the hardware and software used for electronic signature must be under the exclusive control of the signatory.
4) It must have such relation to the document attached to it, that any future change in the document, can be recognized.

The above regulations have been generally adopted from the European Union Directive on electronic signatures.

We therefore, refer to this directive, as follows:

5.2.2 European Union Directive on Electronic Signatures

This Directive, after giving a general definition on electronic signature (section 1 of Article 2), has introduced a special type of electronic signature.

According to section 2 of Article 2 of the Directive, the advanced electronic signature[19], is an electronic signature having the following conditions:

1) It must be exclusively connected with the signatory,
2) It must bring about the possibility of identifying the signatory,
3) It must be produced by using an instrument which the signatory is able to bring under his exclusive control,
4) It must be connected with the data related to it, in such a manner that any further change of data, may be discovered.

Article 5 of the Directive under the title of legal effects of electronic signatures includes two sections:

1) Member states guarantee that the advanced electronic signatures are based on qualified certificates created through secured instrument:
   A- In relation to electronic data, they fulfill the conditions of existence of signature, exactly in the same way that manual signature fulfills these conditions in relation to the paper-based data.
   B- They are accepted in legal proceedings as an evidence.

[14] Decret no. 2001 du 3 Mars 2001 Pris Pour Lapplication Larticle 1316-4: du code et relative a la signature electronique.

[15] Signature Electronique Securisee

[16] Dispisitif securisee de creation de signature electronique.

[17] De Lamberterie, Isaballe et Blunchette, Jean-Francois, Ledecrit du relative a la signature electronique, lecture critique, technique et juridique, 3 Mars 2001, pp.5-7

[18] Certificate lectronique Quelifie

[19] Advanced Electronic Signature

In section 2 of this Article, it is provided that:

2) The member states guarantee that the legal effect and acceptability of electronic signatures as evidence, in legal proceedings, may not be rejected merely due to the following reasons:

A- Due to being electronic

B- Due to not holding a qualified certificate and…….

By scrutiny on Article 5, we find out that section 1 of this Article, has in fact assimilated the advanced electronic signature to the conventional signature. This means that whenever the electronic signature has the required specific conditions, as mentioned in the definition of the advanced electronic signature, it must be admitted as an evidence in legal proceedings. Its strength and validity should be treated as being equivalent to that of a conventional 'hand' signature.

Due to the same reason, the said section is called "Assimilation Clause".[20]

Evidently the assimilation clause, is merely applicable in respect of the advanced signatures.

If the conditions for application of the Assimilation Clause (section 1 of Article 5) are not existing, the second section of the said Article will be applied. This section is known as "Non-Discrimination Clause"[21], by virtue of which the court is not entitled to reject the electronic signature only due to non-realization of the conditions of section 1.

The principle reflected in section 2 of Article 5, must be in fact considered as the general principle of Admissibility of electronic signatures[22]. This means that the judge is bound to admit and consider the electronic signature as evidence, although after careful study, he may consider the provided signature without any strength of proof.

The objection put forward in relation to Article 5 of the Instruction is that the said article has preliminarily expressed the proof value of a special type of electronic signature. Thereafter, it has stated the general principle of admission of electronic signatures, while in principle, firstly it should be stated that the said signatures are admitted by the courts and then their exclusive strength of proof should be discussed.[23]

5.2.3 Electronic Commerce Law of Islamic Republic of Iran

The Electronic Commerce Law of Islamic Republic of Iran provides that:

"When the existence of signature is deemed necessary by the law, electronic signature will be sufficient".

Under this Article, electronic signatures have been generally admitted as equivalent for conventional signatures, but Article 10 of the same law provides:

"Reliable electronic signature, must have the following conditions:

1) Be exclusive in relation to the signatory

2) Clarifies the identity of the signatory of the data message

3) It has been issued by the signatory or under his exclusive will

4) It is affixed on a data message in a manner that any change in that data message, may be recognized and discovered."

Article 15 of the said law provides a particular validity for this type of signature:

"In relation to a reliable data message, reliable electronic records and reliable electronic signature, no denial or doubt may be heard. Only a claim of forgery may be submitted regarding such message or it may be proved that the said data message has lost its validity due to same legal cause."

Although in many statutes some circumstantial evidences have been allocated to a particular group of electronic signatures (under the title of reliable, safe, advanced, etc. electronic signature), only some criteria have been stated for implementation of such evidences. Moreover, no specific technology has been referred to[24] (scientific or technological neutrality). Nevertheless, at the moment, digital signatures, are in conformity with such criteria

[20] Assimilation Clause

[21] Non-Discrimination Clause

[22] Principle of Admissibility

[23] Like the civil code of France & Electronic Commerce Law of Islamic Rep. of Iran

[24] Zarkalam, Sattar, Electronic signature and its standing in the evidence of proof system, Modarres Review, No. 1, 2003

under the said statutes.[25]

6. Conclusion

After studying some of the most important statutes related to electronic signatures, this study concludes with the following findings:

The electronic signature is a data which is attached or affixed to the data message in an electronic space with the intention of being bound to the contents thereof and indicates the consent of the signatory to the contents of such data message and provides the possibility of identifying such person. Under many ratified statutes, there is no reference regarding the role of security issues. Such statutes merely authorize the use of electronic signatures instead of conventional signatures. This approach has been adopted by the Uniform Law of Transactions and Electronic Signatures Law of the United States.

The European Union Directive, contrary to the French Civil Code and Electronic Commerce Law of Islamic Republic of Iran, firstly describes the special legal effect of the advanced electronic signatures and then it generally provides that the electronic signatures must be admitted as a signature by the courts.

The subject statutes, have not expressly declared the security issue as a pre-requisite for enforceability of electronic transactions. However, they have created a circumstantial evidence in favor of the parties using electronic signatures in order to encourage the persons to take appropriate security measures.

Under many statutes, circumstantial evidences have been merely considered for a certain group of electronic signatures (under the title of reliable, safe, advanced, etc., electronic signature) and there is no reference to the technologies required for application of such evidences.

Contrary to the European Directive, which has described the technical problems of electronic signature, the French Law of 13 Mar., 2000 regarding adaptation of the evidences of proof law to the information technology in relation to electronic signature, which supplemented the French Civil Code, has not discussed any technical considerations.

[25] Mazaheri Kouhanestani, Rasoul, comparative study of electronic signature under Iranian law and Uncitral Rules, Jangal publications, 2014, p. 75.