The Social Sciences 13 (6): 1194-1199, 2018
ISSN: 1818-5800

Legal Protection for e-Mail in the United Arab Emirates Law

Mohammad A. Alkrisheh
Department of Criminal Law, College of Law, Alain University of Science and Technology,
Abu Dhabi, United Arab Emirates

Abstract: e-Mail is the most important internet application and most commonly used as the primary means of communication between individuals around the world. In the light of the state's economic revolution and tremendous techniques sweeping the country in the recent years which seeks to establish the concept of e-Government practically, the UAE legislator is keen to report on criminal protection of e-Mail by issuing the Federal Law No. 5 for the year 2012 on combating cybercrimes. This research aims to demonstrate the effectiveness of the UAE law in combating against molestering e-Mail and protecting it from intrusion or espionage. To achieve that, the researcher is opted to check what e-Mail means and stating the advantages and disadvantages of it and then deals with all forms of penal protection of e-Mail in the UAE law as well as the general rules of responsibility for the crimes of assault on the e-Mail and finished the research by conclusion including the most important findings and recommendations.

Key words: Cybercrimes, e-Mail, Federal Law No. 5 of 2012 , combating cybercrimes, penal, protection

INTRODUCTION

The development of information technology and modern communication appears every day in new forms, making the electronic means as the nerve system of activating the e-Commerce. The most of financial and trade transactions have been made electronically and therefore, the traditional means suitable for modern contracts in electronic form is no longer available, so, the e-Mail has recently been used as a substitute for it, so as to comply with the nature of legal contracts in addition to contracts being made by the means of modern electronic devices.

In the light of economic revolution and tremendous techniques sweeping the country in recent years seeking to establish the concept of e-Government practically and with the expansion of its use and access to all segments of society including the list of users and large corporations which own sites for e-Commerce, the process of communication is conducted among them electronically and fully carried out relying on e-Mail, so, the requests, invoices and contracts are sent electronically as well as taking advantage of the multi-banking services provided by banks through the e-Mail as well as the use of e-Mail in the process of marketing, advertising or delivering of products destined for the consumer .

Under that, the crimes began to appear on the network and have increased through time and multiplied its forms, through penetrating e-Mail and accessing to information as well as destroying them or capturing them and then stealing the data or information or just tampering them by programmed viruses or other means.

The protection of e-mail will not be achieved unless by new legal rules facing this rapid development, so, we find that the UAE legislator has responded to this development by issuing Federal Law No. 5 for the year 2012 on combating cybercrimes. (Which was abolished under which the Federal Law No. 2 for the year 2006 on combating cybercrimes). The law included many materials that would provide legal protection for the privacy of what is published and circulated on the network as information, data and figures relating to credit card numbers and bank accounts data or any other means of electronic payment as well as all the use of any means of information technology by rigging, imitating or copying credit cards or any attack on e-Mail.

The importance of this research appears through the statement of criminal protection of e-Mail and the limits of these parameters and the scope of protection through clarifying the criminal acts that undermine it and the statement of the adequacy and effectiveness of the UAE legislator plan to criminalize any acts that impair the e-Mail.

What does the e-Mail mean?": The e-Mail appeared and spread throughout the world under the English label (e-Mail). The emergence of e-Mail is related to the American scientist (Ray Tomlinson) who is the real inventor of e-Mail. He designed a program on the internet

for writing letters called (send message) and the purpose of it is enabling workers to exchange messages with each other on the internet and then he invented another program called (Cypnet) allows the transfer of files from one computer to another and then this leads to merge the two programs into one program and the result of this merger is the birth of the e-Mail (Al-Awadi, 2005).

The development of the internet and the increasing numbers of users of e-Mail in the world is seen everywhere. So, we find that most of legislators have resorted to determine the meaning of the e-Mail as a necessary indispensable means in the field of electronic transactions. In order to identify the nature of e-Mail, the researcher has to make a definition of the e-Mail and then clarifying the most important advantages and disadvantages of it.

Definition of e-Mail: e-Mail can be described as "a way to allow the exchange of written messages between devices connected to the information network" (Abdul-Muti Khayal, 2001). Or that "those documents that are sent or received by postal mail communication system including a real character formality brief notes and attachments that follow it like word processing or any other documents sent to companion of the same message.

US law identified it relating to the electronic communications privacy issued in 1986 and standardized in the Encyclopedia of US Federal Laws e-Mail as "a means of communication by which private correspondence transmission over telephone lines network public or private and often the message is written on the computer, then electronically sent to the service supplier who is storing it in his computer for display where it is sent over telephone lines system to the consignee based computer" (The Electronic Communications Privacy Act of 1986 (ECPA), Pub.

The French law defined it relating to confidence in the digital economy issued on June 22, 2004 as "any message whether text or audio or accompanied by images or sounds sent over a public telecommunications network and stored at the network server or in the terminal of the addressee equipment to enable the latter to restore it (Manara, 1999).

In contrast, we find that the UAE legislator, under Article I of Law No. 5 of 2012 on combating cybercrimes is keen to make a definition of the nature of some of electronic terms. He defined electronic information as: any information that can be stored, processed, generated and transported by means of information technology and in particular, writing, images, sound, numbers, letters, symbols, signs and others. He defined information program: as a set of data, instructions and orders executable by means of information technology which is prepared to accomplish a specific task. The website as: a place that provide electronic information on the information network, including social networking and personal pages and blogs. With this definition, we find that the legislator clarified e-mail within the website considering it as a social networking site and personal homepages.

Advantages and disadvantages of e-mail: Email has several advantages that distinguish it from traditional mail (Khalid, 2010; Al-Awadhi, 2005), the most importantly is that it is an asynchronous communication way which means that there is not synchronization in the presence of people on both sides of contact because the caller via the internet and through e-Mail can contact and get what he wants from the opposite side whenever he wants without interfering in that person, so, sending messages via. e-Mail does not require the presence of the addressee and then having to call again in case of non-existence as the sender can let what he wanted conveyed by a text or graphic, through sound or image in part of the sender computer memory to a dedicated e-Mail box is called e-Mail box.

It is also a quick, easy and cheap communication mean which works all the time without leave, formal or informal holidays with the possibility of sending more than one message to more than one person at one time, that is the most popular internet application and that is most widely used by lawyers because it facilitates the exchange process files with anyone in the world of the attorney office. Consequently, the practice of law depends on the rapid transfer of information and documents across geographic space (Masur, 1999).

In spite of these advantages for e-Mail, there are some disadvantages as follows (Abdel-Fattah, 2004). Sending subversive and disturbing messages loaded with viruses cause harm to e-Mail and also the seriousness of the e-Mail is also reflected through that access from non-owner which leads to the disclosure of secrets in a manner that makes serious damage to his e-Mail as well as there is no real guarantee that the sent message has not been tampered with.

In addition to this, there is another disadvantage for example in some e-Mail messages, the signature of the owner does not appear, so that, his e-Mail related link cannot be known in advance or the way that the message will be received or prove receiving it if the other party communicated with him denies these messages.

But these defects do not impair the advantages of e-Mail in the presence of legal and technical (About technical protection methods (inscription) (Austin, 2003) means by which we protect e-mail from penetration and tinker and also protecting the private lives of individuals (About discrepancy in defining privacy expression, Warren and Brandeis, 1890).

Penal protection forms of e-Mail: The development of information technology and modern communication in every day new situations needs to be organized. This will not be achieved unless by new legal rules facing this rapid development. The UAE legislator has responded to this development and managed to add the penal protection for e-Mail by issuing the Federal Law No. 5 for the year 2012 for combating cybercrimes (According to which the Federal Law No. 2 for the year 2006 relating to combating cybercrimes has been cancelled). The law included many materials that would provide legal protection for the privacy of what is published and circulated on the information network and therefore, the researcher will discuss the penal protection forms for e-Mail which was described in the above-mentioned law as follows.

FIRST: ILLEGAL ACCESS TO E-MAIL

The text for this crime is cited in Article 2 of the Federal Law No. 5 for the year 2012 on combating cybercrimes, saying.

"Shall be punished by imprisonment and a fine not less than one hundred thousand dirhams and not in excess of three hundred thousand Dirhams or either of these two penalties whoever gains access to a website an electronic information system, computer network or information technology means without authorization or in excess of authorization or unlawfully remains therein".

The UAE legislator has stressed punishment in any event that will be resulted through the entry, staying into the system, cancelling, destruction, disclosure, damaging or modifying the data contained on the system for the availability of these circumstances there should be causal relationship between the act of illegal entry or staying in the system and also a relationship between erasing, modifying data or disabling the system from doing its work. But if this erasure or modification is due to other reasons that led to it like outside power or sudden event, the causal link will be interrupted and the culprit in this case will not be required for the aggravating act (It strengthened the punishment according to Article 3 of the same law. He made it a jail for a period no <1 year and a fine no <250.000 Dirham but not exceeds 1 million Dirham or by both penalties if crimes committed during doing his research. He made the crime as felony and made its penalty by temporary prison or a fine no <250.000 Dirham but not exceeds 1 million and 500.000 Dirham or by both penalties if entry was intended to get government data or information in financial, commercial or economic establishment according to the text in the material (4) of the same law).

It is noted that the UAE legislator does not emphasize on achieving a certain finding resulted from entry into the database or information systems by the offender and all what the legislator requires is that the entry has been conducted without permission or transcend permit or staying there illegally.

This crime is classified as dangerous crime in which the behavior is criminalized without stopping by a particular result because this crime is not a crime of damage that its punishment is linked to causing harm to the victim.

This is a form of intentional crimes, the form of the mental element in it is the general criminal intent connected by racist awareness and will where the offender should know that accessing the e-Mail to someone else without permission, transcending permit, staying there illegally or moving his free will to do this activity, so that, the offender is aware that his entry may be legitimate if it was done by accident or mistake or omission and in this case, this person is required to cut his connection and withdraw immediately but if remained, he should have punishment.

It must be noted here that the UAE legislator made the punishment for this crime by imprisonment and a fine and also the escalation of the punishment value because of losses arising from illegal entry but punished for embarking on offense by half penalty for the full offense (Article No. (40) of the United Arab Emirates combating cybercrimes Act.).

SECOND; ILLEGAL ENTRY FOR INTENTION OF TAMPERING WITH THE SITE OR E-MAIL

The legislator offended illegal entry intending to tamper with the data inside the e-Mail, so as to erase, change, delete some of them or re-deploy it. Article 5 of the combat information technology crimes penalize the other forms of illegal entry by saying.

"Shall be punished by imprisonment and by a fine not <100000 Dirhams and not in excess of 300000 Dirhams or either of these two penalties whoever gains access to a website without authorization intending to change its designs, delete, destroy, modify it or occupy its address".

The UAE legislator emphasized the punishment if the intent of the illegal entry is to obtain data affecting national security or the national economy by saying (Article No. 4 of the United Arab Emirates combating cybercrimes act).

Shall be punished by temporary imprisonment and a fine not <250000 dirhams and not in excess of one million five hundred thousand dirhams whoever accesses a website, electronic information system, computer network or information technology means without authorization whether such access is intended to obtain government data or confidential information relating to a financial, commercial or economical facility.

The punishment shall be imprisonment for a period of at least 5 years and a fine not<250000 dirhams and not in excess of 2 million dirhams, if these data or information were deleted, omitted, deteriorated, destructed, disclosed, altered, copied, published or re-published.

THIRD OFFENSE: FLOODING OR DISABLING E-MAIL MESSAGES

Article 10 of the aforementioned law referred to this crime as follows. Shall be punished by imprisonment for a period of at least 5 years and a fine not <5000 dirhams and not in excess of three million dirhams or either of these two penalties whoever willfully and without authorization runs a software on the computer network or an electronic information system or any information technology means and caused them to stop functioning or being impaired or resulted in crashing, deletion, omission, destruction or alteration of the program, system, website, data or information.

The punishment shall be imprisonment and a fine not in excess of 500000 dirhams or either of these two penalties if the result was not reached. The punishment shall be imprisonment and a fine or either of these two penalties for any deliberate act which intends to flood the electronic mail with messages causing it to stop functioning, inactivate it or destroy its contents.

Fourth offense; Obtaining a secret number, code or password for e-Mail without permission: UAE legislator emphasized the confidentiality of email data and offended obtaining a secret number, code or password for e-Mail without permission. The text of Article 14 of the law referred to this by saying.

Shall be punished by imprisonment and a fine not <200000 dirhams and not in excess of 500000 dirhams or either of these two penalties whoever obtains without legal right, a secret number, code, password or any other means to have access to an information technology means, website, electronic information system, computer network or electronic information.

Shall be punished with the same penalty whoever prepares, designs, produces, sells, buys, imports, displays for sale or make available any computer program or any information technology means or promotes by any means links to websites, computer program or any information technology means designed for the purposes of committing, facilitating or abetting in the commission of the crimes specified in this Decree-Law.

FIFTH OFFENSE: THE CRIME OF ASSAULT ON PRIVACY

The Constitution of the United Arab Emirates has referred to the privacy of the individual and the sanctity of his private life within its provisions. The text in Article 26 referred that personal freedom is guaranteed to all citizens. Article 31 said: everyone has the sanctity of postal, telegraphic correspondence or any other means of communication, emphasizing that viewing, controlling, stopping them is prohibited except in circumstances prescribed by law (Because seriousness of this right, Islam religion granted it the most importance. In Holy Quran, Surat Al-Noor, Verse (27): (O ye who believe! enter not houses other than your own, until ye have asked permission and saluted those in them: that is best for you, in order that ye may heed (what is seemly). And it is also included in Surat Al-Hujurat, Verse (12) (O ye who believe! Avoid suspicion as much (as possible): for suspicion in some cases is a sin: And spy not on each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it...But fear Allah: For Allah is Oft-Returning, Most Merciful. It is also included in the international ad for Human Rights in 1948 edition. Material (3) cited: (Everybody has the right in life, freedom and personal safety). The material (12) cited (Nobody is exposed to any kind of interference in his private life his family, his correspondences or any campaigns against his honor or reputation and ever body has the right protect the law against any interference or any campaign (Coleman, 2006; McArthur, 2001). The UAE legislator followed the same approach under the aforementioned law in Article 21 saying:

Shall be punished by imprisonment of a period of at least 6 months and a fine not <150000 dirhams and not in excess of 500000 dirhams or either of these two penalties whoever uses a computer network or and electronic information system or any information technology means for the invasion of privacy of another person in other than the cases allowed by the law and by any of the following ways:

- Eavesdropping, interception, recording, transferring, transmitting or disclosure of conversations or communications or audio or visual materials
- Photographing others or creating, transferring, disclosing, copying or saving electronic photos
- Publishing news, electronic photos or photographs, scenes, comments, statements or information even if true and correct

Shall also be punished by imprisonment for a period of at least 1 year and a fine not <250000 Dirhams and not in excess of 500000 Dirhams or either of these two penalties whoever uses an electronic information system or any information technology means for amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy (As it is cited in the Article 15 in the same law by saying: “Shall be punished by

imprisonment and a fine not <150000 and not in excess of 500000 Dirhams or either of these two penalties whoever, without authorization, deliberately receives or intercepts any communication through any computer network. Whoever discloses the information which he has obtained through illegal reception or interception of communications shall be punished by imprisonment for a period of at least 1 year").

The question here: Is the principle of the privacy of e-Mail messages an absolute principle and not to be touched and whether there are some exceptions to that exception which allows compromising that privacy.

UAE legislator defined the cases in which penetrating the right to private life is illegible when the interests of the right holder contradict with the interests of the community; the provisions of Article 75 of the code of criminal procedures, saying: (the member of the public prosecution has the right to inspect the accused but not the others who are not accused as well as their house. However, if it turns out from powerful signs that the offender possesses items related to the crime in this case, he has the right and with the consent of the Attorney General to control all correspondences, letters, newspapers, publications, parcels and telegrams, all cables and telecommunications through post offices as well as watching wire and wireless talks when necessary for the requirements of the investigation. Article 76 of the same law defined the limits conducted by a member of the public prosecution by saying: (the public prosecutor alone has the right to see correspondences, letters and other controlled papers and he has the right to order the annexation of those papers to the case file or turning it back to those who possessed them or to those who they were destined to).

The researcher can emphasize the possibility of the application of those texts on e-mail messages. This means that the member of the public prosecution does not have the right to check out those messages unless obtaining the approval of the Attorney General. This procedure should be useful to show the truth in a particular crime. In the case of the availability of these conditions, the public prosecutor determines the e-mail letters they want to check that the investigator chooses which is only related to the crime.

Fifth offense: the crime of preparation, design or acquisition a program for the purposes of attacking an e-Mail. The UAE legislator stressed under the text of Article (14/2) of the Information Technology Crimes Law No. 5 for the year 2012 to criminalize this act by saying.

"Shall be punished by imprisonment and a fine not <200000 dirhams and not in excess of 500000 dirhams or either of these two penalties whoever. designs, produces, sells, buys, imports, displays for sale or make available any computer program or any information technology means or promotes by any means links to websites, computer program or any information technology means designed for the purposes of committing, facilitating or abetting in the commission of the crimes specified in this Decree- Law.

"He also pointed out in the Article 13 of the same law relating to falsifying credit cards Article 13 cited in the same law by saying: "Shall be punished by imprisonment and a fine not less than five hundred thousand dirhams and not in excess of 2 million dirhams or either of these two penalties whoever. Manufactures or designs any information technology means or computer program for the purpose of facilitating any of the acts specified in Paragraph 1 of this Article".

General rules of responsibility for the crimes of assault on e-Mail: UAE legislator cited in the law of the fight against crimes of information technology which shows the general lines of responsibility for the crimes of abuse of e-Mail, particularly with the substantive provisions of criminal responsibility for information technology crimes law in the following manner:

The UAE legislator stressed to maintain e-mail with full protection and offended every attack against it even if not included in the law of the fight against cybercrimes, but it is cited in other valid legislation. This means that the punishment should be according to this text provided that this is conducted by using electronic means (Article No. 46 of the United Arab Emirates combating cybercrimes Act.) and the application of the prejudice should not violate any penalties cited in this act to any severer penalty in any other law (Article No. 48 of the United Arab Emirates combating cybercrimes Act.)

The UAE legislator authorized the court to order putting the convict under supervision or control and deprive him from using any information network, information system or any technical device other information or putting him in a therapeutic shelter or rehabilitation center for a period of time determined by the court (Article No. 43 of the United Arab Emirates combating cybercrimes Act). The court also determines deporting any Foreigner who has convicted to commit any of the aforementioned crimes after the implementation of the sentence on him (Article No. 42 of the United Arab Emirates combating cybercrimes Act).

The legislator put a punishment to those misdemeanors who embark a crime with half penalty of the complete offense (Article No. 40 of the United Arab Emirates combating cybercrimes Act).

The legislator strengthened the punishment in case of the availability of some of the aggravating circumstances. The law cited some circumstances that need emphasizing punishment for the original penalty for the actor of such offenses. Article 46/2 of the Act states

that "It is also an aggravating circumstance of committing any offense under this law for the account or for the benefit of a foreign state, any terrorist group, any association organization or any illegal body".

CONCLUSION

The researcher concluded the most important findings and recommendations. With the development of the internet and the increasing numbers of e-mail users in the world, we find that most of the state legislations have resorted to determine the meaning of the e-Mail as a necessary and indispensable means in the field of electronic transactions.

UAE legislator explained e-mail within the website which includes social networking sites and personal homepages.

E-mail has several advantages but it also has some disadvantages, these disadvantages do not impair the advantages in the presence of legal and technical means by which we protect e-Mail from intrusion and tampering.

E-mail is one of the most important means of achieving e-government and facilitating its performance. E-mail can be exploited in committing of many crimes, such as drug trafficking or human trafficking, crimes of religion blasphemy, crimes relating to state security internal and external, money crimes and other crimes. So, the researcher found that the UAE legislator has responded to this development and managed to bring the penal protection for e-Mail by issuing the Federal Law No. 5 for the year 2012 on combating cybercrimes. The law included many materials that would provide legal protection for the privacy of what is published and circulated on the information network.

The legislator cited some texts in the fight against crimes of information technology which show the general lines of responsibility for the crimes such as abusing e-Mail, particularly with the rules of the substantive provisions of criminal responsibility for information technology crimes.

The UAE Information Technology law is characterized by giving the judge a wide discretion to choose between the type of penalty and its amount.

The UAE legislator determined the cases of excusing of penetrating the right to private life in the case when the interests of the right holder contradict with the interests of the community. It is cited in the provisions of Article 75 of the Code of Criminal Procedure.

RECOMMENDATIONS

The researcher hopes that the UAE legislator can amend the text of Article 75 of the code of criminal procedures, so as to monitor wired and wireless conversations including e-mail. A command should be issued from the judge, so as to be justified and useful in revealing the truth.

Training of specialists, officers, public prosecutors and judges in the area of law enforcement as well as the means and tools of electronic information technology to deal with cybercrimes and the ways of detecting attacks on e-Mail.

Raising public awareness of the dimensions of the phenomenon and the new molester patterns and behaviors that will help the perpetrators of crimes in the implementation of their crimes.

Supporting international cooperation in the field of combating information technology crimes which become cross-border crimes due to technical and technological development. This requires mutual judicial assistance and signing of extradition agreements between countries.

REFERENCES

Abdel-Fattah, B.H., 2004. E-Government and its Legal System. Dar al-Fikr al-Arabi Publisher, Alexandria, Egypt,.

Abdul-Muti Khayal, M.A., 2001. Internet and Some Legal Sides. Dar Annahdha Al-Arabieh, Beruit, Lebanon,.

Al-Awadi, F.A.H., 2005. The Legal Aspects of E-Mail. Dar Annahda Al Arabia, Alaraiah, Egypt.

Austin, L., 2003. Privacy and the question of technology. Law Philosophy, 22: 119-166.

Coleman, S., 2006. E-mail, terrorism and the right to privacy. Ethics Inf. Technol., 8: 17-27.

Khalid, M.I., 2010. E-mail Guide in Proving. Dar al-Fikr Publisher, Egypt.

Manara, C., 1999. [Juridical Aspects of E. Email]. Dalloz Publisher, Paris, France, Pages: 140 (In French).

Masur, J.M., 1999. Safety in numbers: Revisiting the risks to client confidences and attorney-client privilege posed by internet electronic mail. Berkeley Technol. Law J., 14: 1117-1162.

McArthur, R.L., 2001. Reasonable expectations of privacy. Ethics Inf. Technol., 3: 123-128.

Warren, S.D. and L.D. Brandeis, 1890. The right to privacy. Harvard Law Rev., 4: 193-220.