2528-9705

Örgütsel Davranış Araştırmaları Dergisi
Journal Of Organizational Behavior Research
Cilt / Vol.: 7, Sayı / Is.: S, Yıl/Year: 2022, Kod/ID: 22S0-840

A Legal Analysis of E-Signatures in Iranian-Canadian Law Contracts

Seyed Amir Sharif*, Mohammad Ghahraman

Master of Private Law, Faculty of Law, Islamic Azad University, Shiraz Branch, Shiraz, Iran
s.amir.sharif1391@gmail.com
Faculty member of Islamic Azad University of Shiraz
Mm_gharaman@yahoo.com

ABSTRACT

An e-signature is a piece of data linked to communication that identifies the signer and affirms his or her agreement to the message's contents. The present study compares and contrasts the legal treatment of e-signatures in Iranian-Canadian law contracts. The research method is descriptive-analytical, and it is conducted with the use of library resources. An e-signature, according to Canadian legislation, is a signature that must be unique to the person who uses it and not to anybody else. The e-signature must be attached to the e-document in a way that allows the person to make that decision, and the technology or process by which the signature is made must be under the complete control of the person to whom the signature belongs, and that particular technology or process must be such that the person is known by it. The certification body is the organization that gives e-certifications to applicants under Canadian legislation. The applicant's public key, as well as the applicant's information and the certificate issuing center, are all included in these certificates. An e-signature, according to Iranian law, is any mark that is physically or conceptually linked to message data and is used to identify the signer of the "message data." Furthermore, an e-signature by itself does not confirm the signer's identity. As a result, the third party must ensure the message's legitimacy by identifying the digital signer.

Keywords: *E- Signature, Contracts, Iranian Law, Canadian Law*

INTRODUCTION

The sharing of e-documents is common in e-commerce. Sensitive information, such as legal contracts, private technology, or financial activities, is frequently found in these documents. It is vital to encrypt these papers and sign them digitally to avoid computer criminals from stealing in the electronic environment who are always on the lookout for documents. The digital signature ensures the data's validity, completeness, and lack of degradation.

The Iranian legislative defines e-signature as any sort of mark affixed or conceptually related to the "message data" that is used to identify the signer of the "message data" in paragraph "Y" of Article 2 of the Electronic Commerce Law issued in 2003. The legislator's choice of the term "mark" in the definition of e-signature appears to be related to the mentality that existed in jurists' books of the previous definition of signature, which applied to any sort of "mark or writing."[1] According to Article 2 of the aforementioned law, an e-signature is a type of mark that is affixed to or attached to message data and is used to identify the signer of the message data. Explaining

[1] Mazaheri Kohanestani, Rasoul, Nazem, Rasoul, A Comparative Study of E-Signature in Iranian Law and UNCITRAL Regulations, Tehran, Jangal Publications, 2014, p.10.

ideas like message data, signage, concatenation, connection, and signature applications is necessary to expand on this topic.

An electronic document is the message data that can be cited as a claim or defense. Using Iran and other countries' civil and e-commerce laws, the electronic document is divided into three types: official electronic documents, ordinary electronic documents with simple signatures, and ordinary electronic documents with secure signatures. Unlike the Canadian legislature, Iranian law does not have a clear definition of an official electronic document, and to define this type of document, one must refer to the interpretation of traditional rules governing paper documents.

A message data might be mentioned as a claim or defense in an e-document. The e-document is classified into three categories based on civil and e-commerce regulations in Iran and other countries: official e-document, ordinary e-document with a simple signature, and ordinary e-document with secure signature. Unlike the Canadian legislature, Iranian law lacks a clear definition of an official e-document, requiring interpretation of customary standards controlling paper documents to identify this sort of document.

The consideration of contracts is one of the most significant themes in jurisprudence. What requirements must be met in order to form a contract, as well as its legitimacy, is a critical consideration. According to Article 190 of the Civil Code, a transaction must meet four essential characteristics in order to be valid: the parties' intent and consent, the parties' competence, the transaction's specific subject matter, and the transaction's legitimacy are all factors to consider. Each of these circumstances has been the topic of substantial judicial dispute. We know that a contract is an agreement formed between two or more persons to have a legal effect and that the essential ingredient of a contract is the will of the individuals who agree to do something. In order for a legal effect to be created, the two parties must express their intent to each other, which might be explicit or implicit.

The current study examines the nature and legal effects of e-signatures, as well as traders' awareness that they cannot be present at the same time to confirm documents by physical signature and validate their documents with digital signatures for financial exchanges and documents, as well as the level of awareness of people and managers of departments and commercial companies and relevant officials, of the rules of civil liability in relation to electronic signatures.

Theoretical foundations

The literal meaning of signature in Iranian law

In Iranian legal sources, there is no exact definition of a signature, which might be owing to the legislator taking the concept of a signature for granted. As a result, the legal definition of the signature is based on customary sources and is influenced by both custom and judicial processes. Farhikhteh Jafari Langroudi believes that a signature is "writing a name or surname or both, or drawing a mark as an expression of the identity of the owner of the mark under papers and documents to confirm the text of the document that was written or will be written from the signature » in expressing the legal definition of a signature[2]. In addition, the signature has been defined as "writing the name or surname (or both) or drawing a special mark, which is a sign of the identity of the owner of the mark under the documents (ordinary or official) that include the

[2] Jafari Langroudi, Mohammad Jafar, Extensive in Legal Terminology (Vol. I), Tehran, Ninth Edition, Ganj-e-Danesh Publishing, 2012, p. 636.

transaction or commitment or confession or testimony "or it must be recorded on those bonds or transactions later."[3] Dr. Nasser Katozian, the other professor, explains the signature as follows: "A signature is a drawing of a person that generally contains the person's name and represents the person's final choice and agreement." As a result, the signature should be placed in a location that is traditionally regarded as a sign of consent."[4]

"The common and basic element and basis of the validity of ordinary signature documents is the attribution of the contents of the document to the signatory and his firm will to issue the document," according to Article 1293 of the Civil Code, and "written when it has a document against a person whose signature or fingerprint is under the document," according to Article 1291 of the same law. As a result, the signature and certification in which it is entered are responsible for the paper's legitimacy. If a piece of the writing ascribed to a person is signed, it can be referenced. The unsigned document is incomplete and lacks the most crucial ingredient of credibility, as evidenced by basic legal and customary norms. As a result, the signature and certification in which it is entered are responsible for the paper's legitimacy. If a piece of the writing ascribed to a person is signed, it can be referenced[5]. The unsigned document is incomplete and lacks the most crucial ingredient of credibility, as evidenced by basic legal and customary norms.

The literal meaning of signature in Canadian law

A signature is a name, symbol, or word that is used to validate a document in foreign texts[6]. According to Canadian sources, a signature is a personal mark placed on the foot of a text or work to affirm that we are, in fact, the author of the text or work or that we recognize its contents[7].

A signature was defined as a written signature made by someone who made a promise under Canadian law[8]. All of the terms and conditions are agreed upon and signed by the parties in traditional contracts. Electronic signatures are the same way.

E-signature in contracts

The signing of a contract is indeed an act by which the parties' talks become legally enforceable responsibilities for them. The parties to a contract have traditionally signified their agreement to the terms of the contract by signing it in the presence of the other party, with each party keeping a signed copy of the contract. The wet ink technique is the name for this technology. This technique assures that neither party will be able to subsequently contest the contract's contents or make it binding on the basis that it was signed by someone other than him.

The preceding method, on the other hand, necessitates the parties to the contract signing it at the same place or exchanging a printed and signed copy of the contract by mail. Furthermore, in recent years, when it comes to important commercial and financial contracts, the wet ink approach has been supplanted by a signature and scanning approach, which entails each party

---

[3] Jafari Langroudi, the former, p.633.

[4] Katozian, Nasser, Proof and Reason for Proof (Vol. I), Tehran, Fourth Edition, Mizan Publishing, 2011, p. 317.

[5] Asgharzadeh Bonab, Mostafa, Applied Registration Law, Volume II (Lawsuits and Registration Objections Related to Documents and Procedure), Tehran, Majd Publications 2016, p.154.

[6] Garner, A, Brayan. (2012). Black's Law Dictionary. Tehran: Dadgostar.327.

[7] Ki Nia, Mohammad, E-signature in accordance with French law, Tehran, sixth edition, Mizan Legal Foundation Publications, 2016, p. 140.

[8] Ki Nia, Mohammad, e-signature in accordance with French law, Tehran, sixth edition, Mizan Legal Foundation Publications, 2016, p. 140.

manually signing the contract, scanning it, and e-mailing a signature page as an attachment to the contract. The parties to the contract, according to this method, depending on the e-mail sent by the other party to the real signing as adequate proof of the signature page's legitimacy. Although this strategy has helped the conclusion of international contracts by employing traditional office resources such as printing machines, stationery, and scanners, it may not be viable to use such tools in a circumstance when the great majority of workers are away from their workplaces. The electronic signature is a suitable and efficient choice in certain situations for concluding business transactions. The e-commerce legislation in Iran recognizes electronic signatures in such a manner that where laws and regulations need the presence of a signature, the e-signature is adequate and has the same validity as a handwritten signature[9].

Any symbol (for example, a password number) that permits the identification of the signer of the message data is regarded as an e-signature in the electronic space where the writings are not material and cannot be touched, and the interchange of information takes place in a virtual environment. The sender is introduced, and the communication data is assigned to him via electronic signature. When a person buys a book online, it is impossible to know if the buyer is qualified until the buyer signs the message data and the certificate authorities verify his or her identity, which is strongly connected to the issue of e-signatures and certificates authorities[10].

An e-signature, according to some, is any certification that is electronically generated and can be a token, word, number, typed name, scanned picture, handwritten signature, or any other electronic mark created by the issuer or her deputy and linked to a document[11]. An electronic signature is also defined as any electronic mark or mechanism that a party accepts to express its intention to confirm the validity of a document or to be bound by it[12]. It should be emphasized that any non-cryptic sign or symbol is deemed a signature if it allows the author of the sign and the symbol to be identified.

Article 7 of the Iranian Electronic Commerce Law only allows for electronic signatures if the lawmaker deems them essential. However, in order to be certain, the electronic signature must meet the requirements set out in Article 10 of the ICCPR. Those criteria must be unique to the signer, identify the message data signer, and be provided by the signer or under his own authority. It is linked to a message data stream in such a way that any changes in the message data may be noticed. According to Article 15 of the ICCPR, if the electronic signature meets the aforementioned criteria, the denial and doubt against it are not considered, and only the accusation of forgery or proof that the data in the message was legally defective can be incorporated into the data of the message.

Part II of Article 1316-4 of the Civil Code of Canada defines an e-signature as follows: "It is when the signature is electronic that the signature incorporates a secure mechanism that assures that the signature is connected with the document to which it is affixed." Unless there is a cause to believe otherwise, the process's trustworthiness is presumed. When an e-signature is formed, it ensures the signer's identity and the document's integrity according to the standards outlined in

[9] Abdul Elahi, Mahboubeh. 2012. Electronic reason in the system of proof of litigation, Tehran, Khorsandi., P.122.
[10] Shams, Abdullah 2014. Evidence of Proof of Lawsuit, Darak Publishing, Volume I., p.91.
[11] Todd, Paul, E- Commerce law, London: Cavendish Pub. 2012, p 99.
[12] http://www.stoel.com. Ralph Bloemers, Electronic and digital signatures, available at:

the State Council resolution. The criteria indicated in the first sentence of Article 4-1316 BC's second paragraph have been observed and created[13].

E- signature in the legal system of Iran and Canada

1. E-signature terms and conditions in Canadian law

"A signature consisting of one or more digital letters, signs, numbers, or symbols registered or affixed to or accompanied by an electronic document," according to the Canadian Data Protection and Electronic Documents Protection Act (PIPEDA)[14].

A secure e-signature must be unique to the person using it and not to anybody else, according to the law. The person who owns the signature must have complete control over the technology or procedure used to create the signature. In addition, the technology or procedure must be unique enough to identify the individual. Furthermore, the e-signature must be tied to the e-document in such a way that the individual can determine whether the document has changed after the signature was applied.

Cryptographic, biometric, and digital image technologies are used in most e-signatures. Make sure the electronic signature is legal and valid by consulting a computer or technology attorney. The role of the signature is stated in the first paragraph of Article 4 of the Canadian Civil Code: "The signature necessary to complete a legal document identifies and verifies the legitimacy of the signatory." The approval of the parties to the transaction on the obligations emanating from the instrument is indicated by this signature.

Article 16 of this law deals with the substantive regulations of e-signature without discussing or paying regard to the concept of e-signature. The third paragraph of this article states: “By demonstrating the issue of a signature by a specific individual, the contract (agreement) will have the same worth and legality as its paper counterpart." Furthermore, this legislation deems electronic writing to be comparable to and equivalent to written writing, and it is accorded the same legal status as written writing”.

Article 1 of the Canadian Civil Code, in explaining the legal value of an electronic signature, states: "The writing is accepted as evidence electronically, as well as written writing, with the same degree of validity, provided that it can accurately identify the person from whom the writing originates, and the writing is somehow created and maintained to ensure its integrity."

The role of the signature is described in the first paragraph of Article 4 of the Canadian Civil Code, and the concept of validity is described in the second paragraph of Article 4 of the Canadian Civil Code. This section specifies: "A signature is an electronic signature if it employs a reliable way of identifying and validating authenticity, as well as ensuring that it is tied to the document to which it is attached." Until demonstrated otherwise, the accuracy of this procedure is assumed (the principle is correctness). Once the e-signature has been formed, the signer's identity and the document's completeness are guaranteed under the rules established by a decree issued by the State Council[15].

---

[13] See: DAUZON, OLIVIER, Le Droit du Commerec Electronice, Hercity – France, Editions Du Decree NO 2001 – 272 Du 20 Mars 2011, Available at: http://playmendroit.free.fr// droit-des-novellas-technologies / decret-du-.

[14] Zarqalam, Sattar, "Electronic Commerce Law and Electronic Alphabet", p. 79.

[15] Mazaheri Kohanestani, Rasoul, Nazem, Rasoul, A Comparative Study of E-Signature in Iranian Law and UNCITRAL Regulations, Tehran, Jangal Publications, 2014, p.59.

A simple e-signature, according to Canadian law and Article 1 of the Government of Canada By-Laws, is the use of a trustworthy identification technique that confirms its link to a document to which it is regular. A secure e-signature, on the other hand, must first be created by methods that are under the exclusive control of the signer and, second, ensure the relationship of the signature to the attached document so that any subsequent changes to the document can be detected, in addition to having the conditions for an electronic (simple) signature[16]. The certification body in Canada is the organization that offers electronic certifications to applicants. Customers' identities are unknown to certificate authorities; thus, they require a trusted person to authenticate their identity and function as a liaison between the certificate authority and the client. The registrar's office is in charge of this. The registration office thereby delivers the required information to the certified authority, allowing that authority to provide its services to clients. Before issuing the certificate, the registry is responsible for identifying and certifying the person. It is in charge of administrative duties such as registration, details, and statements of applicants, as well as ensuring that the applicant meets the requirements for receiving the certificate. Persons are authenticated using documentation given by the applicant for an electronic certificate to the registration agencies. However, depending on the degree of the certificate granted, the sort of proof required to identify persons, whether natural or legal, will vary.

Simple identifying papers, such as credit cards, are acceptable for low-level certificates, while stronger documents are required for certificates with a greater level of protection. A digital certificate will be issued by the owner of the future signature after receiving the registration offices' report.

2. Terms and conditions of e-signature in Iranian law

A secure electronic signature must meet certain conditions, according to Article 10 of the Iranian Electronic Commerce Law, which governs paragraph 2 of Article 2 of the same law: "A secure electronic signature must meet certain conditions: it must be unique to the signer, and it must specify the identity of the message signer. It should be issued by the signatory or under his own authority, and it should be connected to a message data in such a way that any modification in the message data may be detected". The integrity of the document, the confidentiality of the information (if necessary), and the security of the data are all assured when utilizing the electronic signature technique or a signature-based on asymmetric cryptography. However, one significant issue remains unresolved: ensuring the signer's identity. Indeed, the most significant legal impact of a signature is to establish the document's link to the person to whom the signature is attributed[17].

"Any message data captured and preserved by a third party in compliance with Article (11) of this legislation is legal," it adds, confirming the necessity to ensure the identification of the signatories of Article 16 of our country's e-commerce law. As a result, the necessity for a competent third-party authority to certify the accuracy of the attribution of the secure message contents and the secure e-signature to the issuer is indisputably crucial.

In comparison to other centers, Articles 12 and 14 of the by-Laws provide extensive rules and regulations surrounding the creation and operation of e-registration offices. "Registration offices

[16] Ibid, P. 59

[17] Zarkalam, Sattar, e-signature and its place in the system of evidence. Modares Magazine, No. 1, 11392, p.45.

may be established, as the case may be, by natural or legal persons, whether governmental or non-governmental," according to Article 12 of the By-Laws.

Regarding Iranian legal procedure, paragraph 15 of Article 2 in the second chapter of Iran's e-commerce law states: "The signatory is any person or his deputy who provides the electronic signature."[18] People are defined as natural or legal persons in paragraph 17 of the preceding article. The preceding article should be interpreted as a personal signatory who creates an e-signature under the guise of a valid electronic certificate. The legal entity that has the certificate and the private key, as well as the natural person who holds the key, are both liable for the created signatures in this situation.

3. Legal issues arising from e-signatures in domestic laws

Since most nations' domestic law (on e-signatures), including ours, does not require the signatory to appear before a competent notary public to record the signature. As a result, there is no need to go through the procedures of the registration legislation to identify the signatory, which raises the risk of a signature being issued by someone who does not exist (imaginary people). As a consequence, the signatory can establish rights and duties for him/herself in contracts with others, yet her obligations can be avoided owing to her lack of true identity.

In terms of conformity between local law and Canadian law and legislation, it is worth noting that, under Article 86 of the ICCPR, "If a request to register a document is made, it is the office owner's job to verify the identity of the interlocutors or party who has made a promise, and if the aforesaid man does not know them personally, he must act in line with the terms of this legislation[19]."

Article 102 also relates to Article 101, which provides for the offender's expulsion from public employment for a period of one to three years. "If the person in charge of the office has any doubts about the identity of the interlocutors or the party who undertakes, both well-known and trusted persons should confirm their identities in person, and the person in charge of the office registers the ranks in the registry office, signs them to the witnesses, and states this point in the documents," according to Article 50 of the Penal Code[20].

In specifying the prerequisites of a secure electronic signature, Article 10 of the ICCPR does not explain with whose authority these conditions are met: Despite the fact that the signature itself may be unique to the signatory and issued by her or under her own authority (Article 10, paragraphs a and c). However, there is no assurance that the identification revealed to the signer by the digital signature is the signer's genuine identity, and this is something that should be left to a responsible authority.

Utah's inability to identify the function of notaries in re-registrations has been extensively criticized by attorneys and registrars in Canada as a consequence of the enactment of some Canadian laws mandating the existence of a digital signature in notaries. As a result, the National Association of Notaries of Canada saw it as an unofficial heist of its profession.

4. E-signature certificate authorities

A secure or digital e-signature by itself does not verify the signer's identity. As a result, the third party must ensure the message's legitimacy by identifying the digital signer. "Any message data

---

[18] Zarqalam, Sattar, "e-Commerce Law and e-Alphabet", p. 65.

[19] Ibid. P. 25

[20] Abdollahi, Mahboubeh, Electronic Reason in the System of Proof of Litigation, Tehran, Khorsandi, 2012, p. 37.

captured and preserved by a third party in compliance with Article (11) of this legislation is legal," it states in this respect, reinforcing the requirement to prove the identity of the signatories of Article 16 of our country's Electronic Commerce Law[21]. As a result, the necessity for a competent third-party authority to certify the accuracy of the attribution of the secure message contents and the secure electronic signature to the issuer is indisputably crucial.

E-service agencies are also required by Canadian legislation to ensure the signer's identification.[22] As a result, e-certificate offices' job is to identify the signature and, as a result, to document the electronic data. Indeed, by managing the link between the public key and the holder of the appropriate private key, the digital certificate issued by the electronic service offices ensures the signer's identity.

Conclusion

There are two ways to e-signatures in the Canadian legal system: first, it identifies the person from whom the document was issued, and second, it establishes the legitimacy of the document's content and legal implications. However, in Iranian law, the signatory's approval of the document's requirements is ignored, and just the signatory identity is recorded. As a result, it was only natural that the Iranian legislature, in completing its definition, said that the signing intended to abide by the document's requirements. An e-signature, according to Canadian legislation, is a signature that must be unique to the person who uses it and not to anybody else. The person who owns the signature must have complete control over the technology or procedure used to create the signature. And that technology or procedure must be unique enough to identify the individual. Furthermore, the e-signature must be tied to the e-document in such a way that the individual can determine whether the document has changed after the signature was applied. "The signature necessary to complete a legal document identifies and certifies the legitimacy of the signatory," the Canadian Civil Code says of the signature function. The approval of the parties to the transaction on the obligations emanating from the instrument is indicated by this signature. "A signature is an e-signature when it employs a reliable way of identifying and confirming authenticity, and (and) assures that the signature pertains to the document to which it is affixed," according to the Canadian Civil Code. Until demonstrated otherwise, the accuracy of this procedure is assumed (the principle is correctness). Once the e-signature has been formed, the signer's identity and the document's completeness are guaranteed under the rules established by a decree issued by the State Council.

The institution that offers e-certificates to its applicants is the authority to issue certificates in the Canadian legal system. The applicant's public key, as well as the applicant's profile and the certificate issuing center, are all included in these certificates. Indeed, the public key is linked to this certificate of identification. The center continually monitors the issued certificates, and if the holder's identity is compromised after the certificate's expiration, the center will revoke the certificate's validity and place it on a list of revoked certificates. In Iranian law, demonstrating the issue of a signature by a specific individual gives the contract (agreement) the same worth and validity as its paper counterpart.

---

[21] Ibid, P. 44

[22] KAINIYA, Mohammad.(2011). La dématérialisation des actes et conventions (de l'expérience francaise à sa réception par le droit iranien?), Thèse de doctorat. Université Jean-Moulin Lyon3:68.

Acknowledgment: NONE

Conflict of Interest: NONE

Funding: NONE

Ethical statements: NONE

References

- Asgharzadeh Bonab, Mostafa, *Applied Registration Law*, Volume II (Lawsuits and Registration Objections Related to Documents and Procedure), Tehran, Majd Publications 2016, p.154.
- Jafari Langroudi, Mohammad Jafar, *Extensive in Legal Terminology* (Vol. I), Tehran, Ninth Edition, Ganj-e-Danesh Publishing, 2012, p. 636.
- Zarkalam, Sattar, *"Law of e-Commerce and e-Alphabet"* Tehran, Khorsandi, 2012.
- Zarkalam, Sattar, *e-signature and its place in the system of evidence*. Modares Magazine, 1, 2013, p.45.
- Shams, Abdullah 2014. *Evidence of Proof of Lawsuit*, Drak Publishing, Vol.
- Abdul Elahi, Mahboubeh. 2012. *E-reason in the system of proof of litigation*, Tehran, Khorsandi., P.122.
- Katozian, Nasser, *Proof and Reason for Proof* (Vol. I), Tehran, Fourth Edition, Mizan Publishing, 2011, p. 317.
- Ki Nia, Mohammad, *e-signature in accordance with French law*, Tehran, sixth edition, Mizan Legal Foundation Publications, 2016, p. 140.
- Mazaheri Koohestani, Rasool, Nazem, Rasool. 2014. *A Comparative Study of e-Signature in Iranian Law and UNCITRAL Regulations*, Tehran, Jangal Publications, p.145.