Asian Social Science; Vol. 16, No. 12; 2020
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Criminal Protection of Privacy in the Jordanian Cybercrime Law No. 27 of 2015

Wejdan Suleiman Irtaimeh[1]

[1] World Islamic Sciences and Education University (WISE), Jordan

Correspondence: Wejdan Suleiman Irtaimeh. E-mail: wejdan02@yahoo.com, or wijdan.irtaimah@wise.edu.jo

Received: September 15, 2020 Accepted: November 24, 2020 Online Published: November 30, 2020

doi:10.5539/ass.v16n12p64 URL: https://doi.org/10.5539/ass.v16n12p64

Abstract

This study deals with the issue of criminal protection of privacy in the Jordanian Cybercrime Law No. 27 of 2015, as the great developments in computer technologies and the widespread use of the Internet have led to the emergence of new forms of electronic crimes related to the protection of the privacy of individuals. The study indicated that the Jordanian legislator did not include in the Jordanian Constitution or in the Cybercrime Law any definition of the right to privacy that delineates its boundaries and clarifies its features. The study concluded that the Cybercrime Law was ambiguous in some of its articles, especially those related to the protection of the right to privacy. The Jordanian legislator did not include special provisions that explicitly criminalize assault on privacy, as it included provisions for other crimes that include assault on this right, which made it lose clarity, precision and accuracy of wording. Moreover, such provisions omitted other forms of electronic crimes related to the right to privacy, which constituted a legislative deficiency. The study concludes that there is a need to amend the Cybercrime Law No. 27 of 2017 and to have explicit provisions that stipulate the criminalization of assault on privacy, as well as the need to issue a special law to protect the personal information of individuals.

Keywords: Criminal Protection, Privacy, Jordanian Cybercrime Law

1. Introduction

The right to privacy is one of the most important human rights stipulated in international human rights legislation and one of the constitutional rights inherent to a natural person for his human character. It is a basic principle in every democratic society. It is a right based on the freedom of a person to practice his life naturally without interference in his affairs, away from being watched by others. It indicates tranquility, solitude and calm. Therefore, privacy received constitutional and legal protection throughout the world.

Modern technologies have a clear impact on the right to privacy, as these technologies have facilitated easier ways to violate this right. If the use of computers in the field of collecting information and processing data related to the privacy of individuals has a positive impact on the State's regulation of civil and commercial legal transactions for individuals, making use of them at the general national level, this positive impact of the use of modern technologies has a negative impact, as the development of modern technologies, and the accompanying collection and storage of personal data, have facilitated assault on the private lives of individuals, through the illicit dealing with this data and the unlawful exploitation thereof, which constitutes a real threat to the privacy in the digital environment. If the traditional provisions are sufficient to a large extent to protect the privacy of individuals in the face of the attacks that affect them by traditional means, they are not sufficient in facing this assault on the private lives of individuals in the digital environment, which required legislative intervention to enact laws to confront the new crimes that target information systems. As a legislative response, the Jordanian legislator has issued the Cybercrime Law No. 27 of 2015.

Study Problem: It is represented in showing the adequacy of criminal protection of privacy in the Jordanian Cybercrime Law No. 27 of 2015

Study Objectives: This study aims to clarify the nature of privacy and the development of its concept, highlight the most important forms of assault on privacy in the digital environment, and identify the features of the criminalizing and punitive policy of the Jordanian Cybercrime Law in confronting the assault on privacy through modern electronic means, in order to highlight the extent of adequacy of the criminal protection of privacy in the Jordanian Cybercrime Law No. 27 of 2015.

Study Methodology: The descriptive and analytical approach will be used to address the topic of the study and analyze its content, by describing the privacy of what is the situation in the Jordanian legislation, and analyzing the relevant provisions of the Cybercrime Law. This study will also depend on the comparative approach in some parts to demonstrate the strengths and weaknesses in Jordanian legislation.

2. What Is Privacy

The right to privacy is one of the basic rights guaranteed by international covenants, as stipulated in the Universal Declaration of Human Rights[1], and in the International Covenant on Political and Civil Rights (ICCPR)[2], as well as the Jordanian legislator explicitly stipulated the right to privacy in the Jordanian Constitution of 1952 and its amendments of 2011, in the second paragraph of Article 7, which states:" *Every infringement on rights and public freedoms or the inviolability of the privacy of Jordanians is a crime punishable by law".*

Despite the criminal protection granted by international and national legislation to privacy, it did not set a clear and comprehensive definition for the concept of privacy, due to the difference in customs, traditions and values in society, as well as the perception of some members of society for some concepts that some consider to be a secret that should be concealed, while others consider the same not to be confidential, and thus must be declared to others. In some societies, for example, there are those who conceal the secret of their marriage for personal reasons, therefore some consider this marriage not to be confidential, and thus must declared to others, and this is because the principle of privacy sometimes follows the traditions, customs, and the nature of the structure of society.

The French jurist Arthur Mullor summed up the dangers of using information systems on the privacy of individuals, that because the computer has an insatiable appetite for the collection of information, and because of its accuracy and huge memory, life may be turned with it upside down, therefore it would be subject to a strict control system with which society turns into a transparent world in which people's homes, financial transactions, and their physical condition are watched by anyone.[3]

It is evident in the studies that dealt with the right to privacy that there is no agreed general definition commensurate with the legal use. Therefore, the legislations that stipulated the right to privacy did not define it, for example the French legislator, and this applies to the Jordanian legislator. Despite the Jordanian legislator's declaration of the principle of the right to privacy in Article 7 of the Constitution, however, it did not provide any definition thereof and did not specify its content, because the idea of privacy is one of the flexible ideas that do not have fixed or stable boundaries, so the jurisprudential views on defining privacy have varied in a way in which there is no specific definition for privacy that could mark a legal scope for application and practice. Jurisprudence and the judiciary in various legal systems have made privacy in two trends: The normative trend, whose supporters try to define the meaning of the right to privacy based on a specific standard without addressing its elements and defining its cases. As for the enumerative trend, it defines the concept of the right to privacy by drawing up lists enumerating its cases and identifying the constituent elements. This is what the French jurists did, as they tried to compile a list of cases and matters that fall within the limits of privacy, including professional life, family life, illness, salary disclosure, the right to image, name and the right to oblivion. Some added the inner spiritual life that one practice behind their closed doors.[4]

Some of them put privacy in two frameworks; an objective framework based on the distinction between the public life of people and what is considered privacy; and a relative framework that deals with the privacy of persons by studying people in society from one angle, and the difference of time and place from another angle.[5]

According to historical development, privacy has three main stations; first: recognition of privacy as a right to protect individuals from physical assault on their lives and property, such as the inviolability of home, the

[1]Article 12 of the Universal Declaration of Human Rights stipulates the following: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.*

[2] As Article 17 of the International Covenant on Political and Civil Rights stipulates the following: *"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks".*

[3] Bahar, Mamdouh Khalil. *Protection of Private Life in Criminal Law*. Dar Al-Nahda Al-Arabiya 2011, Cairo, p. 16.

[4] See in detail Bahar, Ibid, 228.

[5] Al-Ustaz, Suzan. *Violation of the Privacy via the Internet*, Damascus Journal of Economic and Legal Sciences, Volume 29, Issue 3, 2013, P.429.

confidentiality of correspondence, and the inviolability of the body, which is known as material privacy; second: moral privacy, which is the beginning of the recognition of the privacy of the individual and the protection of his values and moral elements. Then comes the third stage, which established privacy as a general right the scope of which extends to protect the person from all aspects of attacks and interference in his privacy, whatever its appearance or nature. Within the scope of the latter meaning, a new concept of privacy emerged, which related to the impact of technology on privacy, represented in the privacy of information or the right of individuals to control their private information and data in the face of the challenges of the digital age.[6]

Because of the difficulty in setting a specific definition of privacy, some have argued that it is better to leave the matter to the judiciary according to the circumstances and facts of each case, in accordance with the traditions, culture, religious values and political system in every society, which guarantees the privacy of each individual and achieves peace and safety for him away from the interference of others in his life.[7] This study is with this view, as privacy is a flexible and relative idea that develops with the development of time, place and people. It is difficult to define it through the provisions of law. Therefore, it is better for this matter to be assigned to the judiciary.

The American Institute defined the right to privacy by defining the violation of privacy, and accordingly it defines privacy as "every person who seriously violates, without having the right to do this, the right of another person not to have his own affairs being reached the knowledge of others, and for his image not to be exposed to the public's eyes, is considered responsible for this crime".[8] As for the jurisprudential definition, the jurist Martin defined the right to privacy as "the right to the family, personal, internal and spiritual life of a person when he lives in his home behind his closed door." The jurist Dennis defines it as "a description or a status of isolation or not observing and watching others". The jurist Nersom defined privacy as "the right of a person to keep his own secrets that the public cannot know except by his own will ... ".[9]

2.1 Elements of the Right to Privacy

Since it was impossible to completely and comprehensively define the elements of the right to privacy, legal thought tended to enumerate the elements that fall within the scope of privacy. Among the most important of these elements are family life, health status, medical care, phone conversations and private conversations, financial disclosure, political opinions, religious beliefs, the person's place of residence, and the inviolability of home, correspondence, name, image, body, professional and career life, and spending spare time.[10]

2.2 The Legal Nature of Privacy: Is It a Property Right or a Personal Right?

The question arises about the legal nature of the right to the inviolability of privacy, is it considered a property right or a right inherent to the human personality? In this context, the jurisprudence was divided into two main trends: a traditional trend that goes to regard it as a property right. According to this approach, a person has the right of ownership of his body, thus it is permissible for him to dispose of it and make use of it. The adoption of this trend leads to that the person has the right to stop the assault on his own life without the need to prove material or moral damage, in accordance with the rights of the owner. This trend has been criticized on the basis that the idea of ownership presupposes the existence of a right holder and the subject matter of the right, so if the right holder and the subject matter are united, it becomes impossible to exercise such powers.[11] As for the other trend, it is a modern trend that considers the right to privacy among the personal rights inherent to the character of the human being.[12] They are those rights that focus on the constituents and elements of personality because they aim to protect the moral interests of the individual. Considering the right to privacy to be a personal right leads to the victim has recourse to the judiciary to stop this abuse with compensation for the damage caused thereto, without the need to prove that harm.[13] The Jordanian legislation followed the same trend, as the

[6] Ayoub, Pauline Anthony (2009). *Legal Protection of Privacy in the Field of Informatics*. First edition, Al-Halabi Legal Publications, Beirut, p. 43.

[7] Qayyed, Osama Abdullah. *Criminal Protection of Privacy and Information Banks* Without publisher, 1988, p. 6.

[8] Al-Ahwani, Opt. Cit., p. 49.

[9] Al-Obeidi, Osama Ben Ghanem. *Protecting the Right to Privacy in the Face of Computer and Internet Crimes*. The Arab Journal for Security Studies and Training, vol. 23, issue 46, Riyadh, p.53.

[10] Al-Ustaz, Opt. Cit., P. 429.

[11] Bahar, pp. 310 and what follows.

[12] Al-Ahwani, Hossam El-Din. *The Right to Private Life (The Right to Privacy)*, A Comparative Study. Dar Al-Nahda Al-Arabiya, Cairo, pp. 146-152.

[13] Bahar, p. 322.

Jordanian Civil Code of 1976 explicitly stated in Article 48 thereof that there are a set of rights called the rights inherent to the human being. Its recognition of these rights led to legal consequences, as it decided that everyone who has encountered an unlawful assault on a right inherent in his personality may request the cessation of this assault without the need to prove the harm, and thus the principles of Jordanian law have actually recognized that the right to privacy is within the personal rights.[14]

2.3 Legislative Protection of the Right to Privacy in Jordanian Legislation

The right to privacy as one of the rights attached to the personality has received constitutional and legal protection in Jordanian legislation. The Jordanian constitutional legislator explicitly guarantees the right to privacy in Article 7 of the Jordanian Constitution of 1952 and its amendments. Paragraph (1) of Article 7 stipulates that *"personal freedom shall be guaranteed."* The second paragraph of the same article stipulates that *"every infringement on rights and public freedoms or the inviolability of the privacy of Jordanians is a crime punishable by law."* By adopting this right to privacy in the Constitution, it becomes a constitutional right that cannot be violated either by the State or individuals, and the Constitutional legislator has listed some applications of the right to life, including the secrecy of correspondence, as Article 18 of the Constitution stipulates that *"all postal and telegraphic correspondence, telephonic communications, and the other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law,"* and the inviolability of home, as Article 10 stipulates that *"dwelling houses shall be inviolable and may not be entered except in the circumstances prescribed by law, and in the manner provided for therein.."* Article 14 of the constitution also stipulates that "*the State shall safeguard the free exercise of the rites of religions and creeds in accordance with the customs observed in the Kingdom, if such is not inconsistent with public order or morality*". Despite the constitutional and legal protection of the right to privacy, this right is not an absolute right, as exceptions are made thereto, which are represented in the legal authority and the consent of the right holder.

Although the Jordanian Constitution of 1952 and its amendments have explicitly stipulated the right to a privacy, the Jordanian legislator has not provided any definition of the right to privacy that delineates its boundaries and clarifies its features, and this is a praiseworthy deed of the Jordanian legislator, as privacy is a flexible and relative idea that is difficult to define and which develops with the evolution of time, place and people.

In application of the constitutional provisions of the right to privacy, the Jordanian legislator criminalized assault on privacy in the Penal Code by adding Article (348 bis) of the Penal Code relating to eavesdropping or voyeurism, as part of the amendments to the Penal Code of 2011, as Article 348 stipulated Duplicate of the Penal Code as follows: *"Whoever violates the privacy of others by eavesdropping or* voyeurism, *including audio recording, taking photos or using binoculars, shall be punished, based on a complaint, with imprisonment for a period not exceeding three months, and the penalty shall be doubled in case of repetition".*

The Jordanian legislator also incriminated the violation of the freedom of correspondence in Article 356 of the Penal Code, which stipulated the following: *"1. Any person who works for the cable or postal services and misuse the duties of his/her job by viewing sealed letters or destroying or embezzles a letter or reveals its content to another person other than the addressee, he/she shall be punished by imprisonment from one month to one year. 2. Any person who works for the telecommunications services and by reason of his / her office reveals the content of a phone call; he / she shall be punished by imprisonment for six months or a fine up to twenty dinars (JD20)".*

The Jordanian legislator also criminalized assault on the secrecy of correspondence in Article 5 of the Postal and Parcel Regulation No. 2 of 1955, which stipulated the following: *"The secrets of letters and postcards delivered to the postal services shall be protected and it is forbidden to disclose them. Everyone who, by reason of his/ her office, among the employees of the postal services, knows the content of a letter and reveals it to another person, other than the addressee, without legitimate cause, he/ she shall be punished according to Article (348) of the Penal Code.* Article 6 thereof stipulates: *Every employee of postal services who conceals or opens a letter delivered to the postal service or facilitates that to others shall be punished according to Article (349) of the Penal Code".*

The Jordanian Telecommunications Law No. (13) of 1995 emphasizes the inviolability of telephone calls and private communications, as it stipulated in Article (56) thereof: *"Telephone calls and private Telecommunications shall be considered confidential matters which may not be violated, under legal liability".* It also criminalized the

[14] AL-Rawashdah, Sami Hamdan. *Criminal Protection of the Right to Private Life*. Master thesis, Faculty of Law, University of Jordan, 1998, pp. 88-89.

dissemination of the content of any communication by means of a public telecommunications network or a telephone message that he/ she revealed by reason of his/ her office or if the same was registered without legal basis. Likewise, the legislator in the Telecommunications Law criminalized assault on privacy, as Article 76 of the Telecommunications Law stipulated the following:" *Any person who intercepts, obstructs, alters or strikes off the contents of a message carried through the Telecommunications networks or encourages others to do so shall be punished by imprisonment for a period not less than one month and not exceeding six months, or by a fine not more than (JD200), or by both penalties".* Article 77 of the Telecommunications Law also stipulated: "*Any person who withholds a message he is obliged to transmit through Telecommunications networks to another person, or refuses to transmit messages he has been asked to transmit by the Licensee or the Commission, or copies or reveals a message or tampers with the information related to any subscriber, including unpublished telephone numbers and sent or received messages, shall be punished by imprisonment for a period not exceeding six months or a fine not more than (JD1000), or by both penalties".*

3. Objective Criminal Protection of Privacy in the Cybercrime Law

The Jordanian legislator did not provide specific and explicit provisions for assaulting privacy by electronic means in the Cybercrime Law, while it included provisions for other crimes that include an assault on this right such as the crime of penetration or illegal entry stipulated in Article 3 of the Cybercrime Law, as well as the crime of using a program for assault on an information system or website, which is stipulated in Article 4 of the Cybercrime Law. Article 5 of the same law dealt with the crime of receiving, obstructing or eavesdropping on electronic correspondence through the information network or information system.

We will discuss and analyze the forms of crimes of assault on privacy in the Jordanian Cybercrime Law No. 27 of 2015.

3.1 Violating the Right to Privacy Through Unlawful Access to Computer Networks or Information Systems

Unlawful access to the information system is considered a necessary stage for the commission of many electronic crimes, as most of these crimes cannot be committed without first accessing the information system, so whoever wants to destroy a specific program in an information system, he/ she must access this system and then destroy it, so it is legislative wisdom to criminalize the act of unlawful access itself. Criminalization provides additional and preventive protection of information systems and websites. The Jordanian legislator criminalized unlawful access in Article 3 of the Cybercrime Law, which states the following:"A- *Anyone who intentionally accesses a website or information system in any manner without authorization or in violation or excess of an authorization, shall be punished by imprisonment for a term not less than one week and not exceeding three months, or by a fine of not less than (100) one hundred Dinars and not exceeding (200) two hundred Dinars, or both punishments. B- Where the access stipulated in paragraph (a) of this Article is for the purpose of cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or stopping or disabling the operation of an information system, changing a website or cancelling, destroying or altering its content or assuming its identity or the identity of its owner, the perpetrator shall be punished by imprisonment for a term not less than three months and not exceeding one year or by a fine of not less than (200) two hundred Dinars and not exceeding(1000) one thousand Dinars, or both punishments".*

By extrapolating the provisions of Article (3), we note that the Jordanian legislator has distinguished between two things: The first one is unlawful access (mere penetration), and the second is access with the purpose of achieving a specific goal. Some believe that linking criminalization to achieving a specific goal is difficult to prove, so the results must to be taken into consideration in order to tighten the penalty.[15]

3.1.1 The Subject of the Crime

It is the information and data related to the privacy of people sent on the information network, information system or website. The Jordanian legislator defined information and data in Article 2 of the Cybercrime Law, where it defined data as figures, letters, symbols, shapes, sounds and images that have no significance on their own. As for the information, it defined it as the data that have been processed and have a significant meaning. From reviewing the definition of the Jordanian legislator for the definition of data and information, we note that the Jordanian legislator has expanded the scope of criminal protection of the information and data sent on the information network, information system or website, including written documents, pictures and audio recordings.

[15] Al-Mana'sah, Osama Ahmed; Al-Zoubi, Jalal Muhammad, Crimes Relating to Information Electronic Systems and Technology, (2017), Dar Al-thaqafah for Publishing and Distribution, Amman, p. 279.

3.1.2 The Physical Element

The physical element of the crime of assault on privacy through unlawful access to the information network or information system is based on three elements, which are criminal conduct, the use of certain means, achieving a result, and the causal relationship.

The crime of violating privacy is achieved by unauthorized access to the information and data related to the privacy of people, which is considered an assault on their privacy, as they are personal and private data and information that the owner wishes to keep secret.

For the crime of abstract access to information and data related to the privacy of persons, it is required that accessing the information network or information system be an unlawful access. If the access is permissible for all people, authorized by law or with a judicial permission,[16] or if it is done with the consent of the data owner, then no crime is established in this case, as the illegality of access is achieved by the access without authorization or in violation or excess of the authorization. Article two of the Cybercrime Law defined the permission as:" *the authorization granted by the person concerned or the competent judicial authority to one or more persons or the public to access or use information system, website or the Internet in order to view, cancel, delete, add, change, re-disseminate data or information, block access, or stop the operation of the hardware, change a website or cancel or modify its contents"*. The permission may be in the form of a password or identification code.

Unlawful access to information and data related to the privacy of persons in this case is achieved by anyone accessing the website or information system using a password obtained illegally or by penetrating the protection system by breaching the password or identification code. In some cases, the permission is not a password or an identification code, but rather it is by allowing a certain group or persons to access an information system or an information network located inside a certain place, such as an institution or a company. Therefore, this crime occurs through the exploitation of a person for his physical presence within that institution and thus intentionally accessing the information system or its own website without being among the persons authorized to access.

Likewise, the criminal conduct is achieved by the perpetrator's exceeding of the limits of the permission or license granted to him, such as allowing a specific person to access a website or information system for a certain period but he/ she intentionally exceeds that period, or if he/ she is allowed to access a specific section within the information system or the website but he accesses beyond that and intentionally accesses another section within it, such as the system of employees or their mails. The Jordanian legislator did not require that access be carried out by a specific manner, as all manners in its view are the same, and this is expressly stated in Article 3/1 of the Cybercrime Law which states: *"Anyone who intentionally accesses a website or information system in any manner without authorization…".*

The criminal conduct of this crime is achieved through the realization of the fact of complete or partial access to personal information and data, that is, the perpetrator's intention is merely personal access to personal data, and this is done with full the perpetrator's understanding and perception of this information and personal data. However, if this data is personal information in a language that the perpetrator does not understand, then this access cannot be achieved.[17] The Jordanian legislator has criminalized the act of mere access as a formal crime that is completed by simply performing the act of unauthorized access, even if the perpetrator did not access or obtain the data.

The Jordanian legislator criminalized unlawful access and exceeding the limits of the permission, but it did not criminalize the illegal continuance, which is in the cases in which access is legitimate, i.e. authorized, but the permission expires and the person remains accessing the system, or in cases where access is illegal, where the crime does not exist, like accidental access, which constitutes a legislative failure that leads to the impunity of criminals.

3.1.2.1 Criminal Result

The crime of unlawful access in the Jordanian Cybercrime Law is a formal crime that simply takes place by accessing the information system or the information network on the website with the purpose of assaulting data or information. The crime of unlawful access is not required to achieve the criminal result, and the occurrence of

[16] As Article (88) of the Jordanian Criminal Procedure Code stipulates *that the public prosecutor may confiscate all letters, newspapers, publications, and parcels of post offices, as well as all telegraphic messages of telegraph offices and he may monitor telephone conversations whenever this is useful for revealing the truth.*

[17] Al-Mana'sah, Opt. Cit., p. 246.

damage or its amount is not taken into consideration.[18] The Jordanian legislator has tightened the punishment for this crime if the perpetrator intended to achieve a specific result, whether this result was achieved or not, as the Jordanian legislator distinguished between the purposes of accessing the information network or information system on the one hand and the purposes of accessing the website, on the other hand, in Article 3 of the Cybercrime Law. According to Paragraph B, the punishment for accessing the information system is increased if the purpose of access is to cancel, delete, add, destroy, reveal, destroy, block, modify, change, transfer or copy data or information, or stop or disable the network or the information system. As for the purposes of accessing the website, it is stipulated in Paragraph C of this Article, where the penalty is more severe if the act is for the purpose of cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or stopping or disabling the operation of an information system, changing a website or cancelling, destroying or altering its content or assuming its identity or the identity of its owner.

3.1.3 The Moral Element

The crime of unlawful access to information and data related to the privacy of persons is an intentional crime, for which the general criminal intent, represented in knowledge and will, must be met, as the perpetrator must be aware that he is accessing the crime scene, which is the information system, information network, or website for the purpose of viewing personal data and information, and that his/her access is without authorization or in violation or excess of the authorization. It is stipulated that his/ her will shall be directed to the place of the crime just for personal access to this information or data and shall not go beyond this intent.

3.1.4 Punishment

The Jordanian legislator punishes whoever commits the crime of unlawful access to the computer network or information system by imprisonment for a period of no less than a week and not exceeding three months or a fine of no less than (100) one hundred dinars and not exceeding (200) two hundred dinars, or with both penalties. As for the crime of unlawful access to websites, it is punishable by imprisonment for a period of no less than three months and not exceeding a year, and a fine of no less than (200) two hundred dinars and not more than (1000) thousand dinars.

By extrapolating the provisions of Paragraph (B) of Article 3 of the Cybercrime Law, it becomes evident to us that there is a required condition related to the intent of the perpetrator, represented in the existence of a specific goal and purpose for cancelling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring or copying data or information or stopping or disabling the operation of an information network or information system.

We note that the legislator has expanded on the goals that constitute an aggravating circumstance for the crime of penetration or unlawful access, and this aggravating circumstance is not based upon achieving any of the unlawful access's goals provided for, as the aggravating circumstance is established whether or not the perpetrator's goal of access is achieved, i.e. the goal of the acts provided for, or not achieved, which results in the difficulty of proving this goal.

On the basis of this personal aggravating circumstance, the punishment is increased so that imprisonment becomes for a period of no less than three months and no more than a year, or a fine of not less than 200 dinars and not more than 1,000 dinars. As for the penalty for the crime of unlawful access, it was imprisonment for a period of not less than a week and not exceeding three months, or a fine of 100- 200 dinars. We see that this aggravated punishment does not fit the philosophy of aggravation, since we note that the judge does not have the right to combine the two penalties of imprisonment and fine even though the aggravating circumstance has arisen, as the judge may not sentence the perpetrator to imprisonment, contenting himself with passing a fine to the stipulated minimum of two hundred dinars, which does not constitute a deterrent punishment. Therefore, we have to ask: How is the penalty of a fine of 200 dinars considered a penalty for an aggravating circumstance.

3.1.4.1 The purposes of illegal access to the information system stipulated in Clause B of Article 3 of the Cybercrime Law

They are as follows:

- Cancelling, deleting, adding, destroying, extinguishing or altering data or information:

Cancellation means removing personal data or information, whether in whole or in part, and the meaning of

[18] Al-Nawaysah, A.-E. (2017). *Information Technology Crimes.* Wael Publishing and Distribution House, Amman, Jordan, p. 258.

deleting does not differ from the meaning of cancellation, but it is a technical term more than the term of cancelling, both of which mean removal. Adding means increasing, regardless of its type or form. Destroying means complete removal and elimination. Disclosing is achieved by dissemination.[19] Extinguishing means damage to the data or personal information. As for altering the data or personal information, it means any amendment of the data or personal information that the perpetrator makes without leading to the destruction of this data or information or non-use of it.[20]

The purpose of criminalizing these acts is to grant the data and information stored in an information system or information network the protection granted to the properties and rights protected by law. According to what was stated in the explanatory note of the Temporary Information Systems Law of 2010, these acts were criminalized for lack of explicit legal protection of electronic data and information in penal legislation, in addition to the necessity to treat it as properties and other rights, because electronic information and data have a material and intangible value that is not less than the value of documents, properties and other protected rights. Any of the aforementioned acts may constitute an assault on data and information that may contain studies and personal and private information, which is an assault on privacy.

- Disclosure of personal data or information:

Disclosure is achieved by dissemination.[21] The purpose of criminalizing the intent to disclose personal data or information is to protect the right of the owners of that information and data to maintain privacy and confidentiality. Privacy is based on the idea of a person's right to decide when, how, and to what extent others may share his/her professional, private or personal data or information.

As for the idea of confidentiality, it is based on the idea of a person's right to hide his/ her professional, private or personal data and information from others.[22]

- Changing data or personal information:

Under this clause there are many acts, some of which are deemed to be harmful to individuals, and among them are acts that change personal data or information so that it becomes incomprehensible and the result of changing it extends to causing damage to public service information.

- Transferring personal data or information:

These provisions deal with access to the information system or the information network with the aim of transferring the data or personal information, stored within the information system or the website, from one site to another, as the transfer of data or personal information results in a violation of privacy and confidentiality.

- Copying data or personal information:

Copying means that the perpetrator obtains a copy of the personal data or information belonging to the victim, and thus transfers or stores it in a tool, program, or system, or prints it without deleting it from its original site. Since such an act is considered theft, however, the Jordanian legislator has explicitly stated that it is criminalized due to the seriousness of copying data and information stored by electronic means and the difficulty of detection and proof.[23]

3.1.4.2 As for the crime of unlawful access to a website stipulated in Paragraph (C) of Article 3 of the Cybercrime Law, it differs from the crime stipulated in Paragraph B in terms of the subject matter and form of assault, as Article 3/B criminalizes assault on the information network or system information, while the subject matter of assault in Article 3/C is the website.

Unlike the assault on the information system stipulated in Article 3/A, the Jordanian legislator did not stipulate in Article 3/C that accessing the website be done without authorization or in violation or excess of the authorization, and the reason is that access to websites is generally available. Unlike the crime of unlawful access stipulated in Paragraph (A) of Article 3 of the Cybercrime Law, the Jordanian legislator requires in the crime of accessing the website the availability of a special criminal intent in addition to the general criminal intent, that is the

[19] Al-Nawaysah, Opt. Cit., p. 255.

[20] Qashqosh, Hoda Hamed. *Cyber Crimes in Comparative Legislation*. Dar Al-Nahda Al-Arabiya, Cairo, p. 70 and what follows.

[21] Al-Nawaysah, Opt. Cit., p. 255.

[22] Explanatory memorandum for the Information System Crimes Law, p. 4.

[23] Abu Issa, Hamza Mohamed (2019). *Information Technology Crimes*. Wael Publishing and Distribution House, Second Edition, Amman, Jordan.

perpetrator's goal of accessing the website is cancelling, destroying, altering, changing, operating or assuming the identity of the website or the identity of its owner. Since we have previously shown change, cancellation and destruction as goals of assault on the information and the data stipulated in Clause (b) of Article (3), and in order to prevent repetition, we will explain the meaning of operating and assuming the identity of the website or the identity of its owner.

Operating the site means controlling this site, or what is called occupation of the site, and assuming the identity of the website is to design a site that resembles the original site to delude visitors that this site is the original site, where visitors access this site and put their personal and confidential data related to health, professional, or social status and so on, thus the perpetrator obtains this information for later exploitation.

As for assuming the identity the owner of the site, it is the perpetrator's conduct that would deceive others that he/she is the owner of the site.

Article (8) of the Cybercrime Law[24] included an aggravating circumstance related to the status of the perpetrator in the crime of assaulting the right to privacy by unlawful access to the information network or information system, so that the penalty is doubled if it is committed by those in charge of managing the systems, sites and networks, or if they commit their crimes in connection with the performance of their jobs or works, or by exploiting any thereof.

3.2 The Crime of Assault on Privacy for Using a Program to Attack an Information System or Website Stipulated in Article 4 of the Cybercrime Law, Which Stipulated the Following

"Anyone who installs, publishes or uses intentionally a program through an information network or information system, with the purpose of canceling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring, copying, capturing, or enabling others to view data or information, or obstructing, interfering, hindering, stopping the operation of an information system or preventing access to it, or altering a website or canceling it, destroying it, or altering its content or operating it, assuming its identity or the identity of the owner without authorization or in violation or excess of the authorization shall be punished by imprisonment for a term not less than three months and not exceeding one year or by a fine of not less than (200) two hundred Dinars and not exceeding(1000) one thousand Dinars".

This crime aims to protect data, information and websites from attacks on them, through malicious programs (viruses), with the aim of achieving one of the results mentioned in Clause (b) of Article (3) of the Cybercrime Law. The difference between Article (3) and Article (4) of the Cybercrime Law in this regard is that Article (4) does not require access to the system with the aim of achieving any of the results or goals stipulated in Clause (b) of Article (3). Rather, it is sufficient to use a remote program. With regard to the violation of privacy, a remote program can be used to assault personal data and information, such as sending a virus via e-mail or using a program to attack a website or sending a mail that contains a program that works automatically to make the recipient's information system attack any other information. There are other types of these programs that can steal, cancel, delete, add, destroy, disclose, extinguish, alter, change, transfer, copy, or receive personal information and data, or enable others to access to the same.

3.2.1 Criminal Conduct

The crime of using a program to attack an information system or a website stipulated in Article 4 of the Cybercrime Law is represented in inserting, publishing or using programs without authorization or in violation or excess of the authorization. This conduct is required to be through an information network or an information system or a website. This crime differs from other previous crimes in the manner, as the perpetrator uses information technologies in this crime while the previous crimes are carried out by the conduct of the perpetrator by accessing the information system by any manner. The acts of insertion, dissemination or use must be based on the program. Among the programs that cause damage to information systems are viruses, worm programs, Trojan horse, and logic bombs, as all lead to the destruction of electronic information and data, but they differ from each other in the manner of destruction.

Therefore, inserting, publishing, or using a program through the information network or by using an information system, all these are the acts constituting the criminal conduct for the purpose of having a specific result. It is a

[24] Article 8 of the Cybercrime Law stipulates the following: The punishment for the crimes stipulated in Articles 3:6 of this law shall be doubled against anyone who commits any thereof because of his/her performance of job or work or by exploiting any thereof.

formal crime that occurs once the act is done and does not require the occurrence of a result.[25]

There must be a causal relationship between the act of inserting a program, without authorization or in violation or excess of the authorization, into the computer information system or the website, and the result of inserting the malicious program into the computer information system and the information network in the broad sense, or the website.

3.2.2 The Moral Element

This crime is a deliberate crime, and for its existence the criminal intent is required with the two elements of knowledge and will. The Jordanian legislator was not satisfied with the general criminal intent, rather it stipulated a special criminal intent that shall be established in accordance with the provisions of Article 4 of the Cybercrime Law, which is canceling, deleting, adding, destroying, disclosing, extinguishing, blocking, altering, changing, transferring, copying, capturing, or enabling others to view data or information, or obstructing, interfering, hindering, stopping the operation of an information system or preventing access to it, or altering a website or canceling it, destroying it, or altering its content or operating it, assuming its identity or the identity of the owner without authorization or in violation or excess of the authorization.

The concept of most of these purposes has already been explained when dealing with the crime of assaulting the right to privacy by unlawful access to the computer network or information system in accordance with the provisions of Article 3 of the Cybercrime Law, with the exception of the capturing and interfering such information and enabling others to access data and information as this was required by the Jordanian legislator in the crime of assault on privacy, according to the provisions of Article 4, but it did not require it in the crime of assaulting the right to privacy by unlawful access to the computer network or information system in accordance with the provisions of Article 3 of the Cybercrime Law.

Capturing means obtaining data and information through the programs that are inserted into the information network. As for interfering, it means affecting the functioning of the systems and occurs with every action that leads to disruption and mixing of data and information. As for enabling others to view the data and information, it means using decryption programs for the encrypted information and data and making it permissible.

It is worth noting that the Jordanian legislator did not criminalize the preparation or manufacture of malicious programs as an independent conduct, but criminalized their use to achieve one of the purposes referred to in Article 4 of the Cybercrime Law and at the same time did not require that the use of such programs shall result in damage. Rather, it suffices to achieve the intent of achieving these objectives.

3.2.3 Punishment

According to Article (4) of the Cybercrime Law, the punishment for this crime is imprisonment for a period of no less than three months and not exceeding a year, and a fine of no less than (200) dinars and not exceeding 1,000 dinars. According to Article 8 of the same law, the penalty is doubled if the perpetrator committed it because of performing his job or work, or by exploiting any thereof. The penalty is also doubled in case of repetition according to Article 16 of the Cybercrime Law.

3.3 The Crime of Assault on Privacy Stipulated in Article 5 of the Cybercrime Law

Article 5 of the Cybercrime Law states:

"Anyone who intentionally captures, intercepts, eavesdrops on, obstructs, alters or strikes off what is transmitted through an information network or any information system shall be punished by imprisonment for a term not less than one month and not exceeding one year or by a fine of not less than (200) two hundred Dinars and not exceeding (1000) one thousand Dinars, or both punishments".

This crime is similar to the crime stipulated in Article 76 of Telecommunications Law No. 13 of 1995, which states the following:

"Any person who intercepts, obstructs, alters or strikes off the contents of a message carried through the Telecommunications networks or encourages others to do so shall be punished by imprisonment for a period not less than one month and not exceeding six months, or by a fine not more than (JD200), or by both penalties".

According to the explanatory memorandum of the Information Systems Crimes Law, the crime has been stipulated in the Information Systems Law because there is a difference between information networks and public or private communications networks; public and private communications networks are subject to the

[25] Al-Nawaysah, Opt. Cit., pp. 260-264.

Communications Law and they are not established or linked except in accordance with the Communications Law, where the public communications network needs a license according to the Telecommunications Law. As for the information network, it does not need such a license even if it needs to pass through a communications network.

3.3.1 The Physical Element

The Jordanian legislator has defined the criminal conduct that constitutes the material element of the crime of assault on privacy stipulated in Article 5 of the Cybercrime Law by the following acts: capturing, intercepting, eavesdropping on, obstructing, altering or striking off what is transmitted through an information network or any information system, and this includes eavesdropping. Below we show pictures of the physical element of this crime.

Capturing: The Jordanian legislator did not define capturing in the Cybercrime Law, and the Arab Convention to Combat Crimes of Information Technology defined it as *viewing data or information or obtaining it*. The purpose of capturing is to view or obtain what is sent through the information network or any information system, whether it is in the form of writings, recordings, signals, or images, data, or information.

As for capturing, as one of the acts of criminal conduct that constitutes the physical element of the crime of violating the privacy of persons, it is achieved by watching, hearing or obtaining it by any way without a legitimate purpose, for example when a person takes a picture sent through the information network or information system without the permission and consent of its owner.

Intercepting: It is intended to prevent what is sent through the information network or information system from reaching the destination intended by the sender, using an electronic means, and this concept does not extend to the issue of impeding its arrival later than the supposed time.[26]

Eavesdropping: It means monitoring what is sent through the information network or information system without violating it[27], such as listening to what is sent through the information network or information system, for example the perpetrator's eavesdropping on phone calls and conversations on the Internet.

Obstructing: It means delaying the arrival of what is sent through the information network or information system to its destination in the actual time of its arrival.[28]

Altering: It means modifying what is sent through the information network or information system, that is, to modify the data or information before it reaches its destination, for example, amending speeches, images or scenes by deleting part thereof, adding or merging another part, or making a combination of conflicting parts in order to form influential or ridiculous situations, using the information network or information system, with the intention of violating the privacy of another person and insulting and defaming him/her.[29] The montage is an example of the alteration contained in the Jordanian Cybercrime Law.

Striking off: It means making a change to what is sent through the information network or information system by deleting the data or information contained in some or all thereof.

As for the means of committing the criminal conduct constituting the material element of the crime of violating private freedom: According to the general provisions, the Jordanian legislator does not consider the means of committing the crime. By extrapolating the provisions of Article (5) of the Jordanian Cybercrime Law, we find that the Jordanian legislator has deviated from the general provisions and considered the manner to be a condition for the completeness of the legal model for cybercrime in general, and the crime of assault on privacy in particular, as it required for the crime of assault on privacy, in order to be considered an electronic crime, the use of information systems as a tool to commit the crime, i.e. the perpetrator's use of the information network or information system.

Article (2) of the Jordanian Cybercrime Law defined the information network as "*a link between more than one information system to acquire and exchange the data and information*".

According to the same Article, the information system means: "*a set of programs and tools designed to create, send, receive, process, store, or manage data or information electronically*".

[26] Al-Mana'sah, Opt. Cit., p. 290.

[27] Abu Issa, Opt. Cit., p. 104.

[28] Abu Issa, Opt. Cit., p. 106.

[29] Al-Bahar, Opt. Cit., 407.

3.3.2 The Moral Element

The crime of assault on privacy mentioned in Article (5) of the Cybercrime Law is an intentional crime in which the moral element takes the form of criminal intent, with its two elements of knowledge and will. This is evident in the provisions of Article 5 of the Cybercrime Law, as the Jordanian legislator stipulated that assault on privacy shall be in the form of criminal intent. This can be deduced from the wording of Article 5 of the Cybercrime Law, which stipulates the following: (Anyone who intentionally ... shall be punished…). This crime is intentional and cannot be committed by mistake. Therefore, capturing, intercepting, eavesdropping on, obstructing, altering or striking off what is transmitted through an information network or any information system is considered a crime if it is intentionally committed and it is not a crime if it is committed by mistake.

- **Elements of criminal intent:** The perpetrator must know at the time of committing the criminal conduct that constitutes the physical element of the crime that he is capturing, intercepting, eavesdropping on, obstructing, altering or striking off what is transmitted through the information network or any information system. The perpetrator must be also informed that it is without authorization (consent of the victim), and he/she must be aware that his/her act of capturing, intercepting, eavesdropping, obstructing, altering or striking off constitutes is an assault and breach of the privacy of others. Accordingly, whoever captures, intercepts, eavesdrops on, obstructs, alters or strikes off what is transmitted through an information network or any information system, by mistake or negligence, cannot be held accountable for the crime of violation of privacy.

In capturing, being one of the forms of the physical element of the crime of violation of privacy in accordance with Article 5 of the Cybercrime Law, there is no crime committed by someone who captures a phone call as a result of interlaced lines without having the intention to do so. The crime does not also occur if someone inadvertently leaves the camera, recording device, or computer open, so that it transfers the person's image or records a call that took place between him/her and another person, without having the intention to do so. Likewise, there is no crime committed by someone who alters or strikes off what is transmitted through the information network or information system (example p. 85, Shashani)

3.3.3 The Penalty Prescribed for This Crime

The Jordanian legislator stipulated a single penalty for all forms of assault on privacy mentioned in Article 5 of the Cybercrime Law for all that is sent through the information network or information system, as it imposed the penalty of imprisonment for a period of no less than three months and not exceeding a year or a fine of no less than (200) two hundred dinars and not exceeding (1000) one thousand dinars.

The legislator has granted the judge discretionary power to impose any of the imprisonment and fine penalties, as the judge may be satisfied with the imprisonment penalty for a period of no less than three months and not more than one year without the fine, or he may be satisfied with the fine penalty of no less than (200) two hundred dinars and not more than (1000) one thousand dinars without imprisonment, as the judge cannot apply the penalty of imprisonment and the fine together.

According to Article 8 of the Cybercrime Law, this penalty is doubled if it is committed by a person because of his performance of his job or work, or by exploiting any of them, as well as in the case of repetition in accordance with Article 16 of the Cybercrime Law.

3.3.4 Supplementary Penalties

A supplementary penalty is a secondary penalty to be ruled with in the presence of an original penalty, which must be pronounced by the judge, within his discretionary power, represented in the confiscation of the devices, tools and means used in committing any electronic crime, as well as the money generated from these crimes as a supplementary and permissible penalty. The removal of the violation shall be at the expense of the perpetrator, and this is explicitly stipulated in Paragraph C of Article 13 of the Cybercrime Law, which stipulates the following: *"It is permissible for the competent court to confiscate equipment, tools, programs, and means or stop or hinder the operation of an information system or website that is used to commit any of the crimes stipulated herein or included in this Law and any means and any money generated from such crimes and order that the violation is removed at the expense of the perpetrator of the crime".*

3.3.5 Punishment for a Legal Person

The Jordanian legislator recognized the criminal liability of a legal person in Article 74 of the Penal Code[30], and

[30] Article 74 of the Jordanian Penal Code states: *No one shall be sentenced to punishment unless he/ she has acted consciously and willingly. 2- A legal person, except for the governmental department or the official or public institution, is*

public legal persons were excluded from this responsibility, which is the governmental department or the official or public institution. The Jordanian legislator did not include in the Cybercrime Law No. (27) of 2015 provisions related to the liability of a legal person for electronic crimes. The responsibility of a legal person for crimes of privacy is subject to the general provisions contained in Article 74 of the Penal Code.

3.3.6 Attempt to Commit Crimes of Assault on Privacy

The forms of assault on privacy mentioned in Articles 3 and 4 of the Cybercrime Law are considered delinquent crimes. According to the general provisions, there is no punishment for attempting misdemeanors except under law. By reviewing the provisions of the Cybercrime Law No. 27 of 2015, and the provisions of Articles 3 and 4, 5 of the same law, it becomes clear to us that the Jordanian legislator did not stipulate punishment for attempting any of these crimes, so there is no punishment for attempting to assault privacy in the forms contained in articles 3, 4, 5 of the Jordanian Cybercrime Law.

3.3.7 Criminal Participation in Crimes of Assault on Privacy

Article 14 of the Cybercrime Law stipulates the following: Anyone who intentionally participates in, interferes or incites the committal of any of the crimes stipulated in this law shall be punished in the same manner specified for its perpetrators. By extrapolating the provisions of Article 14, it becomes clear to us that the Jordanian legislator has deviated from the general provisions of the crime, and punished whoever participates, interferes or incites by the penalty imposed on the original perpetrator, and we think that this would expand the scope of penal protection of privacy in the Cybercrime Law.

4. Legislative Deficiencies in the Jordanian Cybercrime Law No. 27 of 2015

We have explained above that the Jordanian legislator did not include in the Cybercrime Law special and explicit provisions for assaulting the right to privacy, but it has stipulated some forms of assault on privacy in Articles 3, 4 and 5 of the Cybercrime Law, which can be relied upon to prosecute everyone assaulting on the privacy of individuals through information systems, as well as the Jordanian legislation is devoid of a specialized law to protect personal data. Violating the right to privacy through information systems is a broader and comprehensive concept that takes new dimensions and forms that the Jordanian legislator neglected, most notably:

4.1 Illegal Saving and Collecting of Personal Data

Collecting data on individuals illegally, such as when the data is collected in a hidden or unlawful way by fraud. Also, information and nominal data- such as information related to religious and political beliefs, party affiliations and ethnic origin of individuals- must remain far from the collection on computers without their consent, as the content of these data is considered part of the privacy of individuals. Moreover, the nominal data relating to crimes and penalties or measures imposed, in cases other than those determined by law, must be far from collection and storage due to their connection to the privacy of individuals.[31]

4.2 Electronic Data Processing (EDP) Without Permission

Although some countries recognize the principle of communication and transfer of information, they may adopt the licensing system, as the law requires that those wishing to collect, store and process personal data obtain a prior license to practice this activity before practicing its business. Among the legislation that stipulated that isthe French law where Article (226-16) of the French Penal Code stipulated the following: *"Whoever electronically processes, even if by negligence, nominal data without taking into account the preliminary procedures that must be taken, which are legally defined, shall be punished by imprisonment for a period of three years and a fine of three hundred thousand francs."* According to the French law, the approval of the National Commission for Information and Freedoms must be obtained.

4.3 Unlawful Disclosure of Personal Data

The meaning of "data storage" does not mean turning from private to public, as the data or information on computers is stored according to the user's permission and approval in this matter, however, this data or information stored on computers or in information banks may be viewed by a large number of those working in

criminally liable for the actions of his/her boss or any of the administration members, managers, representatives or workers thereof when they commit such acts in his/her name or by one of his/her means in his/ her capacity as a legal person. 3- Legal persons are not sentenced except with a fine and confiscation, and if the law provides for an original penalty other than a fine, the said penalty shall be replaced by the fine within the specified limits in Articles (22) to (24) of this law.

[31] Qayyed, Opt. Cit., p. 60.

the field of informatics, so that its confidentiality and privacy is violated and disclosed to others.[32]

4.4 Deviation from the Purpose and Goal of Electronic Data Processing

The information and data that are collected and stored in the computer or in the data banks must have a clear and predetermined goal, provided that this goal does not conflict with public order or public morals. The entity in charge of the information system must adhere to the purpose for which it has collected and processed information electronically. An example of deviation from the purpose and goal is the investment of communication companies in the personal data of their customers, as many citizens suffer from short advertising messages and promotional emails that are sent to individuals without obtaining a prior written permission from the customer by which it is allowed to receive these messages. This also appears through advertising e-mail messages that are sent to individuals without their knowledge of how and when information related to their mobile phone numbers or their e-mail address was obtained.

Moreover, allowing data or information to be collected about people without knowing their future use represents one of the dangers that threaten the privacy of individuals, and this risk is evident through the information banks created by insurance companies, stock companies, banks and other institutions that collect information related to the personal or health lives of their customers or related to the volume of their transactions, their competitors, and other information that may be illegally exploited in the future, especially through some of these institutions selling this information to companies, institutions or other bodies for financial gains.[33]

4.5 Error in Electronic Processing of Data and Information Without Taking Necessary Measures to Ensure Information Security

The storage of wrong and incorrect information of certain information for people leads to incorrect results about their social status or their real position in terms of financial, political, or professional aspects. Among forms of assault on privacy, whether the errors are technical errors or human errors. These wrong and incorrect information may leave bad effects on a person's life and image and cause great harm and dangers to him, especially on his career and social future. An error in information related to the financial conditions of a person may close the doors of banks and insurance companies in his face, which means the elimination of his financial and economic future.

The Cybercrime Law did not regulate the right of the individual to see and access information about him, the right to be aware of all the data stored on him, and his right to cancel false information about him or correct and amend it if the need arises.

4.6 Saving Data for a Certain Period That May Not Be Exceeded

The Cybercrime Law did not include any provisions specifying the period of saving of data and information. One of the most important rights associated with the right to privacy is the individual's right to oblivion. Information and data pertaining to the individual must be kept for a specified period except in exceptional circumstances stipulated by the law. It must be destroyed after a specified period and must not be a ghost that haunts the individual wherever he goes,[34] and this is what the Committee on Civil and Political Rights emphasized in its comment on Article 17 of the Covenant relating to the right to the privacy of the privacy of the individual, noting that *"the law must regulate the processes of collecting and saving personal information using computers and other means, whether conducted by public authorities, private persons, or private bodies. States must take effective measures to ensure that information about a person's privacy does not fall into the hands of persons not authorized by law to obtain it, and must not use it for purposes contrary to the Covenant. In order to be able to protect the privacy of the individual in the most efficient way, it should be the right of every individual to easily verify what data are stored, and the purpose of saving them. Each individual should be able to verify the identity of the public authorities, private persons or private bodies that control this data. If there are incorrect personal data or data collected or processed in a way that conflicts with the provisions of the law, it should be the right of every individual to request their correction or deletion."*[35]

According to the above, we conclude by saying that the provisions contained in the Cybercrime Law do not accommodate all forms of violations of the privacy of individuals using modern technologies, and as Jordanian

[32] Al-Momani, Opt. Cit., p. 177.

[33] Al-Momani, Opt. Cit., pp. 175-176.

[34] Maghabghab, Naeem (1998). *The dangers of informatics and the Internet (Risks to Private Life and its Protection)*, Halabi Publications, Beirut, p. 193.

[35] Al-Momani, Opt. Cit., p. 171 and what follows.

legislation is devoid of a specialized law to protect personal data, therefore, the Jordanian legislator must keep abreast of developments in the field of informatics and issue a law to protect the personal data of individuals in light of the legislative shortcomings that characterized the Cybercrime Law No. 27 of 2015, in providing complete legal protection for life for individuals by establishing a specialized body that is responsible for granting or preventing the necessary license to carry out the electronic processing of personal data and information, and control it from the start of the collection of these processes data and the storing and processing thereof. In this regard, we refer to a new study published by ImpACT International for Human Rights Policies and Access now [36], in which it revealed that the major Internet provider companies in Jordan violated the privacy of their customers to a large extent, allowing them to monitor their use of the Internet, record their browsing history and the information that is sent through browsers. The study stated: The study targeted five Internet provider companies in the Kingdom (Zain, Umniah, Orange, Damamax, and TE Data), and relied on collecting and analyzing information from Internet provider companies and questionnaires to measure the awareness of each of these companies' employees and customers, and found that some companies clearly violate the privacy of users, while customers remain unaware of the degree to which these companies can collect and record their personal information, which in many cases includes highly confidential information. In the conclusion of the study, the two institutions called on the Jordanian government to put on the top of its priorities the implementation of a bill that gives adequate guarantees to protect personal information and the right to privacy, so that Internet providers comply with local standards and international rights to privacy.

5. Results

1. There is no comprehensive definition that prohibits the right to privacy, because it is a flexible and relative idea that is difficult to define and it develops with the development of time, place and people.

2. The Jordanian legislator did not include special provisions that explicitly criminalize the assault on privacy in the Cybercrime Law, but rather it included provisions for other crimes that include an assault on this right, such as the crime of unlawful access stipulated in Article 3 of the Cybercrime Law, as it did not state explicitly the unlawful access for the purpose of assaulting the privacy of individuals, but it can be relied upon to pursue those who violate the privacy of individuals, as well as the crime of using a program to attack an information system stipulated in Article 4 of the Cybercrime Law, as part of the perpetrator's aims to use the program without stating explicitly that the data and information, the subject of the abuse relate to the privacy of individuals. Article 5 is limited to the criminalization of the assault on the secrecy of electronic correspondence.

3. The Jordanian legislator has neglected new forms of electronic crimes related to the protection of the privacy of individuals. These images are represented in the electronic processing of personal data without authorization, the collection and storage of data in an illegal manner, the electronic processing of data without taking the necessary measures to ensure the security of information, the unlawful disclosure of data and nominal information, and deviation from the purpose and goal of electronic data and information processing

4. The insufficient criminal protection of the right to privacy of individuals in the Cybercrime Law, as the Cybercrime Law was characterized by legislative shortcomings, as it did not explicitly protect the right to privacy, nor did it provide for the criminal protection of personal data.

6. Recommendations

1. Amending the provisions of Article 3 of the Cybercrime Law and stipulating the criminalization of unauthorized staying within the information system, the electronic network, or the website, in the event of accessing the system by chance, omission or error, and staying within it.

2. Amending the provisions of Articles 3, 4, and 5 of the Cybercrime Law and tightening the penalty for assaulting data and information sent because the stipulated punishment is not a deterrent.

3. Amending the Jordanian Cybercrime Law No. 27 of 2015, and including explicit provisions to criminalize the assault on privacy by using modern technologies.

4. The need to issue a law to protect the personal data of individuals in light of the legislative shortcomings of the Cybercrime Law No. 27 of 2015, which did not provide criminal protection for this data.

References

Abu Issa, H. M. (2019). *Information Technology Crimes* (2nd ed.). Wael Publishing and Distribution House, Amman, Jordan.

[36] https://www.accessnow.org/new-study-jordanian-isps-violate-customers-privacy/

Al-Ahwani, H. El-Din. *The Right to Privacy, A Comparative Study.* Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

Al-Mana'sah, O. A., & Al-Zoubi, J. M. (2017). *Crimes Relating to Information Electronic Systems and Technology*. Dar Al-Thaqafah for Publishing and Distribution, Amman, Jordan.

Al-Momani, N. A.-Q. (2008). *Information Crimes*. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan.

Al-Nawaysah, A.-E. (2017). *Information Technology Crimes.* Wael Publishing and Distribution House, Amman, Jordan.

Al-Obeidi, O. B. G. Protecting the Right to Privacy in the Face of Computer and Internet Crimes. *The Arab Journal for Security Studies and Training, 23*(46). Riyadh.

AL-Rawashdah, S. H. (1998). *Criminal Protection of the Right to Privacy*. Master thesis, Faculty of Law, University of Jordan.

Al-Ustaz, S. (2013). Violation of the Privacy via the Internet. *Damascus Journal of Economic and Legal Sciences, 29*(3).

Ayoub, P. A. (2009). *Legal Protection of Privacy in the Field of Informatics* (1st ed.). Al-Halabi Legal Publications, Beirut, Lebanon.

Bahar, M. K. (2011). *Protection of Privacy in Criminal Law*. Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

Maghabghab, N. (1998). *The dangers of informatics and the Internet (Risks to Privacy and its Protection).* Halabi Publications, Beirut, Lebanon.

Qashqosh, H. H. *Cyber Crimes in Comparative Legislation*. Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

Qayyed, O. A. (1988). *Criminal Protection of Privacy and Information Banks.*

Legislation

Jordanian Constitution of 1952 and its amendments .

Jordanian Penal Code of 1960 and its amendments .

Jordanian Cybercrime Law No. 27 of 2015.

French Penal Code.

Websites

https://www.accessnow.org/new-study-jordanian-isps-violate-customers-privacy/