Cybercrime and Penal Code: A Comparative Study between United Arab Emirates and Japan

by

Fawaz Abad Aldurra

A thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Law

Department of Criminal Law
Faculty of Law
Fukuoka University, Japan

December 2013

Abstract

Criminal law plays a prominent role in the life of society and performs several functions: people from committing acts that harm others or society; determining the conditions under which people who have performed such acts will be punished; and providing some guidance on the kinds of behavior that are regarded by society as acceptable.

This study tackles the subject of association that is increasingly growing in the comparative law studies, which is the information technology law with some specification, i.e. specific branch of law which is criminal law. Therefore, this subject tackles the relation of information technology with the criminal law.

In this study, we will tackle such relation in the comparative legislation between information technology and criminal law as the state of the United Arab Emirates (UAE) represented in the law of information technology crimes and Japan represented in the penal law have approached two different schools to combating the information technology crimes.

The Japanese school adopts the approach that considers the crimes of information technology as a traditional crime. Notable, Japan has not issued to date any law of the information technology crimes, except for some special cases such as the law of unauthorized access issued in 1999. The Japanese legislator amends the articles of penal law as the case in 1987 in order to plug the legal loophole in such type in the penal law.

The UAE School adopts the approach that considers such type of crimes of a special nature that needs a special law. In 2006 the first UAE Law was issued to combating the information technology crimes (UAE cyber law). We will clarify the features of this type of crimes, the most important of which are the tremendous development of the means of information technology and difficulty of detecting and gravity of such crimes.

We have chosen this subject in order to know the means used by Japan and UAE to combating the information technology crimes and extent of applying the traditional legal rules in addition to the necessity of issuing new legislations especially in the presence of the international agreements that require such legislations. Thus, this research tries to:

- State the concept of information technology crimes, recognize the features thereof and state how the characters of cybercrime focused on the punishment of the committer thereof.
- State how valid is the criminal provisions of the Japanese and UAE Laws in order to know all the aspects of such crimes,

- State the legislative failure and propose the necessary solutions for replenishment as much as possible.

Acknowledgment

First and foremost, I thank Almighty Allah for His Divine Favor in granting me the strength and presence of mind to carry out this work.

I would like to express the deepest thanks and appreciation to HH Lt. General Sheikh Saif bin Zayed Al Nahyan, Deputy Prime Minister and Minister of Interior, for his prudent directives and ongoing support to the UAE students and researchers to be able to achieve the aims and objectives.

Special thanks to Major General Mohammed bin Al Awadhi Al Menhali, Director General of Human Resources, for supporting my research.

I owe special gratitude to my family for their continuous and unconditional support: to my wife for the interest she showed in my studies and the motivation she gave me during those tiring times when I had doubts about my studies, and to my children for their love and spiritual encouragement.

Above all, this thesis is dedicated to my mother and father. Their love, support and prayers in all that I have done until now are the keys to all my achievements.

Contents

CHAPTER 1

INTRODUCTION

CHAPTER 1

1.1 General View

Successive technical sophistication in computer's hardware, software and networks as well as anyone's ability to own and use a computer or mobile phone at home, in the coffee shop or other public place has contributed in a significant change regarding criminal act commission and creating new methods in order to commit cybercrimes. Therefore, the criminal concept has developed, as a criminal no longer need criminal tools and non-traditional tricks; it is enough for a person to be familiar with the use of computer and its systems in order to commit a cybercrime, whether informatics means are a tool of the crime or was the victim of a criminal act. Penal Code's general principle in various legislation and legal systems based on not to expand in applying and interpreting penal rules, as giving a criminal description to an act in addition to impose sanctions on it subjects usually to state's cultural, social and economic necessities considerations. In other words, what is deemed an offense affecting public morals in the United Arab Emirates may be regarded as an expression of public opinion in Europe.

Computer crimes or cybercrime can be divided into two main types:

First type: in which a computer is a tool of committing the crime, such as crimes of embezzlement, plagiarism and pornographic acts. It is common crimes and computer is simply the mean by which it was committed.

Second type: in which computer and computer's networks and software are the crime's subject, i.e. the criminal act has committed on this device, such as penetrating a security system, sending a malicious program or infringing a Web site title. This type constitutes an offense affects intellectual property rights.

Informatics programs and tools have become used as an effective means in order to commit ordinary crimes; as the concept or criminal elements of these crimes have not been changed, such as fraud, embezzlement, stealing, damaging or threating, however, the way to implement them became by informatics' means instead of the common traditional tricks, for example, threating via e-mail or committing a fraud by manipulating in the information system that stores the details of customers' accounts. The damage with using informatics means may be much larger than previously known cases. In addition, informatics means, like informatics' software and data, may be the crime's subject, such as, abusing informatics' software and data, modify and delete such

data or intercept it. E-commerce and electronic transactions' growth and its spread among the public have contributed in increasing the commitment of such new way of crimes. Courts faced difficulties in amending the general legal provisions contained in the Penal Code to criminalize acts under the subject matter of informatics tools, as the penal text is explained, exclusively, pursuant to the rule (no crime [and] no punishment without a pre-existing penal law), accordingly, it was necessary to adopt new laws that criminalize acts committed to informatics' software and data as recent crimes. Because of information networks as it exceeded geographical borders, such as internet networks that are not subject to the sovereignty of any state and accordingly to the rule of any law issued by a particular national legislation, cyber-crimes have exceeded the national scale. Cyber-crime's situation aggravates daily, where in addition to the crimes committed individually, cyber-crime has become organized to the extent that it has considered as one of war's new methods and one of terrorist attacks means. Therefore, and according to the existing legislative status, it was required to create solutions to the loopholes in the cyber legislation to prosecute cyber-crimes, which exceed the national borders in order to activate its control, and to ensure compatibility of national legislation with it so as not a criminal escape from punishment after committing it and move to another country and in order to pursue a common criminal policy, and promote cooperation among countries.

1.2 Research Plan

This study is divided into eight chapters:

Chapter one is an introduction of cybercrime, research plan, difficulties of the research and the aim of this research.

Chapter two (General significance of the Information Technology Crimes) included six subjects. *The first subject* is definition and the characters of cybercrimes. *The second subject* is discussion the UAE Penal Code showing that the Islamic Sharia is a key source of the law and its impact as well as the division of sanctions in the UAE law. *The third subject* is discussion the legislative stages of Information Technology Crimes Law issued on 2006. *The forth subject* is summary of UAE Information Technology Crimes Law (Cyber law) 2006. *The fifth subject* is UAE Cyber law as amended in 2012. *The sixth subject* is Japanese Penal Code in combating cybercrimes showing the followed approach in facing information technology crimes.

Chapter three (illegal access crime): shows the nature of the illegal access crime in Information Technology Crimes Law and what is meant by the act of illegal access crime. Subsequently, we will explain punishments of illegal access in the law. Furthermore, we will discuss the punishments of illegal access in the Japanese law no. 128 of 1999 punish illegal access to computers and explain the rules, forms and sanctions of this law.

Chapter four (anti-public morals crimes in the internet crimes act): shows articles of the UAE cyber law punished the person who commits crimes related to public morals and ethics. In this chapter, we will address the UAE penal code and how the same punished for committing crimes related to public morals and ethics in compare with the articles of UAE cyber law. In addition we will discuss the consequent on the non-obviously of the term public morals in this act. The second part of this chapter is discussing the act of obscene in the Japanese law. Article 175 of the Japanese penal code punished the act of obscene using modern technology including digital photos, E-mail messages, etc.

Chapter five (crimes of informatics destroy) first: discussing the destruction crime in UAE cyber law. This included the Article 424 UAE panel code and information destruction in the UAE cyber law and its types. Moreover, this chapter discussing Japan penal code and the information destruction crime act.

Chapter six (Information Fraud): in this chapter we will discuss fraud crimes of UAE cyber law. Also, we will explain Article 399 in the UAE penal code and credit card crimes. Secondly, we will show and explain Japan penal code articles of information fraud crimes.

Chapter seven (cyber forgery): this chapter illustrated the information forgery in UAE cyber law in the penal code and the forgery of E-card. Additionally, we will discuss the information forgery in Japan penal code and the E-card forgery.

Chapter eight (recommendations and conclusion): this chapter shows the recommendations and conclusion of this study.

1.3 The Difficulties of Research

The researcher tackle the criminal law and information technology crimes with a rootless subject due to the rarity of references and books in this area as the UAE law of information technology crimes, for example, was issued in 2006,i.e. before few years

and was amended after six years per general decree in 2012. It is difficult to find any research tackling this area before. The study of the UAE law of information technology crimes issued in 2006 started in my Master phase in Japan. We were surprised in October 2012 that the law was amended and consequently we had to amend the research plan in order to amend the legal articles which were considered a legal loophole such as requirement of intention for punishment imposed on Illegal access and punishment on preparation of malicious programs such as viruses.

The subject of information technology crimes is one of the complicated legal subjects due to its association to several criminal, civil, commercial and economic aspects in addition to its connection with technology.

1.4 The Aim of this Research

To study the means used by Japan and UAE for combating the information technology crimes and extent of applying the traditional legal rules in addition to the necessity of issuing new legislations especially in the presence of the international agreements that require such legislations.

Thus, this research tries to:

- State the concept of information technology crimes, recognize the features thereof and the character of cybercrime.
- State how valid is the criminal provisions of the Japanese and UAE Laws in order to know all the aspects of such crimes,
- State the legislative failure and propose the necessary solutions for replenishment as much as possible.

CHAPTER 2

GENERAL SIGNIFICANCE OF THE CYBERCRIME

CHAPTER 2

2.1 Introduction

Cybercrime is defined as all illegal deeds committed by, using or targeting information technology means which damages a right or interest upon which the legislator surrounded with criminal protection.

From that definition, it is clear that the information technology crimes are classified to three key categories as follows[1].

First category: information technology means such as the internet and included information, data or linked systems or devices which deems the subject and target of the crime. An example of such crimes is hacking, information destroying, operating systems malfunction or interruption, virus crime, etc.

Second category: information technology tools or means to commit the crime such as violating private life, assaults and defamation, terrorist crimes, spying, money laundry, drugs trade, etc.

Third category: information technology means is the environment in which crimes are committed. For instance, the internet: building pornographic websites, publishing rumors and reputation defamation, propagating of deviated thoughts, etc.

On the whole, such new category of crimes can be attributable to two types:

First: traditional type that can be divided to two sections, first; crimes that are committed on the internet such as violating private life, assault and defamation, moral turpitude crimes, etc. The second section; the crimes committed through the internet such as banks burglary and money laundry.

Second: new crimes such as information destroying, operating systems malfunction or interruption, virus crimes, etc.

2.1.1 Characters of Cybercrime

This characteristic is not limited to internet crimes. As the computer might be a tool to commit such crimes, it is also a tool to commit many information crimes such as information forgery, stealing information stored in the computer and others. In addition, Internet crimes don't take place using internet only but it could be by using mobile phones as accessing the internet can be trough such phones. Internet crimes are of the

1 Dr. Kamal Alkarki. Investigation in Computer Crime. Abu Dhabi Police College. 2003, pp. 29-33.

modern crimes which use the internet to commit or facilitate the crime. The internet deems the link between all potential targets such as banks, companies of all types, individuals, etc., who falls a victim in most cases.

The profile of information technology crimes' criminal.

The most significant characteristics of information technology crimes' criminal are the broad experience and super knowledge of computer and internet in general, it's not only attributable to internet crimes but its common characteristics in all information crimes including internet crimes.

No borders:

Of the most characteristic of the internet is its pan the world and links countries together without natural nor political borders and allows its users virtually or incorporeal movement amongst countries and continents without difficulties or obstacles. Its' a huge, diversified, renewable world free of borers and constrains.

Therefore, we notice that crimes committed through it is borderless and don't acknowledge place or time elements whereas time factor (time difference amongst countries), place factor (possibility of committing a crime remotely and legal factor (which law shall apply?) play significant role in dispersion of international investigations and coordination to trace them.

Crimes here are not limited to a specific country but the all the world will be its scene as someone may commit his crime from any place or anytime.

Gross damage:

Internets crimes are of sever dangerous from many sides: firstly, we find that its resulting losses are very huge when compared to traditional crimes, specially, money crimes. Secondly, it's committed by mane classes which complicate predicting the suspected. Thirdly, they involve unfamiliar behaviors.

Difficulty of investigation, questioning and prosecution:

Internet crimes are mysterious, they are difficult to be proven as its investigation, questioning, and prosecution involve many administrative and legal issues and challenges which occur initially on pursuing the criminals succeeding which conviction shall be difficult due to the easiness of spoiling the evidences by the criminals or due to the difficulty in reaching evidences or the absence of legal recognition of such crimes evidence nature. Since these crimes are borderless and deem cross border crimes, this

factor of itself raises challenges and obstacles in the judicial competency, prevailing law, investigation requirements, pursuing, arrest and inspection. Those combating information crimes face many and renewable difficulties due to the following reasons (human – investigation):

- Electronic crimes victims whether establishments, bodies or individuals' unawareness of the committed crime nature and their inability to find out the damages and its extent in the due course.
- Information criminal's scientific intelligence and capabilities.
- Lack of digital criminal evidence laboratories, artificial evidences and judicial technical research experts for computers.
- The old fashion of criminal investigation bodies in computer science and high technology areas.
- Electronic crime is committed with fewer efforts which decrease the chances of its discovery.

2.1.2 The Motivation of Cybercriminals

The motive or incentive is the driver of the will which drives the criminal behaves such as love, pity, ill feeling and revenge. It is a psychosomatic power pushes the will towards committing the crime so as to attain a particular goal. It differs from a crime to one other according to differences between people in terms of age, sex, education level and other influencing factors. It differs as well in the same crime from one to another[1].

In this novelty crime, many and varied motives drive the criminals for its commitment. It could be for information either stored on computers or convoyed through the internet or could be for incurring damages on specific people or entities or for attaining financial interest or exhibitionism, etc.

First motive (passion of information collection and learning):

Some may commit the crime to obtain new information. Researchers in systems piracy, Prof. Live, in his publication; systems pirates, pointed out the ethics of pirates

1 Dr. Muhammad Al-Ulema. Accountability of Internet Crime. Naïf Arab Academy.2003, pp. 6-9. And see Dr. M. Al-Amin Al-Bushra. Investigating Computer and Internet Crimes. Dubai Police. 2012, pp. 36-40.And see Dr.Hussen Alwheepy. Report in the Internet about Cybercrime.www.omanlaw.com.

relies on two main pillars; the first is that entering to computers educates you how the worlds goes on and the second is that information collection shouldn't be subject to burdens.

Pirates always announce that they wish access information sources, computers and networks only for the purpose of leaning

Systems pirates find out security leaks in the systems and they try making use of it as it's there for not destroying information or stealing them" quoted one of the pirates. I think that what they do is similar to what a person will do to find new method to obtain information from the library and turns into a case of excitement and absorption. We shouldn't disparage the efficiency of the networks from which pirates learn their profession, they already search and discover systems and work in a group and teach each other.

Some pirates seems specialty and collaborate in researches projects, share programs, news and expertise which help them implement what they learned in objective activities even if not legal.

Second motive (Information takeover):

Many crimes are committed using information technology targets the information itself. This target is accomplished either by obtaining the stored or convoyed information or amending, deleting or ultimately delete them. The motive here might be competition, blackmailing, attaining benefits or attaining economic privileges and interests. Therefore, we find that most of these crimes targeting information are mostly of economic or political trait.

Third motive (the desire to beat the system and excel the technological means):

The motive behind crimes could by beating the system more than the passion of attaining financial interests whereas the criminals of such crimes would like to show their excellence and ascension of their mastership to the extent that whenever any new technology comes to light, the criminals of these crimes who have (machine passion) try finding appropriate means to beat such innovated technology and they succeed in most cases. Such motive widely spreads amongst the minors of committing the virtual crimes who spend prolonged times before their computers trying to break the security firewalls of computer Systems and internet and show their excellence over the technological means.

Forth motive (individuals or entities):

Some crimes committed using information technology is driven by incurring damage to specific individuals or entities. Most of these crimes are direct and take the form of blackmail, threaten or defamation like that case in Dubai – UAE when someone called "girls images pirate" hacked the e-mail accounts of a group of girls in that country and stolen their personal photos and published them on the internet along with pornographic images. Other examples include what happened in Al Ain – UAE when the accused could illegally access the victim's personal computer and copied her personal data and information. He threatened her that he'll publish it over the internet unless she adds him to her friends list in the "Messenger" audio video chat application. In RAK – UAE, one person published – using the e-mail service of an internet provided corporation- new related to private life sanctity and touches her honor, reputation and financial judiciary. Those crimes could be indirect in case which it is represented in obtaining such entities or individuals' information to use it later in committing direct crimes.

Fifth motive (seeking profits):

Some crimes committed using information technology are driven by attaining financial profits and interest such as using the internet for human trafficking. A recent studies, conducted by a British researcher, found out using the internet for white slavery by concluding sale deals to sell girls from forty developing countries and Eastern Europe to western citizens for pleasure and sex through gangs specialized in white slavery transactions through which they attain profits of millions of dollars which finds its way to be washed by money laundry. Such transactions are now of a wide and growing increasingly over the internet. Furthermore, the gambling and narcotics trade which found the internet a fertile soil.

Sixth motive (threatening national and military security):

Some crimes committed using information technology are driven by political motives represented in threatening national and military security and the occurrence of what is known as electronic and spy war and electronic terrorism. Press releases in 2009 indicated that Chinese entities well known with wide range of internet hacking hacked hundreds of computers over about 103 countries. The hacking process was well organized and targeted particularly a group of computers of diplomatic, security and international figures. A Canadian research center working in information domain called

"Information War Watch" revealed the details of this incident to the media. The center quoted that an electronic spy network functioning from China could hack 1295 computer in 103 countries. The Chinese government denied any connection to this incident.

2.2 UAE Penal Code and Cybercrime

The UAE is a federation of seven Emirates, As the UAE Constitution considers in Article (7): Islam is the official religion of the UAE. The Islamic Shari'a is a main source of legislation in the UAE. The official language of the UAE is Arabic. Article (1) of the UAE Penal code states that the committers of some crimes must be punished according to the provisions of Islamic Sharia, we will present the divisions of penalties in the UAE Penal Law in the first party of this research, while the second party will be dedicated for the divisions of penalties in Islamic Sharia.

2.2.1 An Overview of UAE Penal Code[1]

Subject to the first article of the UAE Penal Law, the provisions of Islamic Sharia are applied to the retaliation and blood money crimes and the supportive crimes and penalties according to Article (1) of the law.

The UAE Penal Law[2] divides the crimes as per the gravity thereof, which gravity depends on the nature of projected interest and aggression. The crimes are divided into three types in terms of gravity:

- Felonies (Article 28 of the Penal Law): the most grave crimes per the penalty imposed thereon (temporary imprisonment from 3 to 15 years)
- Misdemeanor (Article 29 of the Penal Law): imprisonment from one month to three years.
- Violations (Article 30 of the Penal Law): detainment (one to ten days).

It is not difficult to distinguish between the felonies from one part and misdemeanors and violations from the other party as it is sufficient to refer to the legally established penalty as different from each other.

1 Refer to Appendix 2 (Articles 1, 28, 29, 30)

2 Dr. Ali Hamoda. Explanation of UAE penal code. 2008, pp. 105-120. Dubai Police Academy.

It is not difficult to distinguish between the felonies and violations if the legally established penalty imposed on the crime is imprisonment, blood money or whipping in case of inebriation and slander, etc., or detention of not more than 10 days.

Importance of division[1]:

Attempted crime: The origin is to punish the committer thereof a felonies, unless otherwise is provided by the law (Article 35/ 1) while the committed of attempted misdemeanors and violations shall be punished only per Articles 37 and 36 of Penal Law.

- The legislator imposes punishment on the criminal agreement in case of crime or felony. Therefore, the agreement on any violation must not be punished (Articles 192 and 172) of the Penal Law.
- The provisions recurrence of are restricted to the felonies and misdemeanors without any violation (article 106).
- The elevated circumstances system is restricted to felonies and misdemeanors other than violations (article 100, 98).
- The scope of application of seizure system is restricted to felonies and misdemeanors other than violations (Article 82).

2.2.2 Crimes in Islamic Law

Islamic law is known as Sharia law, and Sharia means the path to follow God`s Law. The life of a Muslim is governed in every aspect be the command of Allah the only law-giver of the Muslim community.

Islamic law is known as Sharia. Islamic criminal law as well as the whole Islamic legal system is not codified or enacted by normal legislative bodies in the form of written articles; however the basic principles and legal rules are delineated and clarified by the following sources:

Original Sources[2]:

1. The Holly Book (Quran)

1 Refer to Appendix 2 (Articles 35, 36, 37, 82, 98, 100, 106, 172, 192)

2 Prof. Mohamed Al bushra. Criminal Justices System Islamic Law Perspective. Sharjah Police Research Center, 2013, (22).

2. The Prophetic reports (Sunna)

Complementary sources:

1. The consensus of the opinion (Ijma')
2. The Analogy (Qyass)
3. Equity (Istihsan)
4. Textually unspecified interest of the people (Maslaha Mursala)
5. Avoidance of harm (Sadd Addharaa)
6. Compatibility of the means and the ends (Istishab)

Checking what is permissible and what is prohibited. Crimes are defined and classified into three categories in the Islamic Justice System.

Hudood, which are crimes punishable by fixed punishment:

1. Adultery (Zina).
2. Defamation or false accusation (Qadhf).
3. Consuming Alcohol (Sokarr).
4. Theft (Sariqa).
5. Highway Robbery (Qat Al-Tariq).
6. Apostasy (Ridda).

Punitive and blood-money crimes (Qisas / Diah): Blood money is paid to the family of the murdered by the murderer in cases of accidental death. The family can accept the money (Diah) or refuse and request (Qisas) a one for a one.

Taazir, which are crimes punishable by discretionary punishments. Taazir include all types of crimes, contravention, and negative social or religious behavior and ***cybercrime***.

Islamic Sharia' Law has also defined the type of punishment that should be implemented for each categorized crime. Many people view Islamic Sharia's penal code as to harsh and inhumane; however they are only looking at the penalties for crimes committed without understanding the rules of Sharia enforcement and rules of evidence. Below are the types of crimes and the penalties provided for each crime with its rule of evidence.

Adultery Punishment:

Married adulterers are stoned to death. Unmarried adulterers receive 100 lashes.

Accusation Process: given the severity of the punishment for Adultery, Sharia Law requires solid proof before convicting anyone of adultery .A confession by the person

guilty of committing adultery, or the testimony of four reliable Muslim male eye-witnesses, all of whom must have witnessed the actual intercourse at the same time.

Defamation (Qadhf) Punishment:

It is eighty lashes. Any person convicted, their testimony shall never be accepted in future in any matter, and as such he shall stand defamed in the society.

Consuming Alcohol (Sokar) Punishment:

It is eighty lashes.

Theft (Sariqa) Punishment:

It is an amputation of one hand.

Accusation Process: given the severity of the punishment for theft, Sharia Law requires solid proof before convicting .A confession by the person guilty of committing theft, or the testimony of four reliable Muslim male eye-witnesses, all of whom must have witnessed the convicted committing theft.

Highway Robbery (Qataa Al-Tariq) Punishment:

Punishment for highway robbery with homicide is the death penalty by sword. Punishment for theft and highway robbery without homicide is amputation of hand.

Accusation Process: given the severity of the punishment for Highway Robbery, Sharia Law requires solid proof before convicting anyone of highway robbery .A confession by the person guilty of committing highway robbery, or the testimony of four reliable Muslim male eye-witnesses, all of whom must have witnessed the convicted committing highway robbery at the same time.

Apostasy (Ridda) Punishment:

The rejection in word or deed of one's former religion; by a person who was previously a follower of Islam. Punishment for apostasy is the death penalty by sword.

Accusation Process: given the severity of the punishment for Apostasy, Sharia Law requires solid proof before convicting anyone of Apostasy .A confession by the person guilty of committing apostasy, or the testimony of four reliable Muslim male eye-witnesses, all of whom must have witnessed the convicted committing apostasy at the same time.

Sharia Court in UAE:

In the UAE have Sharia courts that are organized and limited based on the law and it specializes in accordance to Article one of the penal code to crimes of "Hudood" such as adultery, alcohol (intoxication), defamation, theft, prostitution, banditry, apostasy and crimes of retribution (murder) in the event these crimes are applicable to the terms of Islamic Law (Sharia) and these crimes are not proven unless a plea is made i.e. admission in more than one sitting, or a witness testimony that viewed the crime in full as it occurred. And In the event that the terms of Hudood were not applied, and this is the case for most issues because of the difficulty of proving them whether with witnesses or admission the courts will apply provisions of the law as well as hearing drug, juvenile and libel crimes. In conclusion there are no contradictions between the enforcement of Sharia Law and the law on the grounds that the original application of Sharia law in the specific crimes is in accordance with the previous permissions

2.3 Legislative Stage before Issued UAE Cyber Law 2006

In 1998 a Committee was established at the Ministry of Justice to consider the amendment of the Federal Penal Code No. 3 of 1987. The Committee was consisted of an elite of judged and counselors at the Ministry of Justice. The committee was tasked with the study of the articles which required to be amended. At that time the idea of adding provisions to the penal code concerning the computer crimes was introduced. In the memorandum attached to the amendment concerning the computer crimes (to the federal penal code did not include any provisions incriminating detrimental acts as a result of the misuse or illegal use of the computer or those occurring to the computer itself by the others or to any information systems or programs and that our era is called (the computer era) and hence it is imperative to think of introducing laws to tackle the crimes related thereto).

According to the memorandum the committee discussions resulted in forming two teams:

- The first team thinks that a special penal code should be promulgated for such computer crimes because these crimes are many repeated and diversified.
- Second team to introduce a set of provisions incriminating the misuse of the computer and include them in the penal code being the public penal code through which the acts representing an abuse of the computer can be incriminated.

The opinion of the second team was taken with the addition of a new section in the penal code within the eighth chapter of the second book under the title (computer crimes). Within the memo regarding the proposed provisions there were four articles for the computer crimes and one article addressing the money stealing through credit cards.

For unknown reasons the draft amendment to the penal code kept in the drawers for many years. However, the proposed amendments after not less than seven years involved an extensive research and consultation leading to the promulgation of the UAE cybercrimes law in 2006. Elite of specialist, legal counselors and judges from the Ministry of Justice, prosecution, and technical specialists from the Ministry of Interior, finance and universities have taken part in the preparation and construction of the law and other legislations.

Numbers of laws, international agreements in the field of information technology were addressed to help in the construction of this law such as:

- The British Computer Misuse Law of 1990.
- The French Computer Crimes Law No. 1170 of 1990.
- The American Federal Laws concerning the Computer Crime.
- The Malaysian Computer Crimes Law of 1997.
- The Thai Computer Crimes Law.
- European Agreement for the Computer Crimes of 2001.

The title Cyber Crimes Law promulgated in 2006 was selected to express the contents of the provisions set out therein by using the terminology (means of information technology) instead of the computer so that the provision shall include all the equipment related to the computer and also related to other equipment as accessories through a new means of telecommunication i.e. the internet.

2.4 UAE Cyber Law 2006[1]

The combating cybercrimes law no. (2) Of 2006 comprises (29) articles where the first article provides terms and phrases such as the web site, e-document, etc.

In the remaining articles of law No (2) UAE cybercrimes law namely articles from (2) through (27), the law stipulated incrimination of information technology related acts and defined original and aggravated punishments as briefed below:

1 Refer to Appendix 4 (Articles 1-28)

Firstly: Illegal access to the website and information system which includes the following:

1. Second and third article: (general article)

- Illegal access to the information system without permission or overstepping the granted permission.
- Committing illegal access during or due to his responsibilities or facilitating the same.

2. Article 6 (virus related article)

- Who intentionally installs an information application which malfunctions or stops the information system functionality. This article includes all malware such as viruses.

3. Article 11 (e-cards crimes)

- Punishes unauthorized access to figures, e-cards information to obtain money or interest.

4. Article 14 (websites)

- Punishes websites violation over the internet for the following purposes:

1. Changing website design.
2. Cancelling, destroying or amending the website.
3. Engaging website address.
4. Article 22 (Government confidential information and data).

- Punishes unauthorized access to collect confidential governmental information and such crime deems an aggravated condition for which the law aggravated its punishment (temporary imprisonment).

Secondly: Electronic document forgery (article 4).

Article 4 concerns forging electronic documents in the information system including the following forms:

1. Official document forgery (whether related to federal or local government).
2. Forgery of non-official document.
3. Using a forged document knowing its forgery.

Thirdly: Impeding, hindering and intercepting information technology means or its interruption, hacking confidentiality and spying including the following forms:

- Hindering and interrupting service access (article 5).

- Intentional and illegal spying and stoppage (article 7).

Fourthly: Cybercrimes related to general ethics and norms and what offenses religious sanctities and its icons:

- Article (12,13): Relates to producing, developing, sending of storing materials for utilization and distribution which may touches the general norms and inducement to allure others of any gender to commit pornography and lewdness and the law aggravated the punishment if the victim is a Joinville.
- Article (15): Relates to punishing acts that offences religious sanctities and practices such as divine religions cursing.

Fifthly: Using the internet to offence private life in accordance of article (16) such as the following forms:

- Publishing images related to private or family life sanctity.
- Posting news and quotes related to private or family life sanctity.

Sixthly: Using or building a website or publishing information on the internet or another IT means or using them for criminal purposes as provided in articles (18, 17, 9, 19, 21, 20) of which forms:

- Threatening or blackmailing (article 9).
- Human trafficking (article 17).
- Narcotics promotion (article 18).
- Money laundry or transferring them (article 19).
- Facilitating disruptive programs or ideas or against general norms or promoting the same (article 20).
- Supporting terrorist acts and the activities of terrorist groups (21).

Seventhly: Inducement, help or agreement to commit any of the acts stipulated herein article (23).

2.5 UAE Amended the Cyber Law

In this article, we outline Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes. Better known as the Cyber Crimes Law 2012, the law which came into effect in December 2012 - replaces the earlier Cyber Crimes Law 2006.

The Cyber Crimes Law 2012 provides for a range of new offences, including offences intended to address the UAE's obligations pursuant to international treaties. Additionally, the Cyber Crimes Law sets out significantly higher penalties than those found in the 2006 law[1] .

General themes:

The general themes of the provisions of the Cyber Crimes Law can be broadly categorized as follows:

1. IT security.
2. State security and political stability.
3. Morality and proper conduct.
4. Financial and commercial issues.
5. Miscellaneous.

1. IT security:

The provisions that relate to IT security address issues like hacking IT networks to steal data, change websites, interrupt service, distribute viruses, and the like. More specifically, the provisions in this category can be summarized as follows:

- Accessing an IT System ("IT System") without authorization. (Greater penalties are provided where the subject data was personal data, or when the perpetrator commits the offence in the course of his or her employment.)[2]
- Unauthorized access to an IT System to obtain government or commercial information. (This provision specifically references government information, but also refers to information relating to financial, trade or economic establishments licensed in the UAE.)[3]
- Accessing a website without permission to damage, delete or change its content[4].
- Disabling access to an IT System[5].
- Circumventing an IP address for the purpose of committing or concealing a crime[6] .
- Introducing virus programmers to an IT System; and spam emails. (This provision provides significant penalties for the introduction of computer viruses, being either

1 Nick O'Connell. Developments in the UAE cybercrimes Law. 2013.
2 Refer to Appendix 1 (Article 2 UAE cyber law).
3 Refer to Appendix 1(Article 4 UAE cyber law).
4 Refer to Appendix 1 (Article 5 UAE cyber law).
5 Refer to Appendix 1(Article 8 UAE cyber law).
6 Refer to Appendix 1 (Article 9 UAE cyber Law).

or both of five or more years imprisonment and AED500,000 to AED3,000,000 fine, with imprisonment and a fine of up to AED500,000 being available for unsuccessful attempts) [1].

- Obtaining, without authorization, passwords to an IT System. (This provision does not specify that the act of obtaining such password/code need occur via an IT System, and the language appears broad enough to cover obtaining by way of IT System, or otherwise. Additionally, this provision includes a broad prohibition on making available (whether by making directly or procuring; and including by way of importation, sale, etc.) any means or information designed to commit/facilitate/incite others to commit crimes specified under the law)[2].
- Unauthorized interception of communications via an IT System. (This provision seems to mirror the prohibition on intercepting communications (i.e. eavesdropping on phone calls and intercepting mail) found in the Penal Code and (in the case of phone calls) the Telecommunications Law. Additionally, the act of disclosing information so gathered is also captured by this provision)[3].
- Unauthorized disclosure of confidential information via an IT System. (This provision appears to be designed to capture 'Wikileaks' type situations, namely, situations where workers who obtain confidential information in the course of their employment release such confidential information without authority)[4].

2. State Security and Political stability:

- Unauthorized access to an IT System to obtain government or commercial information[5].
- Operating a site, or posting information online, that stirs sedition, hatred, racism or sectarianism, or hurts national unity or social peace or prejudices public order or public morals[6].
- Operating a site, or posting information, for a terrorist group or illegal organization[7].

1 Refer to Appendix 1(Article 10 UAE cyber law).
2 Refer to Appendix 1 (Article 14 UAE cyber law).
3 Refer to Appendix 1 (Article 15 UAE cyber law).
4 Refer to Appendix 1 (Article 22 UAE cyber law).
5 Refer to Appendix 1 (Article 4 UAE cyber law).
6 Refer to Appendix 1 (Article 24 UAE cyber law).
7 Refer to Appendix 1 (Article 26 UAE cyber law).

- Operating a site, or posting information online, that exposes the State's security and interests to danger and prejudice public order[1].
- Publishing information/news/rumors online for the purpose of harming the status of the State[2].
- Operating a site, or posting information online, for overthrowing the government of the State, or undermining the Constitution[3].
- Publishing information online to incite non-compliance with laws[4].
- Using an IT System to provide others with information that harms the interests of the state or offending its dignity[5].

3. Morality and proper conduct:

A number of provisions are pointed at proper conduct. These include sanctions on using the internet for conduct that is disrespectful to Islam, as well as prohibitions on the use of the internet for activities that are otherwise inconsistent with public morals and good conduct. In summary, these include using an IT System to:

- Offend religious sanctities or encourage sins[6].
- Provide pornography, gambling activities, and other materials prejudicial to public morals[7].
- Promote prostitution/debauchery[8].
- Slander another person[9].
- breach the privacy of another (e.g. by intercepting communications, taking
- Photographs, publishing information, etc.)[10].

4. Financial and commercial issues:

There are a number of provisions that can broadly be understood as relating to ecommerce and online financial activity. These include:

1 Refer to Appendix 1 (Article 28 UAE cyber law).
2 Refer to Appendix 1 (Article 29 UAE cyber law).
3 Refer to Appendix 1 (Article 30 UAE cyber law).
4 Refer to Appendix 1 (Article 31 UAE cyber law).
5 Refer to Appendix 1 (Article 38 UAE cyber law).
6 Refer to Appendix 1 (Article 35 UAE cyber law).
7 Refer to Appendix 1 (Article 17 UAE cyber law).
8 Refer to Appendix 1 (Article 19 UAE cyber law).
9 Refer to Appendix 1 (Article 20 UAE cyber law).
10 Refer to Appendix 1 (Article 21 UAE cyber law).

- Forging electronic documents or knowingly using forged electronic documents[1].
- Using an IT System to obtain goods fraudulently and without legal right[2].
- Using an IT System to unlawfully access bank account details[3].
- Producing credit / debit cards without legal right or knowingly using and/or dealing with such illegal cards[4].

5. E- Miscellaneous:

There are a number of other provisions of interest that do not neatly fall into the categories outlined above.

Articles 23[5], 25[6], 33[7] and 36[8] appear to be aimed directly at addressing international obligations as specified in related treaties. These provisions relate to human trafficking[9] and trafficking in human organs, trading in weapons[10], ammunition and explosives, trading in antiquities [11] and trading or promoting narcotics [12]. Of the other 'miscellaneous' offences, there are prohibitions on:

- Using an IT System to blackmail someone into committing an offence or doing something that would prejudice honor[13].
- Operating a site, or posting information online, for the purpose of gathering donations without license[14].
- Using an IT System to unlawfully benefit from, or facilitate the use by others of, communications services[15].

1 Refer to Appendix 1 (Article 6 UAE cyber law).
2 Refer to Appendix 1 (Article 11 UAE cyber law).
3 Refer to Appendix 1 (Article 12 UAE cyber law).
4 Refer to Appendix 1 (Article 13 UAE cyber law).
5 Refer to Appendix 1 (Article 23 UAE cyber law).
6 Refer to Appendix 1 (Article 25 UAE cyber law).
7 Refer to Appendix 1 (Article 33 UAE cyber law).
8 Refer to Appendix 1 (Article 36 UAE cyber law).
9 Refer to Appendix 1 (Article 23 UAE cyber law).
10 Refer to Appendix 1 (Article 25 UAE cyber law).
11 Refer to Appendix 1 (Article 33 UAE cyber law).
12 Refer to Appendix 1 (Article 36 UAE cyber law).
13 Refer to Appendix 1 (Article 16 UAE cyber law).
14 Refer to Appendix 1 (Article 27 UAE cyber law).
15 Refer to Appendix 1 (Article 34 UAE cyber law).

Mechanical provisions of note:

There are a number of important 'mechanical' provisions, including provisions that provide for the extra-territorial application of the Cyber Crimes Law[1], and the liability of site owners for failure to remove offending content[2].

Penalties:

Besides providing for significant financial penalties and custodial sentences, and the deportation of foreigners convicted[3] of any offence under the law, the Cyber Crimes Law empowers the authorities to seize and destroy equipment used in the commission of the offence[4].

The following table illustrates the addition of new articles to fill the gaps needed to fight cybercrime in the UAE.

Crimes	Number of Articles Cyber law 2006	Number of Articles Cyber law 2012
Government security	2	13
Attempted crimes in the misdemeanor	0	1
Moral and religious crimes	4	5
Procedural articles	6	7
Technical Crimes	7	12
Traditional crimes	8	13

2.6 Cybercrimes in Japan

The penal code, as it stands now, was enacted in 1908. The constitution enacted by the Emperor was in effect in 1890. Article 1 of this constitution provided that the Emperor exercised the sovereignty of the nation.

World War II ended in 1945, Japan did the unconditional surrender to the Allied Occupation Forces. Promulgation of the new constitution of Japan was made in 1947. This constitution proclaims that sovereign power resides with the people.

1 Refer to Appendix 1 (Article 47 UAE cyber law).
2 Refer to Appendix 1 (Article 39 UAE cyber law).
3 Refer to Appendix 1 (Article 42 UAE cyber law).
4 Refer to Appendix 1 (Article 41 UAE cyber law).

Penal code of 1908 continues to be enforced under the constitution of 1947. The Penal code of 1908 was amended several times. With the coming into effect of the constitution, the following provisions of the penal code were amended. (1) Provisions of crimes against the Imperial Family of Article 73, 74, 75, 76, were deleted. (2) Provisions of crime of adultery of Article 183 were deleted. Only a married woman who committed adultery was punished by Article 183. Married man who have illicit with another woman except wife was not punishable. Constitution of Article 14 paragraph 1 provides that all of the people are equal under the law and there shall be no discrimination in political, economic or social relation because of race, crud sex, social status or family origin. The Article 183 of the penal code is contrary to the Article 14 of the constitution. (3) Article 230-2 was provided in addition to Article 230. Article 230 provides that a person who defames another by alleging fact in public shall, regardless of whether such facts are true or not, be punished. If the following conditions of Article 230-2 are fulfilled, a person who defames another by alleging fact in public shall not be punished by Article 230. (1) Alleged fact which comes under Article 230 is related to the matter of public interest. (2) An act which defames another by alleging facts in public should be conducted for the benefit of public. (3) Defendant should certify the truth of alleging fact.

Article 230-2 was sentenced to try to keep harmonious balance between preservation of private honor and guarantee of freedom of speech by Article 14 constitution.

After World War II, Japan has changed greatly. Individualism has permeated in the society of Japan. From about 1965, A new age of high economic growth has arrived .Several kind of pollution has become issues of public concern and it becomes an important problem to make plans to promote the social welfare compatible with rapidly aging society. On 11 March 2011 there was a radiation leak in the nuclear power plant for the Tokyo electronic power company. The issue of electric power supply is a serious problem in present society.

Computer Crime becomes a social problem in the computer age. Legislators have had to choose ways of how to deal with computer crime. Legislators did not choose the way to make a new independent cybercrime law but to amend the criminal law of 1908.

White paper classifies the computer crime into two groups.

- Computer crimes which object are electromagnetic record.
- Computer crimes by using computer network.

- Computer crimes related to electromagnetic record.

Article 7-2, 111-2,161-2, 234-2 and 246-2 were added to the Penal Code revision of 1987.

These Articles are related to electromagnetic record[1]. By this amendment, the Penal Code of Japan has some types of cybercrime articles. On Cybercrimes, the current Penal Code has a definitions provision and covers the following activities to be punishable.

- Definition of an electronic magnetic record.
- Illegal production of an electromagnetic record.
- Interference with business transaction by computer system.
- Computer fraud.
- Destruction of electromagnetic record.

2.7 Comparison between UAE law and Japanese law

In Japanese law, the current penal code is applied on computer-related crimes, and there have been some revision in the penal code to handle some illegal activities such as destruction, elimination or unauthorized creation of electromagnetic records. The act on prohibition of unauthorized computer access is a special act related to computer-related crimes. On the other hand, the UAE has established a special act on computer-related crimes, which made it comparatively easier to include many illegal activities conducted by using computers. This advantage is shown in the act revised in 2012 in order to include many articles and contents which were not handled in the law established in 2006. While the Japanese penal code has abstract examples of activities which are subject to punishment, the penal code of the UAE has a specific and concrete punishment for each illegal activity. The difference in such a legislation system of the basic law is related to the possibility to handle computer-related crimes and illegal activities by revising the current penal code.

In the next chapters of this research , the major focus is to explain, understand, and examine the acts on prohibition of unauthorized computer access, publicity of immoral activities through the internet, destruction of information in computers, computer fraud, and the unauthorized creation of electromagnetic records in both the UAE's law and Japanese law, in the end of each chapter there is a summary and comparison between

1 Takato Natsui. Cybercrimes in Japan: recent cases, legislation, problems and perspectives. 2003. http://www.netsafe.org.nz/Doc_Library/netsafepapers_takatonatsui_japan.pdf

the UAE law related to computer crimes and Japanese penal code related to computer crimes.

CHAPTER 3

ILLEGAL ACCESS CRIME

CHAPTER 3

3.1 Introduction

All laws endeavor to protect computer software and websites, especially government websites[1], in addition to protection from all types of attacks in general. Since these information systems and other systems need legal protection and other measures to withstand the intelligence of the information network criminals and skilled hackers[2], it is inevitable, therefore, to enact laws that restrict the abilities of these criminals.

Illegal access crime is one of the most important crimes that distinguish cybercrimes as it is one of most prevalent crimes linked to modern techniques, especially the internet network. Illegal access crime is considered the door that leads to various crimes, like: fraud, destruction of information and data, counterfeiting of documents and other crimes.

Most international legislations punish acts of illegal access, either through enactment of special laws to cover these crimes as when Japan[3] enacted a special law called "Unauthorized Access Crime Act of the year 1999"; or as when the UAE criminalizes such acts in different legal texts within the Information Technology Crimes Act of the year 2006[4], which was amended in 2012[5], as we mentioned before.

In this chapter, we will address the definition of illegal access as defined by the UAE and Japan Acts. Part one covers illegal access as specified by the UAE Information Technology Crimes Act and tackles ways and means followed by each of the above Acts in dealing with crime and punishment.

3.2 Illegal Access Crime in UAE Cyber Law

The UAE Information Technology Crimes Act (Cyber law) does not define crime of illegal access, either in the previous Act of 2006 or the amended Act of 2012. However, it can be defined technically as an act through which a hacker can access[6], from a distance, other persons' or entities' systems. Such access includes all computer usage

1 Dr. Rizgar Mohamme Kadir. The Offense of Unauthorized Access in Computer Crime Legislation-A Compartative Study. Journal of Sharia and Law. 2008, pp. 41-43.
2 D. Nabil Gad. Crime of computer. 2000, pp.78-80. Conference in Dubai.
3 The Law of Unauthorized Access law (128). 1999.
4 UAE cyber law (No.2). 2006.
5 UAE cyber law (No.5), 2012. Amended the old law, 2006. No. 2.
6 Dr. Mohammed Alkappe. The Criminal Protection to E-Trade: A Comparative Study. University of Cairo, Egypt. 2009, pp. 336-340.

without the consent of its owner, whatever the type of this usage may be, as if the user is able to operate it directly or from a distance[1].

Article 2[2] of the UAE Information Technology Crimes Act punishes the act of illegal access to any electronic website, or system, or any electronic means, it also stresses severe punishment if this illegal access results in the destruction or deletion of any data[3]. Article 4[4] of the same Act punishes the act of illegal access to government systems with intension of tampering with government data or other materials.

In order to protect electronic trade and electronic websites, Article 5[5] incriminates illegal access intending to tamper with or inflicting any damage on an electronic website. The UAE legislator, on the other hand, is keen to protect information software and to stand firm against viral attacks launched by all malicious software. Article 10[6] incriminates any illegal access of this type of software and considers it a criminal offense and provides punishment by imprisonment and a fine of not less than 3 million DH (1 US dollar = 3.66 UAE Currency). And finally, in order to protect daily use of credit cards in commercial transactions and to maintain community rights, Article 12[7] of the UAE Information Technology Crimes Act incriminates anyone who unlawfully holds any credit card or other device.

We will explain, in some details, the Article on illegal access as introduced in the UAE Cyber law, and which also incriminate this deed of illegal access.

3.2.1 The Nature of Illegal Access Crime

The act of illegal access to electronic systems, information programs and electronic networks may be committed just for the sake of access to the system, or may be intended to access and obtain information and data, or may be intended to access and damage these data or systems. To stay logged in a computer constitutes a crime if this deed is illegal, or if it contravenes stated instructions.

We will discuss in this part of the research what is meant by act of illegal access as provided in Article Two of the UAE Cyber law.

---

1 Paul Cullen. Computer crime, in law & the internet, regulating cybercrime. 1997, pp. 211-212. Lilian Edwards & Charlotte Waelde, eds.
2 Refer to Appendix 1 (Article 2 UAE cyber law).
3 Refer to Appendix 1 (Article 2-2 UAE cyber law).
4 Refer to Appendix 1 (Article 4 UAE cyber law).
5 Refer to Appendix 1 (Article 5 UAE cyber law).
6 Refer to Appendix 1 (Article 10 UAE cyber law).
7 Refer to Appendix 1 (Article 12 UAE cyber law).

Section 1 (what is meant by the act of illegal access as defined by the Information Technology Crimes Act "UAE Cyber law"):

As we have previously mentioned in the Introduction of this research, the UAE Information Technology Crimes Act (UAE Cyber law) did not define the act/deed of illegal access therefore Article 2 will be explained. Due to the importance of this Article, being gateway to the UAE Cyber law, and as already mentioned, most of information technology crimes use the act of illegal access as a ladder or bridge to realize this goal, irrespective of the difference of means of committing a crime and the type of the crime. In practice, this deed raises many questions: what is meant by illegality of access? And whether this act is of a materialistic nature or is it a formalistic crime?

3.2.1.1 The Concept of Illegal Access

Article 2 of the UAE Cyber law for the year 2012 states that access is not authorized i.e. it is an assault on the victim's approval (access without approval of the system owner)[1], so the hacker accesses the system by any illegal method, like trying numbers, using electromagnetic, audio and mechanical devices in order to obtain the secret code[2].

Generally, the security measures stipulated in Article 2 of this Act were not given the importance they deserve, as the UAE Act, contrary to the Japanese Act, does not require any specific procedure. According to the UAE Cyber law a crime is committed when it is proved that the system owner is unsatisfied, even if he /she refrain from protecting the system against hackers.

It is enough for the owner to express his/her intent not to allow others to access his/her system through any method. Mere access to an information system does not constitute an illegal act; however, it becomes illegitimate from the perspective of lack of authority, meaning that this access is unlawful. This concept is basically associated with finding out who has the right or authority to access the system. Therefore access to the information system is unlawful in two cases: firstly, if there is someone in charge of the system and access to this system is made without his permission; secondly, if the actor access to the system is not limited to licensed domain, in other words the actor has an access permit but he has exceeded the powers granted to him. The definition of un-authorization concept pertaining to access to computer systems raises the question on

1 Dr. Abd Alfatah Hijazi. Computer crimes in the Arabic legislations. 2010, pp, 26-30.
2 Osam Almanaasa, Jalal Zaabi, and Sail Al-Hawawsha. The crime of Internet and computer: A comparative study. 2001, pp. 231-233. Dar Wael (printing and publishing).

cases where access to the system is permitted; but is used for a purpose other than original permitted purpose. Is access in this case illegal[1]?

As a matter of fact, access to information systems should be restricted to the purpose on which this authorization is granted. Whenever there is any contradiction between this purpose and original purpose of access, this access is deemed illegal[2], and hence becomes subject to a crime of illegal access.

The Nature of illegal access:

Jurisprudence divides crimes into two types[3]: materialistic crimes which have a result, and formality crimes, that is, crimes pertaining to mere behavior and activity. This state of affairs raises the following question: What is the nature of the crimes of illegal access to computer systems, are they materialistic crimes with clear results or are they formality crimes of behavior and activity[4]. In other words, is it necessary that illegal access should have a clear impact or result that leads to a specific criminalizing result, like access to the various data contained in this system, or is mere access to the system is considered a crime[5]?

No need to verify a result or damage:

Article 2 of the UAE Cyber law for the year 2012 states that illegal access is considered a crime once the act of access is completed, even if there no result or damage because the purpose of incrimination is to protect information and software programs from being accessed. It is, therefore a formality crime which takes place once the material activity is completed. As long as that access was not authorized, it does not need a realization of any result.

1 Dr. Hussin Algindee. The criminal policy facing cybercrime. 2009, pp. 350-351. Dar Alnahda Alarabia.
2 Dr. Mohammed Alkappe. The Criminal Protection to E-Trade: A Comparative Study. University of Cairo, Egypt. 2009, pp. 338-340.
3 Jonathan Herring, Criminal Law. 2002, pp. 339-340. Oxford University Press.
4 Dr. Medhat Ramadan. Criminal protect E-Trade, 2001, pp. 51-52. Dar Alnahda Alarabia.
5 Omar Alhoseny. Important problems of compute crime and the international effect. 1995, pp. 57.

3.2.1.2 Exceeding an Authorized Access

Article 2 of the UAE Information Technology Crimes Act refers to the act of exceeding an authorized access and it incriminates such deed and considers it as being at the same level of unlawful access (without permit).

The act of access in such type of crimes starts by a legal deed, as the offender has the right of access as per authorities entrusted upon him (being a company employee). A person pays the required fees to access the system (internet cafes)[1]; his legal situation will change once this employee exceeds his authority[2] (e.g. hours granted to him). This person has benefited from the system, although he has not paid an extra amount of money equivalent to these benefits. The system's owner, in this case, does not accept the offender's logging on without payment - the same criminal concept of illegal access.

The issue in this case addresses the situation when access to the system is authorized and accepted, but it has been used for a purpose other than the original one, or when the user exceeds the time allowed.

Access to information system should be restricted to the purpose for which authority is granted in the first place, so whenever this purpose contradicts with original the purpose of access, the act is then deeded criminal and becomes subject to unauthorized access.

3.2.1.3 Staying Illegally

Staying Illegally is added to the new amendment of the UAE Information Technology Crimes Act for the year 2012; in this case the actor is not intending or willing to access the system, and the access was coincidental or by way of error. A person may find himself accidentally navigating a system, as if he intends to access a specific system to which he has the right of access, and then finds himself erroneously on another system. In such a case a person may either log out of the system in question once he realizes his mistake, or continue logging on in spite of the fact that he knows he is not authorized to do so.

There is no doubt that the act of a system user, who mistakenly logs in and continues doing so, does not differ from an act of unauthorized access; both are deemed incriminating. The offender's intent to continue logging in, despite the fact that he

1 Dr. Mohammed Alkappe. The Criminal Protection to E-Trade: A Comparative Study. University of Cairo, Egypt. 2009, pp. 353-355.
2 Dr. Omar Youns. Crimes arising from internet using. 2004, pp. 55-56.

knows that his act is illegal, does not differ, in principle, from the act of unauthorized access to computer systems. The public interest protected by the law, i.e. protection of computer systems and their data contents, is identical in both cases. The legislator did well by imposing punishment for illegally staying, whereas the old UAE Act of 2006 does not incriminate the unintended access to the system as it stipulated the intention to access the system, when someone make changes or deletion in the system, etc. Thus a person will not be punished as per the previous law because of lack of internet. According to the current amendment (2012) if unintended access is being a result of coincidence or of error, and hence the actor stays logging in for some time, and during this period he or she prints or deletes some files , etc. This act of logging in becomes an offense punishable by law and falls under the concept of illegal access as the actor's logging in is undesirable, incriminating and affects the safety and integrity of the system.

From this perspective, we find that the UAE Act pursues the legislative approach which explicitly incriminates illegal stay (logging in) within the system. Article 323-1 of the French Penal Code explicitly criminalizes illegal access or staying within all or part of the automated information processing system. In application to this Article, Paris Court of Appeal stated in, a judgment issued on 5/4/1999[1] that the law incriminates illegal stay within the computer system whether access is accidentally or lawfully, but then the user's access is deemed illegal as if he loses the right to stay because of his error.

A question comes to mind: if access to a system is being authorized by the official in charge and the user exceeds the allotted time, or that his intent to access is just to see and learn without extracting any of the data contained, is logging then deeded illegal?

The wisdom behind criminalizing illegal access to and illegal stay within the system is to protect computer data and shield it against unauthorized persons does not materialize here, as access referred to in both cases above is officially authorized by the person in charge, and this means his approval that others can read information contained in the system. If this person exceeds allotted time or authority granted to him his act will not be considered as a lawful stay but will constitute another crime of computer theft or exceeding authority granted.

1 Dr. Momamed Alkappe. Protection E-Trade: a comparative study. 2009, pp. 390-391. University of Cairo, Egypt.

3.2.2 Types of Illegal Access Punishable by the UAE Cyber Law

3.2.2.1 Article 2

- Article 2 paragraph 1 has been thoroughly explained above.
- Article 2 paragraphs 2[1]: Illegal access to cancel, delete, damage, change, reprint and disseminate data or information.

The offender intent may be to tamper with information stored in the computer as if to erase or change or delete some of it or reprint - Article 2 paragraph 2- of the UAE Cyber law punches this deed, this Article is considered a general article as it is not assigned to a particular type of crime, or a particular category as the legislator did with the rest of legal texts that criminalize the act of illegal access. Article 2 paragraph 2 punishes the result (the damage) that resulted from this illegal access, be it accidental or not; therefore this crime has a result and will not be punishable unless there is damage.

3.2.2.2 The National Security (Article 4)[2]

Illegal access to obtain data affecting the national security or national economy:

In this hypothesis, the offender's intent is to obtain data that affects the national security or national economy; Article (4) of the UAE Cyber law penalizes this deed. By enacting this Article the legislator intends to protect the secrecy and confidentiality of the Federal Government and to protect state security from hackers. Violation of Article 4 is, therefore, considered a felony, bearing in mind the ease of committing such crimes.

Incrimination exists – according to this clear text – even if the accused is unable to obtain confidential or classified information concerning state security or state economy; it suffice that the intent of the accused is to obtain this type of information, then elements of the crime exists, not mere embarking on…

Within the scope of this Article, confidential electronic data and information of banks and financial institutions are considered as confidential government data.

Materialistic aspect: (Mens Actus)

This crime is based on the act of an unlawful access with the purpose of opening a gate to an e-site, informatics system or an electronic network.

- The concept of unlawful access: (government information and websites).

1 Refer to Appendix 1(Article 2-2 UAE cyber law).
2 Refer to Appendix 1(Article 4 UAE cyber law).

Unauthorized access means unlawful access; we have explained this in the preceding chapters.

- *The nature of unlawful access:*

As mentioned above, jurisprudence divides crime into two types, materialistic crimes i.e. crimes with a result; and formality crimes i.e. crimes with mere behavior and activity. This raises a question: what is the nature of unlawful access which incriminates as per the above mentioned Article; is it considered a materialistic or a formality crime? In other words, is it necessary that an unlawful access produces an effect that leads to a criminal result like access to different data contained in this system, or that mere access constitutes a crime?

It is clear from the previous provision that the unlawful and incriminating access is the access that produces an effect, since a crime will not exist by mere access to the system, but on the condition that the actor intends to obtain confidential governmental electronic data or information. It is noticed that the legislator considers, within the scope of this Article, that confidential electronic data and information concerning banks and financial institution are as secret and confidential as their governmental counterparts.

Moral aspect (Mens R):

Unlawful access, referred to in Article 4 of the UAE Information Technology Crimes Act, is considered as an intended crime based on criminal intent with both elements of knowledge and the will to do so; hence the offender should realize that he has no right to access this system, and that this system or website or informatics network are government owned, or that they are confidential information and any access to them will be against the will of the system owner, or he who controls it (the government); and irrespective of that the offender intends to do this unlawful act.

Not only that, Article 4 stipulates that to incriminate an unlawful access, there must be a clear criminal intent that, i.e. obtaining confidential government data or information.

Punishment:

Article 4 Article above and Article 28[1] of UAE Penal Code provide (imprisonment). Article 68[2] of UAE Penal Code imposes punishment by temporary imprisonment (for a minimum period of 3 years and a maximum of 15 years). Article 4 provides that an offender punishment shall be as follows:

A. Simple crime punishment: as specified in the above provision is temporary imprisonment of (3-15 years) and a fine of not less than 250,000 Dirham and not more than 1,500,000 Dirham.
B. Severe punishment of crime: If the incrementing act results in cancellation or change or modification or distort or damage or copying, publishing or re-publishing of information and date, the offender shall be punished by imprisonment for not less than 5 years and a fine of not less than 500,000 dirham, and not more than 2,000,000 dirham.

3.2.2.3 Website (Article 5)[3]:

Illegal access with purpose of tampering the website:

Due to the unprecedented revolution in communications and information technology, the internet, especially internet sites whether personal, communal or corporate, has become one of the most important methods of communicating between people all over the globe. Although those e-sites swiftly transfer information to global navigators but they become a strategic goal to digital hackers who exploited the system in order to sabotage, misinformation or disruption or theft, especially in times of crisis.

In this hypothesis, the UAE laws punish those who unlawfully access the system via one of the following methods: change the design of the site, damage or modify the site or occupy the website's (URL) address. It is known that every site has a name, so he who tampers with a site name to preclude its use in one way or another, will be subject to this incrimination. Article 1 of the UAE Act defines the meaning of website as "the place where internet data is available through a specified address". Likewise, incrimination prevails and full penalty will be imposed upon the actor even though he or she is not able to tamper with the site as long as his/her intent behind unlawful access is to realize that end.

1 Refer to Appendix 2 (UAE penal code Article 28).
2 Refer to Appendix 2 (UAE penal code Article 68).
3 Refer to Appendix 1(Article 5 UAE cyber law).

Firstly: (Mens A)

Reviewing the previous text we find that the materialistic aspect of this crime is based on the act of illegal access to an e-site that produces an effect, since a crime does not materialize with just accessing the site. If the user intends to change the site's design, or modify its content or destroy or cancel or steal its address, he will be incriminated.

Secondly: (Mens R)

This crime is considered as an intended crime based on criminal intent with its elements of knowledge and the will; the offender should realize that he has no right to access this system, and that his access is against the will of the system's owner and in spite of that he intends to commit this unlawful act.

The law requires that to incriminate a behavior, a criminal intent should prevail, but if the user intends to change the site's design, or modify, destroy or cancel its content he, therefore, shall be incriminated. The UAE law does not differentiate between private sites and government site, and we believe that the legislator should have made the punishment more severe if a crime is committed against a government e-site, since most of the government e-sites provide services to members of the community, hence any offense against them disrupts these services.

(Common attacks against electronic websites)[1]

1. Denial of Service Attack

Denial of service means inaccessibility to the site on the internet (denial of service) is unavailable to uses, by way of flooding the network with fake and malicious applications, like lawful application that cannot be realized, or it takes long time to access; henceforth the e-site will not be available at the internet. It is important to be aware that the network has been attacked in order to make corrective measures. If the internet or the server is confronted with one of the following situations, that means the system has been attacked:

- The site is not available.
- If any of the sites cannot be accessed.
- If the network is slow and its performance is much lower than the normal level, i.e. it takes more time to access the web or open files.

1 Dr. Hussen Algafrre. Illegal access to website and E-System. www.omanlaw.com

2. Penetration

This is a method of attacks against internet sites. Penetration is defined as "intentional access to a computer without authorization or exceeding allowable limits". Following are examples of the most common targets in penetrating internet sites:

Distortion of sites

This is the most common target on the internet network. Hackers change or modify the web pages by inserting their messages. The purpose of such attack is to attract attention to a particular problem or issue, or to show the hacker' expertise and offensive capabilities.

Espionage

To spy on visitors or website owners in order to obtain important information.

Theft

Access to information is not available to common browsers. There may be secret information stored in an e-web and access to this information is restricted to specified personnel; hence through penetration attackers can obtain the information in question.

Systems manipulation

In most cases attacks on internet are launched through intermediary devices which were penetrated prior to the attack. A hacker first move is to penetrate those devices and to install some software that may be activated later, i.e. prior to launching a distant attack. The manipulated devices are not targets for an attack, but they are used as intermediary tools prior to attacking the real targets.

3. Electronic fishing

E-fishing is one of the electronic crimes which try to obtain sensitive information from a victim to be used later in a process of impersonation. Deception is usually done through e-mail or instant messages that seem as if they were sent from a well-known and reliable source. These messages contain a link that directs the user to a fallacious site very similar to the real site; and asks him to update his data or to enter/install confidential information.

4. Tampering with the name server of web links

Tampering with web –links name server is another type of attacks on websites and it resembles, to some extent, e-baiting, but technically difficult to implement. The idea is to direct users of a particular website to divert to another phony site having the same name of the real site; this is performed through an attack called" poisoning the domain

naming system memory". Poisoning the domain naming system memory is an attack on the internet sites domain naming system. This state of affairs allows the user to enter a name that has a meaning to the website instead of a series of numbers that are difficult to memorize. And this depends on the web-links name server which changes websites names, demanded by the user, to digits recognizable to the machine, the latter will then directs the user to the website liked to the number. When launching an attack on the web-links name server system, the attacker changes the rules upon which conversion between webs names and their numbers is performed. These result in diverging huge numbers of users from one site to other fake sites that provide services to the attacker without any knowledge on the part of users, because the site name is identical with the true name of the required site.

3.2.2.4 Viruses (Article 10[1])

Article 10 of the UAE Information Technology Crime Act penalizes the act of unlawful access, but the nature of the act differs to some extent from the nature of act prescribed in Article 2 of this Act. Since the act of unlawful access constitutes a special crime, as we have explained above, almost all countries of the world have incriminated this deed. Moreover, the act of illegal access prescribed in Article 10 of the UAE Information Technology Crime Act concerning inserting viruses and malicious software has its own special nature, although it is considered, in its entirety, as an act of unlawful entry, where all elements of the crime of unlawful entry exist, together with illegality. It worth noting that we have dedicated a special section in this research under the title "information destruction" in which we will explain, in details, virus attacks and malicious software crime.

To some up, we believe that because of the importance of computer crimes, like virus attacks, Article 10 of the UAE Information Technology Crime Act is intended to protect against those who transmit viruses and malware through the internet or any other information technology means. These software programs are expected to stop, disable or damage the network, etc.

As mentioned before, transmission of viruses and malware crimes are of paramount importance, hence Article 10 of the UAE Information Technology Crime Act

1 Refer to Appendix 1 (Article 10 UAE cyber law).

incriminates and punishes any wrongdoing pertaining to this matter. Although the UAE Information Technology Crime Act of the year 2012, which reviews and amends the 2006 Act, adds a special Article to address the subject, we realize that it incriminates and penalizes any attempts to spread viruses, following, in this respects, the footsteps of Japan's new legislation, (of the year 2011, Article 168-2[1]) which penalizes preparation of viruses and malicious software.

3.2.2.5 E-Card (Article 12[2])

Article 12 of the UAE Information Technology Crime Act incriminates and punishes any person who accesses, without any right or authorization, numbers or data of an electronic or credit card, etc.

The UAE Information Technology Crime Act specifies a legal text for crimes committed against credit cards and all electronic cards due to the widespread use of these devices in daily transactions.

We devote a special section in this research under the title "electronic fraud", in which we shall discuss, in some details, electronic cards crimes and how the UAE law penalizes this type of crimes.

3.2.3 Punishment for Attempt in Illegal Access Crime

Amendment of 2012 to the UAE Information Technology Crime Act of 2006 has introduced Article 40 since UAE Penal Code does not punish attempt of felonies and violations.

Article 35[3] of the UAE Penal Code penalizes attempt to commit a felony, and as the act of unlawful access referred to in Article 2 of the UAE Information Technology Crime Act is considered a felony, and since this unlawful act is possible, for instance an offender may be able to operate the system without being able to access the data system itself. If the defendant is caught after he operates the computer and before being able to open any of the file stored in the computer he will be then dealing with a crime of attempt to unlawful access.

1 Refer to Appendix 3 (Japanese Penal Code Article 168-2).
2 Refer to Appendix 1 (Article 12 UAE cyber law).
3 Refer to Appendix 2 (UAE penal code Article 35).

Examples of above attempts is the inability of the accused to access files even though he opens the device but failed to recognize the password, or any other procedure no known to the offender.

3.3 Illegal Access Crime in Japan

The purpose of unauthorized computer access law (Law No. 128 of 1999) is to prevent computer related crimes by stipulating penal provisions on illegal access and to maintain the telecommunications-related order.

An information processing starts with accessing a computer. An act of unauthorized computer access hinders the security of information processing. The act of "computer access" under unauthorized computer access law has to fulfill the following conditions:

1. Computer access has to be done through a telecommunication line.
2. Access administrator imposes access control function on a special computer.
3. ID and Password and the likes lift the access control function.

   Identification code means a code attached to a person who is authorized specific use of the specific computer admitted by a access administrator.

The following (1) and (2) are examples of unauthorized computer access.

1. A person who is not authorized special use of a special computer reads ID and Password of another over his shoulder. This person can slip through a access control function by the act to input this ID and Password into a specific computer. He becomes able to keep the specific use of a specific computer in an available state.
2. A person inputs any information (excluding an identification code) or command which evades the restriction placed by an access control function into a specific computer.

   Above case occurs because of a flaw in a program of the access control function.

An act of unauthorized computer access makes special use of a special computer possible. There is no restriction on content of special use. Examples of special use are altering a home page, ordering goods through the internet, accessing data and others.

Unauthorized Computer Access Law prohibits an act of unauthorized computer access (Article 3). A person who has infringed the provision of Article 3 shall be punished by imprisonment with work for not more than three years or a fine of no more than 1,000,000 yen.

3. Article 4 prohibits the act to obtain another person's identification code which is recorded on paper, USB memory or ID card and like for the purpose of unauthorized computer access.

Article 5 prohibits the act to provide another person's identification code to a person who has no right to use it.

Article 4 prohibited the act to provide another person's specified ID code available for specific use of a specific computer.

Article 6 prohibits the act to keep another person's identification code which is obtained for the purpose of unauthorized computer access.

Article 7 prohibits the following act by a person under pretenses of access administrator.

The prohibited act is the act to inform a rightful user of an identification code to input this identification code into a specific computer by electric of obtaining another person's identification code.

Article 8 provides that a person who has infringed the provision of Article 4, Article 5, Article 6 or Article 7 shall be punished by imprisonment with work for not more than one year or a fine of not more than 500,000 yen.

4. Article 4, Article 6, and Article 7 are added and Article 5 is revised in part by the unauthorized computer access law amendment of 2012. These provisions are set forth in order to punish the preliminary act of unauthorized computer access.

3.4 Summary

In the Japanese act on prohibition of unauthorized computer access, it is understood that unauthorized computer access is categorized as one of the crimes which impair credibility in information processing of computers. In Japanese law, unauthorized computer access is limited to access with others' ID's or passwords, or an activity to send a considerable amount of information to a specific computer at the same time. On the contrary, the UAE's law does not indicate any means of unauthorized access that is punishable, but it is subject to punishment if a person sneaks into others' computers without permission. Also, the targeted computers are not specifically required to have access control functions. The law regards not only unauthorized computer access but also illegally staying in others' computers or accessing the computer without permission as illegal activities to be subject to penalty. In addition, there are weighted penalty

provisions for unauthorized access for the purpose of damaging, erasing, or changing information in targeted computers. The activities to obtain specific confidential information such as ID's or passwords that should be classified through the internet is also subject to punishment. However, in Japanese law, providing the illegally obtained ID's of others, illegally asking others to input their ID's or other classified information through the internet, and possessing others' ID's or other information obtained illegally are subject to penalty. The UAE's law does not have such a regulation.

The differences in these two laws may be derived from differences in the legal systems, or to appropriately address cultural differences in the two different regions; however, such vast procedural and substantive discrepancies in the law are bound to produce vast discrepancies in the law's effects in application. This section intends to overview some of the major differences between the two laws that could lead to discrepancies in effect, interpretation, and application in society.

- A very concrete difference to note is what activity is specifically outlawed by each of the acts. Although the acts are very similar in their intents, the activity that each outlaws is defined differently. The UAE Cyber law specifically names several activities which are outlawed. The activities relating to Illegal access crime can be summarized as follows:

1. Illegal access to any electronic website, system, or any electronic means (Article 2).
2. Obtaining National Security Information (Article 4).
3. Entering an Electronic Site without Permission (Article 5).
4. Intentionally Entering without Permission an Information Program to the Information Network (Article 10).
5. Obtaining the Numbers or Statements of a Credit or Electronic Card or Bank Accounts (Article 12).

The Unauthorized Computer Access Law in Japan, however, only delineates one crime of "unauthorized computer access." The only action needed to be in violation of this law is "trespassing" in a computer or cyberspace beyond permitted access. No differentiation is made between intent, causing damage or information related to national security.

The actions criminalized by the UAE Cyber law are much more detailed in their description, and allow for much more differentiated penalties based on intent, whether or not damage occurred, and on the type of information that was illegally accessed or

damaged. The Japanese act does not make such differentiations, and only applies one flat penalty. The Japanese Unauthorized Computer Access Law penal code is much more straightforward.

- Another difference in the UAE cyber law and the unauthorized access law of Japan. Japanese law define the term of The Unauthorized access (Illegal access) and Prescribe the conditions but the UAE Cyber law did not define the term of the illegal access, Article 2 and other articles such as article 4,etc, of UAE Cyber law only punish the Illegal access . The UAE law may expand in the term of Illegal access, unlike The Japanese Unauthorized Computer Access Law penal code is much more straightforward.
- The last different between UAE cyber law and Japanese unauthorized access law:
  UAE cyber law punished the act of Illegal access, even though the law does not specify what kind of security measures required availability in the system in order to criminalize the act, but in general, and as we explained in Chapter III that the lack of legitimacy general word -in-UAE law and it did not required availability of security measures or otherwise. By contrast, unauthorized computer access law in Japan was more clearly and explicitly that select to criminalize the act of unauthorized access to be available in the system security measures.

CHAPTER 4

OFFENSES AGAINST PUBLIC MORALS IN THE CYBERCRIME

CHAPTER 4

4.1 Introduction

Most of legislation does not distinguish between outrageous acts and porn, due to the cultural differences in the laws of morality and social cultural output. This paradox brings out various results in the comparative legislation; however, in the social reality in terms of the civilization differences, the impact of each of these terminologies[1] has a basis associated with the extent of ethical freedom given by the society to the individuals. The legislator did never define a unified meaning to the terminologies of ethics included in the Criminal Law, in the UAE law or the Japanese Law for instance, the term "immoral" is a general term that was not defined by law such as other legal terms?

Based on a legal definition set by a jurist[2], violation of public morals means "What people use to call as overriding decency, where modesty of an individual is hurt by seeing or hearing something such as pictures, movies regardless of the degree of obscenity posed or involved therein.

4.1.1 Examples of Moral Crimes Committed Via the Internet

There are many crimes resulting from the misuse of computers or internet, which affect ethics and morals, the most important of which are:

1. Porn sites:

The Internet had provided the most effective and attractive means to the industry and promulgation of sex pornography, it has made pornography, including display of photos, videos and incidents whether registered or directly, accessible to everyone, therefore, this is considered the greatest cons of the Internet. The problem of pornographic sites and its spreading is not considered a local problem specific to a particular state, whether being a conservative society such as the UAE with its own traditions, customs and ethics, which reject this culture, or any other state regardless of the difference in moral concepts here or there, the various ethnic groups such as the American society, or a single ethnic group such as the Japanese society[3]. That is to say, it is a global dilemma that all countries try to resist and reduce its effects by their own means. For example,

1 Dr. Omar Youns. Crimes arising from internet using. 2004, pp. 447-450.
2 Mohamed Moharam and Khalid Kadfor, UAE penal code .1992, pp. 930-931. Alfatah Publications.
3 Munir Aljanbehi and Mamdoh Aljanbehi. Computer crime and means of protection. 2004, pp. 29. Dar Alfikr Aljamai, Egypt.

the report published by the (CNN) on 15/03/2003, in its web site titled "Easy Access to Pornography files", stating that, access to the pornography files has become as easy as access to music files (MP3) and that is in spite of all the technological measures that have been taken to reduce the same.

2. Sites defaming people:

With the spread of rumors and false news which go on and affect the symbols of peoples, whether ideological, political or religious symbols, some suspicious sites appeared on the Internet, which recruited itself to the goal of serving such rumors and false news with the aim of insulting and defaming those political, intellectual and religious symbols, which people circumvent around, to defame those symbols in order to discredit their credibility before people. The objective of these sites may be to attempt to blackmail some people by all means and forms, by spreading rumours about them if they do not submit and pay financial consideration. There is a famous incident traded between Internet users when the Internet service had first operated in the Middle East, where someone from a Gulf state had created a web site and published a photo of a girl naked with her boyfriend as he had obtained such photos after he infiltrated into her computer and copied him, and when he tried to sexually blackmail her by those photos she refused to respond to him and he published the photos and consequently the girl committed suicide after the scandal he made to her among her relatives and people[1].

In the United Arab Emirates, specifically in the Emirate of Dubai[2], the Police arrested a "girls' pictures pirate" who managed to rob the private email of a group of girls in the UAE and published their photographs on the Internet with another group of pornography and he has been referred to the Public Prosecution.

3- Aannouncement of prostitution and debauchery Crimes:

Sexual exploitation, dissemination of photos, movies and publications against public morals, abetment to practice prostitution for money, trafficking in images of pornographic nature[3], dissemination of numbers and statistics has led to increasing

1 Mariam Mohamed. The situation of computer crime related to morality via Internet. 2009, pp. 52. Police research center of Sharajah, UAE.
2 www.internet.fares.net.
3 Ahmad Wahdan. Evaluating of facing legislation relating to Internet crime. 2004, pp. 56. Police research center of Sharajah, UAE.

number of visitors to the sites that offer these acts and increased participants of such sites from both sexes of all ages.

Punishments of crimes related to ethics and public morals in the UAE laws and the Japanese Law:

As to the applicable laws and legislations concerning cybercrimes relating to public morals online, all types of legislations in the vast majority of states have cared for private life of individuals within the community and outside it, maintained the special protection required to prevent penetration of its sanctity or exposure to all that would impair the public morals and outrage the public modesty. In this research we will identify the laws enacted in the United Arab Emirates and Japan to combat cybercrimes affecting public morals and ethics.

4.2. Offenses against Public Morals in UAE Laws

In statutory systems Legislators are keen to criminalize a range of words and acts that affect ethics, public morals and public order, through the use of the Internet or any of the means of modern technology. Legislators are trying hard to formulate their incriminating words in specific legal provisions to specify the criminal acts to individuals accurately, avoiding generality and ambiguity in order to protect the rights and freedoms away from fancy and tyranny and in line with the principle of criminal legality.

4.2.1 Public Morals in Cyber Law

With the advent of technology and Internet, new types of crimes have emerged which the current legislations failed to face, consequently; a need for new legislations to criminalize acts and actions emerged to keep up with every violation to the social and personal interest. Therefore, the UAE legislator has issued the Federal Law No. 2 of 2006 concerning Prevention of Information Technology Crimes and the amendment thereto No. (5) For the year 2012 to fill the Legislative gap in this important and evolving aspect.

It is noted that the Information Technology Crimes Act had drew some of its provisions from the Federal Penal Code of the year 1987, particularly with regard to crimes of violation of public morals, public order and defamation of religions, and as the Information Technology Crimes Act has been influenced by the Federal Penal Code

and drew some of its provisions from it in a different way- that crimes are committed through the computer - it must follow the Penal Code and be influenced by the religious and moral nature extracted from the Islamic Sharia rules based on the community's religion, culture and customs and then the constitution of the State and to confirm the judgments issued by the Federal Supreme Court on that nature and influence.

Articles[1] (17/19/20/35/22) of the Information Technology Crimes Act have provided punishments for the acts against public morals and ethics, find below explanation of these articles and illustration of the differences from the UAE Penal Code.

4.2.2 Article 17 Cyber Law

Article 17 of the UAE cyber law is a reduction of articles[2] 361 and 362 of the UAE Penal Code, it is noted that in Article 361 of the Penal Code, the act of publicly pronouncing a call, songs, shouting or a speech contrary to morality or temptation of others by any means *Article 9 of the UAE Penal Code* has identified the ways of publicity which is realized in this context by call, songs, shouting or speech of the wrongdoer in a way contrary to the morals, whether heard in any public or private place, as far as there are people hearing what the offender says contrary to morals, because the purpose of this article is to protect the public from all expressions that outrage their decency and feelings, which are contrary to public morals[3] whether being a call, songs, shouting or speech, such as casting an obscene song contrary to public morals in a theater or a wedding ceremony.

The second paragraph of Article 17 of the UAE Law sets a punishment for producing, preparing, sending or storing materials affecting public morals with the purpose of exploitation, distribution or supply to others. However[4], whoever keeps scandalous materials in his personal e-mail without intention to sell them or display them to third parties will not be punished under the above-mentioned article, similarly, Article 175[5] of the Japanese Penal Code, requires the sale or distribution of these materials. Incrimination in the UAE law includes announcement of any obscene materials that are contrary to morals by any way of publicity which are found in the Internet, such as

1 Refer to Appendix 1 (Articles 17, 19, 20, 22, 35).
2 Refer to Appendix 2 (Articles 9, 361, 362, 363).
3 Mohamed Moharam and Khalid Kadfor, UAE penal code .1992, pp. 928-929. Alfatah Publications.
4 Al Shawabkah. Crimes of computer and Internet. 2004, pp. 109. Dar Althaqafah.
5 Refer to Appendix 3 (Article 175, Japanese Penal Code).

advertising a website that provides sexual services on the Internet, likewise, display of obscene materials in a public place or permitting others to display them to the public, such as display in Internet cafes, will render the doer punishable under Article 17 of the UAE Internet Crimes Act.

Article 17 of the UAE Internet Crimes Act also punishes whoever creates or manages an internet website, etc. Creation of sex sites on the Internet with the intention of exploiting or displaying to the public comes within the scope of incrimination provided for in Article 17 of the UAE Internet Crimes Act. Likewise, whoever distributes an e - mail containing obscene pictures or phrases, shall be punished under Article 17 of the UAE Internet Crimes Act.

4.2.3 Article 19 UAE Cyber Law

Article 363 of the UAE Penal Code had set a punishment for abetment to immorality and prostitution. Abetment to immorality and prostitution means influencing the victim in order to convince him to commit immoral acts or prostitution by highlighting the idea or instigating him or promising him to get financial gain because of it. The law does not specify a certain way to realize the crime and thus the crime takes place by any mean the wrongdoer may choose, however, temptation means seducing the victim and making immorality desirable to him, facilitating wrong acts by any means whatsoever, and thus all possible means that the offender may resort to in order to achieve the result may be included.

Article 19 of the UAE Cyber law is a repetition of Article 363 of the Penal Code, however, it had identified the means by using the Internet or an information technology mean, such as sex related photos that are broadcasted in the internet, providing information concerning the brothels in many countries worldwide on the network, broadcasting nude photos and sending them via e-mail, all these crimes come within the scope of applicability of Article 19 of the UAE Cyber Crime Law.

4.2.4 The Ambiguity of the Term Public Moral in the Law

The legislator did not set a definition to the concept of Public Moral as a legal term, under which a set of actions fall, yet it left this issue to jurisprudence and judiciary. Public Moral is a broad and vague concept and the individual does not know which act is authorized or criminalized under that term.

Law had criminalized some acts which are deemed contrary to public morals and had set some specific provisions for them, such as indecent assault, outraging modesty... etc., and it had then set a general provision to punish whoever commits an act that violates the public morals in order to include all acts that may arise, however, the legislator had left it open without controls or basis that can be referred to in order define the concept.

The Supreme Court admitted that, the UAE legislator/legislature did not set a definition of the term public morals and decided that there are controls that can be invoked to determine the acts under this concept, in accordance with usage, customs, traditions and general attributes of Islam morality and ethics, that the judiciary is the competent body to identify those controls and it can assess whether the act is contrary to modesty or not[1]. It is noted that for this crime to be established, it must be proved that the offender has intention to commit the act which is contrary to morals, knowing it is contrary to morals.

Actually the definitions may vary between expanding the concept of public morals and limiting it, yet, they agree on what the society acknowledges as behavior and morals. The concept of morality in the Sharia law is broader than that in the positive laws[2]. The Federal Supreme Court made it clear that the criteria of the concept is the general features of morality and ethics of Islam, as well as the religion of the society and therefore, this concept must be defined within that framework, as, any act contrary to Islamic morality is a sin and therefore is considered a crime that can be entered under the punishing provision that incriminates breach of public morals, in accordance with the opinion of the Supreme Court in the application submitted to consider the constitutionality of paragraph four of Article 58 of Abu Dhabi Penal Code.

It could also be argued that, the concept of "whoever violates any of the family principles or values contained in the provision of Article 16 of the Information Technology Crimes Act" needs to be specified and narrowed, because it is a relative

1 Mohammed Alhammady. Law and computer crime. 2006. Conference at UAE University.
2 Al Mansouri Omar. Idea of general public and the morality in the law and justice. 2010, pp. 443. Dar Aljamaee Aljadeed.

opinion such as the concept of public morals, however, it can be controlled in accordance with the family values and ethics in the Islamic Sharia Law, customs and traditions as an equivalent to the previous court ruling in controlling the concept of public morals.

Article 17 of the Law is one of the articles that show the fact that, law has focused on maintaining law in line with the will of rulers and individuals and in conformity with the provisions of the Constitution and that of Islamic Sharia law, such as "whoever abets any male or female or incited him to commit prostitution or debauchery or assists him to do that by using the Internet or any of the information technology means...shall be punished with imprisonment and a fine[1]. Article (35) has likewise set a punishment for whoever uses the Internet or any information technology mean to commit any of the following crimes: abuse an Islamic sacred or rituals, abuse of a sacred or ritual prescribed in other religions whenever such sacred or rituals are protected in accordance with the provisions of Islamic Sharia[2].

In spite of these legal provisions which criminalize some acts disapproved by Shara, society and individuals, yet some law phrases were general and ambiguous and did not specify the forbidden acts and the punishable acts, although apparently they indicate incrimination of all acts that contravene public morals, based on the principles of Islamic Law and morals[3]. However, the term public morals and the acts it includes is no longer clear and specific to individuals, even if it is restrained with whatever is in violation of Islamic morals and Islamic law as, the principle of legality requires specific conditions in terms of drafting, expression and definition.

In addition to all that had been stated in the Cyber law, incriminating all acts that prejudice public morals or lead to facilitate or beautify a sin, the Telecommunications Regulatory Authority Law No. (3/ 2003) has played a major role in blocking sites that violate public morals which is done by Emirates Telecommunications Co and the Integrated Telecommunication Company , as the policy concerning access to the Internet has provided for the prevention and blockage of the sites that breach public morals, therefore, category No. 13 , is among the blocked categories , which is the banned (Top Level Domains) including the internet contents under top domains that

1 Similar to Article 363 in UAE penal code.
2 Similar to Articles 312, 315, 319 of UAE penal code.
3 Mohammed Alhammady. Law and computer crime. 2006. Conference at UAE University.

contradict with the interest, public morals, public order, national security and the teachings of the Islamic religion or anything prohibited under the laws, regulations or procedures or requirements that are applicable in UAE.

If the ban includes sites containing matters that are prejudicial to public morals or public ethics, there must be a reference to define what is meant by public ethics or public morals, under which light sites can be banned without restricting the freedom of individuals to access information or ideas or to publish them without causing any harm to the society, its appearance and culture, as the high policy of the telecommunications sector in the United Arab Emirates, which has been published by the TRA has made it within its public policy in formulating the policy and regulatory framework [1] that encouraging all community sectors to use the Internet in order to participate in the exchange of information, ideas and experiences, with the direction to the significance of the use of network in a responsible manner that maintains the moral values and social norms applicable in the UAE. If the moral values are heterogeneous, different and unclear, then what is the criterion that will control the exchange of information in a way that is not incompatible with ethics, public morals and social norms, in case all members of the community of different nationalities, races and religions will use the Internet and modern technology.

4.2.5 Implementation Problem of Public Morals Crime

The Legislator aims at maintaining values of virtue and public morals, protecting individuals and the community: hence it criminalizes any behavior that contradicts with public morals. By so doing the community is shielded with a strong fence of morality and virtue. However, the implementation of these provisions faces some problems, such as:

The first problem is that acts are not clearly specified so that an individual can differentiate between what is permissible and what is prevented or prohibited. Concepts on and understanding of public morals differ from one person to another and from one era to another, as well as between different communities. Moreover, differences in

1 www.tra.gov.ae

circumstances of time and place have their impact in defining violation of public morals[1].

The community and judiciary constitute a group of individuals bearing various and different ideas, some of them are conservative while others are liberal, some of them know Sharia (Islamic Law) provisions whereas other are do not, some were reared in a culture which differs from the one in which they live, where they came with different culture. There are more than 180 nationalities that work and live in the UAE. Many of these foreign communities, on the other hand, had established their own schools. Emphasis on differences between individuals, educational syllabus and the large numbers of foreign communities is due to the fact that most of internet users are from younger generations, and hence become more susceptible to imitate others.

If incriminating acts are not clearly stated within the context of a rapidly changing and multi-cultural society, and in the absence of a specified and clear concept on what the legislator has in mind concerning penalties as the legislator may intend to penalize a certain behavior and avoid another, or penalize one uttering and accept another; therefore, in such circumstances any reference to the legality of such provisions violates the principles of legitimacy. Therefore the Supreme Court's ruling was a bit erroneous. When provisions on breaching of public morals were un- clearly specified and pinpointed an individual may be confused; henceforth any penalty provisions should clearly identify incriminating acts.

Freedoms and rights of individuals:

Legal provisions are in principle addressed to the public, as they define behavior and impose restrictions on individuals' conduct. Violation of any legal provision will be subject to civil, criminal or administrative penalty. If legal provisions decide specific penalties on those who breach them, these penalties should be definite or nearly definite and should be accurately drafted without ambiguity as to their meaning and interpretation, leaving no space for doubt.

An individual does not realize the illegality of his acts or behavior, whether he can promulgate or display any materials to others and whether he can express his opinion on a romantic book published in a foreign country? All these questions reflect the individual's hesitance on committing any act or following any behavior that may render

1. Dr. Hussin Algindee. The criminal policy facing cybercrime. 2009, pp. 79-80. Dar Alnahda Alarabia.

him accused of that vague principle concerning violation of public morals, enhancing sinful acts and breaking family principles and fundamentals.

If some people utter, in public, some expressions that they have heard in films or electronic chatting rooms will they be accused of breaching public morals and enhancing sinful acts? Dubai Court of Cassation has addressed such matter, and considered that he who breaches public morals (writings or pictures) with the intention to promulgate and show these acts to others, even if he was kidding, and even if he thought they would not breach public morality, he or she shall be punished in accordance with Article 362 of the Federal Penal Code[1].

The Public Prosecutor accused an offender of committing a flagrant act by displaying in public writings and drawings that outrage modesty when he displayed at the front of his vehicle a metal plate with the inscription:" Kiss my ass". The offender claimed that he did not mean the literal meaning of the phrase, or that it was breaching public morals. However, the Court of First Instance followed by the Court of Appeal ruled that the offender was guilty; and Dubai Court of Cassation upheld the verdict. A question may be raised whether that phrase is in frequent use by some people, and that some others used it in electronic chatting, e-mail correspondence or hear it in cinema halls or TV channels; will this frequent usage change the court's ruling irrespective of the fact that some people believe the phrase is not incriminating, that saying or displaying it to third parties is not a crime?

4.3 Japan Law

4.3.1 Article 175

Article 175 of Penal Code 1908 provided that a person who distributed, sale or displayed in public an obscene document, drawing or other objects. Article 175 also punishes people who possess the same for the purpose of sale.

The objects prescribed in Article 175 corporeal things. Images of obscene electromagnetic record are not a corporeal thing. There is a judicial precedent about Article 175. Defendant opened the online computer service. He stored the obscene electromagnetic record in the hard disk of the host computer. An unspecified large number of people have access to this site. But the obscene electromagnetic record in the hard disk is not visible. If a person wants to look at the image of obscene data, they

1 Dubai Court, Case Number 432, 2007.

have to download the image data from the hard disk of the host computer and have to make a reproduction of the obscene image.

The Supreme Court on 16 July, 2001 decided that a hard disk which stores obscene electromagnetic record comes under the obscene drawing in the old Article 175. The Supreme Court said that the operation for reproduction of obscene image data becomes possible by a simple procedure. And it's easy for a person who looks at the image of obscene electromagnetic record stored in the hard disk.

- *The revision of Penal Code 2011 made a partial amendment of Article 175.*

The new Article 175 paragraph1, a person who distributes or displays in public obscene documents, drawings, the storage of obscene electromagnetic record or other objects shall be punished by imprisonment with work for not more than two years, a fine not more than 2,500,000 Yen, petty fine or either penalties. The same shall apply to a person who distributes the electromagnetic record by telecommunication transmission.

Paragraph2. The same shall apply to a person who possesses or keeps the objects of article 175 paragraph 1, in order to distribute with charge. For example, obscene videotape is a storage mediator of obscene electromagnetic record. Electromagnetic mail is one example of electromagnetic record by telecommunication transmission.

4.3.2 Child Prostitution and Child Pornography

1. Article 2 paragraph 3 is a provision relating to definition of child pornography. The term "child pornography" shall mean photographs, data career containing electromagnetic record or any other things or which pose of children prescribed in Article 2 paragraph 3 Section 1-3 is recorded.

   The term "child" as used in this act means a person less than eighteen years of age.

   Article 2 Paragraph 3 Section 1-3 has been defined as follows:

   - Any pose of a child who has sexual intercourse or similar to sexual intercourse.
   - Any pose of a child having genital organs touched by another person or any pose of a child touching another person's genital organs, which arouses or stimulates the viewer's sexual desire.
   - Any pose of a child wholly or partially naked, which arouses or stimulates the viewer's sexual desire.

2. The main purpose of this child pornography act is to protect children from sex abuse. Article 175 of the Penal Code is to protect sexual manners. Child pornography drawn in cartoons is covered by article 175 of the Penal code but not covered by the Act of child pornography.

   Electromagnetic records or any other records which depict the pose of a child prescribed in Article 2 paragraph 3 are not included in the term "child pornography".
3. A person who provides a specified person with child pornography shall be punished by imprisonment with work for not more than three years or a fine of not more than 3,000,000 yen according to Article 7 paragraph 1. The same shall apply to a person who provides a specified person with electromagnetic records or any other means which depict the pose of a child prescribed in Article 2 paragraph 3. Article 7 paragraph 4 punishes a person who distributes the objects prescribed in Article 7 paragraph 1 to a specific or a number of people by imprisonment with work for not more than five years and or a fine of not more than 5,000,000 yen.
4. Article 7 paragraph 2 punishes any person any person who produces, possesses, transports, imports to or exports from Japan child pornography for the purpose of providing specified people with this pornography shall be punished by the same penalty prescribed in Article 7 paragraph 1.

   The act to make a copy of child pornography is also the act to produce child pornography. Possession of child pornography without intent of distribution is not punished by Article 7 paragraph.

   Article 7 paragraph 4 punishes any person who provides unspecified or a number of people with child pornography or displays it in public shall be punished by imprisonment with work for not more than five years or a fine of not more than 5,000,000 yen. The same shall apply to a person who distributes electromagnetic record of a pose prescribed in Article 2 paragraph 3 to an unspecified person or persons.

   Article 7 paragraph 6 punishes any Japanese national who imports or exports child pornography to or from a foreign country for the purpose of the activities prescribed in paragraph 4 of this article by the same penalty prescribed in paragraph 4.

   The same shall apply to a person who performs the acts provided in paragraph 2 for the purpose of activities prescribed in paragraph 4.

   Act on controlling activities of online dating service business

- Act on controlling activities of online dating service business was enacted in 2003 and was amended in 2008. The purpose of this act is to prohibit luring children to be partners in sexual intercourse by using an online dating service business and to control activities of the online dating service business.

  Online dating service business offers the service to make it known on the electronic bulletin board that a person wants to have a relationship with children of the opposite sex, and to make this relationship possible on the electronic bulletin board.
- Anyone is prohibited to writ the following message on the electronic bulletin board managed by an online dating service provider.

- Luring a child to sex or a similar sex act with a person of the opposite sex.
  The term "child" as used in this act means a person less than eighteen years of age.
- Luring a person eighteen years and older to sex or similar sex act with a child of the opposite sex.
- Luring a child to have a relationship for a price with a person of the opposite sex.
- Luring a person eighteen years of age or older to have a relationship.
- Luring a child to have a relationship without a charge with a person of the opposite sex or luring a person eighteen years and older to have a relationship without charge with a child of the opposite sex. A person who writes a message from the above mentioned (1) to (4) on an electronic bulletin board shall be punished with a fine of not more than 1,000,000 yen.

5. Online dating service provides having the following duties.
   - At the time of starting up the online dating service business, provider has the duty of notifying the public safety commission of the 47 prefectures via chief of the police station.
   - Online dating service provider has to put up the notice on the electronic bulletin board that a child should not use this online dating service.

     If the online dating service provider notices that there is a message relating to the prohibited inducement act to a child on the electronic bulletin board, the provider has to take measures to make it impossible to browse message on board.

4.4 Summary

In accordance with the Japanese Penal Code, a person who distributes media such as tapes containing obscene documents will be punished. Also, the distribution of electromagnetic records containing obscene objects through the internet is subject to punishment. Also, a person who possesses electromagnetic records containing obscene documents for the purpose of distribution for profit will be punished in accordance with the Japanese Penal Code. On the other hand, the UAE's law does not handle possession of electromagnetic records containing obscene objects. However, while Japanese law indicates "electromagnetic records contain obscene objects" as the object of punishment, the UAE's law describes that it will punish the distribution of materials which contain pornography, gambling activity, or the publicity of immoral acts through the internet. The words "pornography" and "publicity of immoral acts" are obscure, and the range of activities to be subject to punishment is significantly unclear. In Japan, the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children which was enforced in 1999 in order to protect children from sexual exploitation and sexual abuse. It provides a specific definition of child pornography and detailed regulation of producing pornography.

CHAPTER 5

INFORMATION DESTRUCTION CRIME

CHAPTER 5

5.1 Introduction

Information destruction is a wide spread crime deployed in the space of the Internet. This crime may take several forms such as data and information destruction, by distorting programs or information in a way that renders them unusable. Another form is when an offender manages to access a computer of someone else and changes the data, information or software by increasing, decreasing, deleting or adding, in which case the crime is deemed to have been committed, whereupon the offender shall be punished even if the consequent change of the data or information did not cause harm[1]. This punishment is set because the protection is planned for the benefit of the victim and his device and the actus reus (criminal act) may ultimately result on deletion of information, data or software rendering them nil, and consequently the owner of the device will be deprived from using the data, information or software[2].

In the first section of this chapter we will address the information destruction in the UAE Information Technology Crimes Act and how the UAE Penal Code had set a punishment for the information destruction prior to the issuance of the Information Technology Crimes Act 2006, as amended in 2012. In the second section we will see how the Japanese Law had set a punishment for the information destruction crime in the Penal Code.

5.2 Information Destruction Crime in UAE Cyber Law

5.2.1 Article 424[3] of UAE Penal Code

Article 424 of the UAE Penal Code had set a punishment for the destruction of real property whether movable or immovable property, whether the immovable is material or in kind, such as valuable letters, IT software or a computer related entity.

Article (424) of the UAE Penal code has provided for four forms of the act which constitutes the physical element of the destruction crime (actus reus) namely;

- Destruction of property.
- Damaging property.
- Rendering property unusable.

1 Dr. Mohammed Alkappe. The Criminal Protection to E-Trade: A Comparative Study. University of Cairo, Egypt. 2009, pp. 336-338.
2 Dr. Omar Youns. Crimes arising from internet using. 2004, pp. 363.
3 Refer to appendix 2 (Article 424 UAE Penal Code)

- Disabling property in any way.

The four forms which constitute the physical elements of the destruction crime are almost connected with each other, the destruction may take place on part of the property and the crime is committed, provided that such destruction would render the property unusable or disabled.

The law did not provide for a specific way of destruction, consequently; the crime takes place upon any act that would disable the property, subject of the crime or renders it defective or unusable afterwards.

In order to the destruction crime to be constituted, the property must be owned by someone other than the offender, in case it is owned by the offender, there will be no crime considering the offender as having absolute right to dispose of his property, provided that the ownership of the damaged property is absolute.

Within the scope of incriminating the informatics property destruction, we must distinguish between two types of property:

• First: Corporal property such as the computer and its accessories.

• Second: logical entities, software, and other data which is "incorporeal property".

Based on the above, the law does punish the destruction of the first type of informatics property, which is the corporal property, for example, destroying computers and their accessories such as printers and scanners , as well as all devices attached to the computer, computer screen, camera attached to it, any connections or devices equipped to be used through the computer, i.e. whatever comes within the description of movable corporal matters, all these things are subjected to the protection under Article No (424) of the UAE Penal Code.

The UAE legislator has dealt with the destruction when made to a movable or immovable property owned by a third party, if the damaged item is a Computer, its tools, hardware, devices related to it, disks, CD-ROMs, or other items related to information, there will be no legal obstacle in the application of the traditional provisions concerning destruction crime, considering the subject of the crime a corporal property owned by a third party.

5.2.2 UAE Cyber Law

Upon the issuance of the UAE Cyber law in 2006, as amended by a decree in 2012, a punishment was set for the crime of informational destruction of automated processing

of data system, whether damaged, cancelled, deleted or destroyed. There are several forms that lead to destruction, change or erasure whether the data or information is stored in the computer or software/programs The UAE legislator did not define a specific way for the occurrence of the destruction crime or any of its forms, while it considers it as a crime subsequent to illegal access and did not specify a specific consequence to its occurrence, therefore, it is conceivable that the offender may direct his criminal activities to information software and the crime may occur through direct contact with the device, as it may fall through the remote connection.

5.2.3 Types of Information destruction in the UAE Cyber Law

- **The first article - second paragraph:**

It has been explained in the earlier part of the research concerning illegal access in the UAE Information Technology Crimes Act. In order to avoid repetition, we will summarize Article (2/2)[1] as follows:

Article (2/1)of the UAE Information Technology Crimes Act had set a punishment for the illegal access and similar acts, such as exceeding an authorized access or illegal stay in the electronic despite the fact that, illegal access could be done without criminal intent to do so, such as accidental access or access by mistake, to avoid the consequences of such act of destruction like cancellation of data, erasure or any other impact subsequent to the illegal access, therefore, this paragraph two of the UAE Information Technology Act Crimes had been enacted as the first form of information destruction and is deemed a general legal provision as it did not punish a particular type of criminal act occurring on the data and electronic information such as Article Four concerning Confidential Government Data confidentiality or Article Five, Concerning E- websites.

The punishment of information destruction in the second paragraph of the UAE Information Technology Crimes Act was worse than that of illegal access in the first paragraph and that is due to the destruction resulting of that access.

The law had stressed the punishment in the third paragraph of Article 2 of the previous Act, if the data and information which was destruction d due to that access was personal; this is in order to protect this personal type of data and information.

1 Refer to appendix 1 (Article 2-2 UAE cyber law).

- **Article 4[1] Illegal Access to Obtain Data Affecting National Security:**

The second paragraph of Article four had set a punishment for illegal access, in case access is intended to get access to government data or confidential information if the result of that access is cancellation, change, modification, distortion, damage, copy, destruction, publication or re-publication of data or information.

The punishment shall be imprisonment for not less than five years and a fine not less than AED 500,000 and not exceeding AED 2,000,000.

It is the most severe punishment set in the UAE law, in order to give government data a great deal of protection and in respect for the prestige of the State and to preserve its security from the frivolous hands those using cyberspace to achieve their goals and facilitate commission of many crimes, as explained in the introduction of the research about the types of e-crime and how it is distinguished from the other traditional crimes.

- **Article 5[2]: Illegal Access with a View to Tamper the Electronic Site:**

In this hypothesis the UAE legal system punishes whoever accesses the system illegally if the intention of the offender was to abuse the Website by any of the following ways: changing the design of this site, destruction or modifying the site, occupying the URL.

Physical element (Mens Rea):

By extrapolating the previous text, we find that the physical element of this crime is based on the unlawful access to websites, knowing that, the crime does not arise upon the mere access to the site, yet it must be intended to change its design, modify the content, destroy, cancel or steal the name.

Moral element (Acts Rea):

This crime is one of the intentional crimes, where the law stipulates/ requires mens rea (criminal intention) as it is stipulated that access shall be with the intention to change the design of the site, to modify its content, to destroy or to cancel it.

1 Refer to Appendix 1 (Article 4 UAE cyber law).
2 Refer to Appendix 1 (Article 5 UAE cyber law).

- **Article 7[1] Concerning destruction of medical documents crime:**

Most of States if not all, are keen to mechanize medical documents and the use of the production of the information revolution of hardware and software has become a salient feature in many health institutions whether public or private, however, the United Arab Emirates was not immune from this great development in the field of health services as all health institutions in the United Arab Emirates are now using information technology and have totally dispensed with papers, this also applies to private health institutions which have in turn been keen to take advantage of the information revolution.

From this point and due to the significance of providing legal protection to medical documents stored and traded in the digital world, the UAE legislator has been keen to single out a specific provision criminalizing destruction occurring on medical documents.

In the next papers we will explain Article 7 of the UAE Cyber law, which had criminalized tampering medical files, in details.

Destruction in this context does not denote traditional destruction; yet, it means destruction directed to the logical and moral side in the computer, which has become financially of high value, as destroying the computer software and data means loss of the benefit of this software and data.

Legal provision:

Article 7of the Prevention of Cyber law has provided "Anyone procuring, facilitating or enabling the modification or destruction of medical examination, diagnosis, treatment or health records through the Internet or an information technology device shall be liable to temporary detention or imprisonment." (Article7).

First: the Physical element:

The above provision shows that while incriminating this criminal conduct, the UAE legislator has identified three forms of informational destruction; namely:

1. Destruction which means extermination of these medical documents and destroying it partially or totally.

1 Refer to Appendix 1 (Article 7 UAE cyber law).

2. Amendment, which means making amendments on medical documents whether medical reports, prescriptions or otherwise, by adding some data to or deleting them from the existing data.

3. Change, which means change of the existing data of the medical documents within the system and replacing them with other data.

It is noticeable from the previous provision that the UAE legislator while criminalizing the crime did not specify the entity of which the data processing is a part, but he stipulated that the documents, subject of incrimination shall be medical, whether part of a government or private medical body .

On the third hand, he did not define specific means by which the informational destruction process takes place, which means that the provision extends to include all the technical and technology methods used in the destruction of information, including the use of malicious software such as viruses, information bombs, worms and other programs.

On the fourth hand, we find that the crime takes place as soon as any of the criminal acts had been committed, likewise, the punishment for information destruction was not associated with unauthorized access to the computer system.

Second: The moral element:

As clear from the above context, this crime deemed an intentional crime that is realized upon the availability of the criminal intention. The intended intention here means availability of two factors, knowledge and intention- knowledge of the offender that he is committing one of the acts mentioned in the legal provision and which may destroy medical documents, and that he has intention to do so.

Third: Punishment:

In terms of punishment, we find that the legislator had stressed the punishment of this crime, where this crime is deemed a felony in the description of the penalty of temporary imprisonment, and we notice that no other punishment was mentioned such as fine, this indicates that the law has stressed this punishment, due to the significance of the subject of the crime which are the medical files and the resulting harm if committed.

- **Article (10)[1]:**

We summarize Article 10 in the UAE Cyber law in this paragraph by stating that, due to the high significance of this type of crimes that characterize cybercrime, which is sending and transplanting viruses, the law had assigned a particular Article to criminalize such acts, namely; (Article 10). This article, as above mentioned, addresses whoever transmits viruses and malware via the Internet or any other information technology and such software/programs of all forms may lead, for example, to turn off the network, disable or destroy it, etc.

As mentioned previously, the crime of disseminating viruses and malicious software/programs was met with interest by all legislations worldwide. The UAE Information Technology Crimes Act Article 10/2 has set a punishment for attempting such an act, although the UAE Information Technology Act 2012, which has amended the 2006 law, added an Article concerning "Attempt". This article has defined a punishment for attempting to disseminate viruses and thus it has followed the same steps taken by the new Japanese legislation in 2011, to punish preparation of viruses and malicious software in accordance with Article 168-2[2].

The third paragraph of Article 10: (Spamming e-mail):

Electronic mail (E-mail) is one of the most superior communication methods in contemporary civil societies, which is a messaging style same as regular mail; however, it is faster and more accurate in the interaction between institutions and individuals.

Law No. 5 for the year 2012, amending the UAE Information Technology Crimes Act, has added a new paragraph concerned with e-mails. Today, spamming e-mail is deemed the most traded form of trespassing databases, trespassing in this context is not trespassing the Internet itself, but it is considered a mean of trespassing, it is a dilemma facing e - mails specifically and affecting database in terms of being vanish because of the dumping that occurs, to non-movement ending with refraining from performing the required service.

Spamming in this context takes the form of entry of anonymous mails to the e - mail account of the end recipient, where some software that is specifically designed for that purpose is used. Such software is prohibited because they threaten the database by the expansion of the working databases of e-mails, so that if it becomes full it can no longer

1 Refer to Appendix 1 (Article 10 UAE cyber law).
2 Refer to Appendix 3 (Article 168-2 Japanese penal code).

be opened and dealt with. These mails usually include scandalous topics or promotional materials for fake projects, etc.

In the terminologies of e- mails, the topics of these mails are named junk-bulk-mail. Article 10/3 has set a punishment for e-mail dumping and considered it a criminal act rather than simply illegal behavior, due to the consequent destruction of the internet work mechanism.

The Definition of E-mail Spamming crime:

The word spam means: correspondence of great number of duplicate copies of the same message through corresponding system, whereupon, the information technical system will not proceed steadily[1].

Whoever opens an account online, through the internet provider and then sends a large group of correspondences as if they are sent by e - mail, and then delete or cancel this internet account, in order to avoid being discovered.

5.3 Japan Penal Code and Information Destruction Crime

5.3.1 Article 234-2

Article 233 provides that a person who damages the credit or obstructs the business of another by spreading false rumors or by the use of fraudulent means shall be punished by imprisonment with work for not more than three years or a fine of not more than 500,000 Yen. Article 234 provides that a person who obstructs the business of another by force prescribed under the preceding Article. In present Japan, many people us the computer to conduct their business. It is very important for these people to put computer's function in full use.

Article 234-2 was added by revisions of the Penal Code 1987. Article 234-2 provides that a person who obstructs the business of another by the following three kinds of acts shall be punished by imprisonment with work for not more than five years or a fine of not more than 1,000,000 Yen. (1) Damaging the computer and chine. (2) Damaging the electromagnetic record used by the computer utilized for the business of the other. (3) Inputting false data or giving unauthorized command or by any other means.

These are the two judicial precedents:

1 Hassan Daood. IT Crime. Published by Naïf Arab Academy. 2000, pp. 93.

1. Defendant inputted the operation program for lathe controlled by a computer which is set up in his place of employment. After leaving his place of employment, he deleted the operation program. The lathe controlled by the computer failed to operate. The decision of the Tokyo District court on 26 March 1990 applied Article 234-2 to this case used by the computer.

2. Asahi Broadcasting Company opened the homepage of weather forecast on the internet. The image data of the weather forecast has been recorded and saved in the server computer. Defendant deleted the image of the weather forecast and replaced it with an obscene image. The general public had free access to the homepage with the obscene image. Defendant damaged the electromagnetic record by the act to delete the image of the weather forecast. And he inputted the false data by the act to replace the image of the weather forecast with the obscene image. Defendant caused the computer utilized for the business of the other to operate counter to the purpose of such utilization because he made possible for the general public to look at the obscene image. Decision of the Osaka District Court on October 3, 1997 applied the Article 234-2 to this case.

5.3.2 Article 168-2

How to deal with a computer virus is the important problem in the computer age. The cyber treaty recommends making provisions to punish the use of viruses. The Penal Code of 2011 added chapter 19-2 which punishes the act relating to computer viruses. Chapter 19-2 consists of Article 168-2 and 168-3.

We call the electromagnetic record prescribed in Article 168-2 by the name of computer virus. Electromagnetic record by virus was punished by Article 258 (Damaging of Documents for Private Use). A person damages the electromagnetic record. If this act results in an obstruction of business, a person is punished by Article 234-2.

The following case occurred before 2011. Defendant used a file sharing software which was infected with a virus. This software looked like music software. A person (X) believed this software was music software. He (X) accessed this software which was infected with a virus. Computer data stored in X's hard disk was damaged by accessing the software. Stored data was not related to rights and duties. Tokyo District Court on 20 July 2011 applied Article 261 (Damage to property) to this case. Function

of the hardware was paralyzed by the virus. Article 261 punishes a person who damages or injures property except documents (Article 258, 259) and building or vessel (Article 260) by imprisonment with work for not more than three years, or a fine of not more than 300,000 Yen or a petty fine.

- The person who makes a following electromagnetic record without due authorization shall be punished by Article 168-2:

1. Electromagnetic record which interferes with the operation of another computer or causes another computer to operate counter to the purpose of utilization.
2. Except the electromagnetic record prescribed in the preceding clause, the electromagnetic record or other record which gives an unauthorized command prescribed in clause 1.

   The person who obtains or possesses the electromagnetic record prescribed in article 168-2 paragraph 1 shall be punished by Article 168-3.

5.4 Summary

Japan added, in its Penal Code, new legal texts in order to incriminate and punishes acts of informational destruction, like Article 234-2,258,259 and Article 168-2 concerning malicious software, like viruses. UAE also incriminates and punishes crimes of informational destruction through enactment of the Information Technology Crimes Act and the many articles it contains. For example in article 258 of Japanese penal code which punishes the destruction of official electromagnetic records, this article is the same as articles 2-2 and article 4 in UAE Cyber Law.

Most of these were results of unauthorized access, with the exception of the destruction of an electronic document (Article 7).

Crime of transmitting malicious software like viruses is one of the most common Information Technology crimes; hence most of the international laws have incriminated and punished this type of crime due to damage produced by them. Both the UAE and the Japanese laws specified legal texts to incriminate not only acts of doing so, but even the intent to do so, like mere preparation for a crime.

In Japanese law, it is punishable to destroy some or whole functions of computers, damaging electromagnetic records, or causing obstruction of others' business. Creating a computer virus is considered an activity to prepare, plot or induce any of the activities

described above. In contrast, creating a computer virus is not subject to punishment in the UAE's law.

CHAPTER 6

ELECTRONIC FRAUD

CHAPTER 6

6.1 Introduction

Before embarking on explaining methods of informational fraud and means of penalties stated in the UAE Cyber law and Japan Penal Code, we would like to account the following incident which took place in Dubai, UAE, before the enactment of the UAE Information Technology Crimes Act of the year 2006, where a conference, with international participation, on information security was convened. This conference witnessed a real trial to one of renowned internet hackers. The wisdom behind narrating this incident is to reach the conclusion that internet networks may be used to commit a lot of crimes on money, with disastrous consequences.

This case[1] starts when a major contracting company (X) bids for a huge tender; and when the competing company (Y) heard of the bid it approached and hired one of the famous hackers, Felix Linder, 26 years. The latter was able to penetrate the competing company's (X) website and access its files. He was able to access the special file that contains the tender via penetrating the personal computer of the company's network systems engineer. So the competing company (Y was able to submit a bid slightly less than that of (X) and so wins the massive contract of 20 million US dollars. This process (mockery) was witnessed by a large crowd of observers from the judiciary, information security experts and UAE, Arab and international media. Thereafter, company (X), by a decision of the Board of Directors, resorted to the police which moved to the scene of the crime. The police confirmed the crime, and was able to follow the hacker's trace by using modern technology methods. The case was referred to the judiciary, and the hacker (pirate) has been punished in accordance with the laws applicable in these countries and USA. The hearing was witnessed by judges from the UAE, Egypt and the USA. A simulation trial took place as per applicable laws of these countries. The court has witnessed thorough discussions centered on whether robbery of information is a complete crime, as it has caused material loss to the affected company (X), despite absence of tangible evidence. After the investigations were completed the US judge convicted the accused of the crime attributed to him in accordance to the US Criminal Code; whereas the UAE's judge acquitted him on the grounds that the current UAE laws do not incriminate this act.

1 Dr. Mohammed Alkappe. The Criminal Protection to E-Trade: A Comparative Study. University of Cairo, Egypt. 2009, pp. 336-340.

Fraud crimes are listed under the category (crimes against money); fraud can be defined as seizure of movable money owned by others through deceiving a victim and then extracts it. Article 399 Of the UAE Penal Code punishes fraud crimes; we will explain fraud crime stated in the UAE Penal Code in comparison with the UAE Information Technology Crimes Act of 2006 and its amendment of 2012.

6.2 Fraud Crime as Stated in the UAE Penal Code

6.2.1 Article 399 of the UAE Penal Code

- Article 399 of the UAE Penal Code, fraud crime consists of three elements:

Subject of the Crime:

It is movable money or bond or signing of this bond; that this money is of material nature and has value. As this should be movable, there will be no fraud against property.

Physical Element:

Money fraud is of the crimes that have results; hence its material element consists of three factors:

A. Criminal behavior: using any of fraud means stipulated by law, for example:

1. Use of fraudulent methods:

Use of fraudulent methods is defined as false allegations supported, on the part of the offender, by external manifestations to convince the victim of something stipulated by the law. To materialize, fraudulent methods should satisfy three conditions:

- Involve a false claim.
- Offender supports this claim with external manifestations.

2. Result of this allegation convinces the victim of something stipulated by the law. Disposition of money not owned by the offender who has no right to dispose of.

3. Claims a false name or incorrect recipe.

To use any of these methods, it is required that this act would result in deceiving the victim and convince him to deliver the movable money or bond or signing of this bond or its cancelation, destruction or modification.

B. Criminal result: Victim delivers his money to the offender.

C. Causality: that links between conduct and result/outcome.

Moral element:

1. Awareness: the offender is aware of all constituent elements of the crime; that his conduct id deceivable.
2. Volition: the offender's intention focuses on the physical aspects of the criminal incident, i.e. fraud and acquisition of money owned by others; fraud crime is a temporary crime which starts and ends when the acquisition act is completed using fraudulent methods and the offender focuses on the acquisition of the victim's money.

6.2.2 Fraud Crime as Stated in the UAE Cyber Law

Article 11[1] of the UAE Information Technology Crimes Act penalizes deceit via various means of information technology. It is noticed that this Article is a repetition of Article 399[2] of the Penal Code; however it sets the means by which crime is committed. These are: information network or an electronic information system or any of the means of information technology. The law also requires that this act is unlawful. The law is silent on acts of deceiving the victim and does not require delivering money to the offender, as this is in line with fraud by modern means of technology. Article 12 of the amended law of 2012 added utility theft or service utilization on which the old law of 2006 was silent.

Application of a fraud case:

This crime was committed in June, 2006 in Dubai. The Public Prosecutor presented two defendants to trial, the first of its kind in the UAE history; in accordance with this law defendants were convicted. The Dubai Public Prosecution accused the first defendant on the grounds that he was able to seize movable money (five travel tickets) by manipulating the information network of a travel and tourism agency based in Dubai by using deceitful means. This defendant has assumed a fake character and accessed the company's website by using the PIN Number and user name concerning the second defendant, also a company employee. So the company has been a victim of deceitful action by which travel tickets were issued. The prosecutor accused the second defendant of participating by agreement and support of the first defendant in committing the above crime. So the crime has been committed in accordance to that agreement and assistance.

1 Refer to Appendix 1 (Article 11/12 UAE cyber law).
2 Refer to Appendix 2 (Article 399 UAE penal code).

The defendant was also accused of disclosing professional secrets, being a ticket sales agent (PIN Number and user name), and manipulated this to his own benefits and that of the first defendant without permission of the concerned person.

The court convicted and accused them under of the Articles (1, 10, 23 and 25) [1] of the UAE cyber law and Article 379 of the Penal Code; and ruled that the first offender shall be punished by imprisonment of two months with deportation. The second defendant was imprisoned for one year with deportation.

Examples of fraud crimes committed via the internet[2].

1. Auction deceiving via the internet:

Since what is available through the internet is not originals that can be read and obtained once the bid is settled, they are only copies of the original. Such state of affairs increases incidents of online fraud and deceit. According to statistics released by the Federal Commerce Commission and Monitoring Committee on Online Fraud this crime is one of the most prevalent in the cyberspace.

2. Private brokerage system:

As there are no adequate guarantees for such types of business it is necessary, therefore, to try to legitimize this kind of business so that there will be no victims, because of its prevalence in the virtual world.

3. Stealing Identity possessions:

Deceptive sites will be displayed through which a hacker can obtain these credit cards numbers and other personal cards, like social insurance cards. The victim starts accessing these deceptive sites and expresses his desire to subscribe using his credit card, and hence falls into a network scam. Or, the victim fills a form which contains details of his identity; this identity will then be used to deceit others hence elements of the crime of identity fraud exists. A hacker was able to obtain names and numbers of social insurance of many US military personnel and used them to deceit one of the US Banks[3].

1 Refer to Appendix 4.
2 Mohamed Chawki. A critical look at the regulation of cybercrime In: cyber crimes and law: an overview (Amicus Books), 2007, pp. 134 – 179.
3 Dr. Mohamed Said. Criminal responsible of E-Card Forgery. 2012, pp. 3-8. Dar Alnahada.

4. Fraud through identity theft:

This type of fraud is among the highest online crime rates, where a fraudster intentionally obtains economic gains through possession, or transfer or use of identity documents of other persons.

6.2.3 Credit Cards Crimes

A credit card is the device that allows its holder to take necessary and direct measures to deduct an amount of money, allotted to another person, from his account at the bank which issues this credit card*; in other words, it is a payment tool that plays the role of cash money and checks in everyday transactions. This credit card contains:

The name of the issuer, its logo, number, holder's name, his signature, account number and validity and expiry dates.

The UAE Penal Code does not contain legal texts on credit cards, hence the main reference in this respect are the general rules specified in the Penal Code.

In recent years credit cards theft crimes had proliferated. There are two major methods for such crimes; firstly the possibility of stealing the credit card and the possibility of being used by the fraudulent. It is easy to control this type of fraud by directly notifying the concerned bank of the theft or loss. The second method of accessing the account requires using some other sophisticated techniques, since the card in question is not available to the hacker[1] (i.e. to order via the telephone or the internet), or having the card and processing it through a special scanner and get hold of the account (i.e. to identify personal information and identity theft). Thus, the hacker obtains all information pertaining to the bank card or credit card.

The UAE Information Technology Crimes Act provides for protection of electronic cards since they have become important tools for online payment during shopping and purchasing activities. This state of affairs makes these cards more accessible and hence an easy target to theft from other parties, and to be used unlawfully.

Article 12 of the UAE Information Technology Crimes Act penalizes crimes against credit cards; in fact the legislator extends this umbrella to cover all types of credit cards. Article 12, on the other hand, is a repetition of Article 11 of the same Act of 2006 which has been amended in 2012; the following were added to the text:

1 Dr. Jamil Alsageer. Criminal protect to E-Card.1999, pp.10. Dar Alnahda, Cairo.

- The use of an electronic information system as a tool to access the electronic card, etc.
- Numbers of any bank accounts, information or any of electronic payment methods.
- A phrase will be added to any publication or re-publication of information or numbers concerning those cards as informational fraud is in continuous progress – it is believed that e- hackers can easily manipulate the cyberspace in order to commit more crimes.

Article 12 is divided into four paragraphs:

Paragraph 1: To use information technology techniques to illegally access credit cards' numbers or information or any other card. In this paragraph three elements of the crime are realized:

Place where the crime is committed: Numbers or information of a credit card, or any card for that matter. As credit cards are materialized in numbers inscribed on them, information concerning their owners and the issuing entity, these numbers and information are therefore considered as material elements of the crime.

Physical element: this is realized through using the information network or any of the information technology systems to unlawfully access numbers or information of a credit card, or any of the other e-cards.

Protection in this context focuses on the numbers or information of these credit cards in case they were illegally accessed, even if they were not used.

Paragraph 2: The law, in Paragraph 2 of Article 12 of this Act, emphasizes on the act of intent, on the part of the hacker, for obtaining numbers and information of the credit card or any special information on the bank account of the victim in order to get hold of other people's money, or benefit from any of the services available.

Credit cards owners may misuse or illegally use their own cards as when they were expired, cancelled, exceeding the equivalent balance. It is important to state that such cases do not constitute a crime, and they are not subjected to criminal penalty[1].

Article 12, paragraph 1, penalizes the mere attempt even if the offender is not able to get hold of others' money. The philosophy or lesson behind this is not to confine to the mere attempt, but to cover any action that enables the offender to get hold on other peoples' money or to benefit from services provided by a credit card. This action, in

1 Dr. Hussin Algindee. The criminal politics on facing with cybercrime. 2009, pp. 160. Dar Alnahda Alarabia.

other words, represents the road that leads to acquire this money or to get benefits from services provided.

Penalties specified in Paragraph 2 of Article 12:

Imprisonment for a period of not less than 6 months and a fine; it is in fact a tough punishment compared with that stated in paragraph 1 of Article 12 because of the special criminal intent (if the intent of using data and information to get hold of other peoples' money).

Paragraph 3: The offender was able to seize for his benefit or the benefit of others unlawful money via using the electronic card. Paragraph 3 of Article 12 concerning the offender ability to seize for his benefit or the benefit of others unlawful money by using an electronic card or any similar method shall be punished by a not less than one year imprisonment and a fine.

Paragraph 3 represents the criminal result of theft via an electronic card or other electronic methods, so it imposes heavy penalties on offenders: a minimum of one year imprisonment and a fine of not less than 200,000 DH and not more than 1,000,000 DH.

Paragraph 4: This paragraph has appeared in the amendment of the UAE Information Technology Crimes Act; it penalizes publishing or re-publishing numbers or information concerning an e- credit or credit card or any other means of electronic payments.

Although only six years have passed since the enactment of the UAE Information Technology Crimes Act of the year 2006, and in view of the ever increasing and sophistication of online crimes, we are in urgent need to develop and update our laws.

6.3 Fraud in Japan Penal Code

6.3.1 Article 246-2

Article 235 is a provision of theft. Article 235 provides that a person who steals the property of another commits the crime of theft and shall be punished by imprisonment with work for not more than ten years or a fine of not more than 500,000 Yen. The meaning of the word provided in Article 235 is restricted to the corporeal property. According to this opinion, information with economic value is not property provided in Article 235.

Another example relating to Article 235 is that a person makes false subway tickets with electromagnetic record and passes through the automatic gate by using it. He

obtained the profit worth of the fare. The act to steal a profit is not punishable by Article 235.

Article 246: paragraph 1. A person who defrauds another of property shall be punished by imprisonment with work for not more than ten years.

Paragraph 2. The same shall apply to a person who obtains or causes another to obtain a profit by the means prescribed under the preceding paragraph.

Fraud is a crime to deceive a person. The person who passes through an automatic gate by using false electromagnetic ticket shall not be punished by Article 246 Paragraph 2.

6.3.2 Article 246-2 (Amended 1987)

Article 246-2 was added by revision of Penal Code 1987. Two kinds of acts are provided in Article 246-2. (1) The act to create false electromagnetic record relating to acquisition, loss or alteration of property rights by inputting false data or giving unauthorized command to a computer. (2) The act to put a false electromagnetic record relating to acquisition loss or alteration of property rights into use for the administration of the matters of another. In addition to the provisions of Article 246, a person obtains or causes another to obtain a profit by the act (1) or (2) shall be punished by imprisonment with work for not more than ten years.

Creditor A lent chief B of credit cooperative a large amount of money. A asks B for payment of his debt. B ordered a member of staff to transfer 46 million Yen to A's bank account by computerized processing when in fact anyone did not request to transfer 46 million yen from credit cooperation account to A's bank account. B used a staff member as a tool to create a false electromagnetic record to acquisition property rights. The court of first instance on this case decided that B should be punished by Article 247 (breach of trust). But court of second instance (decision of Tokyo High Court 29 June, 1993) decided that B should be punished by Article 246-2 Transfer of money by B is a mere sham without reality. The following example belongs to act 2 of Article 246-2 mentioned above. Defendant inserted the altered telephone card into public telephone to hear the program of surcharges telephone information service. He obtained profit by Imputing false telephone card into public telephone. He shall be punished by Article 246-2.

6.4 Summary

UAE side:

Article 399 of the UAE Penal Code punishes acts of fraud; it also specifies ways and means of fraud. By the enactment of the UAE Information Technology Fraud Act states that fraud acts committed via the internet and other technologies shall be punished by Article 11, which is a repetition of Article 399 of the UAE Penal Code; however it specifies the means through which the crime is committed.

Japanese side:

Article 246 of Japan Penal Code punishes acts of fraud. An amendment of Article 246 has been enacted by adding Article 246-1 in order to punish acts of fraud via information technology techniques, like for instance creation of an electromagnetic record, etc.

Each of the UAE and Japan laws punish crimes by electronic credit card by enacting Article 163-1 (Japan Penal Code) and Article 12 of the UAE Penal Code. According to these Articles, any person who issues without authorization any electronic record shall be punished.

Both of the UAE and Japan laws punish acts of frauds committed through addition of amendments of the Penal Code (Japan Penal Code); with the continuous need for amendments where Chapter 18 Section 2 (concerning unauthorized issuance for electronic payment cards) was added to the Penal Code of the year 2001, as a necessary need to follow up this type of crimes. Amendments of the year 2012 on the UAE Information Technology Crimes Act follow the same pattern.

In Article 246-2 of the Japanese penal code, it is clearly indicated that a person who obtains a profit by creating a false electromagnetic record or inputting false data to a computer shall be punished. In the current UAE law, fraudulent activities to obtain personal estate or profit by using the internet or information technology are subject to punishment. This might include the activities conducted to obtain personal property by deceiving others with false information spread by criminal intent through the internet.

CHAPTER 7

ELECTRONIC FORGERY

CHAPTER 7

7.1 Introduction

Most of legislations enacted a punishment for forgery of documents due to damage resulted from such acts. With improvement of technology all over the world financial transactions have been shifted from direct delivery of cash to the most recent modern means such as credit cards, while official and nonofficial transaction have gradually abandoned physical documents and have depended upon the information been provided through information technology.

In this chapter; we shall discuss informational forgery in each of the UAE and Japanese laws. In Section 1 we shall tackle the UAE law and how the UAE legislator has punishes electronic data forgers. In Section 2 we will look into the Japanese law and shed some light on both types of forgery, i.e. the conventional and the electronic and how the Japanese law covered the legal gap and enacted legal provisions that punish informational forgery.

7.2 Electronic Forgery in the UAE Cyber Law

7.2.1 Forgery in the UAE Penal Code

Chapter 5 of the UAE Penal Code of the year 1987 has devoted the first and second sections thereof for punishment of forgery under Articles from (211 - 223). We shall focus on section 2 of Chapter 5 which relates to forgery of documents.

Forgery as per the Article (216)1 of the Penal Code is the amendment of the actual wording or similar marks, symbols, stamps or signatures. Forgery of documents is the change of actual truth in any document by any of the methods provided for in the Law in a manner that would cause damage. The same is accompanied by usage of the said forged document for the purpose for which it has been prepared. Methods of physical forgery have been stated in Article (216):

Forgery of an instrument is a change of its genuineness by any of the means stated hereinafter, resulting in damage, for the purpose of using it as a valid instrument.

The following are considered means of forgery:

1. Introducing a change into an existing instrument by addition, deletion or alteration, whether in writing, numbers, marks, or in photographs appearing therein.

1 Refer to Appendix 1 (Articles 216 to 222)

2. Putting a forged signature or seal, or alteration of a true signature, seal, or thumb-print.
3. Obtaining, by means of surprise or fraud, a signature, seal or thumb-print of a person without his knowing the contents of the instrument or without validly giving consent thereto.
4. Fabricating or counterfeiting an instrument and attributing it to a third party.
5. Blank filling of a signed, sealed or thumb-printed paper without the consent of the person who signed, sealed or thumb-printed it.
6. Disguising or substituting the identity of a person in an instrument made to verify its truth.
7. Alteration of truth in an instrument made for verifying its contents.

While punishment specified for forgery of official document has been stated in Article (217) whereas such forgery has been deemed as a crime. As we have mentioned above the punishment of a crime under the UAE Penal Code is imprisonment for a period of (3 years and not more than 15 years). Article 218 differentiates between official and nonofficial document in accordance with the person who issues it or interferes in the issuance thereof, where the document shall be regarded as an official document if been issued by a public employee (Governmental).

The legislator has further differentiated between document forgery and the usage of the forged one, Article (222) of the UAE Penal Code where each of them is considered as a separate independent crime, and a separate punishment for each of them is stated where the committing party of both crimes might be the same i.e. the same person has forged the document and has used it for the purpose for which it has been prepared. The forgery may be made by a person and the forged document been used by another. The forged document might be an official document or a conventional one whereas the legislator has differentiated the punishment of each one thereof and has specified a severer punishment for the forgery of official document, as the forgery thereof causes significant damage to the community where it affects confidence on official papers.

7.2.2 Article 6 UAE Cyber Law

Article (6)[1] of the Law no (5) of 2012 on Combating IT Crimes has provided for punishment of fraud of e-document and whereas the e-document is a recent term in the field of law; the law has defined the e-document in Article 1. An e-document like other documents could be forged or that its contents may be changed. Forgery of e-documents could be done by any of the methods set forth in Article 261 of the Penal Code by, as we have stated above, amendment of actual truth stated in the said document or forgery of the information by replacing the actual information with other information, manipulating and replacement of factors or destroying of some of the data stated in the document. The language[2] in which a document is written doesn't matter whether Arabic or any other foreign language, or any symbols or signs of special indications.

Pursuant to Article 6 of the UAE IT Act combating cybercrimes e-documents consist of the following: Documents related to the Federal Government and public Federal and Local bodies or institutions provided that the said document has been legally recognized in any informational system i.e. in any software or tools been prepared for processing and management of data, information and e-messages.

The other type of the documents is any other documents regardless of the origin, storage, extraction, copying or sending thereof, etc. The same differentiation has been used by the legislator while differentiating between official and conventional documents in Article 218 of the UAE penal code.

Paragraph 3 of Article 6:

The Law has prescribed the same punishment stated for a forgery crime for the usage of the said forged document, as the case might be. And has further stipulated that the offender should be aware of the fact that the document he is using is a forged one. Using of a forged document is by presenting it and arguing based thereof on the purpose for which it has been forged as if it is a valid one.

Despite the fact that Article 6 of the UAE IT Crimes Act combating cybercrimes is amended by the law no (2) of the year 2006 is a mere repetition of Article (4) we could notice two differences between these articles:

1 Refer to Appendix 1 (Article 6 UAE cyber law).
2 Dr. Abd Alfatah Hijazi. The internet and computer crime in Arabic legislation. 2001, pp. 30-33.

Type of punishment:

Punishment for forgery of an official document (Governmental):

The new law has added monetary fine in case that forgery has been committed on a Governmental e-document (150,000 minimally and 750,000 maximally) while the previous law has contented, as per Article (4) of the amended law with temporary imprisonment i.e. Article (6) of the new law has added further restrictions in order to secure more protection to an official e-document.

Lack of requirement of damage due to forgery:

The law does not stipulated any specific result such as occurrence of damage due to the said forgery in contrast to the Phrase 2 of Article (4) of the previous law which provides that a crime shall not exist unless the said forgery has led to damage. However, the said law has not specified methods of informational forgery where such forgery could be made by the same methods set forth in Article (216) of the Federal Penal Code i.e. the law has equaled the conventional forgery to informational forgery.

Practical case on Electronic Forgery[1]:

The accused (S) has committed forgery of two official documents "Ownership Certificate & House Plan" attributed to be issued by Abu Dhabi Municipality through deletion and addition where he has accessed the informational system of the said Department and has amended both of the documents loaded in the computer of Abu Dhabi Municipality.

A good faith public employee has assisted him where he has submitted the said forged document to the employee and the later has accordingly extracted the house plans.

He has unlawfully accessed the Abu Dhabi Municipality's information system pertaining to amendment of the data of the public housing residences through usage of the user name and password of the competent employee where he has then amended the data of the aforesaid house.

The Public Prosecution has requested the court to punish him under the provisions of Articles 2, 2.1, 3, 4 and 3.1 of the Federal Law on combating IT Crimes.

1 Dr. Hussen Al Wahaybi. Legislation related cybercrime in Oman, UAE and Qatar. (ISQO) 2010, pp. 56.

The court has decided to punish the accused by 3 years imprisonment and deportation from the UAE.

7.2.3 Forgery of Electronic Card

Credit cards are one of the e-payment means, which has been widely spread all over the world where it has become one of the banking services provided by hundreds of thousands of banks to earn huge profits out of the same while hundreds of millions of individuals use them to purchase their commodities and services and to withdraw cash amounts thereby without the need to carry cash money. Credit cards represent an easy mean to obtain short term credit for the holders thereof. Furthermore, millions of the economic institutions around the world accept selling and provision of services under the said cards, which has led to the increase of their sales while guaranteeing obtainment of their rights from the issuer of the said card. Despite the fact that; using of the said cards has commenced at the beginning of the Gregorian twentieth century (1904) in a simple manner in the form of a direct relationship between the seller and the holder of the card, as it has been used at the local level, however, it has been developed during a three successive phases to reach the status thereof today with international organizations to sponsor the card and banks have also started to deal thereby as of 1951[1].

Article 12[2] of the UAE Cyber Law has provided for punishment for informational fraud crimes i.e. the crimes related to e-card, the credit card or any other e-payment means. In this research pertaining to informational forgery, we shall explain another subject related to forgery of the e-card where Article (13) of the UAE IT Crimes Law of 2012m has provided for a punishment for forgery, imitation or copying of any credit or civil card or any of the e-payment means when the informational technology was the mean used in such forgery or imitation.

Crimes of cards forgery and the using thereof, whether in withdrawing or fulfillment of any obligation, have become one of the most crimes that attract focus and generate debate due to their negative repercussions which may too difficult to control sometimes..

Some resources confirm seriousness of cards' forgery crimes when compared with the forgery of bank-notes and checks; where imitation of bank-notes and checks shall have a limited impact that could easily be controlled while forgery of credit cards and

1 Dr. Mohamed Said. Criminal responsible of E-Card Forgery. 2012. pp. 7. Dar Alnahada.
2 Refer to Appendix 1 (Article 12 and 13 UAE cyber law).

the usage thereof all over the world shall actually constitute a cancerous threat that would affect the holder of the forged or imitated card anywhere in the world[1]. Due to awareness by many countries of the seriousness of local and global economic impacts resulted from forgery and using of cards by the forger or third parties the said countries have enacted legislations that organize such crimes (Cards' Crimes), which has been described to be "The next era's crime". We do not exaggerate if we do describe it to be banks' robbery crime –without weapons[2].

It worth to be mentioned here, that cards' forgery crime is a two-perspective crime: one thereof is physical while the other is informational where it includes conventional physical part i.e. focus on the body of the card as well as the obvious data mentioned thereon, and an informational part i.e. the information and data related to the card, the customer, the pin code, the bank account, the insurance coverage and other information and data whether on the magnetic strip – for cards with magnetic strips – or in the e-circuits – for cards with e-circuits or memory.

Article 13[3] of the UAE Cyber Law of (2012) consists of two clauses:

- Punishes forgery, imitation or copying of this type of cards. Article (13) has stipulated that, the said forgery should be done by any of the IT means.
- Provides the same punishment for:

Whoever fabricates or designs technology mean with the purpose to facilitate forgery, imitation or any other acts as per first clause of Article (13).

Using of the e-card to obtain third parties' funds or to benefit from the services it provides. This phrase is of Article (12) that relates to e-card and stealing of third parties' funds and benefiting from the services it provides has been clearly shown in the third clause of Article (13):

(… if he could due to the same; steal funds owned by third parties for himself or for a third party, he shall be punished by, etc.).

Whoever accepts to deal under such forged or imitated e-cards while knowing the illegality thereof, it is similar to Article 222[4] of the UAE Penal Code where the law provides for punishment for using of a forged document and stipulates knowledge by the offender of the fact that; the document he uses is a forged one, etc.

1 Dr. Jamil Alsageer. Criminal protect to E-Card. 1999, pp.10. Dar Alnahda, Cairo.
2 Dr. Riyahd Fatahallah. Forgery of plastic currency-The crime of the future. pp. 2.
3 Refer to Appendix 1 (Article 13 UAE cyber law).
4 Refer to Appendix 2 (Article 222 UAE penal code).

7.3 Japan Penal Code

Article 7-2 provides that the term "electromagnetic record" is used in this code shall mean any record which is produced by electronic, magnetic or other means unrecognizable by natural perceptive functions and is used for data-processing by computer.

Partial amendments of Article 157 paragraph 1, 258 and 259 were made by above revision of penal code. These partially amended Articles are also related to electromagnetic record.

Penal Code provides following 9 Articles in Chapter 19. (1) Counterfeit of Imperial or State Documents (154). (2) Counterfeit of Official Documents (155). (3) Creating false official documents (156). (4) False entries in the original of notarized deeds (157). (5) Uttering of counterfeit official documents (158). (6) Counterfeiting of private (159). (7) Falsifying medical certificates (160). (8) Uttering of counterfeit private documents (161). (9) Unauthorized creation of Electromagnetic records (161-2). Eight Articles from 154 to 161 are the provisions relating to "document". Document is created in written form by using letters or other things. A person expresses or states the will or intention by document or states his will or intention by document (30/7/1910) Supreme Court decision. A document has to visible .And readable and author has to be identifiable in it. Electromagnetic record cannot be regarded as a document.

7.3.1 Types of forgery in Japan panel code

- *Article 157 paragraph 1 of the Penal Code*:

The automobile registrations file case. The problem of this case is related to Art. 157 paragraph 1. Before the revision of Penal Code 1987, Article 157 paragraph 1 provided that a person, who makes a false statement before a public officer and thereby cases the official to make a false entry in the original of a notarized deed relating to rights or duties shall be punished by imprisonment with work for not more than five years or a fine of not more than 1000 yen.

The owner (x) of automobile has to fill out an application for registration of his car and submit it to the official in charge at the Transportation Ministry. The owner (x) did not have parking place for his car. Car dealer (defendant) used another person's name instead of (x) in order to receive (x's) parking certification. Chief of police issued the parking certification. Car dealer (defendant) submitted it to the official in charge at the

Transportation Ministry. The officer accepted the parking certification as true and he registered it on the script with electromagnetic record. This case occurred in 1971. At that time the registration file of an automobile was already made with electromagnetic record.

The problem was whether an automobile registration file could be regarded as the original notarized deed as automobile registration can be regarded as document; the defendant is punishable by Article 157 paragraph 1. Electromagnetic record as automobile registration file can be easily converted into a document. But an electromagnetic record, which is not visible or readable, cannot easily be regarded as a document. Supreme Court (Decision of the Supreme Court on November 24, 1983) decided that an automobile registration file could be regarded as "the original of notarized deed" in Article 157 paragraph 1 of the Penal Code without stating any reason.

Partial Amendment was made to Article 157 paragraph 1 of Penal Code in 1987.

The following sentence was added to Article 157 paragraph 1:

"To create a false record on electromagnetic record to be used as the original notarized deed relating to rights or duties".

- *Article 159 Paragraph 1:*

There is a judicial precedent on counterfeiting of private documents. Article 159 paragraph 1 provides that a person who, for the purpose of uttering, counterfeits, with the use of a seal or signature if another, a document or a drawing relating to right , duties or certification of facts shall be punished by imprisonment with work for not less than 3 months but not more than five years. Defendant x got in a stealthy way a depositor's bank account number and ID. X made a false cash card by inputting bank account numbers and ID on the magnetic part of the card. The bank company's name and depositor's name have been already imprinted on the card. Osaka District Court decided in 1952 that electromagnetic record in this case was included in document ruled in Article 159 paragraph 1.

- *Article 161-2:*

Unauthorized creation of Electromagnetic Records (161-2) was added to Penal Code of 1987. The following provision is introduced as Article 161-2 into Penal Code of 1987.

Article 162-2 Paragraph 1*:*

A person who, with the intent to bring about improper administration of the matters of another person, unlawfully creates an electromagnetic record which is to use in such improper administration and is related to rights, duties or certification of facts shall be punished by imprisonment with work for more than five years, fine not more than 500,000Yen.

Article 161-2 Paragraph 2:

When the crime prescribed under preceding paragraph is committed in relation to an electromagnetic record to be created by a public office or a public officer, the offender shall be punished by imprisonment with work for not more than ten years or a fine of not more than 1,000,000 Yen.

(1) The defendant stole a cash card of another with intent to make a copy of electromagnetic record of that card. He made a card on which he inputted the copy of the electromagnetic record. This case occurred after the revision of the Penal Code 1987. The decision of the Tokyo District court on March 2, 1989 applied Article 161-2 paragraph 1 to this case.

(2). *Article 155* paragraph 1. A person who, for purpose of uttering, counterfeit with the seal or signature of a public office or public officer, a document or drawing to be made by public officer or a public officer shall be punished by imprisonment with work for not less than one year but not more than ten years.

Article 156 . A public officer who, in connection with official duty, makes a false official document or drawing, for the purpose of uttering, shall be punished by the same manner as prescribed for in the preceding Article, but there is not a provision in penal code to punish the Act to make false documents

Article 161-2 paragraph 1 provides that a person who unlawfully creates an electromagnetic record shall be punished. This Article is the provision relating to a private electromagnetic record. Article 161-2 paragraph 2 provides that a person who unlawfully creates an electromagnetic record to be made by public office or public officer shall be punished. A person who, in connection with his duty or business, creates a false official or private electromagnetic record shall be punished by Article 161-2. For example, a bank clerk who is trusted in financial affairs of a bank makes a false data relating receipt of money or money transfer for a professional reason with an electromagnetic record shall be punished by Article 161-2 paragraph 1.

7.3.2 Forgery of E-card.

- *Article 163-2:*

Articles in chapter 18 of the penal code are special laws of document forgery. Article 162 Paragraph 1. A person who, for the purpose of uttering, counterfeits or alters a public bond, securities of a government agency, share certificate of a corporation or other securities shall be punished by imprisonment with work for not less than 3 months but not more than 10 years.

Paragraph 2: The same shall apply to a person who, for the purpose of uttering, makes a false entry in a security. Decision of the Supreme Court on 25 July 1957 decided that securities which fulfill the following two conditions are the securities provided in Article 162 paragraph 1. One condition is that property rights must be shown on the face of the bond. Second is that it's necessary for user to occupy the bond when he exercises the right.

Defendant altered the number of unit's available on the prepaid telephone cards. Art. 161-2 can be applied to this case. But there was a controversy whether Article 162 can be applied to this case. If the prepaid telephone card is securities, Article 162 is applied to the act of the defendant. But the number of units of card is imputed with electromagnetic record. The electromagnetic record of the number of units is not visible.

Statutory penalty of counterfeiting of securities is heavier than that of Article 161-2. If the defendant act to make false record of telephone card comes under Article 162, he shall be punished by Article 162.

Decision of the Supreme Court on 4 May 1991 decided that the defendant should be punished by Article 162. Supreme Court decision admitted that the telephone card with electromagnetic record was included into securities in Article 162. (2) Article 161-2 punishes the act to create unlawfully in electromagnetic record related to rights, duties or certification of facts. Article 163-2 paragraph 1 punishes a person who creates without due authorization an electromagnetic record which is encoded in a credit card or other cards for payment of charges for goods and services and of a card for withdrawal of money. Article 163-2 is a special provision of Article 161-2. Using payment cards such as a credit card has spread rapidly. A payment card has a function equivalent to cash or securities in the present society. Chapter 18-2 (Unauthorized creation of electromagnetic records of payment cards) was added to Penal Coded 2001 in order to

deal with a crime such as forgery of payment card. (3) There are four articles in chapter 18-2:

A person who for purpose of bringing about improper administration of the financial affairs of another person, creates without due authorization on electromagnetic record which is encoded in a credit card or other cards for the payment of charges for goods or services shall be punished by imprisonment for not more than ten years or a fine of not more than 1,000,000 Yen. (Article 163-2 paragraph 1).

A person, who puts an unlawfully created electromagnetic record prescribed for in the preceding paragraph into for administration of the financial affairs of another person, shall be dealt with in the same way prescribed in the same paragraph. (163-2 paragraph 2).

A person who, for the purpose prescribed for in paragraph 1, transfers, lends or imports a card encoded with an unlawful electromagnetic record for in the same paragraph shall be dealt with the same way prescribed in the same paragraph (163-2 paragraph 3).

Article 163-3. A person who, for the purpose prescribed for in 163-2 paragraph 1, passes a card encoded with an unlawful electromagnetic record shall be punished by imprisonment with work for not more than five years or a fine not more than 500,000 Yen.

Article 163-4. A person who, for the purpose of use in for the commission of a criminal act prescribed in 163-2 paragraph 1, obtains information for the electromagnetic record, provides information knowingly the purpose of the obtainer (paragraph 1) stores the information for electromagnetic record (paragraph 2) shall be punished by imprisonment with work for not more than three years or a fine of not more than 500,000 Yen.

A person who, for the purpose prescribed for in paragraph 1 instruments or materials shall be punished by the same penalty with preceding paragraph of Article 163-4.

163-5. An attempt of the crimes prescribed under Article 163-2 and preceding Article paragraph 1 shall be punished.

(3). Statutory penalty of 163-2 is the imprisonment for not more than ten years or a fine of not more than 1,000,000 Yen. Statutory penalty of 162 is the imprisonment with work for not less than three months but not more than ten years.

Decision of the Supreme Court above mentioned applied the Article 162 to the case of the telephone card. According to the decision of the Supreme Court, a person who created the false telephone card should be punished even after the addition of Article 163-2. But Article 163-2 should be applied to the case of altering the electromagnetic record of telephone.

A person who possesses the payment card is punishable. A person who obtains provides or store information which is used for creating electromagnetic record of payment card is punishable. A person who prepares an instrument or materials which is used for creating electromagnetic record of payment is also punishable.

Article 163-2 paragraph 1 punishes a person who creates, without due authorization, electromagnetic record for a payment card. The word "electromagnetic information" prescribed for in Article 163-4 means any information which content is the same with genuine information. If someone encodes the information in a card which he prepares for, he can make another payment card for the use in improper administration of the financial affairs of another person.

7.4 Summary

Fraud is considered as an old conventional crime. Penal Codes of both the UAE and Japan enacted legal texts through which they have specified the meaning of forgery, its types and methods.

Japan Penal Code revision and amendment of 1987 added Articles and paragraphs in order to punish any act of fraud on any electromagnetic record as per Article 161-2. The UAE Information Technology Crimes Act, on the other hand, punishes any fraudulent act on an electronic record as per Article 6.

The UAE Information Technology crimes, as we have discussed in the introductory Chapter of this research, is a special law specified to informational crimes; therefore we believe that there is always need for new amendments and revisions to cater for this type of crimes which are characterized by unprecedented advancement and development. In other words, what is needed here is amendment of the law: whereas in case of the Japanese Penal Code amendment shall be either through adding new legal texts or legal paragraphs or a new phrase. An example of this can be traced in the e- credit card where Article 13 is added to the UAE Information Technology Crimes Act amendment of 2012; and in Japan Penal Code as amendment of the year 2001 where legal articles were

added in order to protect electronic cards from forgery (Article 163-1) as we have explained in the Informational Fraud Section.

In Article 161-2 of the Japanese law, in order to handle the crimes related to electronic documents, the provisions of unauthorized creation of electromagnetic records as one mode of forging documents are placed. On the other hand, in the UAE's law, forgery of electromagnetic documents through the internet is subject to punishment. There is a specific definition and regulation of forgery in the UAE's penal code, but the law of 2012 does not indicate the detailed modes of activities which can be subject to penalty.

CHAPTER 8

CONCLUSION AND RECOMMENDATIONS

CHAPTER 8

8.1 Conclusion

There is a direct relationship between the development and evolution of ICTs and Internet-related applications, and the intensification of cybercrime risks and applications. Technology is truly a double-edged sword that has transformed the classical and traditional forms of criminal behaviors. The proliferation of ICTs and progressive development in the digital transactions and communications has created new opportunities and opened up new windows for the illicit exploitation and utilization of ICTs, which has resulted in the emergence of new forms of criminal behavior and the Cybercrime.

This paper aims to examine laws related to computer crimes by comparing UAE's law and Japanese law. As the table of contents show clearly, the major focus of this paper is to explain, understand, and examine the acts on prohibition of unauthorized computer access, publicity of immoral activities through the internet, destruction of information in computers, computer fraud, and the unauthorized creation of electromagnetic records in both the UAE and Japanese laws.

In the UAE, in addition to the Penal Code, an individual law related to computer crimes was enacted in 2006, and it was wholly amended in 2012 to the present day. On the other hand, in Japan, computer-related crimes have majorly been handled by the Penal Code, which was established in 1908 and has been revised several times, while there is also a special act on prohibition of unauthorized computer access.

The UAE's act on computer-related crimes consisted of 29 articles in 2006, but it was revised in 2012 and now it consists of 51 articles including major unauthorized activities related to computers and electromagnetic records. In the Japanese penal code, computer-related crimes are handled as mentioned above, and this paper focuses on its contents. In this paper, the revised and established articles for computer-related crimes in the Japanese penal code are compared by the UAE's law of 2012 on computer-related crimes.

The following describes the significant and important points in this paper discussing the UAE's law.

In Chapter 1 and Chapter 2, the following points are significant. First, each article in the UAE's law of 2012 was classified into 5 groups which correspond to the contents of the appendix. The 1st group is mainly about the activities which can impair and harm the credibility of computer information technology, such as unauthorized access to other computers by using a computer network, obtaining electromagnetic data or records, obstructing others' services, or impairing computer functions by infecting them with a virus. Unauthorized access to other electronic devices is one of the typical illegal activities, but obtaining specific confidential information such as numbers, codes, or passwords is also considered a preliminary illegal activity and subject to punishment. The 2nd group aims to secure the nation and political stability. These include activities such as operating websites to publish information or opinions related to riots or other activities or matters contrary to public order and morality, and establishing websites for terrorist groups or illegal organizations in order to make it easier to communicate with the masterminds of terrorism or riots. Establishing a website containing pornography, gambling, or the activities which are against public moral and are published through an internet network, and procuring prostitutes through the internet are classified in the 3rd group. The articles categorized in the 4th group are about activities that profit by using a false statement of procedures, names, or certifications made up by using information technology systems. The 5th group is to punish the activities such as human trafficking, organ trade, weapons trade and drugs through the internet.

The major purpose of unauthorized computer access is to illegally obtain information and/or data, or to impair systems, electromagnetic records and data. Unauthorized computer access is considered the start of cybercrime. The UAE's computer law does not regulate the modes of unauthorized computer access to be punished, and there is no specific definition of unauthorized computer access. Article 2 of the UAE's law handles not only unauthorized computer access but also illegally staying in others' computers or accessing to computers out of the access authority as illegal activities to be subject to penalty. Also, the targeted computers are not specifically required to have access control functions.

Moreover, unauthorized computer access for the purpose of obtaining governmental data or classified information issued by organizations related to economy

or trade is subject to penalty. In addition, illegal activities using the internet network and unauthorized computer access, and those who improperly access electromagnetic records such as credit card numbers, or bank account information without due authorization are subject to punishment.

The UAE's penal code has a chapter about crimes related to fame, respect, belief, rape, indecent acts in public, and prostitution are subject to punishment in this chapter. Especially, Article 362 is the registration to handle illegal activities such as producing, exporting, possessing, or obtaining of immoral works, pictures, films or codes for the purpose of publicity. In contrast, the UAE's law of 2012 includes articles about punishment on a person who creates, prepares, or stores immoral information in order to publish or display immoral activities such as pornography and gambling through the internet. In Article 18 of the same law, a person who obtains child pornography through the internet will be punished. The range of activities contrary to "public morality" that the UAE's law of 2012 defines is not clear but there are some description of examples such as pornography and gambling. The issues related to pornography are important in such a conservative society as the UAE values tradition. In countries which contain many nationalities, cultures and customs, the determination of whether a target activity is contrary to "public morality" or not will be left to the judgment of the court.

In the UAE's penal code, destroying a computer itself or other equipment and accessories is subject to punishment. Also, if the destruction causes internet connection inferiority, it is subject to penalty in accordance with Article 8 of the law of 2012. There are also descriptions about the punishment of unauthorized computer access resulting in deleting, destroying or changing data or information. Punishment prescribed is located also may involve unauthorized access or deleting information, erase, destroy, and change. Destroying data or making programs and systems not working by intentionally inserting specific information program to a network system, information system, information devices, or transmitting electronic mail (e-mail) with messages in order to disable the e-mail function are subject to penalty. Moreover, a person who illegally obtains, changes, or erases the information related to medical matters such as diagnosis, medical care, and prescription by using the internet or information equipment will be punished.

In Article 399 of the UAE's penal code, it is indicated that a person who obtains personal estate by fraudulent activities or disposes personal property or real estate knowing he/she does not have authority to do so shall be punished. The fraudulent activities or attempts, such as assuming a false name or certification, to obtain personal property or profit by using the internet, information technology systems, or electronic devices are subject to penalty in accordance with Article 11 of the UAE's law of 2012. The activities used to make a profit by inputting false electromagnetic information through a network can be handled in this article. In Article 12 of the UAE's law of 2012, illegal possession of information of credit cards, electronic cards, bank account numbers and codes used for electronic payment via the internet, information systems or electronic devices are subject to punishment. A person who possesses this kind of information or content with the purpose of obtaining money or services from others will be punished severely.

Forgery of documents is defined in Article 216 of the UAE's Penal Code, and causing damages or disadvantages to someone by changing the quality of documents, in accordance with the way described in Article 216, is required to be considered a crime. In Article 6 of the UAE cyber law of 2012, forgery of official electromagnetic documents used in federal and local governments is clearly defined separately from the other non-official documents. Although the definition of forgery is not clearly indicated, Article 216 includes not only the documents created by a person without authority but also the documents which include false information created by an unauthorized person. The language used in documents does not affect the success or failure of a crime, even if it is written in Arabic or other languages. Since it is difficult to distinguish between an original and copies of electromagnetic documents, both original and copied documents can be a target. In the UAE's law of 2012, copying and using credit cards, debit cards, electronic cards, and other electronic payment methods, or their records and information by using information devices or programs is subject to punishment.

8.2 Recommendations

- Japan as partner in the global convention for cybercrime, may use the term of the convention to accomplish its legal system and efforts for combating cybercrime. However, the UAE is not yet a member in the convention. Therefore, this research recommends UAE to sign the international convention on cybercrimes, as well as adopt bilateral agreements with Japan to exchange expertise in this field.
- The most important issue in facing cybercrime is the procedural law, law of evidence, and implementation of such laws, by law enforcement officials, investigation, prosecution and trial of cybercrimes are in need of officials capable of understanding new technologies. In this context Japan may be well ahead of the UAE. Therefore, this research recommends UAE procedural laws should be amended to outline means of detecting, investigating, and prosecuting cybercrimes, as well as gathering digital evidence required to prove cybercrimes before criminal courts.
- The governments of Japan and UAE must identify and introduce the cyber law punishments and rulings, simply and clearly, for all people in the society in order to protect them from committing such crimes.
- Definition of the “public morality” in the UAE cyber law, and the terminology of “obscene” in Japanese penal code are non-obviously, they need further explanation.

FEDERAL DECREE BY LAW NO. 5 OF 2012
Issued on 13/8/2012 -from the website of Ministry of Justice- UAE.

Article 1

Definitions:

The following words and expressions shall have the meanings set opposite each of them unless the context requires otherwise:

- State: United Arab Emirates
- Competent Entities: Federal or local entities concerned with electronic security affairs in the State.
- Content: Electronic information, data and services.
- Electronic Information: Any information that may be saved, processed, generated and transferred by Information Technology tool in particular writings, graphics, voice, numbers, letters, codes, signals and others.
- Information Program: A set of data, instructions and orders that is executable by methods of Information Technology and are prepared to accomplish a specific task.
- Electronic Information System: A set of information programs and information technology methods prepared to process, manage and save Electronic Information or the like.
- Information Network: A correlation between two or more sets of Information Programs and Information Technology tool that allow the users to access and exchange Information.
- Electronic Document: An Information record or statement established, stored, extracted, copied, sent, reported or received by an Electronic means through an intermediary.
- Electronic Site: A place that makes Electronic Information available on the Information Network such as social networking sites, personal pages and Blogs.
- Information Technology Tool: Any magnetic, visual, electrochemical electronic device or any other device used to process electronic data and perform logical and accounting operations or saving tasks and it includes any directly connected or related instruments that allow this means to save Electronic Information or deliver it to others.
- Government Data: Electronic Data or Information of the Federal Government or Local Governments of the Emirates of the State or Public Authorities or Federal or Local Public Institutions.
- Financial, Trade or Economic Establishments: Any establishment that earns its financial, trade or economic description under the licensed issued by the competent entity in the State.
- Electronic: That is connected to electromagnetic, photoelectric, digital, automated or optical technology or the like.
- Juvenile Pornographic Materials: Any pictures, recordings, graphics or others of sexual organs that are sexually provocative or real or virtual sexual actions or by simulation for a juvenile not exceeding eighteen years of age.
- Protocol Address of the Information Network: A digital identification designated for each Information Technology Tool that is a participant in an Information Network used for the purposes of communication.
- Confidential: Any Information or data the others are not allowed to view or disclose except with a prior permission from the concerned owner.

- Capture: Viewing or obtaining data or information.
- Abuse: Any intended expression on any person or entity considered insulting by the ordinary person or that prejudices the honor or dignity of that person entity.

Article 2

Punishment of Entering an Electronic Site, Electronic Information System, Information Network or Information Technology Tool without Permission and Illegally.

1. Any person who entered an Electronic Site, Electronic Information System, Information Network or an Information Technology Tool without permission or by exceeding the limits of the permission or remaining in it illegally shall be punished by imprisonment and a fine not less than (AED 100.000) and not exceeding (AED 300.000) or by any of these punishments.

2. The punishments shall be imprisonment for a period not less than six months and a fine not less than (AED 150.000) and not exceeding (750.000) or by any of these punishments if any of the actions provided for in Paragraph (1) of this Article entails the cancellation, deletion, destruction, disclosure, damage, change, copying, publishing or re-publishing any data or Information.

3. The punishment shall by imprisonment for a period not less than one year and a fine not less than (AED 250.000) and not exceeding (AED 1.000.000) or by any of these punishments if the data or Information, the subject matter of the actions mentioned in Paragraph (2) of this Article, were personal.

Article 3

Punishment of the Perpetrator of the Crimes provided for in Clauses (1) and (2) of Article (2) of this Decree by Law in the Occasion of Performing his Work.

Any person who committed any of the crimes provided for in Clauses (1) and (2) of Article (2) of this Decree by Law in the occasion or by reason of performing his work shall be punished by imprisonment for a period not less than one years and a fine not less than (AED 250.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Article 4

Punishment of Entering Electronic Sites and the Information Technology Tool for the Purpose of Obtaining Government Data and Confidential Information of a Financial, Trade or Economic Establishment.

Any person who entered without permission to an Electronic Site, Electronic Information System, Information Network or Information Technology Tool whether the entry was for the purpose of obtaining Government Data or Confidential information of a Financial, Trade or Economic Establishment shall be punished by temporary imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 1.500.000).

And the punishment shall be imprisonment for a period not less than five years and a fine not less than (AED 500.000) and not exceeding (AED 2.000.000) if this data or Information was exposed to cancellation, deletion, damage, destruction, disclosure, change, copying, publishing or re-publishing.

Article 5

Punishment of Entering an Electronic Site without Permission for the Purpose of Changing its Design or Damaging, Amending or Cancelling the Site.

Any person who entered without permission an Electronic Site for the purpose of changing its designs or cancelling, damaging or amending it or occupying its address shall be punished by imprisonment and a fine not less than (AED 100.000) and not exceeding (AED 300.000) or by any of these punishments.

Article 6

Punishment of Forging an Electronic Document and using the Forged Document with Knowledge of the Forgery.

Any person who forged an Electronic Document of the Federal or Local Government or the Federal or Local Public Authorities or Institutions shall be punished by temporary imprisonment and a fine not less than (AED 150.000) and not exceeding (AED 750.000).

The punishment shall be imprisonment and a fine not less than (AED 100.000) and not exceeding (AED 300.000) or by any of these punishments if the forgery occurred in the Documents of an entity other than these provided for in the first Paragraph of this Article.

And any person who used the forged Electronic Document with knowledge of the forgery shall be punished by the same punishment prescribed for the forgery crime, as the case may be.

Article 7

Punishment of Amending, Damaging, or Disclosing Information or Data Related to Medical Examinations, Medical Diagnoses or Treatment without Permission.

Any person who obtained, acquired, amended, damaged or disclosed without permission the statements of any Electronic Document or Electronic Information through the Information Network, Electronic Site, Electronic Information System or an Information Technology Tool and these statements or Information were related to medical examinations or a medical diagnoses or treatment or medical care or records shall be punished by temporary imprisonment.

Article 8

Punishment of Disabling Access to an Information Network or an Electronic Site or an Electronic Information System.

Any person who precludes or disables access to an Information Network or Electronic Site or Electronic Information System shall be punished by imprisonment and a fine not less than (AED 100.000) and not exceeding (AED 300.000) or by any of these punishments.

Article 9

Punishment of Circumvention on the Protocol Address of the Internet for the Purpose of Committing a Crime or Preventing its Discovery.

Any person that circumvents the protocol address of the internet by using a delusive address or an address belonging to others or by any other means for the purpose of committing a crime or preventing its discovery shall be punished by imprisonment and a

fine not less than (AED 150.000) and not exceeding (AED 500.000) or by any of these punishments.

Article 10

Punishment of Intentionally Entering without Permission an Information Program to the Information Network or the Electronic Information System or any of the Information Technology Tool and Spamming E-Mails by Messages for the Purpose of Disabling, Suspension or Damage.

Any person who intentionally enters without permission an Information Program to the Information Network or an Electronic Information System or any of the Information Technology Tool and this caused suspending from work, disabling, destruction, erasing, deletion, damage or changing the program, System or Electronic Site or the data or information shall be punished by imprisonment for a period not less than five years and a fine not less than (AED 500.000) and not exceeding (AED 3.000.000) or by any of these punishments.

The punishment shall be imprisonment and a fine not exceeding (AED 500.000) or any of these punishments if the result is not achieved.

The punishment shall be imprisonment and a fine or any of these punishments for any intentional action for the purpose of spamming e-mail with messages and suspend it from working or disabling it or damaging its contents.

Article 11

Punishment of Capturing without Right on a Movable Asset or Benefit or a Document in a Fraudulent Method .Any person who captures for himself or for others without right a movable asset, benefit, document or a signature by using any fraudulent method or by taking a false name or impersonation of a false capacity through the Information.

Network, Electronic Information System or any of the Information Technology Tool shall be punished by imprisonment for a period not less than one year and a fine not less than (AED 250.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Article 12

Punishment of using the Information Network or Electronic Information System or Information Technology Tool for the Purpose of Obtaining the Numbers or Statements of a Credit or Electronic Card or Bank Accounts.

Any person who unlawfully reaches by using the Information Network or Electronic Information System or any of the Information Technology Tool to the numbers or statements or a credit or electronic card or statements of bank accounts or any means of electronic payment shall be punished by imprisonment and a fine or by any of these punishments.

The punishment shall be imprisonment for a period not less than six months and a fine not less than (AED 100.000) and not exceeding (AED 300.000) or by any of these punishments if it was intended to use the statements and numbers to obtain the money of others of benefiting from the services related.

If this resulted in capturing for himself or others money owned for others the punishment shall be imprisonment for a period not less than one year and a fine not less

than (AED 200.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Any person who published or re published the numbers or statements or a credit or electronic card or the numbers or statements of bank accounts of others or any other means of electronic payment shall be punished by the same punishment provided for in the previous Paragraph.

Article 13

Punishment of Forging, Imitation, Copying or Using without Right a Credit, Electronic or Debit Card by Using or Manufacturing any of the Information Technology Tool or an Information Program.

Any person who forged, imitated or copied a credit or debit card or any other means of electronic payment by using any of the Information Technology Tool or Information Program shall be punished by imprisonment and a fine not less than (AED 500.000) and not exceeding (AED 2.000.000) or by any of these punishments.

The following shall be punished by the same penalty:

1. Any person that manufactured or designed any Information Technology Tool or an Information Program for the purpose of facilitating any of the actions provided for on Paragraph (1) of this Article.
2. Any person that used without permission a credit, electronic or debit card or any other means of electronic payment for the purpose of obtaining for himself or for others money or properties of others or benefiting from the services he provides it for others.
3. Any person that accepts to transact with these forged, imitated or copied cards or other means of electronic payment with knowing that they are illegal.

Article 14

Punishment of Obtaining without Permission a Confidential Number, Code or Password to Enter to Information Technology Tool or Electronic Site or Electronic Information System or Information Network.

Any person who obtained without permission a Confidential number, code or password or any other means of entering to an Information Technology Tool or Electronic Site or Electronic Information System or Information Network or Electronic Information shall be punished by imprisonment and a fine not less than (AED 200.000) and not exceeding (AED 500.000) or by any of these punishments.

Any person who prepared, designed, produced, sold, purchased, imported, offered for sale or made available any Information Program or Information Technology Tool or promoted in any way links for Electronic Sites or an Information Program or any Information Technology Tool designed for the purposes of committing, facilitating or incitement to commit the crimes provided for in this Decree by Law.

Article 15

Punishment of Capturing or Intercept any Communication Intentionally and without Permission through an Information Network.

Any person who intentionally and without permission captures or intercepts any communication through any Information Network shall be punished by imprisonment and a fine not less than (AED 150.000) and not exceeding (AED 500.000) or by any of these punishments.

Any person who disclosed the information obtained unlawfully by receiving or interception of communications shall be punished by imprisonment for a period not less than one year.

Article 16

Punishment of Blackmailing or Threatening a Person to perform or refrain from an Action by using an Information Network or an Information Technology Tool.

Any person who blackmailed or threatened another person to make him perform or refrain from an action by using an Information Network or an Information Technology Tool shall be punished by imprisonment for a period not exceeding two years and a fine not less than (AED 250.000) and not exceeding (AED 500.000) or by any of these punishments.

The punishment shall be imprisonment for a period not exceeding ten years if the threat to commit an offence or attribution of issues that prejudice honor or consideration.

Article 17

Punishment of Preparing, Distributing, Publishing or Re-Publishing of Pornographic Materials, Gambling Activities or Materials that Prejudice Public Morals through an Information Network.

Any person who established or operated or supervised an Electronic Site or transmitted, sent, published or re-published through the Information Network pornographic materials or gambling activities and anything that may prejudice public morals shall be punished by imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 500.000) or by any of these punishments.

Any person, who produced, prepared, sent or saved pornographic materials or gambling activities and anything that may prejudice public morals for the purpose of exploitation, distribution or displaying for others through an Information Network shall be punished by the same punishment.

If the subject of the pornographic content was a juvenile not exceeding eighteen years of

age or if this content was designed to tempt juveniles the perpetrator shall be punished by imprisonment for a period not less than one year and a fine not less than (AED 50.000) and not exceeding (AED 150.000).

Article 18

Punishment of Acquiring Intentionally Juvenile Pornographic Materials through using any Information Technology Tool.

Any person who intentionally acquires Juvenile Pornographic Materials by using an Electronic Information System, Information Network, Electronic Site or any of the Information Technology Tool shall be punished by imprisonment for a period not less than six months and a fine not less than (AED 150.000) and not exceeding (AED 1.000.000).

Article 19

Punishment of Temptation and Incitement to Commit Prostitution or Debauchery by using an Information Network or any of the Information Technology Tool.

Any person who incited or tempted another to commit prostitution or debauchery or assisted in that by using an Information Network or any of the Information Technology

Tool shall be punished by imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 1.000.000) or by any of these punishments.

The punishment shall be imprisonment for a period not less than five years and a fine not exceeding (AED 1.000.000) if the victim was a juvenile that did not complete eighteen years of age.

Article 20

Punishment of insulting others and making them subject to Punishment or Contempt by others through using an Information Network or an Information Technology Tool without prejudice to the provisions of slander crime prescribed in Islamic Sharia, any person who insults others or has attributed to him an incident that may make him subject to punishment or contempt by others by using an Information Network or an Information Technology Tool shall be punished by imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 500.000) or by any of these punishments.

If the insult or slander took place against a public employee or a person assigned to a public service by occasion or because of performing his work this shall be considered an aggravating circumstance of the crime.

Article 21

Punishment of Assaulting the Privacy of a Person in Cases other than those Permitted in Law by using an Information Network, Electronic Information System or any of the Information Technology Tool.

Any person who used an Information Network, Electronic Information System or any of the Information Technology Tools in assaulting the privacy of a person in cases other than those permitted in Law shall be punished by imprisonment for a period not less than six months and a fine not less than (AED 150,000) and not more than (AED 500.000) or by any of these punishments by any of the following methods:

1. Overhearing, interception, recording, transferring, transmitting or disclosure of conversations, communications or audio or visual materials.
2. Capturing pictures of others or preparing electronic pictures or transferring, exposing, copying or keeping those pictures.
3. Publishing electronic news or pictures or photographs, scenes, comments, statements or information even if they were correct and real.

Any person who used an Electronic Information System or any of the Information Technology Tool to perform any amendment or processing on a recording, picture or scene for the purpose of defamation or insulting another person or assaulting or violating his privacy shall be punished by imprisonment for a period not less than one year and a fine not less than (AED 250.000) and not exceeding (AED 500.000) or by any of these punishments.

Article 22

Punishment of Using an Information Network, Electronic Site or Information Technology Tool without Permission to Expose Confidential Information Any person who used without permission any Information Network, Electronic Site or Information Technology Tool to expose Confidential Information obtained by occasion or because of his work.

Article 23

Punishment of Establishing or Operating an Electronic Site or Publishing Information on an Information Network for the Purpose of Human or Human Organs Trafficking.

Any person who established or operated or supervised an Electronic Site or published information of an Information network or by any of the Information Technology Tool for the purpose of human or human organs trafficking or dealing with these illegally shall be punished by temporary imprisonment and a fine not less than (AED 500.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Article 24

Punishment of Establishing or Operating an Electronic Site or Publishing Information for the Purpose of Promoting or Favoring Ideas that may Stir Sedition, Sectarianism or Hurting National Unity and Prejudice of Public Morals.

Any person who established, operated or supervised an Electronic Site or published information on an Information Network or any of the Information Technology Tool to promote or favor any programs or ideas that may stir sedition, hatred, racism or sectarianism or hurting national unity or social peace or prejudice of public order or public morals shall be punished by temporary imprisonment and a fine not less than (AED 500.000) and not exceeding (AED 1.000.000).

Article 25

Punishment of Establishing or Operating an Electronic Site or Publishing Information for Trade and Promoting Weapons, Ammunitions and Explosives.

Any person who established, operated or supervised and Electronic Site or published Information on an Information Network or any of the Information Technology Tool for the purpose of trade or promoting weapons, ammunitions or explosives in cases other than those permitted by Law shall be punished by imprisonment for a period not less than one years and a fine not less than (AED 500.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Article 26

Punishment of Establishing or Operating an Electronic Site or Publishing Information of a Terrorist Group or an Illegal Body for the Purpose of Promoting and Facilitating Communications with their Leaderships.

Any person who established, operated or supervised an Electronic Site or published Information on the Information Network or an Information Technology Tool for a terrorist group or any illegal group, association, organization or body for the purpose of facilitating communication with its leaderships or members or to attract membership, promote or favor its ideas, finance its activities or providing actual assistance or for the purpose of spreading the methods of manufacturing burning devices or explosives or any other tools used in terrorist actions shall be punished by imprisonment for a period not exceeding five years and a fine not less than (AED 1.000.000) and not exceeding (AED 2.000.000).

Article 27

Punishment of Establishing or Operating an Electronic Site or Publishing Information to Call or Promote Collection of Donations without License.

Any person, who established, operated or supervised an Electronic Site or published information on the Information Network or any other Information Technology Tool to call or promote collection of donations without a license approved by the competent authority shall be punished by imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 500.000) or by any of these punishments.

Article 28

Punishment of Establishing or Operating an Electronic Site or Publishing Information, Graphics or News that may Expose State Security and Interests to Danger and Prejudice Public Order.

Any person who established, operated or supervised an Electronic Site or used information on the Information Network or an Information Technology Tool for the purpose of inciting actions, or published or transmitted Information, news, cartoons or any other pictures that may expose State security and interests to danger and prejudice public order shall be punished by temporary imprisonment and a fine not exceeding (AED 1.000.000).

Article 29

Punishment of Publishing Information, News or Rumors on an Electronic Site or Information Technology Tool or any Information Network for the purpose of Cynicism and Harming the Status of the State and its Institutions.

Any person who published information, news, statements or rumors on an Electronic Site, any Information Network or any Information Technology Tool for the purpose of cynicism or harming the reputation, dignity or status of the State, any of its institutions, President, Vice President, Governors of the Emirates, Crown Princes, Vice Governors of the Emirates, flag of the State. National anthem, slogan or symbols shall be punished by temporary imprisonment and a fine not exceeding (AED 1.000.000).

Article 30

Punishment of Establishing or Operating an Electronic Site or Publishing Information for the Purpose of Overthrowing or Changing the Regime of the State or Obstruct the Provisions of the Constitution.

Any person who established, operated or supervised an Electronic Site or published information on the Information Network or an Information Technology Tool that aims or calls to overthrow or change the regime of the State or seizing it or to obstruct the provisions of the Constitution or the laws applicable in the country or that is against the basic principles of the regime of the State shall be punished by life imprisonment.

Any person who promoted or incited and of the mentioned actions or facilitated them for others shall be punished by the same punishment.

Article 31

Punishment of Publishing Information for the Purpose of Incitement or Calling to Evasion from Applicable Laws and Regulations.

Any person who called or incited by publishing information on the Information Network or an Information Technology Tool to the evasion from laws and regulations applicable in the State shall be punished by imprisonment and a fine not less than (AED 200.000) and not exceeding (1.000.000) or by any of these punishments.

Article 32

Punishment of Establishing or Operating an Electronic Site or Creating Information for the Purpose of Calling or Promoting Demonstrations without License.

Any person who established, operated or supervised an Electronic Site or used the Information Network or an Information Technology Tool for planning, organizing, promoting or calling to demonstrations or protests and the like without license from the competent authority shall be punished by imprisonment and a fine not less than (AED 500.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Article 33

Punishment of Establishing or Operating an Electronic Site or using the Information Network or the Information Technology Tool for Trade of Antiquities or Artifacts without Right.

Any person who established, operated or supervised an Electronic Site or used the Information Network or Information Technology Tool for trade in antiquities and artifacts in cases other than those permitted by Law shall be punished by imprisonment and a fine not less than (AED 500.000) and not more than (AED 1.000.000) or by any of these punishments.

Article 34

Punishment of Unlawfully Benefiting or Facilitating to others uses Communication Services through the Information Network or the Information Technology Tool.

Any person who benefited or unlawfully facilitated to others the use of communication services or audio or visual transmission channels through the Information Network or the Information Technology Tool shall be punished by imprisonment for a period not less than one year and a fine not less than (AED 250.000) and not exceeding (AED 1.000.000) or by any of these punishments.

Article 35

Punishment of Committing Crimes of Offending Sanctities and Religions and Encouraging Sins through the Information Network, Information Technology Tool or Electronic Site.

Without prejudice to the provisions prescribed in Islamic Sharia, any person who committed through the Information Network, Information Technology Tool or Electronic Site any of these following crimes shall be punished by imprisonment and a fine not less than (AED 250.000) and not exceeding (AED 1.000.000) or by any of these punishments:

1. Offending any of the Islamic sanctities or rituals.
2. Offending any of the sanctities or rituals prescribed in other religions whenever these sanctities or rituals are protected according to the provisions of Islamic Sharia.
3. Insulting any of the recognized monotheistic religions.
4. Encourage, incite or promote sins.

If the crime included an offense to God, prophets or messengers, was against the Islamic religion or prejudices the bases and principles it is built on, was against or prejudiced any necessarily taught provisions or rituals of the Islamic religion or that insults the Islamic religion, preaching to other religions or calling to a doctrine or idea involving any of the above or that favors or promotes the above shall be punished by imprisonment for a period not exceeding seven years.

Article 36

Punishment of Establishing or Operating an Electronic Site or Publishing Information for Trade or Promoting Narcotics or Psychotropic Substances.

Any person who established, operated or supervised an Electronic Site or published information on the Information Network or the Information Technology Tool to trade or promote narcotics or psychotropic substances and the like or the method of taking them or to facilitate dealing with those in cases other than those permitted by Law shall be punished by temporary imprisonment and a fine not less than (AED 500.000) and not more than (AED 1.000.000) or by any of these punishments.

Article 37

Punishment of using an Information Network, Electronic Information System or any Information Technology Tool Intentionally to Commit Criminal Actions Related to Illegal Funds.

Taking into consideration the provisions provided for in the Money Laundering Law, any person who intentionally performed any of the following actions using an Information Network, Electronic Information System or any of the Information Technology Tool shall be punished by imprisonment for a period not exceeding seven years and a fine not less than (AED 500.000) and not exceeding (AED 2.000.000):

1. Transferring, moving or depositing illegal funds for the purpose of concealing or disguising the illegal source.
2. Concealing or disguising the reality, source, movement of the illegal funds or the rights related or ownership.
3. Earning, acquiring or using illegal funds with being aware that it is from an illegal source.

Any person, who established, operated or supervised and Electronic Site or published information on the Information Network or an Information Technology Tool to facilitate or incite committing any of the actions provided for in Paragraph (1) of this Article shall be punished by the same punishment.

Article 38

Punishment of using the Information Network or any of the Information Technology Tool for the purpose of Harming the Interests of the State and Offending its Dignity.

Any person who provided for any organizations, institutions, authorities or any other bodies' incorrect, inaccurate or misleading information that may harm the interests of the State or offend its reputation, dignity or status by using the Information Network or any of the Information Technology Tool shall be punished by temporary imprisonment.

Article 39

Punishment of the Owner or Operator of the Electronic Site or Information Network to Save or Provide an Illegal Content.

Any owner or operator of an Electronic Site or Information Network that stored or made available intentionally any illegal content with being aware of that or did not commence

to remove or preclude entrance to this illegal content during the period determined in the written notice directed to him by the Competent Entities that states the content is illegal and is available on the Electronic Site or Information Network shall be punished by imprisonment and a fine or by any of these punishments.

Article 40

Punishment of Attempt of the Offenses provided for in this Decree by Law Attempt of the offenses provided for in this Decree by Law shall be punished by half of the punishment prescribed for the complete crime.

Article 41

Adjudging to Confiscate the Devices and Programs or Erasing Information or Statements or Closing the Site where the Crimes are Committed.

Without prejudice to the right of others of good faith, it shall be adjudged in all cases to confiscate the devices, programs or means used to commit any of the crimes provided for in this Decree by Law or the resulting amounts or by erasing the information or statements or destroying them as well as adjudge to close the place or site where any of these crimes are committed, either once and for all or for the period estimated by Court.

Article 42

Adjudge to Deport the Foreigner Convicted for Committing the Crimes provided for in this Text.

The Court shall adjudge to deport the foreigner convicted for committing any of the crimes provided for in this Decree by Law after executing the prescribed punishment.

Article 43

Adjudge to put the Convict under Supervision or Control or Deprivation from using an Information Network, Electronic Information System or Information Technology Tool.

Without prejudice to the punishments provided for in this Decree by Law, the court may order to put the convict under supervision or control or deprive him from using any Information Network, Electronic Information System or any other Information.

Technology Tool or place him in a therapy shelter or rehab center for the period the court deems appropriate.

Article 44

Crimes that Prejudice Security of the State.

Crimes mentioned in Articles (4), (24), (26), (28), (29), (30) and (38) of this Decree by Law is from crimes that prejudice the security of the State. Also, any crime provided for in this Decree by Law shall be considered to prejudice the security of the State if it was committed for the account or benefit of a foreign State, any terrorist group or any illegal group, association, organization or body.

Article 45

Adjudge to Mitigate the Punishment or Exemption based on a Request of the Public Prosecutor.

That Court shall adjudge, based on a request of the public prosecutor, to mitigate of exempt from the punishment any perpetrators who gave information to the judicial or administrative authorities related to any of the crimes related to the security of the State according to the provisions of this Decree by Law whenever this leads to exposing the crime and its perpetrators or prove the crime or arrest any of them.

Article 46

Aggravating Circumstance.

Using the Information Network, Internet, any Electronic Information System, Electronic

Site or Information Technology Tool when committing any crime not provided for in this Decree by Law shall be considered an aggravating circumstance.

Also, committing any crime provided for in this Decree by Law for the account or benefit of a foreign State or any terrorist group or illegal group, association, organization or body shall be considered an aggravating circumstance.

Article 47

Scope of Validity of the Provisions of this Decree by Law.

Without prejudice to the provisions of Chapter Two of Part (2) of Book (1) of the Penal Code, the provisions of this Decree by Law shall apply on any person, who committed any of the crimes mentioned abroad, if its subject was an Electronic Information System,

Information Network, Electronic Site or an Information Technology Tool of the Federal Government or one of the Local Governments of the Emirates of the State or any of the public authorities or institutions belonging to any of them.

Article 48

Non-Prejudice to the Severer Punishment Provided for in the Penal Code or any Other Law.

Applying the punishments provided for in this Decree by Law shall not prejudice any severer punishment provided for in the Penal Code or any other Law.

Article 49

Giving the Capacity of Judicial Officers for the Employees Determined by a Resolution of the Minister of Justice.

The employees determined by a Resolution of the Minister of Justice shall have the capacity of Judicial Officers to prove actions that occur in violation to the provisions of this Decree by Law and the Local Authorities in the Emirates shall provide the facilitations needed for these employees to enable them to perform their work.

Article 50

Repealing Federal Law No. 2 of 2006 and all Contrary and Conflicting Provisions Federal Law No. 2 of 2006 concerning combating information technology crimes shall be hereby repealed as well as any provision contrary or conflicting with the provisions of this Decree by Law.

.

FEDERAL LAW NO (3) OF 1987 ON ISSUANCE OF THE PENAL CODE
Ministry of Justice –UAE.

Article (1)

Provisions of the Islamic Law shall apply to the crimes of doctrinal punishment, punitive punishment and blood money. Crimes and chastisement punishments shall be determined in accordance with the provisions of this law and other penal codes.

Article (5)

The following shall ipso jure be considered a public official:

1. Persons entrusted with the public authority and employees working in ministries and governmental departments.
2. Members of the Armed Forces.
3. Chairmen and members of legislative, consultative and municipal councils.
4. Whoever is delegated by any of the public authorities to perform a specific assignment within the limits of the work entrusted to him.
5. Chairmen and members of boards of directors, managers and all other employees working in associations and public corporations.
6. Chairmen and members of boards of directors and all other employees working in associations and public welfare institutions.

Whoever is not included in the categories stated in the preceding clauses and performs work connected with public service in accordance with instructions issued to him from a public official having the authority to give such an instruction according to prescribed laws or regulations, concerning the work assigned to him, shall be considered ipso jure to be entrusted with a public service.

Article (9)

The following shall, pursuant to this law, be considered means of publicity:

1. By saying or shouting publicly by any mechanical means in a public gathering, in a public road or in a permissible or frequented place or if it is announced by any other means.
2. By actions, signals or gestures if they take place in any of the aforementioned places, or if they are transmitted to any person in such places by any mechanical means or by any other means.
3. By exhibiting writing, drawings, pictures, films, symbols and other means of expression in any of the aforementioned places, by distributing them indiscriminately, by selling them to people, or by offering them for sale in any place.
4. Article (21)
5. This law shall apply to any one who is found in the State, after being involved abroad as a principal offender or an accomplice in an act of sabotage or impairment of international communication systems, crimes of traffic in drugs, women, or children, slavery, acts of piracy or international terrorism.

Article (26)

Crimes shall be divided into the following categories:

1. Doctrinal crimes.
2. Punitive and blood-money crimes.
3. Chastisement crimes.

Crimes are of three types: felonies, misdemeanors and contraventions.

The category of the crime shall be determined in accordance with the penalty provided thereto by law, and if the crime is punishable by fine or by blood money with another penalty, its category shall be determined in accordance with the other penalty.

Article (27)

The category of a crime shall not change if the court replaces the punishment determined thereto with a lighter punishment, whether for legal reasons or for extenuating discretionary circumstances, unless the law provides otherwise.

Article (28)

A felony shall be a crime punishable by any of the following penalties:

1. Any of the doctrinal punishment or punitive punishments except penalties for drunkenness and defamation.
2. The death sentence.
3. Life imprisonment.
4. Temporary imprisonment.

Article (29)

A misdemeanor is a crime punishable by one or more of the following penalties:

1. Imprisonment.
2. A fine exceeding one thousand Dirhams.
3. Blood money.
4. Whipping in punishment for drunkenness and defamation.

Article (30)

Any act or omission punishable by law or regulations by one or both of the following two penalties shall be considered a contravention:

1. Custody for a period not less than twenty-four hours and not exceeding ten days in any of the places designated for that purpose.
2. A fine not exceeding one thousand Dirhams.

Article (34)

An attempt is the commencement of the execution of an act with the intention to commit a crime, if its effect is prevented for reasons beyond the control of the felon.

Commitment of an act, if in itself it is regarded as a constituent part of the practical element of the crime or gives rise to it immediately and directly, shall be considered commencement of execution.

Neither a mere intention to commit a crime nor preparatory deeds shall be considered an attempt to commit a crime unless the law provides otherwise.

Article (35)

An attempt to commit a crime shall be punishable by the following penalties unless the law provides otherwise:

1. Imprisonment for life if the penalty designated for the crime is the death sentence.
2. Imprisonment for a certain term if the penalty designated for the crime is life imprisonment.

3. Imprisonment for a period not exceeding half of the maximum penalty provided for the crime or detention if the penalty provided for is imprisonment for a certain term.

Article (43)

An offender shall be answerable for a crime whether he has committed it with or without intention, unless the law explicitly provides for intention.

Article (66)

Principal penalties are:

a. Doctrinal penalties, punitive penalties, and blood money.
b. Chastisement penalties are:
   1. Death penalty.
   2. Imprisonment for life.
   3. Imprisonment for a limited term.
   4. Detention.
   5. Fine.

Article (68)

Imprisonment is to detain a convict in one of the penitentiaries legally designated for such a purpose, for life, if the sentence is life imprisonment, or for a specified term if it is temporary imprisonment.

The term of temporary imprisonment shall neither be less than three years, nor more than fifteen years, unless the law provides otherwise.

Article (69)

Detention is to place a convict in any of the punitive premises maintained for such a purpose for the term awarded to him.

The minimum period of imprisonment may not be less than a month nor exceed three years, unless the law provides otherwise.

Article (70)

Whoever is sentenced to a custodial penalty shall be instructed to perform the jobs required in punitive facilities, taking into consideration his circumstances, with the intention to correct and qualify him, and an appropriate recompense. Regular reports on him shall be made in order to observe how he behaves, and all this shall be subject to the law governing punitive facilities.

Article (71)

Punishment by a fine is to oblige a convicted person to pay the treasury the adjudged amount. The penalty may not be less than one hundred Dirhams nor exceed one hundred thousand Dirhams in crimes, and thirty thousand Dirhams in misdemeanors, unless the law provides otherwise.

Article (97)

If an extenuating excuse exists for a crime punishable by the death penalty, it shall be commuted to life or temporary imprisonment or to a penalty of detention for not less than one year; and if it is punishable by life or temporary imprisonment, it shall be

commuted to a penalty of detention for not less than three months unless the law provides otherwise.

Article (98)

If the court finds in a felony that the circumstances of the crime or the culprit calls for clemency, it may extenuate the penalty prescribed by law for the felony as follows:

a. If the penalty prescribed for the crime is death, it may be commuted to life or temporary imprisonment.
b. If the penalty required for the crime is life imprisonment, it may be commuted to temporary imprisonment or detention for no less than six months.
c. If the penalty prescribed for the crime is temporary imprisonment, it may be commuted to detention for no less than three months.

Article (99)

If an extenuating excuse becomes available for a misdemeanor, commutation of the penalty shall be as follows:

a. If a penalty has a certain minimum limit, the court shall not comply therewith in assessing a discretionary penalty.
b. If the misdemeanor is punishable by detention and fine together, the court shall apply either one of the two penalties.
c. If a penalty is detention without a certain minimum limit, the court may commute the sentence to a fine.

Article (100)

If the court finds in a misdemeanor that the circumstances of a crime or culprit calls for clemency, it may extenuate the punishment as stated in the preceding Article.

Article (101)

If an extenuating excuse and mitigating circumstance coexist for a misdemeanor, the court may award a judicial pardon in favor of the convict.

CHAPTER II
AGGRAVATING CIRCUMSTANCES

Article (102)

Without prejudice to the cases in which the law states special causes for severity, the following shall, inter alia, be considered to be aggravating circumstances:

a. Commitment of a crime for a vicious motive.
b. Commitment of a crime, by exploiting the victim's mental weakness or his inability to resist, or circumstances where others are unable to defend him.
c. Commitment of a crime in a savage way or by mutilating the victim.
d. Commitment of a crime by a public official, by taking advantage of his official authorities or his capacity, unless the law provides a certain punishment, owing to such a capacity.

Article (103)

Where there is an aggravating circumstance, the court may impose the penalty as follows:

a. If the principal penalty for a crime is a fine, its maximum limit may be doubled or a judgment of detention may be awarded.
b. If the principal penalty for a crime is detention, its maximum limit may be doubled.
c. If the principal penalty for a crime is imprisonment with a maximum period of less than fifteen years, the penalty may be imposed to such an extent.
d. If the principal penalty for a crime is temporary imprisonment with a maximum period, it, may be commuted to life imprisonment.

Article (104)

If a crime not punishable by a fine has been committed with the motive of making a profit, the culprit may, apart from the principal penalty determined for the crime, be awarded with a penalty not exceeding the amount of profit made by him unless the law provides otherwise.

Article (105)

If aggravating circumstances coexist with extenuating excuses or mitigating circumstances in a single crime, the court shall first apply the aggravating circumstances, followed by the extenuating excuses, then the mitigating circumstances. Nevertheless, if aggravating circumstances and excuses vary in their effect, the court may give priority to the stronger of the two of them.

Article (106)

A person shall be considered a recidivist:

First: If he has been convicted of a crime with a final judgment in a penalty of a crime, and then he relapses into another crime.

Second: If he has been sentenced to six months' detention or more and then commits a misdemeanor before the lapse of five years from the date of completion of such a penalty.

The case of recidivism shall not arise except where crimes are united as regards premeditation and error. The court may, in such cases, consider recidivism an aggravating circumstance.

Article (212)

If crimes indicated in the preceding Article are committed in respect of seals, stamps or marks pertaining to a juridical person other than those indicated above, a penalty of detention shall be awarded.

Article (216)

Forgery of an instrument is a change of its genuineness by any of the means stated hereinafter, resulting in damage, for the purpose of using it as a valid instrument.

The following are considered means of forgery:

1. introducing a change into an existing instrument by addition, deletion or alteration, whether in writing, numbers, marks, or in photographs appearing therein.
2. Putting a forged signature or seal, or alteration of a true signature, seal, or thumb-print.
3. Obtaining, by means of surprise or fraud, a signature, seal or thumb-print of a person without his knowing the contents of the instrument or without validly giving consent thereto.

4. Fabricating or counterfeiting an instrument and attributing it to a third party.
5. Blank filling of a signed, sealed or thumb-printed paper without the consent of the person who signed, sealed or thumb-printed it.
6. Disguising or substituting the identity of a person in an instrument made to verify its truth.
7. Alteration of truth in an instrument made for verifying its contents.

Article (217)

Unless otherwise provided, forgery of an official instrument shall be punished by imprisonment for a period not exceeding ten years, and forgery of an unofficial instrument shall be punished by detention.

Article (218)

An official instrument is that in the writing of which an ex officio public official interferes in any mariner, or to which he gives an official character.

Except for this, all other instruments shall be considered unofficial instruments.

Article (219)

A prison sentence not exceeding five years shall be inflicted upon any physician or midwife who knowingly issues a false certificate or statement concerning a case of pregnancy, birth, illness, deformity, death or other cases related to his profession, even if the act takes place as a result of a request, recommendation or intercession.

Article (220)

Imprisonment for a period not exceeding two years or a fine not exceeding ten thousand Dirhams shall be imposed upon anyone who, in cases concerning proceedings of death, succession or testament before the competent authority to issue a doctrinal certificate, confirms untrue statements on facts required to be proven although he is ignorant of their truth, or knows that they are untrue, where the certificate notification is issued on the basis of such statements.

Article (221)

Detention for a period not exceeding two years or a fine not exceeding ten thousand Dirhams shall be inflicted upon anyone who gives a false statement on his place of residence, and who assumes a name other than his own, in a judicial or administrative inquiry.

Article (222)

Whoever knowingly uses a forged instrument shall be punished by the penalty prescribed for the crime of forgery as the case may be.

Whoever uses or unjustifiably benefits from a genuine instrument in the name of another person shall be punished by the same penalty, as the case may be.

Article (223)

Provisions contained in this section shall not apply to cases of forgery provided for in special punitive laws.

Article (279)

Anyone charged with preservation of a stamp placed in accordance with a judicial or administrative order, and or causes by his negligence, any of the crimes mentioned in the preceding two Articles, shall be punished by detention for a period not exceeding six months and by a fine not exceeding five thousand Dirhams, or by one of these two penalties.

Article (312)

Detention and a fine, or one of these two penalties shall be imposed upon any one who commits any of the following crimes:

1. Abuse of any sacred or holy Islamic rites.
2. Blaspheming any of the divine recognized religions.
3. Condoning or encouraging sin, publicizing it, or acting in a manner that tempts others to commit such sins.
4. Knowingly eating pork by Muslims.

If any of such crimes is committed publicly, the penalty shall be detention for at least one year, or a fine.

Article (315)

Whoever profanes any of the sacred beliefs or rites in the other religions, so far as such sacred beliefs and rites are respected according to the teachings of Islamic Law, shall be punished by detention and by a fine or by either of these two penalties.

Article (319)

Whoever resists or defames the fundamental principles or teachings of the Islamic Religion or what is essentially known of its doctrines or vilifies such a religion, practices missionary work in favor of another religion, preaches for a sect or ideology which envisages any of the said matters, or tempts others to accept such ideologies or circulates such beliefs, shall be punished by imprisonment for a period not exceeding five years.

Article (352)

Whoever threatens another person to commit a crime against his life or property or against the life or property of another person, or to disclose matters which compromise his honor or modesty in cases other than those mentioned in the preceding Article, shall be punished by detention.

Article (353)

Whoever threatens by words, deeds or signs, in writing or verbally, or indirectly through another person, in cases other than those mentioned in the two preceding Articles, shall be punished by detention for a period not exceeding one year or by a fine not exceeding ten thousand Dirhams.

Article (361)

Whoever publicly appeals, sings, or engages in lewd speech, and whoever seduces others publicly into debauchery in any manner whatsoever, shall be punished by

detention for at most six months and by a fine not exceeding five thousand Dirhams, or by either of these two penalties.

Article (362)

The penalty provided for in the preceding Article shall apply to any one who manufactures, imports, exports, possesses, acquires or transports items with the intention of investing distributing or displaying to others writings, drawings, pictures, films, symbols or other matters if they are prejudicial to public morals.

The same penalty shall apply to any one who advertises any of the above mentioned things.

Article (363)

Whoever entices a male or female under eighteen years of age, by any means into committing debauchery or prostitution, or who assists them in such an act, shall be punished by detention for at least two years, and a fine.

Article (372)

Whoever attributes to another person, by any means of publicity, an incident which makes him liable to punishment or contempt, shall be punished by detention for a period not exceeding two years or by a fine not exceeding twenty thousand Dirhams.

Punishment by detention and a fine or by either of these two penalties shall be applied if the libel is committed against a public official or one who is in charge of a public service, during, in respect of, or on the occasion of performing the duties or public services assigned to him, or if the libel affects the honor or injuries the reputation of families, or if it is observed that the libel is intended to achieve an illicit purpose.

If libel is committed by means of a publication in any of the newspapers or other printed media, it shall be considered an aggravating circumstance

Article (373)

Detention for a period not exceeding one year or a fine not exceeding ten thousand Dirhams shall be imposed upon anyone who, by any means of publicity, disgraces the honor or the modesty of another person without attributing any particular act to the defamed party.

Detention for a period not exceeding two years and a fine not exceeding twenty thousand Dirhams, or either of these two penalties, shall apply if a public official or one who is in charge of a public service has been abused during, because of, or on the occasion of performing his duty or public service, if the abuse affects the honor or injures the reputation of families, or if it is noticed that the abuse is intended to achieve an illegal purpose. However, if the abuse is published in any newspaper or printed media, it shall be considered an aggravated case.

Article (374)

Punishment by detention for a period not exceeding six months or by a fine not exceeding five thousand Dirhams shall apply if slander or abuse is transmitted by telephone, or face to face with the victim and in the presence of a third party.

Punishment by a fine not exceeding five thousand Dirhams shall be imposed if slander or abuse occurs face to face with the victim alone without the presence of a third party.

It shall be considered an aggravated case, if libel or abuse is committed in any of the cases mentioned in the preceding two paragraphs, against a public official or one who is in charge of a public service during, because of or on the occasion of performing the duty or public service, if it affects the honor or injures the reputation of families, or if it is noticed that it achieves an illicit purpose.

Article (379)

Punishment by detention for a period of not less than one year and by a fine of not less than twenty thousand Dirhams, or by either of these two penalties, shall apply to any one who is entrusted with a secret by virtue of his profession, trade, position or art and who discloses it in cases other than those lawfully permitted, or if he uses such a secret for his own private benefit or for the benefit of another person, unless the person concerned permits the disclosure or use of such a secret.

A penalty of imprisonment for a period not exceeding five years shall apply to a culprit who is a public official or in charge of a public service, and has been entrusted with the secret during, because of or on the occasion of the performance of his duty or service

Article (381)

If infliction of a doctrinal penalty for theft becomes impossible, the culprit shall be punished by corporal chastisement according to the characterization of the crime, subject to the provisions of this law.

Article (399)

Detention or a tine shall be imposed upon any one who seizes, for himself or for another, a movable property, or obtains a document or signature thereon, cancellation or destruction thereof or amendment thereto by fraudulent means, or by assuming a false name or capacity, where such an act leads to deception of a victim and leads him to surrender. The same punishment shall apply to any one who disposes of real estate or movable property knowing that such a property is not owned by him or that he has no right to dispose thereof, or if he disposes of a thing knowing that it has been previously disposed of or contracted upon, provided that such acts cause damage to a third party. If the subject of a crime is a property or a bond which belongs to the State or to any of the authorities indicated in Article (5), it shall be considered an aggravating circumstance.

The attempt of an act shall be punished by detention for a period not exceeding two years or by a fine not exceeding twenty thousand Dirhams. However, when a recidivist is sentenced to a penalty of detention for a period of one or more years, a maximum period of two years' police surveillance may be awarded to him, provided that such surveillance not exceed the sentence inflicted upon him.

Article (424)

Detention for a maximum period of one year and a fine not exceeding ten thousand Dirhams, or by one of these two penalties shall be imposed upon any one who destroys or damages property owned by another, whether movable or immovable, and renders it unfit for use or impairs such a property in any other manner.

A penalty of detention shall apply if the crime results in disruption of a public utility or facility, or if such a crime exposes the life, security, or health of people to danger.

A penalty of imprisonment for a maximum period of five years shall apply if the crime is committed by a gang of at least three persons.

PENAL CODE OF JAPAN AFTER AMENDED IN 1987, RELATING TO COMPUTER CRIME.

Article 1 - Crimes within Japan

1. This Code shall apply to every person who commits a crime within the territory of Japan.
2. The provision of the preceding paragraph shall also apply to a person who commits a crime on board a Japanese vessel and or a Japanese aircraft outside the territory of Japan.

Article 2 - Crimes outside Japan

This Code shall apply to every person who commits any of following crimes outside the territory of Japan:

(1)-(4) omitted.

(5) Crimes specified in Article 154, 155, 157, 158 and 161bis.

(6) Crimes specified in Article 163bis through 163quint.

(7)-(8) omitted.

Article 7^{bis} – Definitions

The term "electromagnetic record" used in this Code shall mean the record made by any electronic method, magnetic method or other methods unrecognizable with human perception and provided for the use of data processing in computer system.

Article 155 (Counterfeiting of Official Documents)

1. A person who, for the purpose of uttering, counterfeits with the seal or signature of a public office or a public officer, a document or drawing to be made by a public office or a public officer, or counterfeits, with a counterfeited seal or signature of such public office or public officer, a document or drawing to be made by a public office or a public officer, shall be punished by imprisonment with work for not less than 1 year but not more than 10 years.
2. The same shall apply to a person who alters a document or drawing bearing the seal or signature of a public office or a public officer.
3. Except for the cases provided for in the preceding two paragraphs, a person who counterfeits a document or drawing to be made by a public office or a public officer or who alters a document or drawing which has been made by a public office or a public officer shall be punished by imprisonment with work for not more than 3years or a fine of not more than 200,000 yen.

Article 156 (Making of False Official Documents)

A public officer who, in connection with his/her official duty, makes a false official document or drawing, or alters an official document or drawing, for the purpose of uttering, shall be dealt with in the same manner as prescribed for in the preceding two Articles, depending on whether or not the document bears a seal or signature.

Article 157 (False Entries in the Original of Notarized Deeds)

1. A person, who makes a false statement before a public officer and thereby causes the official to make a false entry in the original of a notarized deed, such as the

registry or family registry, relating to rights or duties or to create a false record on the electromagnetic record to be used as the original of a notarized deed relating to rights or duties, shall be punished by imprisonment with work for not more than 5 years or a fine of not more than 500,000 yen.

2. A person, who makes a false statement before a public officer and thereby causes the official to make a false entry in a license, permit or passport, shall be punished by imprisonment with work for not more than 1 year or a fine of not more than 200,000 yen.
3. An attempt of the crimes proscribed under the preceding two paragraphs shall be punished.

Article 158 (Uttering of Counterfeit Official Documents)

1. A person, who utters a document or drawing prescribed for in the preceding four Articles or provides the electromagnetic record prescribed for in paragraph 1 of the preceding Article for use as the original of a notarized deed, shall be punished by the same penalty as a person who counterfeits or alters a document or drawing, makes a false document or drawing, or causes a false entry or record to be made.
2. An attempt of the crimes proscribed under the preceding paragraph shall be punished.

Article 159 (Counterfeiting of Private Documents)

1. A person who, for the purpose of uttering, counterfeits, with the use of a seal or signature of another, a document or drawing relating to rights, duties or certification of facts or counterfeits a document or drawing relating to rights, duties or certification of facts with the use of a counterfeit seal or signature of another, shall be punished by imprisonment with work for not less than 3 months but not more than 5 years.
2. The same shall apply to a person who alters a document or drawing bearing the seal or signature of another and relating to rights, duties or certification of facts.
3. Except for the cases provided in the preceding two paragraphs, a person who counterfeits or alters a document or picture relating to rights, duties or certification of facts shall be punished by imprisonment with work for not more than 1 year or a fine of not more than 100,000 yen.

Article 160 (Falsifying Medical Certificates)

When a physician makes a false entry in a medical certificate, an autopsy report or a death certificate to be submitted to a public office, imprisonment without work for not more than 3 years or a fine of not more than 300,000 yen shall be imposed.

Article 161 (Uttering of Counterfeit Private Documents)

1. A person who utters a document or drawing prescribed for in the preceding two Articles shall be punished by the same penalty as a person who counterfeits or alters a document or drawing or makes a false enter.
2. An attempt of the crime proscribed under the preceding paragraph shall be punished.

Article 161bis - Illegal production and use of an electromagnetic record

1. Any person who with the intention of misleading any business management of others, illegally produces such an electromagnetic record relating to legal right, duty

of certification of a fact as to be provided for the use of the business management shall be punished with penal servitude for not more than 5 years or a fine form of not more than 500,000 yen.

2. The crime under the preceding paragraph involved in the electromagnetic record to be made by public offices officers shall be punished with penal servitude for not more than 10 years or a fine of not more than 1,000,000 yen.
3. Any person who with the intention of paragraph 1, provides such an electromagnetic record which is produced illegally and relating to legal right, duty of certification of a fact as to be provided for the use of the business management shall be punished with the same penalty as person who illegally makes the electromagnetic record.
4. Any person who attempts to commit any crimes set forth in preceding paragraph shall be punishable.

Article 163bis - Illegal production and use of an electromagnetic record on payment card

1. Any person who with the intention of misleading any business management of others, illegally produces such an electromagnetic record as to be provided for the use of the business management which consists credit card or other similar payment card for any fee or charge shall be punished with penal servitude for not more than 10 years or a fine of not more than 1,000,000 yen. Any person who illegally produces such an electromagnetic record as to be provided for the use of debit card for withdrawal shall be same.
2. Any person who with the intention of paragraph 1 provides such an electromagnetic record as to be provided for the use of the business management shall be punished with the same penalty of paragraph 1.
3. Any person who with the intention of paragraph 1, transfers, lends or imports a card which has an electromagnetic record illegally produced set forth in paragraph 1 shall be punishable with the same penalty of paragraph 1.

Article 163ter - Illegal holding of an electromagnetic record on payment card

Any person who with the intention of paragraph 1 of previous Article, holds such a card set forth in paragraph 3 of previous article shall be punished with penal servitude for not more than 5 years or a fine of not more than 500,000 yen.

Article 163^{quater} - Preparation of illegal production of the electromagnetic records of the cards for payment

1. Any person who has, for the purpose of using for the criminal acts under Article 163bis paragraph 1, obtained the data of electromagnetic records under the said paragraph shall be punished with penal servitude for not more than 3 years or a fine of not more than 500,000 yen. The same shall also apply to the person who has provided such data with recognition of the circumstance.
2. The same shall also apply as paragraph 1 to the person who has stored the data of electromagnetic records under Article 163bis paragraph 1 which are obtained illegally for the purpose of criminal acts under preceding paragraph.
3. The same shall also apply as paragraph 1 to the person who has prepared any instruments and materials for the purpose of the criminal acts under said paragraph.

Article 163^{quint}- Attempt

Attempts of crimes provided in Article 163bis and paragraph 1 of the preceding Article shall be punished.

.

Article 234bis - Interference with business transaction by computer system

Any person who intentionally and knowingly, illegally, causes disruption or interference with regular execution of valid performance of computer system which is being used or intended to be used for business transactions of others, or causes executions which are contrary to the proper use or purposes of such computer system, by destruction of such computer system or electromagnetic record which is being used or intended to use in such computer system, by introducing false information or wrong instructions into such computer system, or by the other similar means, and causes interference with business transactions of others shall be punished with penal servitude for not more than 5 years or be fined not more than 100,000 yen.

Article 246bis - Computer Fraud

Any person who intentionally and knowingly, illegally, obtain unlawful profit or cause to obtain unlawful profit to any others, by introducing false information or wrong instructions into computer system which is being used or intended to be used for business transactions of others, by producing a false electromagnetic record relating to take, loss or change of property of others, or by using such false electromagnetic record on any business transactions, shall punished with penal servitude for not more than 5 years.

Article 250 Attempt to commit fraud or threatening

Any person who attempts to commit any crimes as set forth in this chapter shall be punishable.

Article 258 - Destruction of official electromagnetic records

Any person who destroys any documents or electromagnetic record which ought to be used at a State office shall be punished with penal servitude for more than 3 months and not more than 5 years.

Article 259 - Destruction of private electromagnetic record

Any person who destroys any documents or electromagnetic record relating to take, loss or change of property of others shall be punished with penal servitude for not more than 5 years.

Article 264 – Prosecution

Anyone who commits any crimes as set forth in Article 259 or Article 261 shall not be prosecuted without any accusation by victim.

THE FEDERAL LAW NO. (2) OF 2006 ON
From the website of The United Arab Emirates Computer Emergency Response Team.

THE PREVENTION OF INFORMATION TECHNOLOGY CRIMES

Article (1)

Definitions

The following words and expressions shall have meaning set out opposite unless the context shall require otherwise:

The State/ UAE	The United Arab Emirates
Electronic Information	Means any information stored, processed, generated and transmitted by an information technology device in the form of text, images, sounds, numbers, letters, codes, signs or otherwise
Information Program	A set of information, instructions and orders executable by an information technology device and designed to accomplish a specific task
Electronic Information System	A group of software and devices for processing and managing electronic data, information, messages or otherwise
The Information Network/ the Internet	A data communications system that interconnects information technology devices
Electronic Document	A record or document that is created, stored, generated, copied, sent, communicated or received by electronic means, on a tangible medium or any other Electronic medium and is retrievable in perceivable form
Website	Data access point on the Internet
Information technology device	An electronic, magnetic, optical, electrochemical or other device used to process information and perform logical and arithmetic operations or storage functions, including any connected or directly related facility which enables the device to store information or communication
Government Data	The data pertaining to the Federal Government, local governments and federal and local public entities and corporations

Article (2)

1. Any intentional act whereby a person unlawfully gains access to a website or Information System by logging onto the website or system or breaking through a security measure carries imprisonment and a fine or either
2. If such act results in the deletion, erasure, destruction, disclosure, damaging, alteration or republication of data or information, the punishment shall be imprisonment for a term of at least 6 months and a fine or either
3. If the data or information is personal, the punishment shall be imprisonment for a term of at least 1 year and a fine of not less than AED 10,000 or either

Article (3)

A person who commits or facilitates the commission of any of the offences defined in Sub-Article 2-2 of this Law in the course or by reason of his duties shall be liable to imprisonment for a term of not less than 1 year and a fine of not less than AED 20,000 or either.

Article (4)

The penalty shall be temporary detention for anyone who forges a document of the federal or local government or federal or local public entity or corporation that is legally recognized in an Information System.

The penalty shall be imprisonment and a fine or either for forging any other document with intent to injure.

The penalty prescribed for forgery applies, as appropriate, in the case of anyone who knowingly uses a forged document.

Article (5)

A person who in any way hinders or delays access to a service, system, program or database through the Internet or an information technology device shall be liable to imprisonment and a fine or either.

Article (6)

A person who uses the Internet or an information technology device in order to disable, disrupt, destroy, wipe out, delete, damage, or modify programs, data or information on the Internet or an information technology device shall be liable to temporary detention and a fine of not less than AED 50,000 or either.

Article (7)

Anyone procuring, facilitating or enabling the modification or destruction of medical examination, diagnosis, treatment or health records through the Internet or an information technology device shall be liable to temporary detention or imprisonment.

Article (8)

Anyone who intentionally and unlawfully eavesdrops, or receives or intercepts communication transmitted across the Internet or an information technology device shall be liable to imprisonment and a fine or either.

Article (9)

Anyone who uses the Internet or an information technology device to threaten or blackmail another to act or not act shall be liable to imprisonment for up to 2 years and a fine not exceeding AED 50,000 or either. If threat is used to induce the commission of a felony or cause defamation, the penalty shall be imprisonment for up to 10 years.

Article (10)

Anyone who through the Internet or an information technology device appropriates to himself or to another moveable property or procures a deed or signature upon deed, using deception, a false name or impersonation with intent to defraud the victim shall be liable to imprisonment for a term of at least 1 year and fine of at least AED 30,000 or either.

Article (11)

Anyone who uses the Internet or an information technology device to unlawfully access the number or details of a credit card or other electronic card shall be liable to imprisonment and a fine. If the offence is committed with intent to acquire the property

or avail of the services of another the penalty is imprisonment for a period of at least 6 months and a fine or either. If the property of another is appropriated for the account of the perpetrator or someone else the penalty is imprisonment for at least 1 year and a fine of at least AED 30,000 or either.

Article (12)

Anyone who produces, arranges, sends or stores with intent of using, circulating or offering, through the Internet or an information technology device, information that is contrary to public morals or operates a venue for such purpose shall be liable to imprisonment and a fine or either.

If the act is committed against a minor, the penalty shall be imprisonment for a period of at least 6 months and a fine of not less than AED 30,000.

Article (13)

The penalty shall be imprisonment and a fine for whoever incites lures or assists a male or female into committing an act of prostitution or fornication by means of the Internet or an information technology device.

If the victim is a minor, the penalty shall be imprisonment for at least 5 years and a fine.

Article (14)

A person who unlawfully login to an Internet website in order to change, delete, destroy, or modify its design or take over its address shall be liable to imprisonment and a fine or either.

Article (15)

The penalty of imprisonment and a fine or either applies to whoever commits any of the following offences through the Internet or an information technology device:

1. Abuse of an Islamic holy shrine or ritual
2. Abuse of a holy shrine or ritual of any other religion where such shrine or ritual is protected under Islamic Sharia
3. Defamation of any of the divine religions
4. Glorification, incitement or promotion of wrongdoing

The penalty shall be imprisonment for up to 7 years for an offence involving opposition to Islam or injury to the tenets and principles of Islam, opposition or injury to the established practices of Islam, prejudice to Islam, the breaching of a religion other than Islam or the propagation, advocacy or promotion of any discipline or idea of such nature.

Article (16)

A person who violates family principles and values or publishes news or pictures in violation of the privacy of an individual's private or family life, even if true, through the Internet or an information technology device, shall be liable to imprisonment for at least 1 year and a fine of at least AED 50,000 or either.

Article (17)

A person who set ups a website or publishes information on the Internet or an information technology device for the purpose of conducting or facilitating human trafficking shall be liable to temporary detention.

Article (18)

A person who sets up a website or publishes information on the Internet or an information technology device for the purpose of selling or facilitating the trade of narcotics, mind altering substances and the like in other than legally prescribed circumstances shall be liable to temporary detention.

Article (19)

Subject to the provisions of the money laundering law, the penalty shall be imprisonment for up to 7 years and a fine of not less than AED 30,000 and not more than AED 200,000 for whoever transfers or moves dirty money or conceals the illegal source of such money or knowingly uses, acquires or possesses money derived from an illegal source or knowingly transfers resources or property of illegal origin through the Internet or an information technology device with intent to make the money appear legal or sets up or publishes information on a website in order to commit any such acts.

Article (20)

A person who sets up a website or publishes information on the Internet or an information technology device for a group engaged in facilitating and promoting programs and ideas contrary to public order and morals shall be liable to imprisonment for up to 5 years.

Article (21)

The penalty shall be imprisonment for up to 5 years for whoever sets up a website or publishes information on the Internet or an information technology device for a terrorist group using pseudonyms to facilitate contact with its leaders or members, promote its ideas, provide financing to the group or publish know how related to the manufacture of incendiary, explosive and other devices used in terrorist activities.

Article (22)

The penalty shall be imprisonment for whoever unlawfully accesses a website or system, directly or through the Internet or an information technology device, for the purpose of obtaining Government data or information that is confidential in nature or confidential pursuant to directives.

If data or information so accessed is deleted, damaged, destroyed or disclosed, the penalty shall be imprisonment for at least 5 years.

This article applies to data and information belonging to financial, commercial and economic institutions.

Article (23)

A person who incites, aids, or conspires with another person to commit any of the offences described in this Law where the offence occurs as a result of such incitement, aid or conspiracy shall be liable to the same penalty.

Article (24)

Without prejudice to the rights of bona fide third parties, the court shall in all cases order the confiscation of the equipment, software, and devices used in the commission of any of the offences stipulated in this Law or the proceeds resulting therefrom and make a closure order which closes the shop or venue at which the illegal activities are carried out-with the knowledge of the owner altogether for such period as the court shall deem appropriate.

Article (25)

In addition to the penalties prescribed in this Law, the court shall order the foreign national deported after serving his jail term in accordance with this Law.

Article (26)

The penalties for violators of this Law will be subject to severer punishments stipulated by the Penal Code or any other law.

Article (27)

Employees appointed by the Minister of Justice, Islamic Affairs & Awqaf shall act as law enforcement officers for the purpose of detecting and establishing offences which are committed in violation of this Law. The local authorities in the individual Emirates shall extend to those employees the assistance required to enable them to carry out their duties.

Article (28)

All provisions contravening the provisions of this Law are hereby repealed.

Article (29)

This Law shall be published in the Official Gazette.