Scientific Research Publishing

Journal of Information Security, 2017, 8, 8-22
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Comparative Study between the Jordanian and Omani Digital Crimes Law

Ali Abu Romman

Department of Investigation and Law Enforcement, Jordan Integrity and Anti-Corruption Commission, Amman, Jordan
Email: ali.aburomman@jiacc.gov.jo

How to cite this paper: Romman, A.A. (2017) A Comparative Study between the Jordanian and Omani Digital Crimes Law. *Journal of Information Security*, **8**, 8-22.
http://dx.doi.org/10.4236/jis.2017.81002

Received: November 30, 2016
Accepted: December 11, 2016
Published: December 14, 2016

Abstract

The nature of crime has dramatically changed after the revolution of the new digital era. It is no longer based on violence but on the criminal computer abilities and technical expertise. This paper presents a comprehensive comparison between the Jordanian digital law 2015 and the Omani information technology digital crime law 2010. The results of this study indicate that the Jordanian Digital law requires some enhancements in order to cope with the trends of the ever-changing nature of the digital crimes.

Keywords

Jordan, Digital, Crime, Law & Oman

1. Introduction

The transformation of civilization and progress that swept the world in the modern era has made a significant change in the quality of crimes and criminals, and contributed to the evolution of the concept of crime to traverse geographical boundaries. After crimes were mostly based on violence, cruelty and related accessories, what now dominates is a list of crimes based on mental potency, and employing intellectual cleverness and technical expertise in the commission of crimes.

Information technology is considered one of the results of this cultural transformation and scientific progress in the field of networks and computers that swept the world to make it borderless and unlimited. The world became an enormous and diverse place after information technology marched in all its passages a place that contributed to the production and development of many criminal behaviors that affected the lives of individuals and society gravely.

Through this research paper, I will try to identify this newly created kind of crime, namely, digital crimes and the laws governing them in the Hashemite

Kingdom of Jordan and Oman, as well as compare between these laws in many ways.

Information systems crimes began in the sixties when they were in the form of physical damage to computer systems and sometimes in the sabotage of external phone lines, but in the seventies information system crime's changes began when "Neil Jerry" used the Dumpster Diving method of retrieving publications from the trash from the company (PT & T) in Los Angeles. After years of collecting information, he was able to impersonate the company's staff on the phone [1].

In the eighties and nineties, some professionals became famous like Kevin David Mitnick, who was one of the first to use social engineering, Crack, to analyze the information systems.

Later in the nineties a few non-proliferation crimes heightened, such as (Extortion), the development and spreading of viruses, harmful files, Trojans of all kinds (viruses & Trojans) and crimes of "Credit Card Fraud", which are classified under identity theft, as well as the manifestation of the "Denial of Service" crime, which is one of the most dangerous forms of information systems crimes.

Data diddling crimes started with the beginning of processing data electronically, this crime is considered one of the most common crimes. It modifies data illegally in unauthorized ways before or during the input process, or before the output process [1].

Keeping in mind that the United Kingdom's cyber laws are one of the best laws in the world, in 2010, the United Kingdom estimated a total loss of 27 billion pounds due to information system crimes. 9.6 billion pounds of that was related to intellectual property rights.

The United Kingdom's losses on the impact of information systems crimes in 2010 were estimated of more than 27 Billion pounds, of which 9.6 Bellion pounds were related to intellectual property rights, noting that the United Kingdom's cyber law is one of the best laws in the world [2]. Nowadays, almost 10 million emails are sent every second. The statistical average of "Spam mail" is almost 73% [3].

Public security information statistics reported that the number of crimes in the Kingdom of Jordan systems crimes during 2014 reached 2305 crimes. These crimes included theft and breach of websites, manipulating electronic data, stealing and robbing banks electronically and crimes of sexual abuse of children [4].

The increase of crimes' commission through modern electronic communication means demanded attention to such crimes from competent security authorities, the need to resort to legislative legal amendments to keep pace, and the increasing of staff, which tracks and deals with complaints of such crimes.

According to the unit of electronic crimes in the CID in public security, the number of communication crimes that was dealt with last year reached 75 crimes, while in the year of 2014 there were 58 crimes. They also dealt with 687 crimes of impersonation, for the purposes of defamation last year, and 481 crimes of the same kind in 2014.

The unit dealt with 680 crimes of electronic threat and extortion in 2013, while the number reached 536 in 2014. Financial fraud cases were 100 cases in 2013, and in 2014, they were 113 crimes.

Furthermore, in 2013, 64 crimes of email theft were dealt with while in 2014, they amounted to 89 crimes, in addition to six "theft of data" crimes in 2013, versus 36 in 2014, as well as 18 crime of "breaching web sites".

2. Digital Crime

2.1. Definition

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the custom paper size the definition of crime and determination of its elements and characteristics is of great importance to law enforcers and to judicial police who are trying to find a relationship between these elements and the person accused.

Some researchers first defined the crime of information systems as a traditional crime committed in a new form, but then some crimes that surfaced invalidated this definition, such as crack crimes, which are dependent on the technological development and cannot be committed in the non-digital environment.

Jurisprudence then defined cybercrimes as crimes that know no geographical boundaries and that are committed with a computer, through the Internet, by someone particularly familiar with both internet and computers.

The author do not agree with this definition, because for instance, (Script Kiddies), who use scripts or programs that are, developed to attacks information systems, do not have to be very familiar with computers and internet, but at the same time, the use of these texts and programs is a crime punishable by law if it aims to harm others.

Therefore, it is difficult for the jurisprudence to agree on one definition for information crime, probably due to its close relation with information technology that is characterized as constantly renewed, as well as the difficulty of achieving international cooperation in controlling it and some other reasons related to the difference between them and conventional crime, which will be described throughout this paper.

System, technology, information, computer, cybercrime or electronic and cyber technology can be defined as illegal conduct paired with criminal intent and is punishable by law, since information system may be used as a tool to commit the crime, or may target that system itself. The author will explain when and how information system is the target of the crime.

2.2. Properties

Perpetrators might use the modern electronic method, because of the many reasons that distinguish them from ordinary traditional crimes: their financial and physical requirements are fewer; the physical presence of the offender is not required. Encryption is a much easier disguised than masks, and having an eye-

witness for the crime is very rare, besides this kind of crime is a cross-border one that perpetrators do not need a passport or tickets to commit. Finally, disposing of criminal evidence does not require sophisticated computer skills. As well as the fact that retrieval is sometimes almost impossible, especially if the crime scene used is cloud computing [5].

2.3. Differences

There are differences between cybercrime, whether traditional or innovative, be it in cyber or electronic crimes the crime scene or facts are usually a computer, website or database for example, which is why researches often consider this kind of crime scene non-existent due to its unmaterialistic presence differing from the traditional crime scene.

In addition, the offender and the victim are not required to be in one place or in one country, unlike with ordinary crimes. This is where the author face the issue of international criminal laws and jurisdiction, which states than any offence or crime committed in the territory of its country is considered an act of crime against that country and is subject to its laws and regulations to deter the offender or stop him [6].

Being mainly linked to the rapid development of the digital and information technology, internet technology crimes or cybercrimes are scalable and innovative. New types of information system crimes are constantly surfacing with the ongoing development and advances of digital technology.

In cases of IT and cybercrimes the investigator has to come up with proof based on the analysis of certain computer devices using tools like Access Data Forensic Toolkit to extract and export files that can help provide tangible evidence of a crime being committed. For example, this method can be used to prove a computer device was used to send an electronic message. Unlike conventional crimes, where eyewitnesses would be brought in to prove that an actual crime or action has taken place.

During the procedures of the criminal investigation, there is a likelihood that the personal computer of the perpetrator has personal information on it that has nothing to do with the case, but can somehow be of high economic value. It is not logical to give permission randomly to judicial employees to enter and search places that contain or may contain information systems that were to commit a crime. It is certain that some of this information may be damaged if these tools were seized by non-specialists.

2.4. Legal Issues

In this fast-paced era where there is a constant development of information, information systems that are connected to cyberspace have become a necessity. Another important aspect of information systems is providing a solid legal infrastructure enabling the development of the times we live in. As for the reason that e-commerce, for example, would not be possible if legal infrastructure was not available, as well as the rapid spread of conducting and closing business,

agreements and contracts online replacing the traditional methods of business transactions.

On the other hand, the existence of this cyberspace has provided a new way of expressing crime tendencies in a civil, criminal, conventional and innovative ways, with the ability to commit these crimes on a limitless area of space as well as having endless victims. For this reason, the legislation of a special law for the digital environment must be created to ensure the safety and protection of good people using it as well as create trust and safety for the use of information technology. In addition, there should be laws for punishing those who abuse the use of information technology for criminal purposes.

The penal code states that no crime or punishment can be measured without a predefined law. For this reason, special laws for cybercrimes and information technology crimes were created due to the great difference between these crimes and traditional crimes in terms of situation, reasons, and properties.

In the third quarter of 2010, a temporary law was passed by Jordanian legislation to deal with cybercrimes and information technology crimes. In 2015, the previous law was modified and turned to a permanent law, which will be stated in the first section of this paper. Also, in 2011 an anti-cybercrime act was promulgated In Oman by royal decree number 12 which will be stated in the second section of this paper and will be compared to the Jordanian anti cybercrime act [7].

3. Compression between the Jordanian Digital Law and the Omani Information Technology Digital Crime Law

3.1. Definitions and Terminologies

Jordanian legislation did not impose a clear and comprehensive definition of digital crimes in Jordanian law, but only referred to the forms of digital crimes covered by the law of Jordanian electronic crimes for the year 2015, where Jordanian law covered some aspects of encroaching on the safety, confidentiality and availability of data and electronic information and computer systems, in addition to some forms of content crimes pertaining pornography and prostitution. The law also mentioned some forms of violations of credit cards, and the offenses of slander, libel, and derogation plus some affairs regarding the criminal investigation procedures.

Jordanian law addressed digital crimes when committed to the detriment of one of the foreign interests of the kingdom only through Article 12, where law stated the punishment without specifying the geographical boundaries' frameworks.

Omani legislation defined digital crime in an explicit definition as the scientific use of computing and electronics and communications for processing and distributing data and information in all its different forms, and defined digital crimes as the crimes stipulated in cyber security law promulgated by Royal Decree for the year 2011.

Omani law referred to forms of digital crime more than Jordanian law did. It

included maintaining safety, confidentiality and availability of data, electronic information and computer systems. As well as; the prevention of using any means of information technology in: forgery and digital fraud, infringement of credit cards, pornography and prostitution, assault on the sanctity of personal or family life, gambling and breach of public morality, threats of extortion, offending religious or public values, terrorism, illicit fund trading, human trafficking and human organs, arms and drugs, monuments and artifacts that are not authorized by law, infringement of copyright and related rights, and industrial property rights.

As well as the mentioning of some criminal investigation procedures, the Law explained that its provisions apply to digital crimes even if it was committed wholly or partially outside the Sultanate when it hurts one of its interests, or if the criminal result was achieved in its territory or was meant to be achieved there even if it did not materialize [8].

3.2. CIA in Legal Terms

Jordanian law, Article III, paragraph (a) states that any person who intentionally accesses any website or a computer system without a permit or in violation of, or exceeding that permit.

Penalty: imprisonment for no less than a week and no more than three months, or a fine of no less than 100 dinars and not exceeding 200 dinars, or both penalties.

Paragraph (b) of the same article, distinguishes between what is stated in section (a) and whether this entry is meant to cancel, delete, add, destruct, disclose, obscure, amend, modify , move or copy data or information. Or was it meant to discontinue or disrupt the work of an information system; change, cancel, or destroy a website and modify its contents or functions, and/or impersonate its attributes or owner.

Penalty: imprisonment for no less than three months and no more than one year or a fine of no less than 200 dinars and not exceeding 1000 dinars, or both penalties.

Paragraph (c) includes any person who intentionally accesses a website to change, cancel, or modify it, or destroy its contents or functions, and/or impersonate its attributes or owner.

Penalty: imprisonment for no less than three months and no more than one year or a fine of no less than 200 dinars and not exceeding 1000 dinars.

The Jordanian legislator incriminates this act in a more serious penalty than just access; however, did not place a stringent punishment when the information system contains data or personal information.

Omani law, in article III—incriminates three criminal acts, the first act is illegal access to websites and electronic systems. This crime is based on illegal entry with the intent to access a website or an information system.

Penalty: imprisonment for no less than a month and no more than six months, and a fine of no less than 100 OMR, not exceeding 500 OMR, or one of

these two penalties.

The second act is illegal remain, a person might find himself in an unauthorized information systems that he accessed by mistake, but remaining within that information system after discovering his mistake is not different from all unauthorized access in terms of criminalization, the criminal result is the unauthorized access to a none authorized system.

Penalty: Imprisonment for no less than six months and no more than one year and a fine of no less than 500 OMR and no more than 1000 OMR or either penalties.

The third act is to exceed authorized access, this situation happens, when access to the system is authorized, but it is used for other than its original purpose, or the time allowed is exceeded.

Penalty: Imprisonment for no less than one year and no more than three years, and a fine of no less than 1000 OMR and no more than 3000 OMR or either penalties.

The fourth article of Jordanian legislation emphasizes the third act, which is if a person commits the acts that are mentioned in Article III during the time of his work duties. The legislator should have integrated the two sections in one article rather than separating them, since the emphasis laid down in this article is the same emphasis laid down in article III.

Article IV also, was set to punish any person who intentionally accesses, publishes, or uses a program via the Internet or by using an information system in order to cancel, delete, add, destruct, disclose, obscure, amend, modify, change, move or copy data or information. Or enable others to access unauthorized date or information. As well as cases meant to disarrange, discontinue or disrupt the work of an information system or accessing it. Change, cancel, or destroy a website and modify its contents or functions, and/or impersonate its attribute or owner with no authorization or overriding the clearance.

Penalty: Imprisonment for no less than three months and no more than one year and a fine of no less than 200 dinar and no more than 1000 dinars.

This article did not criminalize the admission of anything other than the program.

Omani law, Article VI clearly states that access to the system by itself is not considered a crime unless it was done to obtain data or electronic information that are a government security in nature or under instructions. It is noted here that the legislature considered confidential data and electronic information related to banks and financial institutions in the same category as government data and confidential information in the scope of application of this article.

Sentence of paragraph (a): imprisonment for no less than one year but no more than three years and a fine of not less than 1000 OMR and no more than 3000 OMR or either sentences.

Sentence of paragraph (b): imprisonment for no less than three years but no more than ten years and a fine of not less than 3000 OMR and no more than 10,000 OMR.

Sentence of paragraph (c): electronic data and confidential information for banks and financial institutions are considered in the same role as government data and confidential information in the scope of application of this article.

The author find that the crime set forth in Article VII is not considered a crime by accessing the site alone, but when a change to the sites format, modification of its content, destruction, cancelation, or theft of the sites title intentionally occur then it is considered a crime.

Penalty: Imprisonment for no less than one month but not more than one year and a fine not less than 1000 OMR and no more than 3000 OMR or either penalties.

The offender must know and understand that he is not entitled to access this system, and that accessing the system is prohibited by the system's owner, but still commits this illegal act. Legislation also stipulates the condition of criminal behavior's intent to the purpose of changing the site's format, modifying its content, destroying, or cancelling it, or stealing the site's title.

The author note here that the Omani legislator did not distinguish between private sites and government sites. Despite the fact that most government sites offer electronic services to members of the community and therefore attacking these sites disables the interests of community members, which leads us to believe that it may have been better for the legislature to differentiate between the two cases.

Jordanian law, Article V incriminates anyone who intentionally obtains intercepts, taps, hinders, modifies or deletes any contents that are transmitted across networks or any information systems.

Penalty: imprisonment for no less than three months not exceeding one year or a fine of no less than 200 dinars and no more than 1000 dinars.

Jordanian legislator did not criminalize the disconnection of transmission, which represents the DoS crime, and did not set conditions regarding the nature or subjection of data and information, which are the subject of the crime, it might have been better for both Jordanian and Omani lawmakers to state varying penalties according to the nature of the data and information.

Article XII , section (a) specified if the access mentioned in Article (3) section (a) was intended to obtain data or information which are not available to the public, and could affect national security, foreign relations of the Kingdom, public safety or the national economy.

Penalty: imprisonment for no less than four months, and a fine of no less than 500 dinars but not more than 5000 dinars.

Paragraph (b) of the same article, distinguished between the acts stated in section (a) and whether the intent of this entry is to delete data or information, damage, destroy , alter, change, move, or copy them.

Penalty: punishment by temporary hard labor, and a fine of no less than 1000 dinars but not more than 5000 dinars.

With this conviction, the author notes that access is conditioned on the same terms set by the Omani law, which is access without authorization or in excess of

the permit. In addition, information that is not available to the public is considered confidential by nature or by issued instructions.

The legislator gave Article VIII the same kind of emphasis with cases of committing the acts set forth in Article III, pertaining unauthorized access. Article IV, which regards malware, article V, about obtaining, intercepting, or tapping contents, and the sixth article, pertaining data and information on credit cards and financial and banking transactions, because of taking advantage of a job or employment.

Omani legislator's application of Article IX was extensive, it incriminated the admission of anything that would cause any kind of the mentioned damages to the information system , information network or information technology device, this includes all kinds of hardware , software, or even information and data that might cause damage.

Penalty: Imprisonment for no less than one year and no more than three years, and a fine of no less than 3000 OMR, but no more than 10,000 OMR or either one of these penalties.

Article X by the Omani legislator exclusively incriminates DoS that uses any mean of information technology.

3.3. Abuse of Information Technology

The Jordanian law, Article IV was set to punish any person who intentionally accesses, publishes, or uses a program via the Internet or by using an information system in order to cancel, delete, add, destruct, disclose, obscure, amend, modify, change, move or copy data or information. Or enable others to access unauthorized date or information. And the cases meant to disarrange, discontinue or disrupt the work of an information system or accessing it, change, cancel, or destroy a website and modify its contents or functions, and/or impersonate its attribute or owner with no authorization or the overriding of clearance.

Penalty: Imprisonment for no less than three months or no more than one year and a fine of no less than 200 dinar and no more than 1000 dinars.

This article did not criminalize the admission of anything other than the program.

Omani law, Article XI incriminates anyone who uses the Internet or methods of information technology in the production, selling, purchasing, importing, distributing, displaying, or providing of: programs, materials, designed or adapted devices for the purposes of committing digital crimes, and/or passwords and symbols used to access information systems, or possesses such methods and programs to use in committing a digital crime.

Penalty: Imprisonment of no less than six months and no more than three years, and a fine of no less than 3000 OMR and no more than 15,000 OMR or either penalty.

Omani legislator assigned Article XI to incriminate providers of the mentioned tools in addition to the users of these tools who are called (Script Kiddies) giving both sides the same punishment.

3.4. Payment Cards Fraud

Jordanian law, Article VI assigned punishment for whoever obtains or uses data or information related to credit cards, financial transactions, or electronic banking illegally.

Penalty: imprisonment for no less than one year but no more than three years and a fine of no less than 500 dinars but no more than 2000 dinars.

Article VII incriminates anyone who executes any of the acts mentioned in articles (3), (4), (5) and (6) of this law. If acts are executed on an information system, website or an information network connected to transferring funds, providing payment services, clearing, settlement, or any of the banking services provided by banks and financial companies.

Punishment: temporary hard labor for no less than five years and a fine of no less than 5000 dinar and no more than 15,000 dinars.

Jordanian legislator stressed the punishment if the acts set forth in Article VII were executed on credit cards and everything related to it.

Through Article VI, Jordanian law had incriminated one branch, for one form of fraud, which is the theft of data or information regarding credit cards, which is one of the branches of (Credit card fraud).

The law only incriminated two cases in terms of credit cards through Article VI, the first case is intentional illegal access, through information systems, to data related to credit cards, or the use of financial transactions or electronic banking. The second case is intentional use, without a legitimate reason.

Omani law, Article XII is divided into three paragraphs as follows:

- Paragraph (a) Any person who uses information technology devices in the commission of a crime of information forgery, by changing the reality of data or electronic information in addition to deletion or replacement of information for the purpose of using them as trusted data or electronic information to be legally admissible in an information system, to achieve benefits for himself or others, or to harm someone else, shall be punished by imprisonment for a period of no less than one year, nor more than three years and a fine of no less than 1000 OMR and no more than 3000 OMR or either of these two penalties.
- Paragraph (b): If this data or electronic information described in paragraph "a" are related to the government, penalty shall be temporary imprisonment for no less than three years and no more than fifteen years, plus a fine of no less than 3000 OMR but no more than 50,000 OMR .
- Paragraph (c): anyone who uses counterfeit electronic information despite knowing they are forged shall be punished with the same penalties prescribed in the preceding two paragraphs, according to the case.

The author noted that the Omani legislator assigned strict punishment if the data and information are related to government because of the seriousness of the results of fraud.

Unfortunately, in spite of the seriousness of electronic fraud and the way it differs in concept, element, and characteristics from traditional crime of fraud , Jordanian legislator incriminated only one act related to electronic fraud

through Article IV of the digital crime's Act regarding changing a websites and impersonating it or its owner.

Article XIII can be divided into two paragraphs as follows

- Paragraph (a): anyone who adds, modifies, destroys, damages or deletes data or electronic information in an electronic information system, blocks data, interferes in a system's functions, or disrupts information technology device or software's or websites intentionally and illegally aiming to circumvent and causing harm to beneficiaries or users, to gain advantages for himself or someone else illegally shall be punished by imprisonment for no less than one year but no more than three years, and a fine of no less than 1000 OMR and no more than 3000 OMR or either penalties
- Paragraph (b): if the information system mentioned in paragraph (a) of the same article, is related to a special region of government, a bank, or a financial institution, the penalty shall be temporary imprisonment for no less than three years and no more than fifteen years, and a fine of no less than 3000 OMR but no more than 20,000 OMR.

Omani Digital Crimes' Law allocated this article to punish the perpetrators of circumvention of information systems crimes, Fraud or Scam. This article was formatted in a flexible and comprehensive way, it realized new fraud crimes such as (Email Spoofing), falsifying web pages (Phishing), (Auction Fraud), automatic transfer or redirecting course of data (Pharming), and other various forms of fraud. Strict punishments were assigned if the intended circumvent is used on an information system related to the government, a bank, or a financial institution.

Article XXVIII can be divided into three paragraphs as follows

- Paragraph (a): anyone who forgers a credit card for whatever means, synthesizes or makes devices or material to help the forgery of a card, seized, used, or gave out financial statements information, or helped someone to obtain that information. In addition to whoever uses of Internet or information technology devices to access financial data illegally, or accepts using a stolen credit card knowingly.

Penalty: imprisonment for no less than one month and no more than six months and a fine of no less than 500 OMR but not more than 1000 OMR or either penalties.

- Paragraph (b): If any of the acts set forth in paragraph (a) were committed to seize or facilitate the acquisition of money or whatever services offered by the card.

Penalty: Imprisonment for no less than six months and no more than one year and a fine of no less than 1000 OMR and no more than 5000 OMR or either penalties.

- Paragraph (c): if any of the money or services were seized.

Penalty: imprisonment for no less than one year and no more than three years and a fine of no less than 3000 OMR and no more than 10,000 OMR or either penalties.

The author note through this text, which the meaning of the word "synthesized" in the first paragraph, is exaggerated in making a device, because it did

not criminalize the acquisition of these devices or their selling.

3.5. Content Crime

Jordanian law, Article IX criminalized harmful content, which concerns pornography and prostitution as follows:

- Paragraph (a): Any person who intentionally sends or disseminates audible or visual information, through information systems or information networks, which includes anything related to pornography or sexual exploitation for those who did not complete the age of eighteen will be punished.

  Penalty: imprisonment for no less than three months and no more than one year and a fine of no less than 300 dinars and no more than 5000 dinars.
- Paragraph (b): Any person who intentionally uses an information system or information network to create, prepare, save, process, display, print, publish, or promote activities or acts of pornography for the purpose of influencing those who are not eighteen years of age, or the psychologically or mentally disabled, or directing and inciting them to commit a crime.

  Penalty: imprisonment for no less than two years and a fine of no less than 1000 dinars and not more than 5000 dinars.
- Paragraph (c) punishes any person who intentionally uses an information system or information network for the purposes of exploiting children under the age of eighteen or the disabled or mentally retarded, in prostitution or pornography.

  Penalty: temporary hard labor and a fine of no less than 5000 dinars and no more than 15,000 dinars.
- Article X criminalizes harmful content that consists of acts of prostitution by stipulating that anyone who intentionally uses the Internet or any information system, or sets up a website to facilitate or promote prostitution shall be punished.

  Penalty: imprisonment for no less than six months and a fine of no less than 300 dinars and no more than 5000 dinars.
- Article XI incriminates anyone who intentionally sends, forwards or publishes data or information, via the Internet, a website, or any information system, involving the defamation, libel, or demeaning of anyone.

  Penalty: imprisonment for no less than three months and a fine of no less than 100 dinars and no more than 2000 dinars.

  Omani law, Article XIV can be divided into three paragraphs as follows:
- Paragraph (a): Any person who uses the Internet or information technology devices for the production, displaying, distributing, providing, publishing, buying, selling, or importing of pornographic material unless it is for scientific or artistic authorized purposes.

  Penalty: imprisonment for no less than one month and no more than one year and a fine of no less than one hundred OMR and no more than one thousand OMR or one of these penalties.
- Paragraph (b): If the pornography contains a minor who is not eighteen years

of age yet, or the criminal act is directed towards them.

Penalty: Imprisonment for a period of no less than one year and no more than three years and a fine of no less than one thousand OMR and no more than five thousand OMR.

- Paragraph (c): Any person who uses the Internet or information technology devices for the possession of pornographic material of minors.

  Penalty: the same penalty listed in paragraph (b) applies to this act as well.

Omani legislator through article fourteen and its sub articles (a) (b) and (c) excluded the scientific and authorized technical purposes, and stressed punishment if the pornographic content in question has not completed eighteen or if this young adult was addressed by the content. The law also punished the act of possession of the materials of young adults with the same tough sentence.

Jordanian legislation has a different perspective than Omani legislation, in Article IX Jordanian legislator incriminated anyone who intentionally sent or disseminate through information systems or information networks any audible, legible, or visual works that include pornographic or are related to sexual exploitation to those who did not complete eighteen years of age. The legislator excluded the rest of the cases.

Omani legislation Article XV can be divided into two paragraphs:

- Paragraph (a): Any person who uses the Internet or information technology devices in enticing or seducing a male or a female to commit prostitution or debauchery, or helping them to do so.

  Penalty: temporary imprisonment for no less than three years and not exceeding five years and a fine of no less than 3000 OMR and not more than 5000 OMR.

- Paragraph (b) if the victim is a minor who has not completed eighteen.
- Penalty: temporary imprisonment for no less than five years and no more than ten years and a fine of no less than 5000 OMR and no more than 10,000 OMR.

Article XVI specializes in incriminating assault of individuals' privacy using information technology devices, while the Jordanian legislation in short did not incriminating any assault of individuals' privacy in digital crimes Act.

Jordanian law, Article XII, States that:

- Paragraph (a): incriminates whoever intentionally, violates or exceeds authorization, accesses Internet or an information system by any means in order to obtain data or information that is not available to the public, which might affect national security, foreign relations of the Kingdom, public safety, or the national economy.

  Penalty: imprisonment for no less than four months, and a fine of no less than 500 dinars but not more than 5000 dinars.

- Paragraph (b): If the entry referred to in paragraph (a) of this Article is intended to delete, damage, destroy, alter, change, move, copy or disclose such data or information.

  Penalty: temporary hard labor and a fine of no less than 1000 dinars and no more than 5000 dinars.

- Paragraph (c) Any person who intentionally accesses a website to find data that is unavailable to the public and might affect national security, foreign relations of the Kingdom, public safety, or the national economy will be punished.

  Penalty: imprisonment for no less than four months and fine of no less than 500 dinars.
- Paragraph (d): If the access mentioned in paragraph (c) of this article is meant to delete, damage, destroy, alter, change, move, or copy such data or information.

  Penalty: temporary hard labor and a fine of no less than 1000 dinars but no more than 5000 dinars.

Omani legislator singled article seventeen to criminalize many forms of content crimes and did not leave out gambling and breach of public morality by using technical means of information. It is clear that the Omani legislator tries to categorize most traditional crimes that could be applied in the digital environment under the title of content crimes.

Article nineteen states that anyone who uses the Internet or methods of information technology in the production, publication, distribution, purchasing, or possession of anything that would involve prejudice against religious values or public order will be punished.

Penalty: Imprisonment for no less than one month and no more than three years, and a fine of no less than 1000 OMR and no more than 3000 OMR or either one of these two penalties.

4. Recommendations for the Jordanian Law

This section introduced some of recommendations to be addressed in the Jordanian law:

Article XXI of the Omani law incriminated acts related to, illicit money and property, and criminalized the request to assist in money laundering; it also criminalized the dissemination of ways to do so, and punished the perpetrators of any such act in the same sentence. The Jordanian legislator did not mention this. In addition, the author noted that the Omani legislator incriminated human trafficking by means of information technology through one article, and incriminated trafficking human organs through another article, but Jordanian legislator did not regard any of that material in digital crimes act for the year 2015.

There is no article that criminalizes trafficking arms by means in the Jordanian law; In addition, there is no special article that criminalizes trafficking, selling and advertising drugs and substances, methods of deploying it, or facilitating the dealing in other than legally unauthorized circumstances by means of information technology in the Jordanian law.

Jordanian digital crime law did not protect any copy of rights for authors or owners, or neighboring rights, or industrial property rights. Nevertheless did not regulate the trafficking of antiquities or works of art. Also, did not protect any of the individuals' medical information.

5. Conclusions

Digital crime is different from traditional crime, being beyond temporal and spatial boundaries of any country prompts legislators to take into account the prescribing of regulatory provisions to set rules for dealing with these crimes and their implications.

This study presents the Jordanian and the Omani law in regard of digital crimes, and provides a detailed comparison study between the two laws.

References

[1] Kabay, M.E. (2008) A Brief History of Computer Crime. Norwich University, Northfield.

[2] Guitton, C. (2011) What Is the (Real) Cost of Cybercrime in the UK? www.kingsofwar.org.uk

[3] worldometers (2012) Real Time World Statistics. www.worldometers.info

[4] M86 Security Labs (2012) Spam Statistics. Available from www.m86security.com

[5] Watson Business Systems Ltd. (2007) A Guide to Computer Crime: Benefits to the Criminal. http://legal-dictionary.thefreedictionary.com/legal+practitionercomputer-crime/computercrime

[6] Bhasin, P. (2009) Need and Importance of Cyber Law. http://www.slideshare.net/poonambhasin33/need-and-importance-of-cyber-law?qid=00e2b56d-4091-4aab-90b4-2426fcca7b25&v=&b=&from_search=1

[7] Alhusenawe, A.J. (2009) Computer Crime and Internet. Yazouri, Jordan, 176-178.

[8] Al Ghafri, H.B.S. (2012) legal Information 2011-2012 Windows on Combating Cybercrimes Law. Hussein Ghaferi Blog. www.hussain-alghafri.blogspot.com