2528-9705

Örgütsel Davranış Araştırmaları Dergisi
Journal Of Organizational Behavior Research
Cilt / Vol.: 7, Sayı / Is.: S, Yıl/Year: 2022, Kod/ID: 22S0-933

Legal Nature of Electronic Signatures in Electronic Contracts and Terms and Conditions Governing Them

Seyed Amir Sharif*, Mohammad Ghahraman
Master of Private Law, Faculty of Law, Islamic Azad University, Shiraz Branch, Shiraz, Iran
s.amir.sharif1391@gmail.com

Assistant Professor , Faculty of Law , Islamic Azad University , Shiraz Branch, Shiraz, Iran

Mm_gharaman@yahoo.com

ABSTRACT

One of the most critical issues in examining the formation of electronic contracts, in the sense of contracts that are concluded using various electronic media such as telephone, telegram, fax, in the network environment, or using email, is the issue of electronic signature. Electronic documents and especially electronic are completed by signing, and as a result, they become assignable. Accordingly, this research aims to investigate the legal nature of electronic signatures in electronic contracts and the terms and conditions governing them. The research method is descriptive and analytical using library resources. Investigations showed that the increased attention to the concept of this type of signature has reached such an extent that it has forced all national and international legislators to be particularly sensitive to it and, along with the approval of electronic commerce regulations, to establish special laws for electronic signatures. Signing is an important condition for the completeness of the document, in the sense that the document can be relied upon against the issuer when it has been signed by him/her or has his/her fingerprints; in this sense, it is said that the handwriting and written words belong to the person who signed it. Currently, due to the prevalence of electronic commerce, the electronic signature, like the manual signature, has been accepted by various legal systems.

Keywords: *Electronic Signature, Electronic Contract, Legal Nature, Electronic Documents*

INTRODUCTION

Signature is an important part of a person's legal, commercial, and even artistic personality and credibility, and it is necessary to authenticate the most important international documents, even a greeting card. The existence of a signature at the bottom of a document is the most important reason for assigning the contents of the document to the signatory and shows the acceptance of the contents of the document by the parties who have signed it with their consent. Therefore, the common feature of documents, whether official or non-official, commercial or non-commercial, contract or agreement, and even friendly letters, is the existence of a signature. Also, along with the progress of science and the benefit of technology, and the developments caused by the emergence of new electronic phenomena, the signature has evolved and today, it can be issued in new and electronic forms. However, although benefiting the achievements of electronic signature is due to the efforts of experts in computer science, information, and communication technology, according to any emerging social phenomenon, its legal effects make the intervention and presence of lawyers inevitable. This is the reason why the increasing attention to the concept of this type of signature has reached such an extent that it has forced all

national and international legislators to be particularly sensitive to it and, along with the approval of electronic commerce regulations, to establish special laws for electronic signatures. One of the most important factors that make a contract or any other document valid is the correctness of its attribution to the issuer of that document or contract. In the past, this is usually done by sealing or signing the document. Based on what is conventional and the fact that the seal and signature are acceptable reasons for the correctness of assigning the document to the issuer, in electronic contracts, the correctness of their assignment should also be verified based on the special characteristics of this type of contract. In written documents, the signature is considered a confirmation of the obligations accepted in that document. In electronic commerce, since "electronic documents" have the same status as written documents, therefore, the signature on these documents has also the same probative value. Generally, a writing attributed to a person can be cited if it is signed. The signature shows the confirmation of the declarations contained in the document, as well as the acceptance of the commitments arising from it, and before that, the writing should be considered a plan that is the subject of consideration and deliberation, and the final decision has not yet been made about it. At the moment, due to the prevalence of electronic commerce, the electronic signature, like the manual signature, has been accepted by various legal systems. In terms of authentication of the parties in the cyber environment, the electronic signature is considered vital; a very important factor that emerges according to the role of the authority of the signature confirmation certificate.

The first electronic transactions in the specific sense were conducted using the Internet; the creation of electronic markets is a clear example of the impact of the Internet on business. Generally, cyberspace has its characteristics and effects in terms of the new structure it has given to human behavior and interactions, and the importance of these effects is so great that it caused the creation of a new branch in the field of law entitled "Cyberspace Law", and the science of law should deal with it in a completely separate way and examine the relationship of this new science with other different fields in law. In the science of law, these effects have been so great that finally in 1996, the first Model Law on Electronic Commerce (MLEC) was approved by the United Nations Commission on International Trade Law (UNCITRAL). The present research aims to clarify the legal nature of electronic signatures in electronic contracts and to examine the terms and conditions governing its various types.

Theoretical Foundations of Research

Terms and conditions governing the types of electronic signatures in electronic contracts

1- Types of electronic signatures

Any kind of electronic data that is attached to a message or logically related to it and specifies the relationship of the signatory with the data that is associated with it, is called a simple electronic signature; as soon as these conditions are fulfilled, the electronic signature is created. The major difference between simple and secure electronic signatures is the existence of public and private keys in the signature process. This makes a secure electronic signature similar to a digital signature. In a simple electronic signature, there is no process called cryptography. An electronic signature in its usual form is a very simple way of entering texts or specific forms into an electronic device. Any person can produce and use a simple electronic signature in his/her electronic documents without relying on the presence of a third party; of course, according to

Article 1287 of the Iranian Civil Code, in this case, it certainly cannot be said that documents produced in this way are official and valid documents.

It should be noted that for these signatures to give legal value to the documents, they require certain conditions, one of which is the presence of a third authority to control them, who acts like a notary public; in commercial documents, which are always of special importance, the existence of a simple or normal electronic signature cannot be relied upon.

"Secure/Enhanced/Advanced Electronic Signature" is provided for in paragraph K, Article 2 of the Electronic Commerce Law of Iran (ECLI). A secure signature is a signature that provides a high degree of certainty that the signature belongs to the intended person and that the message has not been changed during transmission. To achieve this, the signature must have the conditions that Article 10 of ECLI has predicted as follows. A secure electronic signature must contain the following requirements:

a) Be unique to the signatory.
b) Identify the signatory of the "data message".
c) Be signed by the signatory or under his/her sole intention.
d) Be affixed to "data message" in a way that any change in the data message can be detected and identified.

Document integrity, information confidentiality, and data security are guaranteed using a secure electronic signature, but identifying the signatory's identity is another important issue in electronic signatures. Legally, the most important effect of a signature is to prove the relationship between the document and the person to whom the signature is attributed. A secure electronic signature cannot guarantee alone the signatory's identity. In the assumption that the parties to the contractual relationship are large companies that know each other well in terms of history of business dealings or reputation in the international scene, this problem occurs less often, because the parties are aware of each other's financial and human capabilities.

The provisions of the aforementioned article 7, according to what is stipulated in article 10 of this law regarding the necessary conditions for a secure electronic signature, show that the legislator, referring to the absolute term "electronic signature", tried to state the rule that in cases where the law requires a signature, an electronic signature is sufficient, and to put it better, this requirement through a signature made in an electronic environment is considered a simple electronic signature, and it is natural that such a signature may not meet the conditions mentioned in Article 10 of this law and is naturally not considered a secure electronic signature. In this case, this question is raised: does this signature still have the same function as a manual signature in the real environment? The answer is negative. However, the use of the term "electronic signature" in Article 7 strengthens the assumption that this legal requirement is fulfilled by a simple electronic signature.

The electronic signature was created by the science of encryption. Encrypting is a science that uses mathematics and hardware and software methods to convert a message into a meaningless text, and the receiver again, with the same algorithm, returns this meaningless text to his/her desired message.

To ensure the authenticity of the electronic signature, a public key is used, the output of which converts the hash algorithm sent to the recipient into a normal signature. To sign a text or anything else, the signatory must first determine the validity range of the signature, that is, what

he wants to sign. Then, the hash function in the signatory's software converts a hash output into an electronic signature; therefore, the desired signature will be unique.

The most critical issue in the electronic signature is its assignability to the originator or the sender of the data message; in other words, the sender and the receiver, that is, the parties of a legal relationship, must have the necessary confidence regarding the authenticity and security of the data of the sent message, as well as its integrity, relatively and in proportion to the value and subject of the business relationship in question.

The security of electronic information is provided by the establishment of electronic certification authorities, and the most important technical tools used by this new institution to provide security are the Public Key Infrastructure (PKI) and the formation of the certification authority (CA).[1] Public key infrastructure is engineering the security of information exchange in the insecure environment of the Internet to provide a high level of trust and confidence to users. The parties to commercial relations all over the world are facing the problem of insecurity in exchanging information on the Internet. This, as well as the necessity of using the Internet, shows the need to provide a solution to this problem.

2- Electronic Registration

Electronic registration is considered a relatively new concept. Regarding this, as well as the failure to establish electronic registration offices in our country, to find the meaning of this phrase, one should refer to the laws and practices of pioneer countries in this field. Of course, "Certification Service Providers" are provided for in Articles 31 and 32 of ECLI and its criteria can be used for electronic registration offices as well. According to Article 31, "Certification Service Providers are established to provide electronic signature services nationwide. These services consist of the generation, issuance, transmission, confirmation, dismissal, and update of electronic signature certificates.[2]

In Canada, the Model Law of Notary Public devotes Article 3 to the discussion of "Electronic Registry Offices". This article covers in detail, from sections 14 to 23; all the concepts related to electronic registration and explains the principles and rules governing this new institution. In the explanatory introduction (interpretation) of Article 3, it is stated that electronic registries are not institutions separate from notaries and any notary public can obtain the necessary permission and training to an "electronic notary public". Of course, registering offices do not have any obligation to do this.

3- The importance of electronic contracts

Generally, the electronic contract is subject to the general rules and regulations of the law of contracts and obligations in terms of the basic conditions of the contract and the regulation of its consequential effects. However, in terms of technical features and methods of conclusion and the way of supporting its legal effects, it requires re-recognition and exact compliance with the general principles and rules governing contracts. Electronic contracts do not have a different

[1] - Articles 10 and 11 of ECLI have mentioned this issue.

[2] - Fathi, Ali, ***the Legal Nature of Electronic Signature in Commercial Documents***, Institute for Trade Studies and Research, Tehran, 2011, p. 23.

nature than conventional contracts in terms of the accuracy of the case or the subject; rather it is a new description of the environment of formation of the contracts that the legislator has not provided special regulations for it. The term “electronic contract” is used for the first time in the bylaw of Electronic Commerce of the European Union. In this bylaw, in the section on commercial transactions, the same legal status of electronic contracts as other contracts based on paper and traditional instruments has been mentioned, and a specific definition of electronic contracts has not been specified. The legal doctrine has generally defined electronic contracts as contracts that are concluded using modern electronic tools such as electronic data exchange networks, electronic mail, and Internet pages.

Considering that traditional contracts are legally subject to written or official form, contracts concluded in the electronic environment due to the unavailability or impossibility of performing these formalities such as the official signature of competent authorities or its validation and registration in official records such as purchase contracts and the sale of immovable property, face structural or safety obstacles. However, solving this matter and the ability to conclude contracts subject to special legal formalities depends on the creation of a structural framework for the establishment of specific legal regulations regarding it, which should be accompanied by the active role of the government in this matter. Establishing offices to provide signature authenticity certificates or transaction confirmation procedures by legal authorities requires the provision of a technical mechanism and a legal regulation about it.

In the laws of Iran and most countries, in terms of the written form of the contract, the parties to the contract, according to the relevant law, can verify the written form of their contracts with an electronic signature approved by the said authority by referring to the electronic signature certificate service centers. However, at present, technical and legal grounds have not been provided for formal contracts such as real estate purchase and sale contracts in the electronic environment. The form of concluding an electronic contract is not uniform according to the methods of electronic communication technology.[3]

4- Parties to electronic contracts

In the conclusion of electronic contracts, transactions are usually carried out using electronic tools, and in some of these methods of conclusion, human power is not directly involved, and the computer acts automatically on behalf of human will. Therefore, regardless of the formalities of conducting electronic transactions, it is generally assumed that the will of the parties exists in every part of the transactions. Not providing the necessary environment for common knowledge of each other's eligibility and true personality to conclude a contract is one of the most important difficulties in concluding an electronic contract. In this case, each of the parties must be satisfied with the information provided, and it will be the responsibility of the claimant to prove the invalidity of the electronic contract due to the incompetence of the other party.

According to the law of electronic commerce, the conclusion of a legal relationship in the electronic environment requires the existence of the originator and the receiver, as well as the

[3] - Ali Akbari, Ali Jan, 2013, ***Legal Aspects of Electronic Signature Based on the Laws of Different Countries***, Master's Thesis of Economics and Electronic Commerce, Under the guidance of Dr. Asadullah Farzin Vash, Faculty of Economics, University of Tehran, August, p. 56.

exchange of data messages between them. However, according to clauses b and c of Article 2 of the Electronic Commerce Law, the reference to these parties will in no way include a person who acts as an intermediary in connection with the data message. In addition to this law, the legislator has limited the attribution of data messages to the originator to two cases. According to the usage in cases other than that, the data message will not be attributed to the originator. According to Article 18 of the said law, the cases of attribution of the data message to the originator are: "a) if it was sent by the originator or by a person authorized to do so by the originator; b) If it is sent by the programmed information system, or automatic administration by the originator". In this way, in electronic contracts, the transactions of which are concluded automatically, the computer acts as a tool under the control and prior will of the parties.

In the Electronic Commerce Law of Iran (ECLI), referred to in paragraph "b" of the second article, in the concept of electronic technology, the term "originator" is used to refer to the offeror. According to this law, the originator is "the main source of the data message that is produced or sent by him/her or on his/her behalf but does not include a person who acts as an intermediary regarding the data message. Third, due to the electronic aspect of the offer, the location of the offeror loses its importance and the electronic offer takes on a cross-border attribute, i.e. a global attribute. But the offeror, i.e. the originator, can limit his/her offer to certain geographic regions or countries, or restrict the effects of his/her offer, i.e. his/her obligations, for example, the obligation to deliver goods or services to certain geographical regions. Declaration of consent to the offer's requirements in the electronic environment is called electronic acceptance. Whether the declaration of acceptance is electronic or non-electronic does not affect the nature of the will and how it implies the establishment of legal relations.

As long as the offeror does not specify a certain method of electronic declaration of consent, the electronic acceptance can be announced by any electronic method such as e-mail or filling out the form on the website page or in the form of electronic payment of the sales price. If, despite the agreement of the parties to announce the acceptance electronically, the addressee declares his/her acceptance by traditional mail, fax, or by telephone, this acceptance is not considered an electronic acceptance and the declared acceptance will not be valid.[4]

Legal nature of electronic signature in electronic documents

1- Electronic documents

One of the advantages of the electronic exchange of commercial documents is that electronic data while being exchanged quickly can be printed and received in the real world of business. For this purpose, Utah law stipulates: "If the sender of an electronic document prevents the recipient from storing or printing it, that document will not be valid against the recipient". Article 413 of the draft of the amendment bill of the trade law states: "Electronic commercial document is created in two ways. The original electronic commercial document and its replacement document, which considers the replacement document prescribed in Article 414 of

[4] - Ahwani, Hossam El Din, 2009, ***The General Theory of Commitment, Part 1, Commitment Sources***, 4th Edition, Cairo, p. 105.

the above law as the printed document. Anyway, what is being discussed is the documents that were issued after receiving the output of an electronic device.[5]
Preserving such documents means their practical protection for a long time. But really, how is the preservation of such documents that have an electronic texture? These paper documents contain digital data. So they must be signed in a way that is suitable for paper documents. Because in many cases, digital data is incomprehensible on paper and it is difficult or impossible to match them. Although some electronic signatures meet this demand, on the other hand, they have many shortcomings in cyberspace that endanger the exchange of documents. The current legal system is only written about paper documents and their registration and archiving while stating how to register and validate them in the world of papers in a legal form has become an ever-increasing need. Today, technology has taken an important step in creating devices to preserve digital data after printing. Media sec technologies have developed systems that prove authenticity in electronic documents that appear in printed form. However, with all these cases, the same traditional method of authenticating documents by official document offices, if a notary oversees the creation of these documents, seems to be a moderate solution.

2- Probative value of an electronic document

To prevent Internet problems and attacks, as well as to secure the cyberspace of the web, there are centers in the world that provide services for signature certificates and electronic documents. In this case, ECLI has accepted the principles of the unity of the signatory key and the monopoly of the private key, and the ability to identify changes in the data. However, the truth is that there is a very weak connection between the signature key and its owner because, in various ways, there is a possibility that the signatory is not the owner of the key. Therefore, it is very important that the signature used in the document is created by secure software and must be verified based on a valid certificate from the authority issuing the certificate. Various factors endanger the validity of the private key. For example, the owner of the key may carelessly reveal the key's password to an intelligent person, the device on which the key is stored may be stolen, or a copy of the private key may be taken. In very exceptional cases, it is possible that the software-developer produces a similar private key, and makes it available to others or uses it him/herself.

3- Legal problems with the content of commercial documents and electronic data

There are many problems facing e-commerce and consequently document exchange in cyberspace.
The most important problem in electronic data exchange is information theft or unauthorized reception of data. This causes a huge disruption in the world of business and commercial and private relationships of people. Many people are afraid of exchanging data in this space, the basis of which is the fear of their personal information or credit card numbers being exposed by computer hackers and fraudsters, and their unauthorized use.
Always creating good passwords cannot mean creating good security, especially in a large commercial system where many sensitive points may be attacked and exploited by the above

[5] - Elsan, Mostafa, ***Computerized Commercial Documents***, Monthly of the Association of Registrars and Clerks, Vol. 42, 2011, p. 22.

programs, such as deceptive Javas. In this way that a person, by using it, introduces him/herself as a legal service provider and receives illegal fees from the customers of the real service provider.

Another problem in the commercial documents exchange is the existence of protocols, each of which defines a format for the exchange of messages because professional programmers have always tried to create programs to conduct electronic commerce. Most of these programs require a lot of money for this type of business.

Essentially, legal problems in commercial documents are discussed in three issues: privacy, identity, and the unprovability of transactions. Since cyberspace is a public space and no one can be prohibited from entering it, the presence of security disruptors is always inevitable. Therefore, it needs to have a high-security factor to apply this security in the mentioned virtual space.

One of the major limitations of the electronic space is the recognition of the identity of the persons who exchange in the above space. In the best case, a smart device confirms personal information based on experimental data, but it is unable to prove his/her true identity. This problem causes identity falsification in the electronic space. This means that anyone can gain access to his/her data and violate his/her privacy by introducing him/herself as another person, who is desired by the other party.[6]

Every day, a large volume of electronic transactions are done anonymously, that is, people buy goods or services in the aforementioned way and pay for them with credit cards. In this case, at least for one of the parties, the real identity of the other party is not very important, and what is presented to him/her as the identity of the other party is only a code or transfer code. Now, this question is raised: is the above anonymity possible for the signatures and certificates issued by the certification authority for individuals? Answering this question requires examination of the presence of individuals and their commercial exchanges in cyberspace; that is, whenever we confirm an anonymous e-commerce transaction it indicates that the answer to the above question is positive. However, to answer the above question, we should have a correct understanding of the concept of anonymity; anonymity means that one's identity is unknown in the eyes of some people, and it does not mean being invisible.

According to paragraph 17, article 2 of ECLI, computer systems under the control of humans are among the persons who can be the owners of electronic signatures. The truth is that today intelligent electronic systems are widely used in the space of electronic commerce. But it is clear that, with all the intelligence and certainty of the performance of these systems, there are always concerns about them. On the other hand, today, commercial exchanges have gained more speed, and in the commercial world, someone is successful who takes greater steps. If real and legal persons, who exchange electronically their important business data and documents, are always in constant worry about the end of their exchanges and business transactions, they will not achieve much success. In electronic systems, the mentioned concerns are more, because in issuing signatures by real or legal persons, the signatory is always an intelligent real person who

[6] - Jamalzadeh Bahaabadi Kerman, Tayebeh, ***Validity and Legal Effects of Electronic Documents in International Contracts***, Tehran, HaghGostar, 2011, p. 78.

bears the responsibility for his/her actions, but in electronic systems, this is a bit confusing; for this reason, a real person should accept responsibility in this matter.

Conclusion

The electronic signature is data that is attached or connected to the electronic platform, to adhere to the contents and provisions of the data message, and it expresses the signatory consent to the contents of the data message and provides the means to identify him/her. The signature, regardless of the form and method of creating it (manual or electronic), has the same and similar function. In other words, it has a functional equivalence. In addition, the UNCITRAL model law, the Canadian model law, and the European Union directive, by introducing the electronic signature as "data", have acted more appropriately than the domestic laws of other countries, because as mentioned, according to the definition of electronic signature, the term "sign" used in the Electronic Commerce Law of Iran (ECLI) does not seem correct.

Currently, due to the prevalence of electronic commerce, the electronic signature, like the manual signature, has been accepted by various legal systems. In terms of authentication of the parties in the cyber environment, the electronic signature is considered vital; a very important factor that emerges according to the role of the authority of the signature confirmation certificate. On the other hand, in connection with the discussion of considering data-message as one of the proofs of the claim, the said electronic document can be considered and cited as proof.

Acknowledgment:

none

Conflict of Interest:

none

Funding:

none

Ethical statements:

none

References

- Ahwani, Hossam El Din, 2009, ***The General Theory of Commitment, Part 1, Commitment Sources***, 4th Edition, Cairo, p. 105.
- Jamalzadeh Bahaabadi Kerman, Tayebeh, ***Validity and Legal Effects of Electronic Documents in International Contracts***, Tehran, HaghGostar, 2011, p. 78.
- Elsan, Mostafa, ***Computerized Commercial Documents***, Monthly of the Association of Registrars and Clerks, Vol. 42, 2011, p. 22.
- Ali Akbari, Ali Jan, 2013, ***Legal Aspects of Electronic Signature Based on the Laws of Different Countries***, Master's Thesis of Economics and Electronic Commerce, Under the guidance of Dr. Asadullah Farzin Vash, Faculty of Economics, University of Tehran, August, p. 56.

- Fathi, Ali, ***The Legal Nature of Electronic Signature in Commercial Documents***, Institute for Trade Studies and Research, Tehran, 2011, p. 23.