PalArch's Journal of Archaeology of Egypt / Egyptology

FORMS OF FAULT CREATING E-TORT LIABILITY

Dr. HazimAkramSalal

College of Law – Imam Ja'afar Al-Sadiq University

hazim.a@sadiq.edu.iq

Dr. HazimAkramSalal, Forms of fault creating E-tort liability, -Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(7),ISSN 1567-214x

Abstract

The formsof fault developed in terms of electronic negligence responsibility, as in the case of electronic destruction and requisition which are both related to the hacking action of abstract objects,is different from what the traditional form of electronic tort responsibility. This issue requires the development of these rules to guarantee the protection of the affected side and the safety of the electronic environment in terms of legal actions resulting from them. The current study discusses the application of tort responsibility regarding electronic destruction of property by destroying data and cultivating viruses.

Ke words: civil responsibility, electronic tort, electronic destruction,electronic requisition.

1. Introduction

The fast scientific and technological development impacts law because it is a reaction of the social reality enacted by the legislator in order to keep the safety of the society. This type of development in the electronic techniques was accompanied by another side of threats and attacks to material and personal rights. In other words, the available electronic tools are utilized to create physical damage in the economy of countries, companies, and individuals; which is why it is necessary to

provide procedures and tools to secure the modern tools and prevent using them to hurt others.

Based on the facts stated above, the term of electronic negligenceresponsibility in law studies and legislations to decide solutions of security in the electronic environment. Generally, the traditional understanding of the civic negligenceresponsibility refers to (a total commitment of individuals not to cause damage to others or else they will be responsible of a compensation). This traditional concept is also related to the electronic negligenceresponsibility because both traditional and electronic responsibilities are alike in terms of parts; however, they are different regarding means of causing damage. In other words, electronic means of damage develop parallel to the development of the digital environment. As far as the previous reasons are concerned, the current study is important because it focuses on electronic attacks as the core error in the electronic negligenceresponsibility unlike other research studies which consider the attack as an image of damage in the electronic negligenceresponsibility. The electronic mistake error is a deviation of the regular behavior in the electronic environment and causes damage to others.

The scope of the responsibility investigated in this study indicates that the error initiative action occurs as a result of the use of an electronic tool. The limitation of such tools is impossible because they are in continuous development, as well as their attacks such as destroy actions

and sending viruses. The issue become more complicated if we consider the difficulty of programming when looking for a program without an error, which is a pure technical issue. That is why we investigated the image of error in the electronic negligenceresponsibility in two parts. Part one studies electronic destruction and part two explains requisition. The current research does not mean that there are no other images of the electronic mistake error but rather assures the multiplicity of such error. Moreover, this research copes the development of this error in the digital environment. The study uses comparative analytical methodology in its research.

2. Electronic destruction

Destruction, traditionally, means making things unusual (Thannon, 2006: p.225). This meaning is related to physical items. On the other hand, electronic damage has a different and more important meaning. As we know, property could be physical or abstract. Concerning electronic tools, the attack action is applicable to both physical electronic devices or abstract information inside these devices. Both types of electronic damage are investigated in the current study because the damage of electronic devices are easily defined within the concept of the traditional damage. The dispute occurs regarding the abstract damage of the information in these devices (Qashqosh, 2004: p.891). is it sufficient to follow the acts of the civic law of compensating damaged people for this type of damage? At this point a recognition is needed in terms of purposeful damage or

obstructing the operation of the data treatment systems; because the programs could be damaged aside from the system. For instance, deleting some files in the system without affecting its function and vice versa, because the system could be obstructed using an electronic tool without damaging any software components such as inserting a program to prevent accessing the system without damaging the software components of the information system.

To sum up, this part is divided into two sections: First to investigate kinds of the electronic damage, and second to explain the application of the mastery of general rules on electronic damage.

2.1.Kinds of the electronic destruction

Electronicdestruction includes all kinds of electronic attacks which lead to the destruction of the programs and electronic data totally which makes them totally or partiallynon-functional (Al-Khalayla, 2009: p.109). As a result, partial or total electronic destruction is restricted to saved data or programs in the electronic means such as messing up electronic payment devices, breaking into websites and destroying them, or accessing certain websites – for example power run websites- and disabling them. These examples explain the various shapes of electronic destruction which can be summarized as follows:

First: direct unlicensed interference in the systems of the electronic means (cyber breakthrough)

Breakthrough refers to the ability of accessing certain goal illegally through gaps in the protection system of the targeted entity (Mohammed, 2020). The illegal side is in the power of the doer in accessing the information system, which entails that cyber breakthrough is anunlicensed access and control of the information system of individuals or institutes. The breakthrough occurs usually on the internet or in certain networks used by some institutes, which means that breakthrough takes place remotely most of the time because the hacker can breakthrough systems of the targeted electronic devices or their saved data and destroy or mess them up (Science and Tech). One of the applications of cyber breakthrough, which led to great argument, was what was published on Facebook concerning the breakthrough of more than million account (Salman, 2019: p.73). As a result, some software solutions were suggested to enable the user save his data securely by activatingthe second verification (Khalid and Mahmoud, 2017).

Some international companies provide support to certain devices and software by intercepting any breakthrough such as the protection offered by the American Microsoft Company to ATM machines through special program (Microsoft website).

Second: spreading viruses in the electronic devices or publishing them on the internet which causes damages to the hardware or the electronic means. The destruction might affect the programs because hackers could cultivate a virus in the system of a particular institute to

destroy data (Al-Sagheer, 2002: p.13). An example of that is what happened in Monmouth University in the United States. It shows the destructive impact of viruses which explode after a while of inserting them in the system. The virus targeted the e-mail system of the university which connects important activities such as registration, research exchange, and fees. The virus led to the collapse of the e-mail system and a loss of ten thousand dollars. An investigation FBI team could determine the day, time, and computer ID of the computer used in the crime. The team confronted the accused person who tried to justify his deed stating that he did not aim at destruction but his justification was in vain because the court considered him guilty and sentenced him three years in prison with a penalty of 100.000 USD (Ababna, 2005: p.104). A similar case took place when Sasser-(Wurm) was sent in 2004 and led to the crash of millions of computers that worked by Windows in various parts of the world. The virus was spreading as soon as the computer is connected to the internet (The Sasser Event, 2004).

Third: Malfunction of a virus cultivation on the purpose of protection against copying. In this case, a particular virus initiator program cultivates a virus which is activated when it is copied to protect the product from uncertified copying process. If someone copies that virus it will be activated causing damage. However, if this virus is transferred to other devises, other than the one which belongs to the uncertified copier, then who is responsible?

Some answers relate that to the despotically theory in using rights stated in Act 7 of the Iraqi Civic Law No.40 in 1951 (offset with the Egyptian Civic Law No.131 in 1948), because damages of a virus cultivation in the goal of protection exceeds the benefits aimed by the program producer. Such damages could reach to those who connect with the person in question in one network (Mansour, 2009: p.253-254; Abdulridha, 2005: p.93). we agree with the scholars (Khalid and Mahmoud, 2017) who consider that protected programs producers should limit their effect on the program itself by deleting data or reducing its competence in order to improve its function but the costumer should be notified first.

2.2.The application of the mastery of general rules on electronic destruction

Based on the nature of electronic destruction in affecting abstract things, there was a dispute on the possibility of its subjection to the mastery of general rules in terms of negligence responsibility in the civic law, because these rules were followed to deal with physical destruction actions. Views , in this respect, were divided into two directions. The first direction goes for the subjection of the electronic destruction to the general rules of the civic law considering that data is transferrable possession, which is irrational because transferrable property are physical (Qashqosh, 2004: p.901).

The second direction regards the destruction of the physical containers of data, such as tapes and CDs, makes it possible to apply the traditional rules on the destruction of programs and data saved in electronic means (Abdul Kadhim, 2000: p.19). We still think that the description of physical possession is inapplicable here because the physical containers will not be destroyed but rather the data saved inside. Inserting a virus in a program will destroy the saved data without affecting the appearance of the electronic means.

Based on the justification above, it is unacceptable to apply the traditional mastery of rules on electronic destruction, which is why there is a view of applying special rules designed for the electronic destruction because legal protected property right does not include abstract entities (Abdullah, 2005: p.98).

Therefore, destructible data is not applicable to what was explained earlier. Furthermore, this data is not protectable by intellectual property rights unless it acquires the qualities of the property in question in order to be protected based on the modified author protection law No.3 in 1971 and the law of patent and industrial samples No.60 in 1970 (Hussein, 2004: p.130-131).

Moreover, jurisprudence regards destruction in the negligenceresponsibility as a physical incident accompanied with the loss of a financial thing, which is the destroyed thing (Allam, 1956: p.53).Thus, electronic destruction cannot be considered a ‘destruction’ as

the previous concept indicates because destruction requires a physical incident whereas inserting a virus is an abstract incident in an electronic atmosphere without any physical destruction to electronic means.

Saying that, we can infer that it is unreasonable not to consider electronic destruction as a form of lawfully listed destruction despite its abstractedness because the information revolution has imposed itself on all sides of life and made electronic destruction more serious than traditional image of destruction. However, that does not mean the unnecessity of civic laws and the legislator interference to organize the issue of electronic destruction and other images of electronic trespass. On the contrary, the legislator in the project of information crimes stated in Act 7 the incrimination of forms of electronic destruction, which will assure the possibility of vindicating compensation to damages resulting from electronic destruction.

It is worth noting that the revised English Computer Misuse Actin 1990 referred in its first Article to considering electronic damage as anforms of error which requires compensation. And so was the position of the Egyptian legislator in the Act of electronic signature No. 15 in 2004 in Article(23).

3. Electronic Requisition

Requisition means capturing others' property without the right to do so (Thannon, 2006: p.234-240). The infringing person in this case is

responsible for compensating the legal owner about the electronic requisition because it includes seizing data and other information systems without legitimate excuse, which is called cyber piracy. Cyber Piracy refers to information and data requisition by electronic means. This section will be divided into two parts. The first part discusses forms of electronic requisition and part two investigates the subjection of electronic requisition to the mastery of general (traditional) rules.

3.1.Forms of electronic requisition

Forms of electronic requisition vary based on the development of information technology in different field. Ray (cited in Abdullah, 2005; Khalid, 2013) divides electronic requisition into three forms as follows:

First: requisition of computer time by using a specific program which enables others of using the computer for his own benefit.

Second: virus cultivation in the information system of an individual or an institute to capture information.

Third: virus cultivation in an information system of a bank to breakthrough the bank electronic system and withdraw money.

Forms listed above represent types of cyber piracy. Piracy, in its traditional concept, refers to any uncertified violence action aiming at seizing other ships (Khatir, 2011: p. 267). Piracy, in our time, has acquired an absolute description due to seizing published work on the internet and companies' data without permission.

Cyber piracy can be defined as seizing the property of others using electronic means without relying on violence, unlike traditional piracy which used violence and threats, since it takes place in an abstract electronic space (Al-Khalayla, 2009: p.100). cyber piracy does not including seizing physical components of electronic means which contain data and programs (software), because that is a familiar form of requisition of physical items. Recently, the term 'programs piracy' is widely used to describe uncertified copying of programs, seizing, using, or reproducing saved information without permission (Mansour, 2009: p.237).

The most important feature of cyber piracy is that the criminal does not change or take out the ownership of the electronic means despite using it. However, the requisition of the data array takes it out of the possession of its owner, which we see as part of the traditional concept of requisition. We can summarize forms of electronic requisition as follows:

1- Direct electronic requisition: occurs by direct seizing of data.

For example, online intellectual property piracy is related to mimicking computer programs or illegal copying of certain programs. Mimicking programs means that the infringing personmimics the program and creates a copy without permission. On the other hand, direct or indirect illegal copying refers to programs unproductive companies which copy these programs illegally and sell them without the permission of the producing company. Indirect kind of illegal copying entails buying the

seized programs,copying them, then selling and distributing these copied programs (Mohammed, 2017: p.116).

The latter case led many countries to legislate Acts to face this issue. For example, enacting the American Online Piracy Stop Act in 2011 which aimed at protecting online intellectual property.

Piracy might threat banks money and transfer it electronically by cultivating a virus in the information system of the bank to breakthrough the system and transfer the money into private accounts. No doubt that such cases are considered seizing of money because the action is clear(Khalid, 2013). Moreover, in many countries such as Canada, England, and Switzerland written cash transfer is considered a valid situation for requisition. The French court of cassation has issued several Acts that considered written payment equals paying in cash, which is why using computer programs to seize money from banks is considered requisition.

2- Indirectelectronic requisition: represented by deviating from the goal of the electronic treatment of data received to be recorded, classified, or transferred as in the case of companies which provide Cloud services to save various data which might have high financial value. The basic condition in this form requires prior legal seize of the data, such as cancelling the certification or the expiration of the electronic data (Jaafar, 2013: p.453). this form can also be represented by changing the intention

of the data holder who uses it for a different purpose and refuses to give it to the legal owner such as dealing with Cloud services companies.

3.2. Subjection of electronic requisition to the mastery of general (traditional) rules

Subjection to the mastery of general rules stated in the Civic Law in Articles 192-201 is related to the possibility of considering electronic means as subjects of requisition because the general rules controls the requisition of transferrable and non-transferrable property. Some people goes for not considering this case as part of what is controlled by these Acts because the seized item is abstract (Abdullah, 2005).However, this assumption is confronted by some physical cases which took place in one of the American petroleum companies which noticed that it has lost several successive bids. Then the company discovered that electronically treated data related to prices has been transferred to the competing company. The damage was verified in the previous example despite its abstract nature. Compensation would be equal to the loss of the company.

On such bases we can differentiate between cyber piracy and requisition because the latter is connected to physical objects whereas the former keeps the ownership of the information but it is copied by others.

Considering cyberpiracy as a form of requisition is a kind of coping with the development of life because the owner does not lose the possession of his information. However, this information affects his interests mostly because the information revolution has expanded to

include all sides of life. Moreover, the term ‘property’ in Act 192 of the Iraqi Civic Law should be more comprehensive to include abstract possessions represented by software and electronic data due to their importance for companies and banks. That does not mean not issuing a legislation to treat such cases because the Act of electronic correspondences and signature No.78 in 2012 has organized electronic transfer of property, which means there is a legal document to protect electronically transferred money.

4. Conclusion

Electronic negligence responsibility refers to binding the destructor of electronic means of a compensation. As we know, electronic means are various and have several forms which makes errors various in terms of electronic negligence responsibility. However, we preferred in this study to discuss the application of this responsibility on electronic destruction of property (i.e. information and software) by destroying data and cultivating viruses.

Second, the research investigated electronic requisition and the prominent application of this form, which is known as cyber piracy, through seizing electronic data without the right to do so.

Furthermore, the study concluded that it is necessary to expand the term ‘property’ in the Iraqi Civic Law to cope with the information revolution in order to include abstract property in addition to transferrable

and non-transferrable property and the necessity of enacting the project to face the novel applications of the negligence responsibility.

References

[1] Ababna, M.A. (2005). *Computer crimes and their international dimensions*. Dar Althaqafa Publishing.

[2] Abdul Kadhim, A. (2000). Legal civic protection of computer programs. A dissertation in law. University of Babylon. Iraq.

[3] Abdulhay, W. (2000). Dispute of electronic space of intellectual property. A dissertation in law, Alyarmouk University. Jordan.

[4] Abdullah, H.A. (2005). Damage of the using computer in terms of the negligence responsibility. A dissertation in law. University of Baghdad. Iraq.

[5] Al-Khalayla, A. R. (2009). *Electronic negligence responsibility*. (1st ed.). Jordan: Dar Al-Thaqafa.

[6] Allam, A. (1956). Acts of destruction and requisition under the rules of negligence responsibility. *Alqadhaa Journal*. *1956*, 53.

[7] Al-Sagheer, J. A. (2002). *Procedual sides of cyber crimes*. Cairo: Dar Al-Nahdha Al-Arabia.

[8] Dual verification means that user should enter verification code sent to his phone when signing to one of his accounts.

[9] B. AL-Hayani, and H. Ilhan,**"**Efficient cooperative imge transmission in one-Way mult-hop sensor network," International Journal of Electrical Engineering Education, vol.57, no.2, pp.321-339. 2020.

[10] BSA. .Alhayaniand MilindRane,"face recognition system by image processing" International journal of electronics and communication engineering & technology INTERNATIONAL JOURNAL OF ELECTRONICS AND COMMUNICATION ENGINEERING & TECHNOLOGY (IJECET), vol.5, no.5, pp. 80–90. 2014.

[11] BSA. Al HayaniandH. Ilhan,"Visual Sensor Intelligent Module Based Image Transmission in Industrial Manufacturing for Monitoring and Manipulation problems,"Journal of Intelligent Manufacturing, vol.4,pp.1-14.2020.

[12] B. AL Hayaniand H. Ilhan, "Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring," Journal of Medical Imaging And Health Informatics, vol. 10, pp. 160-168.2020.

[13] B. Alhayani, A.A. Abdallah, (2020), "Manufacturing intelligent Corvus corone module for a secured two way image transmission under WSN", Engineering Computations, Vol. 37 No. 9, pp. 1-17. https://doi.org/10.1108/EC-02-2020-0107.

[14] B. ALhayani and H. Ilhan, **"**Hyper spectral image classification using dimensionality reduction techniques**",**International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering**,,** vol.5, pp.71-74.2017.

[15] http://www.microsoft.com/ar-iq.

[16] Hussein, M.A. (2004). *Legal responsibility of network*.

[17] Jaafar, A. (2013). *Modern information technology crimes faced by individuals and the government*. Lebanon: ManshoratZein Al-Huqoqia.

[18] Khalid, N.H. & Mahmoud, R. M. (June 2017). Civic responsibility of electronic destruction. *Journal of Rights in Tikrit University, 1*(4), 134-135.

[19] Khatir, M. (2011). Legal form of navy piracy. *Legal and Economic Journal of the University of Damascus, 27*(4), 267.

[20] Malone, R.J.; Levary, R.R.. (1994). Computer viruses: Legal aspects. *Business Law Review, 125*, 127-132.

[21] Mansour, M.H. (2009). *Electronic negligence responsibility*. Egypt: Dar Aljami'aAljadeed.

[22] Mohammed, A.A. (2017). *Negligence responsibility of private actions and misuse of the internet in the special electronic international Act*. Egypt: Dar Al-Jami'aAljadeeda.

[23] Note that the legislater defined breakthrough in Article 1 of Combating Electronic Crimes Act No.175 in 2018. The Iraqi project of information crimes law did not refer to the definition of breakthrough but to its forms in Act 7 (1 and 2) in addition to some other forms in the proceeding Acts.

[24] Qashqosh, H.H. (2004). Unpurposful destruction of computer programs and electronic data. Conference of Law, Computer, and the Internet. College of Law and Jurisdiction: UAI University, 3(3), 891.

[25] Salman, A. K. (2019). *Civic responsibility of privacy breakthrough*. Lebanon: Dar Al-Nahdha Al-Arabia.

[26] Thannon, H.A. (2006). *Almabsoot in explaining the Civic Law – error*. (1st ed.). Jordan: Dar Wai'l for Publishing.

[27] The Sasser Event: History and implication. TREND MICRO, INC. (June 2004).