

Legal Protection of Electronic Commerce Data in Yemeni Law

الحماية القانونية لبيانات التجارة الإلكترونية في القانون اليمني

Dr. Hussein Al-Ghushami ⁽¹⁾

⁽¹⁾ Assistant Professor in College of Law , Dar Al Uloom University
(Saudi Arabia)

Dr_ghashami@yahoo.com

Received: 08/11/2019

Accepted: 20/01/2020

Published: 26/01/2020

Abstract:

With the advancement of modern information and technology, there has been a parallel progress in this field carrying its name and called “cybercrime”. Consequently, the cybercrime level has increased with the growing use of the network, “Internet”, which has begun an impressive means of knowledge and sharing information. Over time, Internet quickly became a means of committing crimes, and their forms and manifestations were numerous. It was not limited to hacking, sabotaging or stealing information, but also theft crimes of sensitive information of different military, financial, economic and political types have emerged in addition to other crimes on the web.

The research focuses on addressing the level of protection of electronic data by exploring to what extent the legal texts are available, compatible and adequate to provide protection for e-commerce data in Yemeni law.

Furthermore, this research paper aims to analyze the texts of the Yemeni laws related to the subject matter of the study in order to highlight the strengths and weaknesses in relation to the subject matter. To this end, the researcher has used the descriptive analytical method.

Keywords :Legal protection- Electronic data- Commerce data

الملخص:

في الوقت الذي تتقدم فيه ثورة المعلومات والتقنية الحديثة ، يقابل ذلك الإنجاز تقدم آخر مواز في هذا المجال صيغت باسمه وأسميت بالجريمة الإلكترونية أو المعلوماتية، وبالتالي تزايد خط الجريمة الالكترونية مع تزايد مستخدمي الشبكة العنكبوتية "الإنترنت" التي بدأت وسيلة مبهرة للمعرفة وتبادل المعلومات وسرعان ما تحولت بمرور الوقت إلى وسيلة لارتكاب الجرائم وتعددت صورها وأشكالها ولم تقتصر على اقتحام الشبكات وتخريبها أو سرقة معلومات منها فقط بل ظهرت جرائم سرقة المعلومات الحساسة بشتى أنواعها العسكرية والمالية والاقتصادية والسياسية وغيرها من الجرائم على الشبكة العنكبوتية.

يركز البحث على معالجة مشكلة مستوى حماية البيانات الالكترونية من خلال استكشاف مدى وجود أو ملائمة النصوص القانونية وكفايتها لتوفير الحماية للبيانات التجارية الالكترونية في القانون اليمني.

تهدف هذه الدراسة إلى تحليل نصوص القوانين اليمنية المتعلقة بموضوع الدراسة من أجل إبراز مواطن القوة والضعف فيما يتعلق بموضوع الدراسة. ولتحقيق هدف الدراسة استخدم الباحث المنهج الوصفي التحليلي. وتوصلت الدراسة إلى مجموعة من النتائج والتوصيات من أهمها ضرورة إصدار القوانين المتعلقة بأساليب ووسائل حماية المعاملات الإلكترونية التي من شأنها الحفاظ على سرية رسائل البيانات ومنع الأشخاص غير المرخص لهم من الوصول إلى رسائل البيانات أو إفسادها، وحماية البيانات الاحتياطية. ونخص منها:

- قانون مكافحة جرائم المعلوماتية.

- قانون التجارة الالكترونية.

الكلمات المفتاحية: البيانات التجارية - البيانات الالكترونية - الحماية القانونية

Introduction

The world witnesses tremendous and rapid development in the field of Information Communications and Technology (ICT). At the forefront of that development is the Internet, which has become indispensable for providing information and communication among people around the world. Geographical boundaries and temporal differences around the world have been removed and the world has become a small village as one of the key features of the era of globalization.

The most important aspects of these technological developments and the revolution in ICT are the emergence of online contracts, sales and purchases.

In light of the commercial, industrial and economic growth as a result of the modern technological, electronic and informational development and markets globalization, commercial companies, public and private institutions and individuals found themselves facing an evolution in the means of communication represented by the International Information and Communication Network (the Internet) which provides fast and easy communication services all over the world. This reality led people to use the websites provided by the Internet leading to the birth of the so-called e-commerce, which was accompanied by the emergence of new and sophisticated crimes (cybercrime) in its various forms.

Cybercrime constitutes an economic and electronic crime at the same time, the main objective of which is the illegal financial gain of the money of the people consuming individuals, institutions or governments. Cybercrime, moreover, involves an attack on the development of societies because it causes huge material losses in different electronic means that give cybercrime the opportunity to develop and change rapidly and consequently makes it difficult to detect and monitor its cases and prove their physical and visual nature. Herein lies how serious and legal problematic cybercrime is.

For this reason, cybercrime will be addressed here by demonstrating the appropriateness of legal texts and their adequacy to provide protection for electronic data in Yemeni law. Therefore, the importance of this study is highlighted by the importance of the subject-matter and the failure of the governing legal systems to keep abreast of all the risks to which electronic data is exposed. To achieve the study objective, the researcher used the descriptive analytical method.

In the light of the foregoing, the researcher shall address the legal protection of e-commerce data according to the following sections:

The Concept of E-Data

Legal protection of Electronic Business data

The Concept of E-Data

There is generally a synonym between information privacy and data protection. The prevalence of the use of the term “privacy” separately and apart from the word “data” in the electronic environment or academic studies, technical studies, research and reports of business sectors to denote data protection is due to the fact that the term “privacy” is common by itself in light of the increasing risks of technology to the extent associated with its use as if

it were limited in scope and environment, which is definitely not. However, perhaps due to the most violation of this right is by technical means and the risks of e-data processing. Therefore, the use of the term “privacy” in the Internet environment and issues of technology contracts or services generally refers to the protection of information privacy or data protection.¹

Article 2 of Law No. (40) of 2006 on Payment Systems and Electronic Financial and Banking Transactions defines data message as “A set of commands and numbers that need to be processed, organized, or reorganized into information, and may take the form of text, numbers, shapes, graphics, images, recording, or any combination of these elements.”²

Electronic Databases

Computers can handle many types of data. The following are the main types of e-data:

1.Texts: Information in the form of readable text such as the text you are reading now.

2.pictures and drawing

3.video

4.Audio

Computers can deal with mixed data types from the above list such as databases that may contain text and images and sometimes contain video and audio as well. Computer can also convert between many forms of data such as converting text to audio.

Computer data are divided into two parts:

1.Numeric data: the data can only take on certain values, for example, the alphabets are not other than one of the twenty-eight letters known in Arabic. The other example is the decimal which is not less than ten digits specified in the decimal system between 0 and 9.

2.Symbolic data: data that takes too many values such as the sound intensity, temperature, and can have any value between its maximum and minimum limits.³

The Concept of Electronic Databases

Online information resources, also known as a (DATABASE), are a set of logical data elements linked together with mathematical relationships, so that the database consists of one or more tables as needed, and that one table consists of one or more records, and a record contains one or more fields.

In other words, it is a computer system whose general purpose is to store data and allow users to retrieve and update this data when needed.

The European Decree of 11 March 1996 also defined databases as “Each set of independent works, data or other material arranged in a systematic or systematic manner that can be viewed individually by electronic or other means.”⁴ The database has three components; the base itself, the data, and the program it operates. Both the program and the base belong to separate copyright to different authors. The data is a protected work independently of the base. Therefore, the author of the base must obtain authorization of the author or owner of the data in order to use the data. If the data is not protected or a copyright, the owner of the base can use of it at his will.⁵

Electronic Database Parties and Components

The preparation of electronic database and information goes through several stages, the first stage is the selection and tracking of the information field, followed by the stage of building the information system, then the stage of loading and inserting information on the electronic transmission medium. Each stage is specific to a particular person as follows:

1.The Owner\Author of the information: is the source of the information or the author of the message that is transmitted on the Internet, and is responsible for all the contents of the information, whether legal or illegal or contrary to the law, criminally or civilly⁶.

2.The Host Contractor: a natural or legal person that registers applications on web servers and information records for customers. It offers to host paid web pages and provides customers with the means of technology and information that enable them to access that inventory via the Internet around the clock. It is therefore a lessor of a location on the web for a tenant, who is the publisher who publishes texts or images, organizes conferences, or creates information sites linked to other sites.⁷

3.Access Operator: A natural or legal person that performs a technical role to connect the subscriber to the Internet, under subscription contracts guaranteeing connection to the desired sites, where it plays a purely technical role and has no connection with the information material or its subject matter⁸

4.Information Carrier: is the person that is responsible for the physical transfer of information, a natural or legal person or technical body, which, by its own means, connects the networks to the server

computer of the access operator and then transfer information from this latter computer to the computers associated with the Internet site or other network users, where the role of the carrier is limited to securing the transfer of information and linking between the various units. This task is often carried out by the telecommunications authority or company which contracts with Internet service providers and projects and organizations with subscriptions on the public network or rent specialized lines on the network⁹

5. Intermediaries in the Internet Service: The Internet is operated through various activities and roles played by a group of people called intermediaries in the Internet service. Their role is limited to enable subscribers to access the Internet and tour the Internet and see what they want to browse. Some of these people transmit the service, some of which enable the subscribers to access the site, and some store, produce or supply information. Persons who transmit the service, some of which enable the subscribers to access the site, and others store, produce or supply information.¹⁰

Some people call the system installer the natural or juridical person to whom information is produced, whether from the base owner or others, to build a valid information system for transmission via electronic means, where the selected information is placed at the disposal of a specialist to build an information system that ensures permanent and automatic storage.¹¹

6.Information Provider: Any natural or legal person that acts as a mediator between the author of the site content and the Internet user who wants to browse this site. He loads the system with the information he has written or collected in a particular topic so as to reach the audience in the form of information material on the network, so he has full control over the information material that is transmitted over the network.¹²

Thus, the service or information provider on the network is the natural or legal person who puts the integrated end product of a set of information related to one or more areas on the agreed electronic medium so that the subscriber can exploit it and benefit from it in accordance with the terms of the contract concluded in advance.¹³

Database Components:

Database systems consist of several components, which combine to form an integrated and interconnected system as follows:

1.Data: it is the point at which all components of database systems function, and data is entered and stored in an individual database in larger systems, each of which will be intertwined and shared.

2.Hard Ware: The hardware and accessories components of the system consists of:

- Secondary Storage Devices: They are mostly magnetic disks, which are used to save the stored information and its association with different devices and disk drives ... and others.
- Devices associated with the presence of master memory, which is used to support the implementation of system software for the database.

3.Soft Ware: Since the database helps achieve a set of objectives affecting the main activities in the areas of applications of automated data processing, it is necessary to have certain systems for the organization and management of stored data and therefore it is necessary to provide a number of programs, including programming systems for databases in addition to programs for personal computers and networks.

One of the most common programs is Database Management Systems (DMS). All database access requirements are handled by DMS which give the necessary facilities to add or delete files or columns in order to retrieve or update information in such files or tables, and so all these facilities are offered by DMS.

The database as a classification enjoys the legal protection established by the Copyright Protection Act, not as part of it, but since it would not function without such programs. The Yemeni legislator granted protection to the database, as in Article 3 of the Law on the Protection of Copyright and Neighboring Rights provides that databases and the like shall enjoy the protection prescribed by copyright law.¹⁴

Protection Methods of E-Business Data

Data Damage Crimes¹⁵

Crimes of data damage are the most serious, impactful, frequent and loss-making cybercrimes affecting individuals and organizations alike. These felonies include all activities involving alterations, deletion, identity theft or (Digital Form) destruction or disruption of the function of information and databases that electronically exist in the information networks or simply attempting to access them illegally.

The simplest of these activities is the intrusion to information systems and databases and then leaving without creating any negative impact on them. This type of activity is carried out by the so-called White Hat Hackers, who access computer systems, information networks, or websites without permission with good intention to exploit some of the vulnerabilities in those systems, violating the information security policies and procedures of the System And Network Administrators. Unauthorized access to an organization's central computer room without causing any damage is though deemed a breach of the information security policy and procedures of that organization.

Network Intrusion, especially digital networks "Internet", to hacker databases or websites and obtain unauthorized information or most probably take full control over these systems, despite the existence of multi-degree protection measures against firewalls and intrusion detection and prevention systems as well as mechanisms for encrypting data and complex passwords, and then leaving without creating any change or damage to the information systems is the simplest types of hacking that gives a red signal to the managers of systems and information security that their policies and operational procedures for information security need to be modified or changed and that they have to re-build the security system and periodically testing and analyzing threats and vulnerabilities (Risk Assessment) to keep up with new methods of hacking.

As for the alteration, deletion, identity theft, destruction or disruption of the function of information systems, such activities are carried out by amateur or professional individuals called Black Hat Hackers who may do such activities for the purpose of material or moral benefit of the data and information they seize or for the purpose of harming the owner of such systems because of personal, tribal, political or religious hatred, or doing so on behalf of a competing organization.

Denial Of Service Attack (Dos), which relies on disrupting server devices with thousands or millions of requests for information, which is not tolerated by the capacity of hardware components or database systems, applications and software on those servers which are completely paralyzed by their inability to respond and deal with this huge number of requests at the same time. It takes many hours for the system and network administrators to identify the sources of their attack and system defects and restore normal functioning. Of course, these hours when the information system is down, the organization incurs significant material losses, in addition to the disruption of

the interests of their users, the loss of confidence in that organization and losing existing clients to competing organizations whenever possible.

Electronic Commerce Data Protection

With the advent and proliferation of the Internet and information technology and the large number of individuals and institutions who visit this network, it has become easy to commit the most heinous crimes against its users, whether individuals, institutions, countries or entire communities. This makes us wonder whether there is a legal system punish the perpetrators of information crimes in Yemen?

Reviewing the laws of Yemen, it is observed that there is a legislative gap in the protection of electronic data, where no law was passed in Yemen to regulate it, except for the law of electronic payment¹⁶, which deals with these crimes in part. There is also a draft law called the law against information crimes; however, it is still under study and debate by the government side.

The legislative gap in these crimes is due to the fact that they are new crimes, especially when Yemen is still at the beginning of electronic business. However, now, the volume of those crimes that committed on the Internet requires the passing of a law that identifies responsibility and punishment, defines cybercrimes, their elements and criminal intent therein, given that traditional criminal and penal laws no longer serve to deter cybercriminals.

Since we have become in the age of globalization and in the light of the fact that the world has become a small village, it is necessary to have legal models with substantive and procedural rules that do not contradict with the previous national legislation. Therefore, it becomes a prerequisite to study and review all other laws and decrees in force in the fields of communication, electronic payment, procedural or substantive punitive laws, as well as laws on information exchange and protection of the right to privacy so as to be adjusted to keep up with developments in the field of information and communications crimes whenever necessary. To this end, it is necessary and important that legislative amendments be consistent with the prevailing patterns of cybercrime in most countries of the world, given the fact that the nature of those crimes is cross-border and requires cooperation between many countries to be controlled and traced because of the rapid development of means, tools and forms of cybercrime and the necessity that such legislative amendments keep pace with those ongoing developments. In addition, it is necessary to take advantage of the newly legislated agreement on global cyber security and motivate international cooperation in the protection of information security, especially since Yemen has recently joined the World Trade Organization.

Laws on cybercrime should be promulgated and international cooperation in this regard should be conducted through signing special

conventions against cybercrime, in particular the European Convention against Cybercrime of 2001 (Budapest Convention), which is the first convention in this regard, signed by 26 member states of the Council of Europe; and pursuant to Article 37 of the Convention providing for accession by non-members, the Convention has been signed by the United States of America, Japan, Canada and South Africa.¹⁷

It should be noted that Yemen has approved the Arab Convention against Information Technology Crimes.¹⁸

Among the forms of cybercrime, which is the illegal access to the systems of data rules and processing in the websites, hacking websites, whether by deleting, copying, modifying or obstructing the operation of the site, in addition to the crimes of personal electronic data and electronic funds and falsification of electronic signature.

It is clear that crimes committed through the Internet against electronic commercial data may target information in order to manipulate the information stored in the device or intercept information sent between computers connected to one network with the purpose to mislead by altering, misrepresentation and forgery, or targeted funds with the intention to penetrate financial transactions, identity theft or embezzlement.

In view of the seriousness of these crimes, we need to quickly pass laws that take the lead in discussing ways and means of protecting electronic transactions that will keep data messages confidential, prevent unauthorized persons from accessing or corrupting data messages, and protect backup data. Some of them are:

- 1.Law against Information Crimes.
- 2.Electronic Transactions and Trade Law.

Given the fact that the Yemen's traditional penal law does not meet the intended purpose, even if cybercrime is in its early stages, it will not guarantee its future danger.

Conclusion:

At the end of this research, these are the key findings and recommendations:

- There is a legislative gap in the protection of electronic data, where not a single law was passed in Yemen except for the law of electronic payment, which addresses these crimes in part.
- There is a draft law against information crimes which is still under study and debate by the government.
- The necessity to pass laws related to the methods and means of protecting electronic transactions that maintain the confidentiality of data messages, preventing unauthorized persons from accessing or corrupting data messages, and protecting backup data. Some of them laws are:

- a. Law against Information Crimes.
- b. The Electronic Transactions and Trade Law.
 - The need for Yemen to establish a specialized division to investigate computer crimes.

Reference List

Younes Arab: Privacy and Data Protection, a research published online at: www.arablawnet.net.

Article 2 of Law No. (40) of 2006 on Payment Systems and Electronic Financial and Banking Transactions.

Ziad Al-Qadi, Abdul Rahim Al-Bashiti,(2008) Introduction to Computer Science, Dar Safaa Publishing & Distribution, Amman.

Mohammed Mahmoud Zain Uddin,(1431) Digital Databases and Their Importance in Building Search Engines, Journal of Informatics, Issue no. 29.

European Decree of 11 March 1996 on the Legal Protection of Databases supplementing the protection guaranteed by the Copyright Law. Osama Ahmed Badr, Multimedia, New University House, Alexandria, 2004 edition.

Osama Ahmed Badr,(2004)(Multimedia, New University House, Alexandria.

Abdel Fattah Bayoumi,(2000) Legal System for the Protection of Electronic Commerce.

Abdel Fattah Bayoumi,(2000) Legal System for the Protection of Electronic Commerce.

Mohammed Hussein Mansour,(2007) Electronic Responsibility, New University House, Alexandria.

Abdel Fattah Bayoumi,(2000) Legal System for the Protection of Electronic Commerce.

Abdel Fattah BayoumiHegazy,(2009) Crimes Developed in the Scope of Modern Communications Technology, El Maaref Establishment, Alexandria.

SaadHammam, The Legal System of Consumer Contracts in the Field of Electronic Information, Ph.D. Thesis, Faculty of Law, Zagazig University.

Abdel Fattah BayoumiHegazy,(2009) Crimes Developed in the Scope of Modern Communications Technology, El Maaref Establishment, Alexandria.

Aladdin Abdullah Al-Khasawneh,(2010) Responsibility of Internet Service Providers in accordance with the French Law on Confidence in the Digital Economy, a research published in the Research Group of Professional Responsibility Conference, Faculty of Law, Yarmouk University, Jordan, April.

Abdel Hamid El-Dasti Abdel-Hamid,(2010) Consumer Protection in the Light of theLegal Rules of Product Liability, Comparative Study, Ph.D. Thesis, Mansoura Rights, Dar Al Fikr and Law, Mansoura.

Adel Abu Hashima,(2004) Contracts of Electronic Information Services in Private International Law, Dar Al-Nahda Al-Arabiya, Cairo.

Article 3 of the Yemeni Copyright and Related Rights Law of 2012.

Majdi Fouad,(2010) Cybercrime and Protection of Intellectual Property Rights, 2009. Mohammed Ali Qutb, Cybercrime and Countering Methods, Bahrain Police Academy.

Computer and Internet Crimes (Information Crimes) By: Prof. Brigade. Fouad Gamal, <http://almohakmoonalarab.ahlamontada.com/t91-topic>, accessed on 21 Jun. 2019.

Law No. (40) of 2006 on Payment Systems and Electronic Financial and Banking Transactions.

Yemen's accession to the WTO entered into force in June 2014.

Cybercrime in the Gulf Society and Countering Mechanisms, Sultan Qaboos Academy for Research and Studies, GCC General Secretariat, 2016.

Concluded in Cairo, signed on 21 Dec. 2010, and approved by the Council of Ministers in 2011 after which the agreement was referred to the House of Representatives.

Swindells, C. and Henderson, K. (1998) Legal regulation of electronic commerce. *Journal of Information Law and Technology*, 3. ISSN 1361-4169