

**Validity of Evidence of Electronic
Transactions and the Main Features of
Criminality and Impunity Contained in
the Qatari
E-Commerce Law**

Dr. Nazzal Kisswani* & Dr. Basher Saad Zaghloul**

* Assistant Professor of Commercial Law – College of Law – Qatar University

** Assistant Professor of Criminal Law in the Universities of Cairo and Qatar

Abstract:

The Qatari legislature intervened in 2010 to provide that electronic documents have equal legal status to written documents. This new legislation has given electronic transactions the necessary importance and has strengthened the confidence of users of the electronic tools in transaction. It has duly laid down specific sanctions in cases of violation. The adopted law is envisaged to be one useful document that will help lawyers in their future.

Key Words:

Qatar; electronic evidence; electronic signatures; validity; E Commerce Law; Criminal law

Introduction

In light of the technological development which has brought a change in the human life and has become one of the fundamental pillars of modern societies, the contractual processes have brought a set of changes that affected its legal system. Transactions started to be conducted through electronic means, resulting in drawing the attention of lawmakers and the judicial authority.

The proliferation of technology and the continued growing use of means of communication has caused the spread of so-called electronic contracts. Since the contract execution is done through these means, the first thing that was raised in this area the extent to which these electronic documents can be used as a proof, especially if one of the parties to the electronically-concluded contract held that evidence as a full written proof. It also presents electronic signature as a by-product of such transactions.

Before presenting evidence of the validity of the electronic transactions and before presenting the main characteristics of criminalization and punishment provided in the e-commerce Law, issued by decree No. 16, 2010, we should make reference to the limitation provided by the law to its scope of application in terms of the transactions that are governed by the law and those that are not.

1.1 Effective Scope of E-commerce Law:

The Qatari Decree Law No. 16 of 2010 on the Promulgation of the Electronic Commerce and Transactions Law (E-Commerce Law) defined the effective scope of the law relating to transactions between persons who have agreed to conduct their transactions using electronic communications.⁽¹⁾ Electronic communications refer to any contact made using electronic communication devices,

(1) Article 2 of Qatari Electronic and Transaction Law No. 16 of 2010.

both wired and wireless, regardless of the technique used to complete this connection, which may be electrical or electromagnetic or any means of similar techniques.⁽²⁾

The law excluded the applications of written documents and transactions related to family issues and civil status, transactions in kind related to real property, transactions that must be documented in accordance with the law, together with commercial papers in circulation in accordance with the provisions of the E-Commerce Law, such as cheques and bills of exchange.⁽³⁾ The reason behind excluding these documents from the scope of electronic transactions depends either on the nature of the topic which these documents stand to prove, such as matters related to personal and civil status, or transactions in kind and real estate, or on the nature of the written document itself in terms of being a legally negotiable commercial paper.

Nonetheless, according to a Ministerial Decree concluded and followed a recommendation made by the Supreme Council of Communication Technology, the last paragraph of article 3 was drafted to permit adding other transaction as also excluded from taking an electronic form. This has been taken into account in consideration of the public interest.⁽⁴⁾

(2) Article 1 of Qatari Electronic and Transaction Law No. 16 of 2010.

(3) Article 3 of Qatari Electronic and Transaction Law No. 16 of 2010.

(4) Translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=236945.

1.2 Respect for the Principle of the Legality of Crimes and Penalties of Punishment:

The process of criminalization and punishment in the law state is based on the principle of legality of crimes and punishments. This principle ensures the protection of the personal freedom of individuals from abuse of the executive power and ensures respect of the principle for separation between the legislative, judicial and the executive powers.⁽⁵⁾ Article 40 of the Qatari Permanent Constitution 2004, confirms this principle by stating that “no crime or punishment except by law.” This principle means that an act is not considered a crime, and should therefore be not penalized for, unless there is a written legislative provision that states so.

The criminal judge, in his application of the provisions of the criminalization and punishment, looks for descriptive law of the incident attributed to the accused, and by doing so, he is bound by what is known as model legislation of the crime.⁽⁶⁾ That means unless there is a legislative provision that fully applies to the committed incident, the defendant must be acquitted. Accordingly, given the specificity of the transactions governed by the e-commerce law, it was necessary to single out special provisions in this law dealing with the process of criminalization and penalization commensurate with the nature of the acts that can be committed in violation of its provisions. Provisions of penal code may not be sufficient in criminalizing of such acts in order to achieve this purpose on the basis of the idea of the legislative model of crime.

(5) Ali Qahwaji, 'Explanation of the Penal Code: Comparative Study' 2002. Elhalbi Publisher – Beirut (Arabic Text)

(6) Ahmad Sharaf Al-Din, 'Validity of Evidence of Electronic commerce' 2007 the Arab Organization for Administrative Development - Dubai

2. Validity of Electronic Documents As Evidence:

Various items of legislation related to the rules of evidence often require the existence of a written document to prove certain legal action such as real property. Because electronic transactions are based on contracts without paper documents, the issue of evidence and proof constituted an obstacle to the development of e-commerce.⁽⁷⁾ The aim of the E-commerce Law is to reduce the vast amount of paper documents, and replace them with digital data for all transactions, which can make trade more difficult and costly⁽⁸⁾ The issuance of the e-Commerce Law, provided for the validity of electronic transactions and granted electronic transactions the same level of validity as that of traditional paper documents. Article 25 of the Act provides as follows:

‘Nothing shall apply so as to prevent the admissibility of information or a document as evidence on the grounds that it is in the form of data message, or on the grounds that it is not in its original form if it is the only evidence that the person adducing it could be expected to obtain.’

Hence it is clear that the Qatari legislature considered the electronic document exchanged by parties as a means of valid evidence. It follows that electronic documents can be considered against the conditions relating to written evidence, and then to assess the validity of electronic documents in accordance with the general law of Qatar.

(7) Batle Ghania, ‘Electronic writing as evidence’, *Tawasul of Social and Humanitarian Sciences Journal*, 2012 (30).

(8) Batle Ghania, ‘Electronic writing as evidence’.

2.1 Validating the Electronic Contract with Reference to the Conditions Related to the Written Evidence

Writing is considered as a means of primary evidence due to its characteristic of stability and validity.⁽⁹⁾ Writing is not subject to forgetfulness or obsolescence. Hence, the law of civil and commercial transactions, under the chapter on evidence, provides that ‘the plaintiff must provide evidence of the commitment and the defendant must prove otherwise.’⁽¹⁰⁾ Similarly, article 213 of the same Act provides that ‘the judge may not decide based on his knowledge.’ Hence the legislature stressed that the parties to the case have to prove their claim by the evidence set forth in the law. The judge is bound to decide on the evidence in making a judgment. The judge may not pass any ruling over any dispute based on his personal knowledge, even though he is well versed in the subject matter of the case.

The law stipulates that certain conditions must be met in order to use writing as evidence. Most importantly, the written document must be readable and clear, and must be characterized by continuity and stability.⁽¹¹⁾ It must also not be subject to modification or editing without destroying the written document or leaving a material impression on it. To address this topic, it is necessary to establish the conditions for written evidence to be accepted as evidence, and whether similar conditions are available for electronic documents. To consider this issue, it is necessary to identify the conditions relating to written evidence, and establish whether the same conditions are available in the electronic document.

(9) Batle Ghania, ‘Electronic writing as evidence’.

(10) Article 211 of Civil and Commercial Procedure Law No 13 of 1990, Al-Jarida Al-Rasmiya, 1990-09-01, No. 13, pp. 1-83.

(11) Ahmad Sharaf Al-Din, ‘Validity of evidence of electronic commerce’.

- Writing Must be Legible:

It is stipulated that where writing is used as evidence, it must be readable and clear. The written document must be written using known letters and symbols that can be understood to the person that the document intended to be used against. This condition is achieved by using familiar letters in writing. The Civil and Commercial Procedure Law provides that official documents are those issued by a public service officer or a person who is authorized to be in charge of a public service within his limits of authority and competence.⁽¹²⁾ If a document does not have official status, it will only have the value of traditional documents after being signed, finger-printed or stamped by the party concerned, in accordance with article 216. Traditional documents are issued by individuals without reference to the public service employee.

A person cannot read a document in electronic form directly. It can only be undertaken indirectly, through the use of a screen, where the image of writing appears in a legible written and clear form, understandable to both of the contracted parties.⁽¹³⁾ The Electronic Commerce and Transaction Law has confirmed that an electronic message is considered to be valid and enforceable in the same way as written documents, as provided by article 4, which reads:

'In the context of contract formation or conducting transactions, an offer or acceptance of an offer may be expressed, in whole or in part, by means of electronic communications.

(12) Article 216 of Civil and Commercial Procedure Law No 13 of 1990

(13) Ahmad Sharaf Al-Din, 'Validity of evidence of electronic commerce' P 105; Burkhard Schafer and Stephen Mason, 'The characteristics of electronic evidence' chapter 2, in Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 2.04 – 2.05.

A contract or transaction shall not be denied validity or enforceability solely on the grounds that one or more electronic communications were used in its formation.’

- Writing Must be available :

Writings are required to be available. This is related to the continuity of evidence. That is, it is necessary for writing to be available as a pillar of evidence to ensure the parties can refer to the document.⁽¹⁴⁾ This requires the writing to be printed on paper or by using electronic methods such as CDs, CD-ROMs and electronic memory that are capable of storing, preserving and continuously making the document available for a long period of time. This exceeds that of the traditional document, which is subject to being worn out or destroyed by fire, although electronic documents are also subject to being destroyed, manipulated and falsified.⁽¹⁵⁾

- Assurance of the integrity of the document:

To have any evidential value, writing should not be prone to modification or change. Any damage or material changes should be the result of making changes or modifications to the writings. The purpose of this requirement is to provide an element of trust and confidence in the validity of the writing to the parties.⁽¹⁶⁾ This is achieved by understanding the tests to demonstrate the integrity and therefore trustworthiness of electronic documents.⁽¹⁷⁾

(14) Abdul-Aziz Hamod, ‘Validity of evidence of electronic transactions in civil and commercial in the light of the rule of evidence’, *Journal of Legal and Economic Research*, 2002 (11)

(15) See Stephen Masom, gen ed, *Electronic Evidence*, 2.18 – 2.27.

(16) Abdul-Aziz Hamod, ‘Validity of evidence of electronic transactions in civil and commercial in the light of the rule of evidence’.

(17) Mohammed Abu – Zaid, ‘Validity of Evidence of Electronic Transactions Comments on the Provision of Judiciary’ *Dubai Judicial Institute Journal*, 2012 1(1) – *Electronic Evidence*, chapter 4, especially 4.12.

3. Validation of Electronic Documents

Article 20 of the e-Commerce Law provides that the information contained in the data message shall not lose its legal effect, validity or enforceability by being in the form of a data message, and parties can obtain access to it in a usable manner:

‘Information in the data message shall not be denied legal effect, validity or enforceability solely on the grounds that they are in the form of a data message.

Information in the data message shall also not be denied legal effect, validity or enforceability solely on the grounds that it is merely referred to in that data message without details, provided that the data message clearly identifies how to have access to the details of this information, the information is accessible so as to be used for subsequent reference by every person that has a right to access and use the information and the method for accessing the information is clearly identified in the data message and does not place an unreasonable burden on any person that has a right to access the information.’

Article 21 required every document or transaction must be in writing, or consequences must be identified if the document is not in writing. It is considered to have met that condition when it is in the form of a data message, and is accessible and retrievable.

The UNCITRAL Model Law on Electronic Commerce ⁽¹⁸⁾ illustrates the requirements to consider when a data message meets the requirements of writing so as to be considered as valid evidence, as stated in article 6 as follows:

(18) UNCITRAL Model Law on Electronic Commerce Guide with to Enactment with 1996 with additional article 5 bis as adopted in 1998. Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

- (1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.
- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

The text must be written and must be accessible and retrievable. The information must be preserved, saved and accessible. This helps to provide confidence and security for documents.

The Qatari legislature proceeded to determine the consequences of electronic documents in the same context, and where any law requires information or a document to be retained or stored and identified Article 24(2), stipulated that:

‘the data message is retained in the format in which it was originally produced, sent or received, or in a format that can be demonstrated to accurately represent the information contained in the data message as it was originally produced, sent or received.’

4. Electronic Signature

Electronic signature is new to people. No one expected that to happen one day, or ever thought of a signature other than the traditional ones used for evidence. Hence, there have been international and regional efforts to explore ways that ensure security and confidence in that signature.

4.1 Definition of Electronic Signature

There is no fixed legal definition of a traditional signature, many cases over the years, and many judges have defined signatures in different ways. Some of the reoccurring elements include: writing drawing or affixing, by one’s own hand, one’s own name or any

mark which identifies it as the act of the party. Forms of signature accepted in common law countries include, but are not limited to, rubber stamps with the name of a person or company and documents verified by a facsimile signature.⁽¹⁹⁾ It is observed that one of the objects of requiring a document to be signed by a person is to authenticate the veracity of the document.⁽²⁰⁾

An electronic signature can be defined as ‘any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a writing’⁽²¹⁾ or as any method which applies a signature to an electronic message.⁽²²⁾ In the international context, article 2 of the UNCITRAL Model Law on Electronic Signature 2001 defined the electronic signature as ‘data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message’.

In Qatar, the definition of electronic signature is based on the UNCITRAL Model law. Article 1 of the e-Commerce Law defines an electronic signature as ‘letters, numbers, symbols or others affixed to a data message, which uniquely identify the signatory from others in order to indicate the signatory’s approval on the data mes-

(19) Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), 16 – 82. See also Nazzal M. Kisswani and Anas A. Albakri ‘Application of Electronic Signature in Business and Its Influence on Electronic Commerce Implementation’, *International Journal of Liability and Scientific Enquiry*, (2010) 3(4), 282–290

(20) For a list of the other functions that a signature is capable of, see Stephen Mason, *Electronic Signatures in Law*, 8 – 10.

(21) Thomas J. Smedinghoff, *Electronic Contracts & Digital Signatures: An Overview of Law and Legislation*, 564 P.L.I. PAT. 125, 162 (1999).

(22) Alan Tyree et al, ‘Banking Law and Banking Practice’ (2006) 17 *Journal of Banking and Finance Law and Practice*, 47-50

sage.’ This definition stresses that the electronic signature shall provide the traditional functions: to identify the person, and to indicate their approval of the message.

The Validity of the Electronic Signature in Evidence in Accordance with Qatari Law

An electronic signature is capable of assuring the recipient of an electronic message that the message was sent by the sender of the electronic signature. It is also capable of providing reassurance that the message can only be issued or sent by a real sender.⁽²³⁾ Other aspects of a digital signature includes the possibility of providing for the integrity of the electronic message from any fraud or modifications by ensuring that the electronic message received matches the same contents of the sender’s without being amended or changed or any new content added,⁽²⁴⁾ and the confidentiality of the electronic message can also be achieved with a digital signature, ensuring that the electronic message that has been signed cannot be read by anyone who does not have the requisite key.⁽²⁵⁾

The legislator in Qatar provided, in article 28, that the digital signature will have the benefit of a degree of evidential weight as follows:

(23) Brian F. Fitzgerald, Anne M. Fitzgerald, Timothy Beale, Yee Fen Lim and Gaye Middleton, *Internet and E- Commerce Law: Technology, Law and Policy* (Lawbook Co., 2007), 543.

(24) Gavin Jones, ‘Failing in Treatment of Electronic Signature’ (2003) *Hertfordshire Law Journal*, 1(1), 101-106; for a more up-to-date treatment, see Stephen Mason, *Electronic Signatures in Law*, Chapter 7 ‘Digital Signatures’ which includes examples of case law where digital signatures have failed.

(25) Nazzal M. Kiswani and Anas A. Albakri ‘Application of Electronic Signature in Business and Its Influence on Electronic Commerce Implementation’, *International Journal of Liability and Scientific Enquiry*, (2010) 3(4), 282–290.

An electronic signature shall have evidential weight if the following conditions are met:

1. The signature creation information are identified with the signatory and no other person.
2. The signature creation information were, at the time of signing, under the control of the signatory and of no other person.
3. Any alteration to the electronic signature, made after the time of signing, is detectable.
4. Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

The Supreme Council shall issue decisions to determine which electronic signature processes and technologies satisfy the provisions of the preceding provisions.

The procedures of issuing a digital signature (which is only one form of electronic signature) ⁽²⁶⁾ and the relevant documentation, is often handled by a person authorized by the competent authorities to do so.

It is clear from the foregoing that the digital signature enjoys a degree of confidence and security under the e-Commerce Law, and is considered as evidence of the truth and an assured means to verify the information contained.

(26) For a list of other forms of electronic signature, including case law from across the world, see Stephen Mason, *Electronic Signatures in Law*, 187 – 258.

5. The Nature of the Criminalization Provided in the E-Commerce law:

Article 67 of the e-commerce law ensures a legal protection for all aspects of electronic transactions according to the aforementioned law. It criminalizes many acts which fall with these transactions. It is noteworthy in the philosophy of criminalization and penalization provided in article 67 of the Law, that it dealt with the crimes prescribed there as offences. It provided a punishment of two years' imprisonment and a fine not exceeding three hundred thousand riyals or both.

It should be noted that the Qatari Penal Code stipulates that "misdemeanours are those crimes that are punishable by imprisonment for a term not exceeding three years and a fine of more than 1,000 riyals, or both, unless otherwise provided by law."⁽²⁷⁾ While the same law provides that "felonies refer to those crimes punishable by death or life imprisonment or imprisonment of over three years."⁽²⁸⁾

On the other hand, the offences set forth in article 67 above all refer to intentional crimes. Article 67 provides a punishment for anyone who intentionally commits any of the acts contained therein.⁽²⁹⁾ This means that no punishment for committing one of the acts set out in article 67 of this law can be inflicted unless criminal intent was proved, that is proving the knowledge and will towards all the elements of the crime imputed to the offender.

It should also be noted that the criminalization and punishment provided for in article 67 of this law is without prejudice to any

(27) Article 23 of the Qatari Penal Code No 11, 2004

(28) Article 22 of the Qatari Penal Code No 11, 2004

(29) Ali Qahwaji,, 'Explanation of the Penal Code: Comparative Study' 2002. Elhalbi Publisher – Beirut (Arabic Text)

harsher penalty prescribed by any other law. This means that if a legislative provision is identified in the Penal Code or any special criminal legislation which criminalizes one of the acts criminalized under article 67 of the e-commerce law, and a more severe penalty was prescribed than that of article 67, then this harsher penalty should be imposed.

Actually, this purpose is perceivable especially as related to paragraph 5 of article 67, which provides for the criminalization of the forgery of data message, electronic signature or certificate authentication, ..etc. In this case the provision of article 206 of the Qatari Penal Code shall be apply. This provision penalizes the fraud of an official document by imprisonment for 10 years or five years, depending on the characteristics of the offender, if the fraud occurred on an official document or not. This leads to changing the categorization of the crime from a misdemeanour to a felony. The penalty in this case will be imprisonment not exceeding three years if the fraud was on an informal document. The same thing could happen with regard to the e-commerce law which provides that criminalizes identity theft or claiming others' status on applying for e-certificate, or accepting the same.⁽³⁰⁾ the Qatari Penal Code can be applied whereby punishment is imposed for name forgery or claiming of a false status by imprisonment not exceeding three years.⁽³¹⁾

Fraud crime happens when forging a data message through entering, whether legally or illegally, to an existing database and modifying such data by abolition, addition, or deletion.⁽³²⁾

(30) Article 67 (8) of Qatari Electronic and Transaction Law No. 16 of 2010

(31) Article 354 of the Qatari Penal Code 2004

(32) Muner M. Ganbaha and Mamdouh M. Ganbaha, *Cybercrimes and Computer and Means of Control* 2005 Dar Alfaker Al Arabi, Alexandria P 90

Electronic signature method, however, has become commonly used in all countries of the world⁽³³⁾. The crime of electronic fraud happens when someone steals the electronic signature algorithm for someone, and uses the same in signing electronic documents, where the characteristics of the forged signature are the same as that of the original.⁽³⁴⁾ The crime lies in the fact that the signing has happened through the accused person who has illegally got electronic signature algorithm.

5.1 General Deterrence Impact:

Part of the criminal punishment is to recognize justice, general deterrence, and specific deterrence. No doubt that criminal justice is recognized by imposing punishment on those who were found guilty of crime, after a fair trial where the right in defence is assured.⁽³⁵⁾ Further, the imposition of punishment on the offender represents a sort of special deterrence, as the sentenced person expects pains that make him think twice before committing his crime again. General deterrence refers to intimidating others from exposure to the same destiny of the sentenced person, when going in the path of crime. No doubt that assessing punishment on offenders through public criminal sentencing represents a way of recognizing general deterrence. In e-commerce law, article 68, paragraph 2 provides for the option of publishing the conviction judgment in two daily widely spread newspapers, and on open electronic networks, at the expense of the convicted person. This provision ensures the establishment of the two types of deterrence,

(33) Mohamed Amin El-Shawabka, *Computer Crime and Internet-cyber Crime 2007* Dar al-Thakafah, Amman,, p. 234.

(34) Adrian McCullough and William Caelli, "Non-Repudiation in the Digital Environment, volume 5, number 8, August 2000, http://firstmonday.org/issues/issue5_8/mccullagh/index.html at May 2014

(35) Mohammed shawabki, *Computer Crime and Internet- Cybercrime, 2007* Dar Al-thqfa -Amman

the general and the specific, due to the pains caused by publication at the expense of the convicted person. This pain is caused by defamation in a legal way, whereby others are warned against dealing with such a person in the context of electronic transactions; it would also detract the financial credibility of that person because of the expenses required for the publication of the conviction as provided in article 68/2. On the other hand, the above provision ensures the achievement of deterrence through warning the public of meeting the same fate in the case of committing the same act for which the defendant was convicted. In the end this provision ensures the protection of dealers in electronic commerce from falling victims to these crimes. The public warning against the offenders, doing business with them or giving them any trust.

5.2 Liability of Legal Person and those in Charge of Actual Administration:

Article 69 of the e-commerce law provides for the punishment of those responsible for the effective management of a legal entity with the same penalties provided for in article 67 of the code: Maximum two year of imprisonment and a fine not exceeding three hundred thousand riyals or one of them. Article 69, provided for the infliction of such penalties once it was proved that those in charge of actual management were aware of the commission of such a crime, or once it was proved that committing such a crime was a result of breaching the duties of the management of the place.

Article 70 of the e-commerce law provides for the responsibility of non-natural (legal) person. It provides for the infliction of the penalty under article 67 of the code, determined to be a fine of no more than 300,000 riyals, or a fine that equals to the fine imposed on the actual management in charge in cases where the penalty described is not imprisonment.

According to this text:

1. The verification of the juristic person's responsibility relies upon the ability of identifying evidence of convicting the actual management in charge in accordance with article 69 of the e-commerce law.
2. In the event of convicting those in charge of actual management and sentencing to imprisonment only, fine should be imposed on the juristic person as stipulated in article 67 of the Act.
3. When the person in charge of actual management is sentenced to both imprisonment and fine, or only fine, the judge may prescribe a punishment on the juristic person equals to a fine as provided in article 67, or to sentence him to the same fine imposed on the person of actual management.

This responsibility is based on the fact that the person responsible for the management or the legal representative of a legal entity has committed an act criminalised under the law whether for his own account or for the account of a legal entity.⁽³⁶⁾ Punishment on juristic persons should be commensurate with its nature in order to ensure both general and specific deterrence.⁽³⁷⁾

5.3 Repetition of Offence:

Recidivism is the status of the person who commits one crime or more after receiving a final sentence for another crime. Recidivism results in the tightening of the punishments of the latest crime. This is based on the fact that the first sentence was not sufficient to deter and prevent recidivism.⁽³⁸⁾

(36) Ali Qahwaji, above no 4.

(37) Ashraf Shams El Din, above no 5

(38) Ibid

Due to the dangerous impact of such offences on the security and privacy of e-commerce transactions, the law on electronic transactions and trade provided for the doubling of the penalty on offences contained in the Act, that is the punishment is extended to imprisonment not exceeding four years and to a fine not exceeding 600,000 or both.⁽³⁹⁾ Article 71 in reference has also referred to repeat offenders as those who commit any of the offences specified in this Act within three years from the date of completing the sentence or the dropping of the same by the passing of its duration. That means any doubling of the penalty will depend on the relapse of the offender to commit one of the offences provided for in the e-commerce law during a period of three years; this period starts from the moment of completing the sentence for the crime for which he had been convicted as provided for in the Act, or from the date of dropping the penalty due to aging. As the crimes contained in the e-commerce law are considered offences, the dropping of penalty by aging happens after five years from the date of the final judgment. the Qatari Criminal Procedures Law, provides that the sentence on a misdemeanour will be dropped in five years.⁽⁴⁰⁾

5.4 Judicial Control Capacity

The Qatari Criminal Procedure Law stipulates that “It is permissible through a decision by the Public Prosecutor and upon an agreement with the competent minister, to give some employees the status of judicial officers for crimes that take place within their jurisdictions and connected to their profession”⁽⁴¹⁾ In conformity with this text, Article 72 of E-commerce Law states to give the status of judicial officers to some of the employees of the Supreme Council

(39) Article 71 of Qatari Electronic and Transaction Law No. 16 of 2010

(40) Article 375 of the Qatari Criminal Procedures Law no. 23 for 2004

(41) Article 27 (2) of the Qatari Criminal Procedures Law no. 23 for 2004

of Information & Communication Technology by a decision from the Attorney General in co-ordination with the Supreme Council of Information & Communication Technology, provided that they shall have the power to control and approve actions committed in violation of the provisions and judgments based on it.

Article 27 above granted them the relevant authority to access areas related to electronic records and documents, equipment and other related items and to request data and clarifications that they consider necessary, and to report on breaches that take place on sites.

In this context, the employees of the Supreme Council of Information & Communication Technology who are vested with powers of judicial seizure are prohibited from disclosing any secret known by virtue of their profession. The Qatari Penal Code stipulates that “A prescribed penalty of an imprisonment of no more than two years or a fine of no more than ten thousand riyals, or both penalties together, to all person who knowingly disclose a secret by virtue of their job, profession or occupation, and illegally reveal it or use it for private interest, or for the interest of someone else, unless a prior permission is granted by the concerned person”.⁽⁴²⁾

It should also be noted that Article 194 of the Qatari Penal Code stipulates that “The penalty of imprisonment for a period not exceeding three years and a fine not exceeding ten thousand Riyal or one of the two penalties shall apply to anyone who takes possession of, or hides from post office or telecommunication staff, a letter, a cable, a parcel, or a strongbox, or opens any of them or discloses their contents of statements or information or facilitate this to others.” The offender may be sentenced to be removed from Office.“

(42) Article 332 of Qatari Penal Code

5.5 Scope Application of Provisions of E-Commerce and Transactions in Terms of Place:

The territorial jurisdiction of criminal law means that it has a specific legal influence on the crimes committed within a specific sphere.⁽⁴³⁾ With regard to electronic crimes, Article 73 of e-commerce Law stipulates that the provisions on criminalization and penalization shall apply:

to any person who commits an act outside Qatar that makes him/her a principle or an accomplice in a crime committed wholly or partially inside Qatar.

to a person who commits an action inside Qatar that makes him/her a principle or an accomplice in a crime committed wholly or partially outside Qatar, if it is punishable under this Law and the law of the country where the crime took place.

In fact, Article 73 mentioned above has added nothing to the enforcement of the penal code in terms of place. The text of Article 73 is literally copied from the text of Article 16 of the Qatari Penal Code. Therefore, we do not see any need for such text as it has not added anything new to the application of the Qatari Penal Law in terms of place which is organized by Articles 13 & 16 of the Qatari Penal Law.

43 () Ali Qahwaji, above no 4.

6. Conclusion:

The increasing volume of electronic legal transactions revealed the need to regulate these transactions according to specific legal rules that assures no manipulation, and to allow dealers the necessary means in proving the existence of these transactions vis-a-vis creating authoritative legal electronic documents. Such documents shall facilitate an increased use of commercial transactions. As such, the Qatari legislature intervened in making the electronic document an authentic proof as are the regular written documents. Given the importance of this kind of legal transactions, and the desire to strengthen the confidence of clients, the Qatari legislature intervened, in reflection of its embedded authority in the criminalization process, in enacting provisions that shall raise the confidence of clients who are bound to use electronic documents in their dealings, by way of criminalizing the misuse of electronic documents. The content of such contracts was given special care.

The philosophy of criminalizing and penalizing the misuse of electronic commercial transactions comes as a consistent step with the specific nature of the crime. Therefore, the Qatari legislature has made it possible to publish the court's judgment of conviction in two widely circulated newspapers, as well as on an open network medium, at the expense of the convict. This philosophy of criminology pours into the legislature's desire to warn the general public from manipulators of electronic contracts and to ensure wider deterrence policy.

References

- Article 2 of Qatari Electronic and Transaction Law No. 16 of 2010.
- Article 1 of Qatari Electronic and Transaction Law No. 16 of 2010.
- Article 3 of Qatari Electronic and Transaction Law No. 16 of 2010.
- Translation available at http://www.wipo.int/wipolex/en/text.jsp?file_id=236945.
- Ali Qahwaji, 'Explanation of the Penal Code: Comparative Study' 2002. Elhalbi Publisher – Beirut (Arabic Text)
- Ahmad Sharaf Al-Din, 'Validity of Evidence of Electronic commerce' 2007 the Arab Organization for Administrative Development – Dubai
- Batle Ghania, 'Electronic writing as evidence', *Tawasul of Social and Humanitarian Sciences Journal*, 2012 (30).
- Article 211 of Civil and Commercial Procedure Law No 13 of 1990, *Al-Jarida Al-Rasmiya*, 1990-09-01, No. 13, pp. 1-83.
- Article 216 of Civil and Commercial Procedure Law No 13 of 1990
- Abdul-Aziz Hamod, 'Validity of evidence of electronic transactions in civil and commercial in the light of the rule of evidence', *Journal of Legal and Economic Research*, 2002 (11)
- See Stephen Masom, gen ed, *Electronic Evidence*, 2.18 – 2.27.
- Mohammed Abu – Zaid, 'Validity of Evidence of Electronic Transactions Comments on the Provision of Judiciary' *Dubai Judicial Institute Journal*, 2012 1(1) –Electronic Evidence, chapter 4, especially 4.12.

- UNCITRAL Model Law on Electronic Commerce Guide with to Enactment with 1996 with additional article 5 bis as adopted in 1998. Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
- Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), 16 – 82. See also Nazzal M. Kisswani and Anas A. Albakri ‘Application of Electronic Signature in Business and Its Influence on Electronic Commerce Implementation’, *International Journal of Liability and Scientific Enquiry*, (2010) 3(4), 282–290
- For a list of the other functions that a signature is capable of, see Stephen Mason, *Electronic Signatures in Law*, 8 – 10.
- Thomas J. Smedinghoff, *Electronic Contracts & Digital Signatures: An Overview of Law and Legislation*, 564 P.L.I. PAT. 125, 162 (1999).
- Alan Tyree et al, ‘Banking Law and Banking Practice’ (2006) 17 *Journal of Banking and Finance Law and Practice*, 47-50
- Brian F. Fitzgerald, Anne M. Fitzgerald, Timothy Beale, Yee Fen Lim and Gaye Middleton, *Internet and E- Commerce Law: Technology, Law and Policy* (Lawbook Co., 2007), 543.
- Gavin Jones, ‘Failing in Treatment of Electronic Signature’ (2003) *Hertfordshire Law Journal*, 1(1), 101-106; for a more up-to-date treatment, see Stephen Mason, *Electronic Signatures in Law*, Chapter 7 ‘Digital Signatures’ which includes examples of case law where digital signatures have failed.
- Nazzal M. Kisswani and Anas A. Albakri ‘Application of Electronic Signature in Business and Its Influence on Electronic Commerce Implementation’, *International Journal of Liability*

and Scientific Enquiry, (2010) 3(4), 282–290.

- For a list of other forms of electronic signature, including case law from across the world, see Stephen Mason, *Electronic Signatures in Law*, 187 – 258.
- Article 23 of the Qatari Penal Code No 11, 2004
- Article 22 of the Qatari Penal Code No 11, 2004
- Article 67 (8) of Qatari Electronic and Transaction Law No. 16 of 2010
- Article 354 of the Qatari Penal Code 2004
- Muner M. Ganbaha and Mamdouh M. Ganbaha, *Cybercrimes and Computer and Means of Control 2005 Dar Alfaker Al Arabi, Alexandria P 90*
- Mohamed Amin El-Shawabka, *Computer Crime and Internet-cyber Crime 2007 Dar al-Thakafah, Amman,, p. 234.*
- Adrian McCullough and William Caelli, “Non-Repudiation in the Digital Environment, volume 5, number 8, August 2000, http://firstmonday.org/issues/issue5_8/mccullagh/index.html at May 2014\
- Article 71 of Qatari Electronic and Transaction Law No. 16 of 2010
- Article 375 of the Qatari Criminal Procedures Law no. 23 for 2004
- Article 27 (2) of the Qatari Criminal Procedures Law no. 23 for 2004
- Article 332 of Qatari Penal Code

Subject	Page
Abstract	101
Key Words	101
1. Introduction	102
1.1 Effective Scope of E-commerce Law	102
1.2 Respect for the Principle of the Legality of Crimes and Penalties of Punishment	104
2. Validity of Electronic Documents As Evidence	105
2.1 Validating the Electronic Contract with Reference to the Conditions Related to the Written Evidence	106
- Writing Must be Legible	107
- Writing Must be available	108
- Assurance of the integrity of the document	108
3. Validation of Electronic Documents	109
4. Electronic Signature	110
4.1 Definition of Electronic Signature	110
4.2 The Validity of the Electronic Signature in Evidence in Accordance with Qatari Law	112
5. The Nature of the Criminalization Provided in the E-Commerce law	114
5.1 General Deterrence Impact	116
5.2 Liability of Legal Person and those in Charge of Actual Administration	117
5.3 Repetition of Offence	118
5.4 Judicial Control Capacity	119
5.5 Scope Application of Provisions of E-Commerce and Transactions in Terms of Place	121
6 Conclusion	122
References	123