PalArch's Journal of Archaeology of Egypt / Egyptology

# CYBER ESPIONAGE IN JORDANIAN PENAL LEGISLATION

*Professor assistance Dr-Ibtisam Saleh*

Amman Arab University Jordan

ibtisammousasaleh@gmail.com

**Professor assistance Dr-Ibtisam Saleh: Cyber Espionage in Jordanian Penal Legislation-- Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(6). ISSN 1567-214x**

**Keywords: electronic espionage, state secrets, data, information, hacking, Espionageforms, Jordanian electronic crime law, The subject of espionage**

## ABSTRACT

In this study, we will address the most serious electronic crime against information security and the security of individuals, which is cyber espionage according to the Jordanian criminal legislation.

The Jordanian legislation has dealt with espionage crimes in the Protection of State Secrets and Documents Law No. (50) 1971, and addressed cyber espionage in Article (12) of the Electronic Crime Law. In order for an understanding of Article 12 to be straightforward, it is necessary to begin with a clarification of the concept of espionage and in particular cyber espionage and mention its forms. And then address espionage crimes according to the Protection of State Secrets and Documents law in terms of their forms, which are limited to three crimes: 1- entry or attempting to enter prohibited places, 2- theft and obtaining state secrets, 3- reporting or disclosing state secrets which could be obtained by holding a specific post. In addition to clarifying the extent of the possibility of committing these crimes by electronic means. Subsequently, we provided an explanation of the cyber espionage stipulated in Article 12 of the Electronic Crime Law, in which we clarified its three pillars; the physical aspect, the subject of the crime and the moral aspect, and we clarified the penalties imposed on the perpetrators of electronic espionage. Finally, the researcher presents a number of results that are rational based on the topic of the current study.

## 1.Introduction

Espionage is a phenomenon that dates back to ancient timeswhich emerged along with the development of life, science and technology. Since the dawn of history, the information held by different parties about each other was one of the most important factors that determinetheir fate and the preponderance of their strength. The importance of information increased

more and more with the arrival of the digital age, as it became a new force in peoples' lives, state administration and governance. In addition to the fact that controllingdatawarehouses and the means of processing them became more important than natural resources as a source of economic, industrial and military power.

The advent of the digital age, led the great majority of the countries tobecomeconnected to the global information network. Also, the state administration and the functioning of its facilities depended on electronic information systems. These electronic systems were repositories of government documents and secrets, therefore the traditional espionage methods shifted to the cyber espionage including thehacking of systems and networks of countries which as a result gave way to crimes challenging the security agencythroughlegal loopholes. This enabled individuals and other parties to obtain government secrets, which are often stored in a digital format in secret servers (Abdul Muttalib, 2001, p. 31)

## 3. The concept of electronic espionage

3.1 Jurisprudence has attempted to establish a definition of espionage, but there are different definitions that depend on the nature of criminal behavior in the legislation under study, because criminal policy varies from one country to another, and espionage crimes differ fromone legislation to another, as a result definitionvary (Al-Nuwaisah, 2017, p. 357).

It was defined as: the transfer or disclosure of news or an issue that is considered a state secret, and that would harm the interests of the countryby any external or internal party, whether for or without a benefit (Jafar, 2013, p. 568)

In addition to being defined as a type of intelligence work that aims to search and access information related to a country and transfer it secretly from its place to another place by agents of another country (www.fatehmedia.net)

It is noted that most of the penal legislations did not assign a specific definition for espionage, but rather only identified acts that are considered espionage crimes, such as in the Egyptian and French law. As for the Jordanian legislation, we find that it did not use the term espionage. It is not mentioned in any criminalization texts except that it indicates a violation of state secrets as stated by the State Security Court Law. According to Article 3 of this law, the court is concerned with espionage crimes that violate the provisions of Articles 14, 15, 16 of the Law of Protection of State Secrets and Documents of 1971. Although there is no agreement on a unified definition of espionage, what is agreed upon is to consider espionage as a crime against the external security of the state.

Regarding the international law, Article 46 of the 1977 Protocol to the Geneva Convention of 1949 defined the spy as the one who collects or attempts to collect information of military value in secret or by using fraud and deception.

Cyber espionage is defined as the use of modern information technology means to penetrate illegally or in an unauthorized manner into electronic information systems of countries and governments and commit interception, with the intention of obtaining important information related to its systems and its secrets including all types of military, security, political, economic, scientific and social information. (Jaafar, 2013, p. 569)

We can define the cyber espionage intended in Article 12 of the Jordanian Cybercrime Law as: "The offender's access to the information network, information system, or website to obtain electronic content not available to the public that affects national security, the state's external relations, public safety, or the national economy.

### 3.2 Espionage forms

Espionage in the current era has become inclusive to several domains, as it is no longer limited to the military and belligerent aspects, although theyare one of the most dangerous aspects of espionage. The required information is now different compared to the past, therefore, the numbers of armies and their traditional equipment are no longer considered secret matters, we actually find that such matters are circulated in the pages of newspapers and television programs when a crisis occurs in a specific region, and mapping takes place to represent the size of the forces in neighboring countries located near conflict areas. Nonetheless, there is a profound military espionage especially among the major countries, thus these countries seek to obtain military war secrets, in order to obtain information on the progress of others since there is a race in advanced nuclear, chemical, and radiological armaments. As for the countries that import such technology, they receive old armswhich areineffective and considered waste. For this reason, the developed countries seek either to sell them with easy installments plans, or to provide them as aid to the poor third world countries (Al-Nuwaisa, 2017, p. 360).

Espionage may target economic, commercial and financial information to determine the economic capacity of a certain country, its resources, its vital economic facilities, locations, financial and monetary status, level of trade and reserves, and the period during which it can rely on itself in case it became besieged, as well as its debts. (Hafiz, 2010, p. 8).

Espionage can be related to information related to research, studies and scientific inventions at all levels including; military, industry, agriculture, engineering or health. Scientific espionage is committed by accessing these scientific secrets with the aim of stealing them or aiming to take the necessary precautions to confront them (Jafar, 2013, p. 571)

There is also political espionage, which aims to know the political positions of state decision makers and information related to internal and external policy. Espionage can be related to the psychologyof the people and leaders of the state, by obtaining knowledge on the strengths and weaknesses of the people's personalities, factors of unity and separation, prevailing values in society, partisan and religious movements, and the extent of their influence in crises (Kamel, 1996, p. 85)

Accordingly, all previous confidential information, whether military, political, economic, scientific or social, can be in the form of electronic content, and even if this content is surrounded by information security means, the electronic repositories in which these secrets existare vulnerable to access, acquisition and disclosure.

### 3.3 The position of the Jordanian legislation regarding electronic espionage

At the present time, technology has made it possible to create new tools and means that were not previously known for espionage purposes. Among these means that have emerged and were exploited by spies is the use of information systems, information networks and websites to obtain secrets. Therefore, countriesmade sure to providelegal protection to their secrets and most of them criminalize acts that affect their secrets through traditional texts in their penal laws. As for the Jordanian legislation, these crimes were excluded from the Penal Code and wereaddressed in a special law; the Law on Protection of State Documents and Secrets, No. 50 of 1971. It should be noted that these texts were developed to counter conventional espionage.

Cyber espionage was considered an electronic crime under the Cybercrime Law according to Article 12 as follows:

A- Any person who intentionally accesses without a permit or in contravention of or exceeding the permit the information network or an information system by any means with the aim of viewing data or information not available to the public that affects the national security, external relations of the Kingdom, public safety or the national economy shall be punished with imprisonment for a period of no less than four months and a fine of no less than (500) five hundred dinars and not more than (5000) five thousand dinars.

B - If the access, referred to in paragraph (a) of this article, was with the intention of canceling, destroying, damaging, modifying, changing, transferring, copying or disclosing that data or information, the perpetrator shall be punished with temporary hard labor and a fine of no less than (1000) one thousand dinar and not more than (5000) five thousand dinars.

C - Whoever intentionally accesses a website to review data or information not available to the public that affects the national security, external relations of the Kingdom, public safety, or the national economy, shall be punished with imprisonment for a period of no less than four months and a fine of no less than (500) five hundred dinars.

D - If the entry referred to in Paragraph (C) of this Article was with the aim to cancel that data or information, destroy it, damage it, modify it, change it, transfer it or copy it, the perpetrator shall be punished with temporary hard labor and with a fine of no less than (1000) thousand dinars and not more than (5000) Five thousand dinars.

Thus, it is noted that the Jordanian legislation has criminalized access to the information network, information systems, or websites that contain the state's secrets, and increased the penalty if the perpetrator's goal is to do harm with these secrets.

## 4. espionage crimes in the Jordanian protection of state's secrets and documents law and the extent to which they can be committed by electronic means

It is known that the crime of espionage is one of the crimes that affect the security of the state, and in the light of this, it is easily understood since it is the first pillar in this crime. It is by necessity a piece of information or a document related to the state, which the state is keen to keep confidential, and those secrets that individuals keep and do not disclose, regardless of its value to its owners, are not included under this concept. (Al-Manasa, Al-Zoabi, 2010, p. 304)

The second pillar deviates from the same concept to the secret as a concept related to the activities of the private sector, its relationship with society and individuals in it, and the private relations arising from all of that, whether it is of an economic, financial or informational nature, or it is a sporadic data with meaning, or social or environmental secrets. (Naeem,2006, p .229)

### 4.1 The subject of espionage in the Law on the Protection of State Secrets and Documents

The Law on the Protection of State Secrets and Documents was adopted to examine the concept of secret, its applications, and the foundations and framework for its protection.

To achieve protection, Initially, two conditions must be fulfilled: (Al-Manasa, Al-Zoubi, 2017, pp. 302-303)

- The existence of secrets or documents belonging to one of the state institutions or one of its bodies, and that these secrets are related to the security of the state.

- That these pieces of information are confidential and their disclosure would harm the internal and external security of the state without indicating the size and nature of the damage.

Article 2 of the Protection of State Secrets and Documents law has been defined as: "Any oral information or written, printed, stored, or printed on waxed paper documents, photocopies, tapes, personal photos, films, diagrams, graphs, maps or the like that are classified according to the provisions of this Law."

The the law of access to public information No. 47 of 2007 has defined the secret as: "Any verbal information or documents written or printed or stored electronically or in any way or printed on waxed paper or copier or

cassette tapes, photographs, films, diagrams, graphs, maps or the like that are classified as confidential or documents protected by the provisions of the legislation in force.

In the two definitions of the secret mentioned above, it can be concluded that the secret related to state security can be in various forms, and that the information can be stored electronically, as the state's secrets are not stored only on paper. Regardless of the storage form, classification and the precautions followed according to Procedures of the Protection of State Secrets and Documentslaw give the information the status of a secret.

Secrets do not have a single degree of protection. The State Law on the Protection of Secrets and Documents has classified secrets, and singled out specific protection for each of them, dividing them into three categories: very secret, confidential and limited.(Jaafar, 2013, p. 570)

**First: Secrets and documents classified as "secret" according to Article (3)**

Including plans and details of military operations or documents related to internal security and all documents and information related to foreign policy and international relations which include information and documents related to military intelligence or the means of public intelligence and those who are involved in it, as well as any information related to weapons, ammunition, army equipment and sources of its strength.

**Second: Secrets and documents protected in a "highly classified" degree, according to Article (6)**

Including documents and information related to one of the state's institutions or its public bodies, which their disclosure would cause harm to the state or benefit another. These include any information and documents on the movements of the armed forces or public security, as well as on the weapons and forces of the Arab countries.(Naeem,2006, p .229)

**Third: Secrets and Documents Classified as"Limited"according to Article (8)**

The documents and information whose disclosure to unauthorized people would cause harm to the interests of the state, embarrassment, administrative or economic difficulties or benefit a foreign country or any other party that may reflect harm to the state. Including information and documents related to an investigation or judicial trial. As well as reports whose content's disclosure would have a negative impact on the morale of citizens unless it is authorized to publish them and any protected information or document that harms the reputation of any official figure or affects the prestige of the state.(Al-Manasa, Al-Zoubi, 2017, p. 302-303)

In fact, criminalization includes these three types, regardless of the degree of confidentiality. This classification, which was developed by the legislation, is beneficial in two aspects:

The first aspect: differentiating preventive measures to keep secrets, so each type of these secrets is kept differently according to the law's provisions.

The second aspect: determining whether a matter is considered a secret or not was limited to the administration alone, but after adopting this law, it became subject to judicial control and it is not enough for the issuing party to say that it is confidential, it also must fulfill the conditions specified by the law (Abu Issa, 2017 , P. 225)

The Jordanian Court of Cassation ruled: "The third article of the Law on the Protection of State Secrets and Documents determined the degree of secrecy and the type of protected documents that are considered as (highly classified), and thus the accused is guilty of the crime of obtaining a highly classified information based on the testimony of the Public Prosecution witness without the need for the State security court to review the information obtained nor verify its applicability to the third article and the law nor identify whether the information is considered (highly classified) or not. Also,the classification of the information by the witness it is not sufficient, rather it must be subject to scrutiny by the court. Discrimination and sanctions 72/2000 dated 04/18/2002.

It is noted that the Jordanian legislation did not set a clear standard for distinguishing between the three degrees of secrecy. It has also exaggerated the ways in which the state's secrets are preserved. Such methods are consideredtraditional which must be reviewed and the law must be modified to be compatible with modern technology. In terms of criminalization, it did not differentiate in punishment depending on the degree of confidentiality of the information or the document that was disclosed.

As for the secrets and documents of the private sector, they differ from those related to the public sector or the aforementioned state and are therefore outside the scope of protection by those texts related to the protection of state secrets and documents, but they fall within the scope of legal texts regulating the activities related to them. For example, the secrets and documents related to trade and industry are subject to the laws of unfair competition and the protection of trade secrets No. 15 of 2000, and secrets and documents related to a certain profession are subject to the laws governing that professionFor example, the documents and secrets of legal work and all the contents of the secret and the document and its protection within the legal profession are subject to the Law of the Bar Association.(Al-Nuwaisa, 2017, p. 304).

### 4.2 The extent to which espionage can be committedby electronic means according to the Law on the Protection of State Secrets and Documents

Espionage was mentioned in Articles (14-16) of the Law on Protection of State Secrets and Documents, namely the crime of entering or attempting to enter prohibited places, the crime of stealing state secrets and the crime of informing or disclosing security secrets without a legitimate reason. We

will present the provisions of these crimes and the possibility of committing them by electronic means.

### 4.2.1 The crime of entering or attempting to enter prohibited places

Article 14 of the Law on the Protection of State Secrets and Documents addressed this crime, which stipulated that:

"Whoever enters or attempts to enter a prohibited place in order to obtain secrets, objects, protected documents or information that must be kept confidential in the interest of the safety of the state, he shall be punished by temporary labor. If this attempt occurs for the benefit of a foreign country, he shall be punished with labor for life, and if the foreign country is an enemy, the penalty shall be the death sentence."

It is clear from the above text that this crime is based on two pillars: a physicalaspect which is the entry of the perpetrator or his attempt to enter a prohibited place. However, it has a moral aspect which is the intention to obtain secrets, documents or things that must remain secret in the interest of the safety of the state.

The criminal action in this crime assumes entry and bypassing the place. The criterion of criminalizing the act is that the person has moved his body to the place of entry to which he is not authorized that is, he has no right according to his duty or job to enter the place. The legislation did not identify specific means of entry; it may be done by traditional means such as breaking and barging. We adopt the doctrinal trend that criminalizes using means by which pieces of information are obtained without having to enter the place such as photographing and flying over places which are not covered by the text. However, Article 13 of the Aviation Law Jordanian Civil Society for the year 1985 criminalizes Flying over forbidden areas and photography (Jabour, 2011, p. 189)

To consider the act a crime, it is not required that the perpetrator obtains the secret, that is, it is not required that a certain result be achieved, since it isdangerous crime.

Entry or attempted entry must be to prohibited places, and prohibited place are not specified in the law, therefore, identifying them is left to the competent authorities as the situation demands, although these places in time of war and the disturbances are more apparent. These places are mostly military installations and defense facilities, and they are heavily guarded. Signs are often placed to indicate that these places are prohibited, and it is forbidden to cross them, approach them or even take photographs within the area (Al-Fasel, 1965, p. 38).

From the aforementioned, it is clear to us that entry to places must be in the physical sense, as the text of Article 14 above is established on a physical basis. In addition, what is referred to as a prohibited place is a real place and not virtual, such as websites and information systems. Thus, it isimportant to take into consideration the inadmissibility of analogyout of respectfor legitimacy.

### 4.2.2 The crime of stealing or obtaining secrets related to state's safety

Article 15 of the Law on the Protection of State Secrets and Documentsstipulates:

A- Whoever steals or obtains secrets, objects, documents, or information such as those mentioned in the previous article, shall be punished with temporary labor for a period of not less than ten years.

B - If the felony is committed for the benefit of a foreign country, the penalty is laborfor life and if the foreign country is an enemy, the penalty will be the death sentence.

This crime assumes:

First: The perpetrator is one who is not authorized to obtain a secret, that is, he who has stolen or obtained it is not a person whom the law allows by virtue of their work to review it.

Second: That the subject of theft is one of the secrets related to the safety of the state, and this is the basis for the seriousness of this crime and changing its description from theft crime or financial crime to an espionage crime. The subject of this crime must relate to the secrets of the state, by which obtaining them harms the internal and external security of the state. (An-Nawaisa, 2017, p. 368)

Third: The physicalaspect, which the Jordanian legislation has restricted to theft or obtainment, and has equated them. Infact the term obtainmentis not equal to the term theft as it is more general and broad, and it accommodates all the means that the perpetrator uses to obtain a secret, including theft. A perpetrator must have sought to obtain the secret, and if he reached it without intentionally seeking it, then there is no punishment for it as indicated in the article mentioned above.

Regarding the extent to which espionage can be committed by electronic means, we find that the theft of secrets is not committed by electronic means because the Jordanian legislation defined theft in Article 399 of penalties as taking the movable property of another person without his consent. "This means that theft is a physical activity performed by the perpetrator which involves moving the subjectof theft, dispossession and denying the owner of possession. It does not occur except on movable and material objects, and therefore the crime of theft does not occur if the perpetrator obtained electronic content classified as a state's secret in case it is obtained without theprop, such as an electronic memory or disk on which electronic information is classified as a state's secret.(Qurah, 2005, p. 320)

While the term "obtainment" includes all forms and means of obtaining secrets and therefore it is possible that the means of obtaining a secret are electronic, meaning that this crime could be conducted through technological means and is included in the text. To commit this criminal behavior, it is imperativeto fulfill the following: (Al-Manasa, Al-Zoubi, 2010, p. 309)

1- Access to the place whereelectronic secrets and documents are stored.

2- That these electronic secrets and documents be protected.

3- That the perpetrator is able to obtain those secrets and documents or any copy of them, since extortion of the secrets from their place makes it a crime of electronic destruction.

4- That the perpetrator has the moral aspect, meaning that he has knowledge and will. The knowledge of the nature, location and importance of the secrets obtained, and that his actions are criminalized by law and punishment would be imposed. Nonetheless has the will to obtain them.

**4.2.3 The crime of informing or disclosing state secrets obtained through holding a certain job**

Article 16 of the Law on the Protection of State Secrets and Documents addresses this crime stipulating:

A- Any person who came to his possession or knowledge any of the secrets, information, documents that are protected by virtue of his job or as an official or after giving up his job or his responsibilities for any reason, and then informs or discloses it without a legitimate reason, shall be punished by temporary labor for a period of not less than ten years.(Al-Kayyali, 1990,p.229)

B - He shall be punished with labor for life if he discloses the secrets for the benefit of a foreign country, and if the foreign country is an enemy, the penalty shall be the death sentence.

It is noted that the physicalaspect of this crime is reporting or disclosure, and the legislation did not identify a specific method, therefore the concept of the text includes the behavior in its moral sense and its formsin which information systems means and techniques are used. (Abu Issa, 2017, p. 232)

To commit this criminal behavior electronically it is imperative to have the following elements:

1- The assumption that the information, secrets, or electronic protected documents are initiallywithin the perpetrator's access, and this is achieved by one of the following:

- Committing a previous crime, in which the perpetrator obtained those electronic secrets, documents or information that are protected in a traditional way or by new electronic methods.

- The existence of those protected secrets, documents or electronic information within the access of the perpetrator,for example, by virtue of the job.

2- That the perpetrator informs another person or at least another body of those secrets, documents, or protected electronic information, whether with its content and substance, or whether in full or in part. Also, disclosing

those secrets, documents or protected electronic information to all, by placing it on a suitable electronic medium, allowing everyone to review them.

3- That the perpetrator achieves this by electronic means, such as using information systems, the Internet, and others.

4- That the perpetrator has a criminal intention based on knowledge and will (Al-Manasa, Al-Zoubi, 2017, pp. 310-311)

**Espionagein the Jordanian electronic crime law**

According to the stipulations of Article 12, this crime consists of three aspects: the physicalaspect, the subject of the crime, and the moral aspect.

**5.1 Physical aspect**

The unauthorized access or violation of or exceeding the permit of entry to the information network or information system represented in the crime mentioned in Article (12 / A) and if to a website as represented in the crime mentioned in Article (12 / C). The act of entry is the behavior that constitutes the physical aspect of this crime. A perpetrator is not punished for merely attempting since this crime is considered a misdemeanor, and there is no text that punishes misdemeanors in the electronic crime law.

The Jordanian legislation has criminalized hacking in Article (3), but it did not define it, but the explanatory memorandum of the Jordanian law defined it as intrusion or piracy on a website or information system that is not publicly available without permission or in violation of the permit or exceeding it. (Explanatory note to the Information Systems Crime Law, 2013, p. 4)

Accessto a protected information system is virtual that is not realistic, however, it is considered trespassing. It is achieved by performing an activity that enables the perpetrator to have access to the system or any of its parts, for a long or short period of time whether the control over the system is achieved or not. It includes all activities that allow access to an electronic information system, and there is no doubt that the mere access to an electronic information system does not constitute an unlawful act, but this entry derives its illegality from being unauthorized, therefore the illegality in this case is the perpetrator’s lack of the authority to enter such a system while having knowledge of it. (Qurah, 2005, p. 319)

Regardless of the means used to have access, they are all equal in the legislation. In practice, the means used by the perpetrator for an unauthorized access varies. In some casesaccess does not require more than turning on the computer or opening the program that turns it on, and in other cases the methods are more complicated, as using the decoder (Abu Issa, 2017, p. 41)

**5.2 Thesubject of espionage in the Cyber Crime Law**

The subject of the crime is technical electronic information and data that affect the national security, the external relations of the Kingdom, public safety or the national economy.

As for the term national security, it is the sum total of the vital interests of the state, such as the protection of the region and independence. It includes everything related to the safety of the state against external and internal threats that may lead to foreign domination as a result of external pressure or implosion. Therefore, when it comes to national security,information and data must be classified according to the Law on the Protection of State Secrets and Documents because of their dangerousness on the one hand and to provide them with criminal protection on the other hand. (Al-Kayyali, 1990, p .331)

Concerning the external relations of the Kingdom, they include everything related to the Kingdom's foreign policy, its relationship with other countries in various political, economic and military fields, and its relationship with international organizations. As for the term public safety, it means controlling what constitutes a general danger regardless of its source, for example, information and data that relate to the risks resulting from the dumping of hazardous waste or the impact of sit-ins and demonstrations on the safety of citizens. (Badawi, 1963, p. 283)

### 5.3 The moral aspect

The moral aspect of electronic espionage takes the form of a general criminal intent which is the same asin the case of an authorized access crime, therefore, the elements of a general criminal intent must be present that areknowledge and will. The perpetrator must be aware that he is penetrating an information system or information network and that this is not authorized, or violates the permit. The element of will is achieved when the unauthorized entry and its resulting outcomes aredesired. In case the perpetrator desirescommitting a criminal behavior without the will to achieve the results of the access, it would be considered an unintended error. For example, if the person accidentlylogs in to a website that is prohibited, it would be considered an offense ofunauthorized stay if he gets informedand yet remains in the system.

Article (12 / a / c) of the Cyber Crime Law requires the existence of a specific criminal intention, which holds that the purpose of access is to see data or information that affects the national security, external relations of the Kingdom, public safety, or the national economy.

### 5.4 Penalties

The Jordanian legislation shall punish anyone who intentionally accesses without permission or in violation of or exceeding the permit the information network or an information system by any means with the aim of accessing data or information not available to the public which affect national security, external relations of the Kingdom, public safety or the national economy by imprisonment for a period of no less than four months

and a fine of no less than (500) five hundred dinars and not more than (5000) five thousand dinars. (Article 12, paragraphs a, c)

However, if the access is for the purpose of canceling, damaging, destroying, modifying, changing, transferring, copying or disclosing that data or information, the perpetrator shall be punished by temporary hard labor with a fine of no less than (1,000) thousand dinars and not exceeding (5000) five thousand dinars. (Article 12, paragraphs b, d)

## 6. Conclusion

The development of legislation made secrets related to the entity of the state, its activities, plans, and capabilities, in addition to everything related to its strength, the size of its army, its armament etc. secure against others' manipulation. The accelerated growth of the electronics, communications and information systems sectors, led the country to rely more and more on information technology in handling its secrets and documents. This technology contributed to the development of methods of processing information and confidential and regular data. However, It also contributed to the diversity of the means of attacking that secrecy and thus increased illegal behaviors and the access of information systems became possible

1- Espionageby electronic means according to the Jordanian legislation is to commit one of the crimes mentioned in the Law on the Protection of State Secrets and Documents by electronic means.

2- The subject of espionage crimes in the Law on the Protection of State Secrets and Documents is a secret or a document classified as one of the state's secrets while in the Cyber Crime Law, the subject of espionage has an electronic content that affects national security, the state's external relations, public safety, or the national economy. This difference arises from thedissimilarity in the legal description of the crime.

3- The terminology mentioned in the Jordanian legislation in Article 12 of the Cyber Crime Law related to the crime's subject was not precisely defined. For example, (National Security) is considered a broad term therefore, it is better in legislative drafting to avoid unspecified terms.

4- The penalty for unauthorizedaccess mentioned in Article 12 of the Electronic Crime Law is more lenient than the penalty mentioned in Article 14 of the Law on Protection of State Secrets and Documents, even though the objective is the same. In fact, the technical virtualaccess has become the dominant form of committing this crime, because its means are easier than the physical access. As a result, we do not believethat this mitigation is valid, and we hope that the legislation will unify the penalties between physical and moral access.

## References

Mamdouh Abdel Hamid Abdel-Muttalib, Crimes of Using the Computer and the Scientific Information Network, Dar Al-Huquq Library, Sharjah, 2001.

Abdel-Ilah Al-Nawaiseh, Information Technology Crimes, Wael Publishing and Distribution, Amman, 2017.

Ali Jaafar, Modern Information Technology Crimes against People and Government, Zein Legal Publications, Beirut, 2013

Amr Abdullah Kamel, Current Challenges and Future Aspirations, Arab-European Studies Center, 1996.

Majdi Mahmoud Hafez, Encyclopedia of the crime of treason and espionage, Mahmoud Publishing House, Cairo, 2010.

Hamza Muhammad Abu Issa, Information Technology Crimes, Dar Al-Majd for Publishing, Amman, 2017.

Osama Ahmad Al-Manasa, Jalal Muhammad Al-Zoubi, Electronic information systems crimes, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2017.

Muhammad al-Fadil, Crimes against State Security, Damascus University, Damascus, 1965

Muhammad Jabour, Crimes against State Security and Terrorism Crimes, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2011.

Abd al-Wahhab al-Kayyali, Political Encyclopedia, Arab Institute for Research and Publishing, Beirut, 1990.

Mohamed Taha Badawi, National and Political Studies, Monchaat Al Maaref, Alexandria, 1963.

Naela Koura, Economic Computer Crime, Al-Halabi Legal Publications, Beirut, 2005.

Moghabb Naeem Protecting Computer Programs, Rights Publications, Al-Halabi Legal Publications, Beirut,2006

(www.fatehmedia.net)