

# MPRA

Munich Personal RePEc Archive

## **Iranian Electronic Commerce Law**

Zar Rokh, Ehsan

14 August 2007

Online at <https://mpra.ub.uni-muenchen.de/8502/>  
MPRA Paper No. 8502, posted 28 Apr 2008 14:19 UTC

# **Important Concepts**

## **In**

### **Iranian Electronic commerce law**

**Author: EHSAN ZARROKH**

**LL.M at Ashrafi University**

**E-mail: [e.zarrokh@gmail.com](mailto:e.zarrokh@gmail.com)**

#### **Abstract**

*The recently (2003) Iranian legislator authorize act about Electronic commerce in Iran and this Law consists of a set of rules and principles to be applied for easy and secure communication of information in electronic intermediaries using state of the art communication systems.*

*Legislator state many phrase in this act that they don't exist before it. So I going to discussing about these terms such as electronic signature, secure electronic record, Means of Telecommunication, Certification Service Provider, Marketing, Data Protection, Trade Secrets & Trade Names, Fraud with computer, Forgery with computer.*

*In this paper I review and criticize this law and its executive by-law and state it's Contradiction with Islamic laws (SHARIA) and then I offer solution for its problems.*

**Keyword: electronic commerce, Contradiction, criticize, Iranian**

#### **Introduction**

**Near seven years ago electronic commerce starts in Iranian society briefly and slowly boom in our country, but we have many problems with it because there isn't any rule in this topic and our courts has couldn't solve people sums about this, so after three years our legislator decide to authorize in electronic commerce in 2003.**

**Also they predict executive by-law for it, now four years past than approve it so we see the results of its execution and we know its problems bodily; it's necessary to say there is some article against Islamic rules (SHARIA) and Iranian**

institutions. Now we talk about its innovations in our legal system and its problems.

## **1) Electronic Signature & secure electronic record**

### **1-1) Electronic Signature**

In this act it's defined as: any sign appended or logically affixed to a "data message" which may be used to identify its signatory.

It can be scanned sign on paper with scanner, image or any thing else that indicate signature identity.

### **1-2) secure electronic record**

A secure electronic record is a "data message" which is stored by the observance of the requirements of a secure information system and is accessible and perceivable when needed.

Both of them must have following condition for acceptance in court:

- a) Be unique to the signatory.
- b) Identify the signatory of "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 data message can be detected and identified.

### **1-3) Admissibility, Evidential Value, and Consequences of Secure Electronic Record and Signature**

Evidence and any supporting document may be in the form of "data message". The evidential value of a "data message" can by no means be repudiated solely due to its form and framework at any court or governmental office.

In general, the evidential value of a "data message" depends on the methods used to guarantee its security such as selecting a security measure that corresponds to the subject and purpose of the "data message".

All "data messages" which have been generated and stored via secure method are deemed to be valid and reliable documents by judicial or legal authorities in terms of what they contain as well as included signature therein, obligations of both parties or the party who covenants and all persons who act legally on their behalf, and effecting the terms and conditions contained therein.

The validity of a secure "data message", secure electronic record and secure electronic signature may not be questioned or denied; only a claim of forgery of a "data message" or a proof of its invalidity on a legal basis may be considered.

Any "data message" recorded and retained by a third party in accordance with the provisions of Article 11 of this Law, is deemed valid.

There is a problem that we haven't act about identity and identity theft, so it's necessary that our legislator approve act for it.

## **2) Means of Telecommunication**

Means of Telecommunication are: Any means which, without the simultaneous physical presence of the supplier and the consumer, may be used to sell goods and services.

In this act legislator define Means of Telecommunication; there are many difficult such as: there is no article about Telecommunication crimes and related offense in our legal system, the variety of criminal activity which can be committed with or against telecommunications systems is surprisingly diverse. Some of these are not really new in substance; only the medium is new. Others represent new forms of illegality altogether. The following generic forms of illegality involving telecommunications systems as instruments and/or as targets is the subject of our inquiry. These are not necessarily mutually exclusive, nor are the list complete. They do, however, represent the primary areas of concern for policy makers. Also about procedure about this, because or acts aren't based on new offense as cyber crimes.

## **3) Certification Service Provider**

Certification Service Providers are established to provide electronic signature services nationwide. These services consist of generation, issuance, transmission, confirmation, dismissal and update of electronic signature certificates.

Regulations for the establishment of certification service provider, and the detailed liabilities of such centers prepared in their executive by-law, but now there is ambiguity in their criminal liability and we faced with silence of the law.

## **4) Marketing**

Under this act suppliers must observe following terms:

- 1- Suppliers, in the process of marketing their goods and services, shall not commit or exclude an act that may mislead and deceive the addressee in terms of quantity and quality.**
- 2- Suppliers who are advertising for the sale of their goods and services shall not endanger people's health.**
- 3- The supplier shall advertise in such a manner that would enable the consumer to precisely, accurately, and clearly understand the description of the advertised goods and services.**
- 4- In advertising and marketing processes, the identity of the person or business that is advertising should be clear, and evident.**
- 5- Suppliers shall not take advantage of the special features of electronic transactions to conceal facts in relation to their identity or place of business.**
- 6- Suppliers shall provide the consumers with the required arrangements that would enable them to choose whether to receive the advertisements at their mailing or e-mail address.**
- 7- Suppliers shall act professionally.**
- 8- Observe rules about advertisement and marketing for children and young people under the legal age.**

**They are most important terms in marketing that legislator state in this act.**

**May we have telemarketing fraud means: the use of the telephone for fraudulent sales pitches, phony charitable solicitations, or bogus investment overtures is a billion dollar a year industry in the United States. The intensification of commercial activity in the United States and globally, combined with emerging communications technologies, would seem to heighten the risk of sales fraud. Already we have seen the emergence of fraudulent sales and investment pitches on the Internet. Developments in electronic marketing will provide new opportunities for the unscrupulous and new risks for the incautious.**

## **5- Data Protection**

**Data protection is considered with legislator in several way, that express in electronic commerce he said: Storing, processing or distributing private "data messages" which may reveal tribal or ethnic origins, moral and religious beliefs, ethical characteristics, and "data messages" regarding the physical,**

psychological, or sexual condition of people, without their explicit consent is illegal.

Distributing personal "data messages" via electronic means shall be subject to the following terms:

- a) Its goals shall be specified and clearly described.
- b) The "data message" shall be collected to the required extent and in compliance with the goals described to the person who is the subject of the "data message" while collecting the information and be applied merely for the goals set out therein.
- c) The "data message" shall be correct and up-to-date.
- d) The person who is the subject of a "data message" shall have access to those computer files containing his/her personal "data messages" and be able to remove or amend partial or incorrect "data messages".
- e) The person who is the subject of "data message", while adhering to the regulations, shall be able to request the complete removal of the computer files of his personal "data messages".

## **6) Trade Secrets & Trade Names**

### **6-1) Trade Secrets**

Electronic trade secrets are "data messages" consisting of information, formulas, patterns, software and programs, means and methods, techniques and procedures, unpublished writings, business and transaction methods and Procedures, strategies, plans, financial information, customers list, trade projects and the like which have an economic value by themselves, are inaccessible to the public and reasonable efforts have been made for their protection.

In order to protect legitimate and fair competitions in electronic transactions, illegal acquisition of trade or economic secrets of agencies and institutions or the disclosure of such secrets to third parties in electronic environment is deemed an offence and the offender will be sentenced from 6 months to 2.5 years in prison or a penalty of 50,000,000 RIALS.

### **6-2) Trade Names**

In order to protect consumers' rights and encourage legitimate competition in trough electronic transactions, use of trade marks as domain name or any online usage of trade marks which may mislead or deceive the other party in terms of

**the originality of goods and services is illegal and the offender will be sentenced from one to three years in prison and a penalty of 20,000,000 to 100,000,000 RIALS.**

#### **7) Fraud with computer**

**Anyone who deceives others or misleads auto- processing systems and the like, during an electronic transaction, by misuse or unlawful use of "data messages", programs, computer systems, and means of distance transaction, and committing such acts as penetration, removal, and termination of a "data message", interfering with the application of a computer system or program, etc. and by means of this method obtains property or financial concessions for himself or others, is deemed an offender and in addition to the return of property to its owner is given a one to three year sentence in prison and pecuniary punishment equal to appropriated property. And initiation of such crime is also deemed to be a crime and its penalty is the minimum punishment of fraud with computer.**

#### **8) Forgery with computer**

**In electronic transactions, anyone forging "data messages" which are of financial and evidential value in order to use it as a valid "data message" in judicial, financial offices, etc, by means of penetration, removal, and termination of "data messages" and interference with computer systems and "data message" processing, or use of applied means of encryption systems to make a signature – like private keys – without signatory's permission, or by making a signature lacking registration record in electronic registration offices, or non-compliance of those means with the name of the owner in the same list and obtaining a forged certificate and the like, is considered a forger and sentenced for one to three years imprisonment and a cash penalty of 50,000,000 RIALS.**

**The penalty of initiation of this crime is the minimum of the punishment of forgery with computer.**

#### **9) Reasonable Test**

**It is evaluated based on the status of a "data message" communication, taking into consideration the nature of communication, parties' skill and position, their communication quantity, accessibility of the proposed options, and their dismissal by either side, expenses arising from proposed options, customary methods applied in such communications.**

## **Deduction**

**Electronic commerce is a new science in Islamic republic of Iran and it engender for answer to society needs so for best execution it's necessary to approval acts in this case and Iranian legislator do it in electronic commerce law at 2003. Now after 4 years from execution of this law we understand it's difficult and we can critic of it.**

**I state some of the most important concepts of Iranian electronic commerce law and explain most of them.**

## **References**

- 1. Iranian electronic commerce, judiciary publisher ,Tehran, 2003**
- 2. criminal law, judiciary publisher ,Tehran, 1997**
- 3. penal procedure law, judiciary publisher ,Tehran, 2001**
- 4. Iranian fourth developing program, judiciary publisher ,Tehran, 2006**
- 5. Eskini-Rabia, commercial law, Samt publisher, Tehran, 2003**
- 6. Erfani-Mahmoud, commercial law, Dadgostar publisher, Tehran, 2005**