

PalArch's Journal of Archaeology of Egypt / Egyptology

INFORMATIONAL DESTRUCTION CRIME; A COMPARATIVE STUDY

Maitham Mohammad Abd ALNomani¹

Aseel Hatem Toman Birmani²

^{1,2} Al-Furat Al-Awsat Technical University, Babylon Technical Institute, Legal Management
Technologies Dept., Iraq

Corresponding Author: ¹inb.mth@atu.edu.iq, ²Asselhatim80@gmail.com

Maitham Mohammad Abd ALNomani, Aseel Hatem Toman Birmani. Informational Destruction Crime; A Comparative Study-- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(3), 2266-2281 ISSN 1567-214x

Keywords: Destruction, information, crime.

ABSTRACT

Informational destruction crimes are attacks affecting all information, data, programs, or whatever falls within the scope of information, whether it is stored in a computer, mobile devices, tablets, or information systems. These attacks may occur through erasing, destruction, or other actions. They are done by many means, including viruses, logical bombs, etc. The crime of informational destruction is one of the crimes of damage that must be investigated. There has been a juristic debate about the extent of the possibility of applying the traditional legal texts on the damage of information. Some support and others reject it. The international legislation punishes the crime of informational destruction with various penalties; prison, imprisonment, fine, or all penalties; fine with imprisonment or Confinement.

Keywords: Destruction, information, crime.

INTRODUCTION

Crime is a social phenomenon that is not limited to an age, but it is inherent to the human being as it takes different forms depending on the quality of the social system. The phenomenon of crime did not remain traditional, but it changed, diversified, and varied as a result of the tremendous scientific development that has occurred and is still continuing due to the emergence of computers and modern technology, including mobile phones and tablets. Crimes have become committed with the push of a button. One of these crimes that has spread widely recently is the crime of destroying data, information, and others, whether they are for individuals or public.

The problem of study

The problem of the present study is focused on answering the following questions:

1. What is the crime of informational destruction ?? What is the difference between it and the crime of traditional destruction? What are the methods used to commit this crime?
2. What is the extent of the applicability of the traditional texts on the crime of informational destruction? Does the Iraqi legislator criminalize the act of informational destruction?

The aims of study

The present study aims at:

1. Defining the concept of destruction that occurs through information technology and distinguishing it from similar legal situations.
2. Defining the manner in which this crime is committed, as well as the means used in that.

The significance of study

The importance of the present study is evident in finding appropriate legal solutions to address the legislative deficiency occurring as a result of the absence of an Iraqi informational crime law until now despite the spread of informational crimes.

The previous studies

The topic of informational destruction is one of the recent topics. The legal studies are few:

1. Al-Silawi, Alaa Abdulhassan and Al-Salami, Ali Talif Majeed, (2018).

The Effects of Criminal Responsibility for the Crime of Information Destruction and Ways to Combat it, Vol. 1, No. 37, Al-Kufa Journal for Legal and Political Sciences, Iraq.

2. Qashqosh, Huda, (2000).

The Intentional Destruction of Electronic Computer Programs and Data, a research submitted to the Law, Computer, and Internet Conference, Faculty of Sharia and Law, United Arab Emirates University.

The study methodology

In the present study, the two researchers use the analytical and comparative approach to analyze legal texts as well as the opinions of jurists and compare legal texts in the Iraqi, Emirati, and French legislations.

The study plan

The present study is divided into two sections. In the first section, the two researchers deal with the concept of the crime of informational destruction, presenting definitions and uniqueness of the crime. Section two is devoted to discussing elements, judgments, and penalties of the crime.

SECTION ONE

The concept of the crime of information destruction.

This section is divided into two subsections. The first is devoted to the definition of the crime of informational destruction. The second is devoted to showing the uniqueness of the crime.

First; Definition of the crime of informational destruction.

In this section, the definition of the crime of informational destruction in the legislative and juristic terminology is presented as follows;

Legislatively

The term informational destruction was not mentioned in the Iraqi Penal Code No. (111) of 1969. But, the term damage was mentioned in general. The Iraqi legislators did not define the damage, but they left its definition to jurisprudence. The two researchers support it because the legislator is limited to his role in developing legislation. The definition is the mission or competence of jurists. In addition, the legislator, no matter how accurate, cannot come up with an inclusive definition of the term to be defined.

The term destruction is mentioned in its traditional concept in more than one resource in the Iraqi amended Penal Code No. (111) for 1969, including the provisions of articles (164, 177, F2 / A / 183, 197, 239,250,263,264, 293, 301, F2). / 353, 362, 367,451, P1 / 477) and others. The text of the Article (477) of the Iraqi Penal Code is the main text in the field of criminalization of damage to funds. The Emirati legislators indicated that in the text of Article (424) of the Federal Penal Code No. 3 of 1987. The French legislators referred to it in the text of Article (322-1) of the Criminal Code of 1992 in force in 1994.

Juristically

Destruction is generally defined as diminishing the benefit of money or an object which makes it totally or partially unusable (Hosni, 2005: 664). It is also defined as influencing the substance of a thing in a way that reduces its economic value by diminishing competence for the intended use of it (Al-Sagheer, 2012: 127). It is also defined as Anything that reduces or destroys the value of a thing. It is punishable by law as it has reduced the importance and value of the thing (Mustafa, 1984: 646).

It is defined as sabotaging the object of the crime by spoiling it, disrupting it, stopping its activity and its value, destroying it, or making it totally or partially unusable (Qashqosh, 1992: 50).

Informational destruction is defined as an electronic assault directed to informatics, including the data or programs in which the Internet is used as a means for its implementation. This attack deals with the logical, non-physical components of the computer, whether data or programs without the physical components related to the computer ... (Al-Ghoul, 2017: 227). It is also defined as erasing information or programs entirely or destroying them electronically or that information or programs are distorted in a way that destroys them making them unusable (Fikry, 2006: 112). Another jurist defines it as erasing or sabotaging or Any other act with the intention of disrupting a function of the electronic network or the information system (Ananza, 2017: 119).

Second; The uniqueness of the informational destruction crime.

This section deals with distinguishing the crime of informational destruction from similar legal conditions and showing the images of the crime of destruction and the methods used to commit it as follows:

Distinguishing the crime of informational destruction from similar legal situations

There are many similarities and differences between the crime of informational destruction and many other information crimes, including the crime of information forgery and the crime of disrupting or spoiling the information system.

- 1) Distinguishing the informational disruption crime from the informational forgery crime.

The Iraqi legislator defined forgery in Article (286) of the Iraqi amended Penal Code No. (111) of 1969 as changing the truth with the intention of cheating in a document in one of the material and moral ways indicated by the law in a way that would cause harm to the Public or personal interest.

Information forgery means changing the truth in automated documents and information documents with the intention of using them (Hijazi, 2008: 159). Thus, counterfeiting may be traditional forgery. It may be counterfeiting information or what the Budapest Convention (European Convention against Information Crime) signed on November 23/2001 called (computer-related forgery).

The crime of informational destruction is mixed with the crime of information forgery in many similarities and differences listed as follows:

1. Both crimes are similar in terms of the place and the behavior. The actor in both crimes manipulates the programs and information by erasing, adding, or modifying.
2. Both crimes differ in terms of criminal intent as well as the interest that is intended to protect them from criminalizing each of them. The criminal intent in the crime of destruction is devoted to the events of erasing, modifying, or adding any destruction of information, data, or programs in order to harm its owner whether a natural or moral person. This means that the destruction of information, data, or programs is not

intended to obtain any benefit or material profit, but its primary goal is to harm this information, data, or programs for revenge or competition with its owner. In the crime of information forgery, information or data are incorrectly entered with the intention of using them for unlawful purposes on the basis that they are correct (Al-Husseini, 2017: 176). The interests are represented by protecting information, data, and programs as information of money in the crime of informational destruction (Khadr, 2017: 165). For the interest to be protected in the crime of information forgery, it is the protection of public confidence in the documents and information documents.

Distinguishing the informational destruction crime from the crime of disrupting or spoiling the information system.

There are many similarities and differences between the crimes of informational destruction and the crime of disrupting or corrupting the information system. The crime of disrupting or corrupting the information system is defined as any act that causes the system to stop, slow down, or confuse the work of the Informational system (Tamam, 2000: 351). Spoiling the information system means distorting the performance of the information system and making it unfit for use "(Afifi, 2000: 192).

1. One of the similarities between the crime of informational destruction and the crime of disrupting or spoiling the information system is that each of them is a crime of damage that results in erasing data, information, or programs, as in the crime of disrupting, obstructing, or spoiling the information system. The means used in the crime of destruction, such as viruses, logical bombs, and others are the same ones used in the crime of disrupting or spoiling the information system.
2. It is noted that the criminal activity that constitutes the crime of informational destruction does not always lead to obstructing or hindering the information system or disturbing the course of work in it. It is possible that there is information damage that focuses on information, data, or programs in the information system; erasing some files stored in the information system without leading to disruption or corrupting that system. The crime of destruction focuses on information, data, and programs that exist in this system. The crime of disrupting or spoiling the information system is focused on the information system itself (Bhutani, 2016: pp. 254- 255) This is what made most legislations distinguish between the crimes of destruction and the disruption or corruption of the information system, including the French legislator in the article (323 - F2 and 3) of the Penal Code of 1992 in force in 1994.

Second; Forms and methods of the crime of informational destruction.

The destruction is done through two forms and several means as follows:

1. Forms of the destruction in the field of information technology crimes
Destruction occurs in the field of information technology crimes in two forms:

Physical destruction; This form takes the traditional physical character. It happens to the means of information technology. This type of Destruction is that which occurs on

physical devices, such as damage that occurs on a computer, mobile device, tablet, or in one of the tools of those devices as in the case of breaking a screen of a Telephone device or input or output units in a computer. This damage leads to a concrete result to the outside world.

The moral destruction; It is also called informational destruction, which means that damage which takes on a morally new character, whether in terms of criminal behavior committed, or in terms of the criminal result, such as erasing information, data, or programs or canceling it. It is the behavior of a technician into information funds. That behavior leads to an intangible moral criminal result (Khudhr, 2017: 164).

2) The means used in the crime of informational destruction

1. Viruses; A virus is defined as a software that is designed with a limited purpose to cause the greatest possible damage to electronic systems. It is characterized by its ability to link itself with other programs and re-create itself so that it appears to reproduce and generate itself. It is also able to spread from one system to another so that it can travel across borders from one place to another (Ja`far, 2013: 552). Viruses are not considered the offspring of the internet. The concept of computer virus was mentioned by the mathematical scientist von Neumann in the mid-forties of the last century when internet was not at the time. It is the most used method for spreading and distributing viruses (Al-Qur'an 2017: 96). Viruses have many different types. Their strength and severity increase day after day.
2. Worm programs; They are defined as programs that exploit any gap in operating systems to transfer from one electronic system to another or from one network to another via the links that link to it without there being a need for humanitarian intervention to activate it. They occupy the largest possible capacity of the network and reduce its efficiency. They may exceed their goals to start after the proliferation and reproduction of the actual sabotage of programs and information and destroy them (Al-Hussaini, 2017: 145; Moreno-Bird et al., 2020; Ormaechea & Fernandez, 2020; Shliakhovchuk & Garcia, 2020; Talan, 2020; Masitenyane & Mokoena, 2020; Meyer & Klonaridis, 2020).
3. Information bomb programs; They are a type of small size malicious programs that are entered in ways that are not legitimate and hidden with other programs. Formally, it is not a complete integrated file but rather a code that is organized into a group of programs by dividing them into separate parts here and there so as not to be recognized. Thus, they can gather according to the command given to them at a certain time or the occurrence of a specific incident. It is designed to remain static and ineffective only at the specified time or the specific event. Therefore, it cannot be discovered for long periods of months and years. It leads to a lack of ability On operating programs via the information system. These programs are used to destroy data, information, and programs. These programs have two parts; the logical bomb and the time bomb (Jafar, 2013: pp. 555- 556).

SECTION TWO

The provisions of the crime of informational destruction

Research in the informational destruction crime requires a review of the elements of this crime to show the punishment prescribed for it. Accordingly, this section is divided into two subsections. The pillars of the informational destruction crime are presented in the first subsection. In the second subsection, the punishment prescribed for this crime is presented.

First; Elements of the crime of informational destruction

For any crime to occur, its general elements must be determined as they are considered the elements upon which the crime entity is based. If one of these elements is missing, the crime does not have any existence (Al-Saadi, 1976: 148. Al-Durrah, 1990: 180). The crime consists of two pillars. The first pillar is Physical and the second is moral.

First; The Physical pillars

The physical pillar represents the apparent aspect of the crime. The assaulting of the interest protected by law is achieved. It consists of three elements; criminal behavior, which is the most important element of the physical pillar, the criminal result, and the causal relationship (Al-Qahwaji, 2002: 309. Al-Hadithi, 2018 : 192).

Criminal behavior

The criminal behavior of the informational destruction crime is any activity that affects data, information, or programs and causes damage as in the case of an unlawful amendment of information and programs. It is done through the use of a computer or a telephone device. It is the act of unlawful amendment of data within the system, replacing it with other data, and manipulating programs by providing them with different data that leads to different results from the one for which the program was designed for. It may be by destroying information or programs stored in the means of information technology or by erasing information by entering the computer or phone Mobile and deleting information and programs. The erasing action is achieved by removing part of the data recorded in the automated processing system or adding part of the data to the area of memory. The report issued by the European Council on Information Technology Crimes recommended criminalizing acts that lead to erasing information. This recommendation distinguished between two forms of erasing attached to information; the first relates to erasing information completely and the second is achieved by hiding information so that it cannot be accessed without consequent Erasing information (Ja`far, 2013: 536).

Legislations did not agree on a specific behavior in which the crime can be achieved. The French legislator, in Article (323-3) of the Penal Code, has used several terms; insertion, erasing, and amendment. The Emirati legislator, In Article (10) of the Information Technology Crime Law No. (5) of 2012, has used several expressions; destruction,

erasing, deletion, damage, and alteration. The Iraqi Informatics Crime code of 2011 has used many expressions referring to destruction in several places. The most important is stated in paragraph (1 / c) of Article (3) and paragraph (2) of Article (15) thereof. The Iraqi legislator used deletion, destruction, change, and hiding.

Despite the diversity and multiplicity of terms used by various legislations that refer to destruction, the goal is the same and it is to take note of everything that could lead to damaging information, data, and programs (Khudhr, 2017: 213). As for the location of the crime of informational destruction, it must be of a moral nature. Otherwise, it is not considered information damage but rather physical (Hornung, 2020; Janssen, 2020; Hu et al., 2020; Jia & Zhang, 2020; Martinez-martinez, 2020; Moral-campillo & Hernandez-mendo, 2020; Duman et al., 2020; Ekonomi & Jaya, 2020). The location of the crime of informational destruction is mainly information, programs, and data. Information is defined as any message expressed in a way that makes it midwife For transfer or reporting to others. It is an expression intended to make a message deliverable to others through a signal that would convey an idea or some of it to others, so the expression and its communication to others hinder the function of information, which is the transmission of knowledge (Catala, 1984: 97).

Programs are defined as a set of instructions directed from the person to the machine, which allows placing them on the physical medium designated for that in a specific language, transferring them to the devices intended for processing information, with the aim of accomplishing certain tasks or obtaining specific results (Badawi, 2018: 104). With regard to the last form of the crime of informational destruction; the data, it is defined as an expression used to refer to or to describe data represented symbolically on automatic media, which represents orders, operations, and elements that contain numbers, letters, or special signs to express names, acts, or numeric values.

They are the elements that are subject to processing by software using the capabilities of the automated group of the system "(Al-Sharif, 1995: 112). Information, programs, or data may be stored in a computer, phone, or in the local or network of information system. Destruction can be achieved on the information, programs, or data separately or together.

Criminal Outcome and Causation

The criminal result means "the change that takes place in the external world as an effect of criminal behavior. It achieves an aggression on an interest or a right. The legislator describes it as a criminal protection (Al-Khalaf and Al-Shawi, 2015: 140). This effect occurs as destroying, erasing, distorting, or damaging information, programs, and data.

Thus, the crime of informational destruction is considered a crime of damage. Because it requires a criminal result as it is not enough to threaten data, information, or programs only, but it is necessary to get actual damage that occurs on them, whether this harm is the erasing of information, programs, or data or destroying them.

As for the causal relationship, it means that "the harm done is the result of the committed act; The act of the perpetrator is the cause of the harmful result (Al-Saadi, 1976: 170). The result obtained from the erasing, distortion, and destruction of information, data, and programs is the criminal behavior committed by the perpetrator.

Second; The moral pillar

In order for the crime to take place legally, it is not sufficient to provide the material pillar only. There must be a psychological relationship between the physical pillar and the offender expressed by the moral pillar which takes one of two forms; The first is the form of the criminal intent and the second is the form of the unintentional error (Surur, 2015: 642- 643).

The crime of informational destruction is one of the intentional crimes. It requires the availability of a general intent, which consists of two elements; The first is knowledge. The perpetrator must know that he/she is carrying out the acts that are criminalized by law and the actions would lead to the destruction of information, data, and programs. The second component is the element of the will. The will of the perpetrator must be directed to carry out these actions and their consequences. In the event of the absence of any of the two elements, the moral pillar of the crime will be negated (Ibrahim, 2018: 420).

Some legislations require a special criminal intent in the crime of informational destruction beside the general criminal intent. The will of the accused to achieve a special intent, such as intending to harm others or making a material profit. The French Law on Information Crimes No. (19) of 1988 In Article (462-4) is among the legislations confirming this issue. Some jurists criticized private criminal intent for many reasons as this will exclude all cases where the perpetrator's intention does not lead to illegal physical gain from the scope of this crime despite the importance of the information that may be destroyed (Qurah, 2003: pp. 227-228). The two researchers support This idiosyncratic trend because stipulating private criminal intent in addition to the general criminal intent leads to the impunity of many perpetrators.

Third: The penalty for the informational destruction crime

Having clarified the elements of the crime of informational destruction and its privacy, it is necessary to clarify the penalty for this crime and review the difference between the criminal jurisprudence about the possibility of applying traditional texts to the crime of informational destruction and the penalty of the informational destruction crime in Legislation expressly provided for as follows;

First; The extent of the possibility of applying the traditional texts of the destruction to the crime of informational destruction

A side of the jurists considers that the damage that occurs to the information technology devices such as computer, one of its components, phone, or tablet devices is the damage that occurs to the material money, such as destroying the computer screen or the phone or one of the material components of them such as disks, headsets, chips, and others, Whether it contains information, programs, or data, or if it is free from it. According to this opinion, it is treated as the material money to which the provisions of the crime of destruction apply in its traditional way. Thus, it is not considered an information crime (Al-Juburi, 2011: 335. Al-Husseini, 2017: 147). Accordingly, the text of Article (477-1) of the Iraqi Penal Code is the one that applies in this case. Thus, the perpetrator is punished with imprisonment for a period not exceeding two years and a fine not exceeding two hundred dinars or one of these two penalties. The article 424) of the UAE Penal Code and Article (323-1) of the French Penal Code also are applied in such cases. Jurisprudence differed on the extent to which the traditional texts on the crime of destruction can be applied to the crime of informational destruction. There is a trend in favor of that. Another trend rejects it.

1. The rejectionist trend; This tendency believe that it is not possible to apply the traditional texts of the destruction to the crime of informational destruction due to many reasons and justifications, including that the criminal text must be clear and specific in its concept and explicit in its expressions in order not to be subject to interpretation in An area in which interpretation is not permissible. Therefore, the argument is based on the necessity of avoiding the broad interpretation of criminal texts or measuring them in a way that leads to deviating from the principle of legality. In addition, the criminal text is not like any other legal texts as it must apply easily to the incident (Al-Haiti, 2016: 213). It is also argued that the crime of destruction in traditional texts requires that the subject of the crime be of a material nature, which is not possible with the crime of informational destruction because the nature of information, data, and programs is not tangible (Derby and Ismail, 2012: 55). Besides, erasing and destruction of information, data, and programs is mainly by interfering with the functions of the computer and the information system, which is not considered a damage to the physical medium that includes this information, data , and Programs (Qurah, 2003: 194).
2. The supportive trend; Some jurists believe that it is possible to apply the traditional texts of the traditional destruction to the crime of informational destruction. They based this on many justifications, including the fact that the traditional texts do not transform in principle from the occurrence of these crimes on something moral or intangible because it does not require the physical attribute and does not refer either to this condition. It is not permissible to require the physical attribute in the place of the crime of destruction (Senekai & Lenz, 2020; Van Den Berg & Surujlal, 2020; Antoni et al., 2020; Berejena et al., 2020; Matthews & Mokoena, 2020; Mosala & Chinomona, 2020). In addition, the logical entities are considered funds that are protectable under traditional legislation because it has a large economic value that sometimes exceeds the value of material money. Besides, it is subject to all legal behaviors that respond to the right of ownership. Thus, it is subject to ownership and acquisition. It is not only in the exposure to the material of the thing, but also by the extent of compromising its financial value. The thing may lose Its value while

retaining its material. The punishment is achieved as soon as the value of that thing disappears or decreases (Al-Ghoul, 2017: pp. 229- 232. Al-Haiti, 2016: pp. 278- 279). and among other justifications also, not to add funds to information, data, and programs that leads to depriving them of Criminal protection. Thus, it is difficult to punish the perpetrator. In addition, the information stored within the information system is almost an integral part of these devices or system, but it is also possible that these information devices and systems derive their value from this information, data, or programs (Al-Khikani, 2013: 39).

The two researcher believe that the first trend is the closest to the right one. In fact, the traditional legal texts, especially the texts of the Iraqi Penal Code, were drawn up a long time ago before these crimes appeared beside the justifications mentioned by the jurists in this trend.

Second; The punishment prescribed for the crime of information destruction

Having clarified the doctrinal difference about the possibility of applying the traditional texts of the destruction to the crime of informational destruction, the two researchers explain the punishment prescribed to it in the comparative laws.

1. The French Law; The French legislator referred to the sanction prescribed for the crime of informational destruction in Articles (323-2) and (323-3) of the French Penal Code of 1992 in force in 1994. Article (232-2) indicates that everyone who disrupts and spoils the functioning of the information system is punished with imprisonment For a period of five years and a fine of forty-five thousand euros. Article (323-3) indicates that anyone who illegally enters data into a system, deletes, or modifies data contained in the system is punished with imprisonment for a period of five years and a fine of forty five thousand euros.
2. The Emirati law; Article 10 of the Information Technology Crime Law No. (5) of 2012 states that the penalty of imprisonment for a period of no less than five years and a fine of no less than five hundred thousand dirhams and not more than three million dirhams or one of these two penalties is for anyone who intentionally and without the permission of an information program has entered the information network, electronic information system, or any of the information technology means in a way that leads to stopping it from working, disabling, destroying, wiping, deleting, damaging, or changing the program, system, website, data, or information. The penalty shall be imprisonment and a fine not exceeding five hundred thousand dirhams or one of these two penalties if the result is not achieved. The penalty shall be imprisonment and a fine or one of these two penalties for any intentional act intended to dump the e-mail with messages and stop it from working, disrupting it or destroying its contents.

It is clear that the UAE legislator punishes the perpetrators of the informational destruction crime with imprisonment for a period of no less than five years and the estimated fine even if the result is not achieved. Imprisonment and fine or one of these

two penalties is the punishment of committing an act that leads to the destruction of the contents of the e-mail.

The Iraqi law; In the draft law on informational crimes, the Iraqi legislator set the penalty for destruction in various places of this law. Among these texts is the text of Article (6), which stipulates that whoever uses computers and the information network with the intent to commit one of the following acts: ... Second - Destruction or disruption ... shall be punished with life or temporary imprisonment and with a fine of no less than (25,000,000) Twenty-five million dinars and not more than (50,000,000) fifty million dinars. Article (13) stipulates that the punishment is imprisonment For a period of no less than three years or a fine of no less than (5,000,000) five million dinars and no more than (10,000,000) ten million dinars or both of these two penalties for destroying or damaging a signature, medium, or electronic document... The first paragraph of Article (14), stipulates that the penalty is imprisonment for a period of no less than three years or a fine of no less than (10,000,000) ten million dinars and no more than (15,000,000) fifteen million dinars for the destruction, defect, or Malfunctioning an electronic bond or electronic card ... The same article also states that imprisonment for a period of no less than three years or by a fine not exceeding (2 million) two million dinars, and not more than (5000000) five million dinars is the punishment of anyone who intentionally causes damage, disruption, obstruction, or malfunctioning of computers, systems, programs, networks, and the like... The first paragraph of Article (21):“ states A penalty of imprisonment for a period of no less than two years and no more than three years and a fine of no less than (10,000,000) ten million dinars and no more than (20,000,000) twenty million dinars or any of These two penalties are for anyone who enters a site belonging to a company, corporation, or others to change the designs of this site, cancel it, destroy it, or amend it...

As for the level of judicial applications, there is scarcity in judicial decisions regarding the crime of informational destruction despite the fact that the practical reality confirms the occurrence of many at the present time, especially in Iraq.

THE RESULTS

The present study reached a set of results as follows:

1. The crime of destruction in general can be accomplished in two forms; physical; traditional damage and moral damage.
2. The Iraqi legislator did not refer to the crime of informational destruction in the amended Penal Code No. (111) for 1969. Rather, it mentioned the damage in general. There is no effective law criminalizing informational destruction.
3. The crime of informational destruction must be of a moral nature. Otherwise, it is not considered informational destruction.
4. The informational destruction crime is an intentional crime that requires the availability of a general intention.

5. There are many countries that have criminalized the informational destruction in special laws, including the UAE, the Saudi law, and others. Others referred to it in the penal code, including the French law.

CONCLUSIONS

It is clear that the crime of informational destruction is considered one of the crimes of a changing nature depending on the legal system that governs it or the assaulted right. It may be political if it focuses on political rights or the motive was political. It may be a security crime if its commission threatens the security and safety of the state as in the case of destroying information that pertains to the capacity or capabilities of the armed forces because it may be a regular crime in the event that it was the subject of the life information of natural persons.

SUGGESTIONS

The results of the present study lead the two researchers to suggest the following:

1. The Iraqi legislator should adopt the long-standing information crime law and keep abreast of legislative developments in this field as information crimes have become a great danger to society, especially today, with the spread of these crimes significantly.
2. The Iraqi legislator should amend the text of Article (477) of the Penal Code No. (111) for 1969 to add a new paragraph to it that includes a criminalization of informational destruction.
3. All institutions and departments, official and unofficial companies should develop methods to protect their information devices and systems. They should train the staff responsible for these devices and systems in a modern and advanced manner in order to deal with modern methods of penetration and take the necessary measures to prevent them.

REFERENCES

- Afifi, A., (2000). "Computer Crime, Copyright, Artistic Works, The Role of Police and Law, A Comparative Study", Al-Maaref Establishment, Alexandria, Egypt.
- Al-Durrah, M., (1990). "General Provisions in the Penal Code", Dar Al-Hikma Press, Mosul- Iraq.
- Al-Ghoul, M., (2017). "Internet Crimes and the Criminal Responsibility Arising thereof", Badran Law Library, Sidon, Lebanon.
- Al-Hadithi, F. , (2018). "Explanation of the Penal Code - General Section", Al-Sanhouri Library, Baghdad.
- Al-Haiti, M., (2016). "Forensic Research, Specialized in Computer Assaults", Al-Sanhouri Library, Baghdad.
- Al-Hussaini, A., (2017). "Computer and Internet Crime (Information Crime)", Zain Human Rights Publications, Beirut, Lebanon.
- Al-Jubouri, S., (2011). "Legal Protection of Internet Information", Al-Halabi Human Rights Publications, Beirut, Lebanon.
- Al-Khakiani, B.,(2013). "Crime and its Impact on Society", Al-Furat House for Culture and Information, Babylon, Iraq.
- Al-Khalaf, A.,& Al-Shawi, S. (2015). "General Principles in the Penal Code", Al-

- Sanhoury Library, Baghdad-Iraq.
- Al-Qahwaji, A., (2002). "Explanation of the Penal Code - General Section, A Comparative Study", Al-Halabi Human Rights Publications, Beirut, Lebanon.
- Al-Qur'an, M., (2017). "Cyber Crime", Wael Publishing and Distribution, Amman.
- Al-Saadi, H., (1976). "Explanation of the New Penal Code, A comparative analytical study", 2nd edition, Bait Al-Hikma Printing, Baghdad.
- Al-Sagheer, J., (2012). "Criminal Law and Modern Technology", Arab Renaissance House, Cairo, Egypt.
- Al-Sharif, M., (1995). "Encyclopedia of Computer Terminology", 2nd Edition, Academic Library, Cairo, Egypt.
- Ananza, M., (2017). "Criminal Intent in Cyber Crime", Dar Al-Ayyam, Amman.
- Antoni, X. L., Dlepu, A., & Notshe, N. (2020). A Comparative Study Of Financial Literacy Among Undergraduate Commerce And Arts Students: A Case Of A South African University. *International Journal Of Economics And Finance*, 12(2).
- Badawi, M., (2018). "The Role and Responsibility of the Intellectual Property Rights Protection Office for Computer Programs and Databases", An Analytical Authentication Study, Dar Al Kutub and Arabic Studies, Alexandria, Egypt.
- Berejena, T., Kleyhans, I. C., & Vibetti, S. P. (2020). Economic Impacts Of The Rotational Policy On The Food Handlers In The National School Nutrition Programme In Gauteng Province. *International Journal Of Economics And Finance*, 12(2).
- Botani, D., (2016). "Thematic Criminal Protection of Informatics", A Comparative Study, Dar Al-Fikr Al-Arabi, Alexandria, Egypt.
- Catala, P., (1984). "Ebauche d'une théorie juridique de l'information", recueil Dalloz Sirey, paris.
- Derby, A. & Ismail, M., (2012). "Electronic Crime, A Comparative Legal Judicial Study", 1st edition, National Center for Legal Issues, Cairo, Egypt.
- Duman, B., Alpysbaevich, B. T., & Tursynhanovich, Z. E. (2020). Emotional Burnout Syndrome Of Obstetrician- Gynecologists In Different Regions Of Kazakhstan Republic. *11(12)*, 1020–1024.
- Ekonomi, F., & Jaya, U. B. (2020). The Effect Of Corporate Social Responsibility And Good Corporate Governance On Pharmaceutical Company Tax Avoidation In Indonesia. *11(12)*, 977–983.
- Fikry, A., (2006). "Information Systems Crime, A Comparative Study", A PhD dissertation, Faculty of Law, Mansoura University, Egypt.
- Hegazy, A., (2008). "Forgery in Computer and Internet Crime", Legal Books House and Diaspora House for Publishing and Software, Cairo, Egypt.
- Hornung, J. J. (2020). Comments on "Ornitocheirus hilsensis" Koken, 1883 - One of the Earliest Dinosaur Discoveries in Germany. *Palarch's Journal of Vertebrate Palaeontology*, 17(1), 1–12.
- Hosni, M., (2005). "Money Assault Crimes", 3rd Edition, Al-Halabi Human Rights Publications, Beirut, Lebanon.
- Hu, Z., Wang, Y., & Liang, X. (2020). Compatibility of rationality and irrationality reflected by migration behavior in China. *Revista Argentina de Clinica Psicologica*, 29(1), 8–13. <https://doi.org/10.24205/03276716.2020.2>

- Ibrahim, K., (2018). "The Art of Criminal Investigation in Cyber Crime", A Comparative Study, Dar Al-Fikr Al-Arabi, Alexandria, Egypt.
- Ja`far, A., (2013). "Modern Information Technology Crimes Falling on People and Government", A Comparative Study, Zain Human Rights Publications, Beirut, Lebanon.
- Janssen, R. (2020). The Pleated Dress of Nywty.-Palarch's. *Journal of Archaeology of Egypt/Egyptology*, 17(1), 1–11.
- Jia, B., & Zhang, W. (2020). A mental health education strategy based on online videos. *Revista Argentina de Clinica Psicologica*, 29(1), 50–56. <https://doi.org/10.24205/03276716.2020.7>
- Khudhr, S., (2017). "Penal Protection for Informational Money, A Comparative Analytical Study", Zain Juridical Publications, Beirut, Lebanon.

LAWS

- Martínez-martínez, J. G. F. D. (2020). Prosocialidad y dificultades de socialización en la adolescencia . Influencias según sexo y práctica deportiva Método. 29, 117–124.
- Masitenyane, L. A., & Mokoena, B. A. (2020). Antecedents Of Relationship Marketing In A Business-To-Business Concrete Product Environment.
- Matthews, M., & Mokoena, B. A. (2020). The Influence of Service Quality Dimensions On Customer Satisfaction Within Visa Facilitation Centres in South Africa. *International Journal of eBusiness and eGovernment Studies*, 12(2), 122-135.
- Meyer, N., & Klonaridis, R. (2020). The Identification Of Female Entrepreneurs'business Growth Factors: Evidence From South Africa. *International Journal Of Business And Management Studies*, 12(1), 208-224.
- Moral-campillo, L., & Hernández-mendo, R. E. R. A. (2020). Actividad física , funcionamiento cognitivo y psicosocial en una muestra preadolescente. 29(2017), 123–131.
- Moreno-Brid, J. C., Gómez, J. S., & Franco, L. Á. M. G. (2020). Mexico's Latest-And Probably Last-Package Of Market Reforms (2012-18): The Remains Of The Day. *Cuadernos De Economía*, 39(Spe80), 425-443.
- Mosala, K., & Chinomona, E. (2020). Motorists Attitudes Towards Implementation Of E-Tolls In Gauteng Province, South Africa. *International Journal Of Ebusiness And Egovernment Studies*, 12(1), 48-62.
- Mustafa, M., (1984) "Explanation of the Penal Code - Special Section", 8th Edition, Cairo University Press, Egypt.
- Ormaechea, E., & Fernández, V. R. (2020). Discontinuous continuity: Structural change and its (divergent) meanings in Latin American structuralism and neo-structuralism. *Cuadernos de Economía*, 39(spe80), 445-469.
- Qashqosh, H., (1992). " Computer Crimes in Comparative Legislation", Arab Renaissance House, Cairo, Egypt.
- Qurah, N.,(2003). "Economic Computer Crime; A Theoretical and Applied Study", Arab Renaissance House, Cairo, Egypt.
- Senekai, Q., & Lenz, R. (2020). Decolonising The South African Higher Education Curriculum: An Investigation Into The Challenges. *The International Journal Of Social Sciences And Humanity Studies*, 12(1), 146-174.
- Shliakhovchuk, E., & García, A. M. (2020). Intercultural perspective on impact of video games on players: Insights from a systematic review of recent literature.

- Educational Sciences: Theory and Practice, 20(1), 40–58.
<https://doi.org/10.12738/jestp.2020.1.004>
- Sorour, A., (2015). "The Mediator in the Penal Code - General Section", 6th Edition, Dar Al-Nahda Al-Arabia, Cairo, Egypt.
- Talan, T. (2020). The effect of mobile learning on learning performance: A meta-analysis study. Educational Sciences: Theory and Practice, 20(1), 79–103.
<https://doi.org/10.12738/jestp.2020.1.006>
- Tamam, A., (2000). "Crimes arising from the use of computers", Arab Renaissance House, Cairo, Egypt.
- The French Penal Code of 1992 in force in 1994.
- The Iraqi Informatics Crime Bill 2011; not approved yet.
- The Iraqi Penal Code No. (111) for 1969.
- The UAE Information Technology Crime Law No. (5) of 2012.
- The UAE Penal Code No. (3) of 1987.
- Van Den Berg, L., & Surujlal, J. (2020). The Relationship Between Coach Guidance, Feedback, Goal Setting, Support And A Long-Term Development Focus Of University Athletes. The International Journal Of Social Sciences And Humanity Studies, 12(2), 273-288.