**Migration Letters**

Volume: 20, No: 7, pp. 316-327

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

# The Responsibility of the Service Provider in the Field of Cyber Security

Majed Saleh Al shawabkeh[1]

**Abstract**

*The aim was to find out the responsibility of the service provider in the field of cyber security. The descriptive approach and the analytical approach were used in this study and the comparative approach. The study reached a number of results, including: The Jordanian legislator did not address in the Jordanian cyber security law the technical and technical issues of the cyber security incident in terms of nature and impact and classification. This will affect the guarantee of protection that has been established in cyber security and the safety of cyberspace in Jordan. As well as benefiting from the capabilities of information and communication technologies for cyber security, at all levels. The study recommended the need to conduct more studies on protection in cyber security.*

***Keywords:*** *responsibility, service provider, cyber security.*

## Introduction

Civil liability stipulates that any individual is responsible for his personal action, and this rule has been codified in various laws such as Jordanian Civil Law No. (43) for the year (1976) by stipulating: "Any harm to others obliges the doer, even if he is not distinguished, to guarantee the harm." Therefore, the elements of civil tort liability must be present in order to be able to say that it is carried out, represented by a mistake.

Service Provider: A company that enables customers to access the network (the Internet) and related services in return for paying a subscription to it (Ahmed, 2013, 9).

Also, cyber security constitutes the framework for all important economic activities and overall business operations at all levels in time and place, and this is not limited to a user area within the physical borders of a house and even the borders of a country, and at a low cost level, users can meet people anywhere in the world so that they are Obtaining information without the need to know the whereabouts of the real person (Classlessness, , Dem, 2002, 9).

Cyber security has become an issue of global importance and importance. Already more than 50 countries have officially published some form of strategy document outlining their official position on cyberspace, cybercrime, and/or cyber security (Al-Qahwaji, 2013, p. 18).

Cyber security is a set of tools, policies, security concepts, security guarantees, guidelines and methods for risk management, procedures, personnel training, best practices, and emphasis on technology that may be employed to provide protection for the electronic environment, organization, and users (Gion, 2016).

[1] Lecture, Prince Al Hussein Bin Abdullah II Academy for Civil Protection, Al-Balqa Applied University, Majed.s.alshawabkeh@hotmail.com

Study Problem:

The problem of the study emerges in that the matter becomes more difficult in the case of disputes, as there was a need to issue judgments in many issues, which is necessary to clarify the nature of the special laws that apply in the case of conflict, including in the provision of the service so that this responsibility may be multiple in the right This category.

In light of the lack of studies and the inadequacy of legal texts, there is a need to study this subject by investigating it through jurisprudential theories and practical applications, in addition to clarifying the treatment provided by legislation related to the civil liability of service providers in cyber security, justifying conducting this study in light of the lack of Legal studies that dealt with the civil liability of service providers in cyber security.

Study Questions:

The study problem can be presented by answering the following questions:

1- What is the meaning of cyber security and civil responsibility?

2- Who is the service provider in cyber security, its characteristics, controls and legal nature?

3- What is the scope of responsibility of the cyber security service provider?

4- How is the damage caused by the cyber security service provider guaranteed?

Importance of studying:

First: The theoretical importance of the study:

The importance of this study came to deal with its content the civil responsibility of the service provider in cyber security. And that is by returning to the sources on the subject, which constitutes an addition to the Arabic library.

Second: The practical importance of the study:

It is hoped that the following groups will benefit from the results:

1. Judges and lawyers to learn about the civil liability of service providers in cyber security.

2. Researchers by making this study the nucleus of other similar studies.

Objectives of the study:

The study aims to achieve the following:

In order to shed light on this problem, the following questions must be answered:

- Explaining the meaning of cyber security and civil responsibility.

- A statement from the service provider on cyber security, its characteristics, controls, and legal nature.

- Statement of the scope of responsibility of the cyber security service provider.

- A statement of how the damage caused by the cyber security service provider is guaranteed.

Idiomatic Definitions:

- Civil liability: It is the case of a person who commits something that requires culpability, which in general means the obligation to compensate for the damage, and it may not be related to the contractual liability arising from an obligation to breach the contract and may not be related to the tort liability arising from a breach of any obligation in the law through that there is no Harm to others in general (Ibrahim, 2019, 5).

- Service providers in cyber security: They are providers of security services related to the existence of protection from potential risks through third parties, including the Internet, as security specialists in the cyber situation provide protection for the computer from any penetration, threat or penetration through other computers or networks The Internet or any other means that cause risks (Classlessness, , Dem, 2002, 253).

## Previous Studies:

Al-Jubouri's study (2017) The aim of the study was to find out the law that is applicable to the responsibility of Internet service providers,

Where the nature of the liability varies according to the violations committed, as it may fall within the framework of contractual liability or tort liability, which affects the competent law to apply to the relationship between the consumer and Internet service providers due to the lack of special regulation in the roads.

This study agrees with the current study in clarifying the responsibility of Internet service providers and differs from it in limiting it to civil liability and cybersecurity.

Study (Al-Sheikhly, 2017) "The aim of this study was to clarify the role of commercial banks when combating money laundering operations in their commercial and legal employment; and despite the fact that laundering operations are related to the criminal aspect, banks have a major role in combating as it is the easiest and easiest place to carry out this process. Due to the confidentiality, flexibility and speed of the banks, the study also discussed some legislative solutions undertaken by countries in the various control operations.

One of the most prominent results of the study is that banks have a major role in the control operations from a supervisory point of view.

Foreign Studies:

(Zhang, 2013)

The study aimed to reveal the form of the relationship between the internal control systems and the audit committee, its quality and independence tendencies of the auditor. The sample consisted of the number of companies that have problems in the internal control systems in Singapore. One of the most prominent results was that there is a clear relationship between the application of control systems and the quality of auditing in companies. We find that the previous study dealt with the subject of control in companies, while the current study showed the issue of the responsibility of civil service providers in cyber security.

Oqab (2012)

The current study aimed to show the relationship between the audit committees and their roles in the anti-money laundering operations and the tasks they perform and the mechanism of activating the internal control system for the control operations and the extent to which banks use the internal control systems.

The previous study dealt with the relationship between audit and oversight committees, while the current study dealt with the responsibility of civil service providers in cyber security.

## Study Methodology:

1. A descriptive approach, in speaking and clarifying the responsibility of civil service providers in cyber security.

2. Analysis approach: To analyze the nature of this responsibility and analyze all judicial rulings in order to solve the legal problems that the researcher faced in some laws, theories and legal applications.

3. A comparative approach: comparing Jordanian law with some Arab laws, whenever necessary.

The First Topic

Cyber Security Concept

Cyber security is “a set of tools, policies, security concepts, security guarantees, guidelines and methods for managing risk, procedures, assurance, and technology that can be used to protect the electronic environment, organization and users” (Al-Junaihi, Al-Junaihi, 2016, p. 23).

Many areas of the cyber domain are under attack: critical infrastructure, electrical networks, banking, business, government, personally identifiable information (identity theft, medical records, child exploitation, etc. (Rustom, 2017, p. 13).

It is also used to put infected computers into a "botnet": a network of thousands or even millions of computers under the control of an attacker that is used to carry out a wide range of services. Services include sending spam, perpetrating online advertising fraud, launching denial of service attacks, hosting phishing attacks, and anonymizing attacks traffic.

This topic will be dealt with in the following division:

The first requirement: the definition of cyber security

The second requirement: the characteristics of cyber security

The First Requirement

Define Cyber Security

The concept of information security is a set of preventive measures and arrangements used to protect information and prevent hackers from accessing important and valuable information (Maashi, 2011, 36).

There are many definitions of cyber security in the fiqh terminology, including: Rustom (2012, 194) defined it as a set of preventive measures and measures that are used in any field to preserve information, hardware and software, in addition to the procedures related to maintaining workers in this field.

As for Hijazi (2020, 55), he defined it as: “Preserving the information in any information system from the risks of loss and damage, or from the risks of incorrect use, whether intentional or spontaneous, or from the risks of natural disasters.

As for the legal terminology, it is defined as: “the activity, capacity or otherwise that protects and defends information and communication systems from damage, modification, espionage, destruction or unauthorized access (Hegazy, 2012, p. 243)

Cyber security in Jordan is recent, as the law on cyber security was regulated by the Jordanian legislator in 2019 with the issuance of a royal will, and where the system of the National Center for Cyber Security was approved in January of 2020 (Ababneh, 2020, 241).

What is meant by cyber security is to provide protection for the computer and all related devices, programs, networks and data from any malicious attack by theft or destruction of programs or data. Several definitions have appeared for it, such as computer security or electronic information security (Abdullah, 2011, 231).

The Second Requirement

Cyber Security Features

System information is gaining increasing importance in light of the great challenges facing organizations, and this importance increases in light of the increasing importance of knowledge goals that knowledge management focuses on achieving, leading to enhancing levels of productivity, efficiency and effectiveness in organizations. The importance of information stems from the fact that we are in the age of technology and knowledge, which makes the process of owning, transferring, developing and expanding information necessary. Therefore, management scholars agree that knowledge is one of the most important strategic and vital resources for the contemporary organization. This gives an indication of the interest in knowledge for what it builds from the base of the organization, "so that it achieves its existence and growth. Knowledge, through its practical capabilities and strategies, positively affects the speed and spread of creativity, which in turn is reflected in the performance of the organization as a whole" (Quora, 2015, 40-41).

According to the researcher, any cybersecurity framework includes detailed guidance on how to implement a 5-step cybersecurity process: identify vulnerable assets (weaknesses) within the organization, protect assets and data, provide necessary maintenance, detect intrusions and breaches, respond to any of these breaches, and act It is the responsibility of the person to repair any damage caused to the organization's systems, data, finances and reputation as a result of the attack / hack.

There is great importance for information and its sources, as it is a source of nourishment for organizations of all kinds, enabling these organizations to carry out their administrative operations, and to achieve the goals they aim at, enabling them to continue and adapt to the business environment that is described as changing, highly competitive, and technology has a major role in The process of storing, processing and analyzing information and providing users with it accurately and quickly, which facilitates the process of making positive decisions.

The Internet had a great role in enabling individuals to access information sources, and the development of information and communication technology and the presence of information banks had a significant impact on improving the functions of libraries and information centers, including university libraries, and the services they provide, and methods for obtaining, storing and accessing information sources. and its retrieval and distribution (Younes, 2012, 15).

These elements or components are considered basic principles that must be present, namely:

1- Confidentiality: as the secure system is the system that guarantees the confidentiality and privacy of the data stored in it, and hence this data is made available only to its owners, in addition to securing appropriate ways to protect it from reading during its transmission over the network. This is achieved through a set of methods that provide different levels of Degrees of security and speed of information transmission

2- Integrity and safety: It means the safety of information in general, where the security system secures the integrity of the data stored in it, and integrity means the protection of data from any deletion or destruction, and this is secured through a set of methods provided by database systems such as access lists and powers, in addition to the interrelationships between The data stored in it, and the information integrity component consists of two parts: the first is the integrity of the information, which means that the information is not changed in an inappropriate manner, whether intentionally or unintentionally, and the second is the integrity of the source, which means obtaining the information from its original source (Rustom, 2012, 14).

3- Availability and availability:

The secure system ensures the continuity of users' access to their information without any delay, and this feature has a number of characteristics represented in:

Resistance is the system's ability to protect itself from the processes that make it unavailable to authorized users (for example, that the system is able to prevent the implementation of uses that require the reservation of a large amount of server memory).

– Ease of use. – Flexibility represented in the availability of capabilities and tools that enable the management of the system without requiring it to stop.

The ability to expand to meet future needs.

The Second Topic

The Legal Nature of Service Providers in Cyber security

The practical reality proves that the process of circulating information through the network for cybersecurity requires concerted efforts for workers in this field, where the roles and activities in operation vary. Where there must be a number of workers so that individuals can use the cybersecurity network, and these people are service providers or intermediaries who transmit information to those in need. These individuals can also detect all aspects of illegal activities within the legal controls specific to the rights of the parties to electronic activity in the face of Society and confronting each other in general in this context. (Hegazy, 2020:233).

It turns out, the diversity in the tasks of people in charge of cyber security services, and the multiplicity of their mutual roles, as it is possible for one person to perform one or more tasks at the same time. The question arises about how we define the obligations of these people in cyber security. Especially since some of them provide the service and some of them are technicians.

For more details, this study will be covered through:

The first requirement: the commitment of service providers

The second requirement: Cyber security in Jordanian laws

The third requirement: compensation for the obligations of information service providers

Fourth requirement: The basis of the responsibility of cyber security service providers.

The First Requirement

Service Provider Commitment

Whoever provides shelter services to cyber security, shelters on the site he created, manages information and private messages, and gives them access to the network. The following is a review of all of that.

First: The obligations of the shelter operator:

The nature of the service provided by the shelter operator inevitably makes it the closest and most capable of explaining the content of the information activities circulating through the network. Which is circulated over the network, and the other is the obligations of the shelter operator upon knowledge of the circulation of illegal informational content. In the face of these problems, and in the absence of legislative texts, the law in France created a reasonable limit of obligations for the shelter operators (first). The French legislator only responded to this judiciary and codified these obligations similar to the European legislator (second). (Hegazy, 2012: 18). We also hope that both our Jordanian judges and legislators will follow the example of their French counterparts, so that they do not hesitate to address these issues.

1- The judicial position It was not easy for the judiciary of France to begin with, and during the consideration of a case against the shelter contractor, they determined the scope and content of the obligations that fall upon them, so he tried hard to overcome the difficulties he faced so that cyber security would not be a lawless area. In view of the nature of the service provided by the shelter operators, and in the absence of special legal texts, this judiciary showed a degree of leniency in the quality of the obligations imposed on them, according to the text of Articles: 1382 and 1383 of the Civil Code in France, which oblige the owner of any harmful act that by mistake led to harm Third party warranty on damages.

2- The response of the legislator between the previous ruling the tendency to oblige service providers to take the necessary care to prevent the circulation of illegal content or information, through vigilance efforts that are proportional to their capabilities. However, the content and extent of these efforts remain ambiguous (Mansour, 2003: 6).

This helps in the process of securing the necessary technical means to prevent the dissemination of illegal information content and circulation over the network, on the other hand, as well as in preparing an open means of communication that connects directly with cyber security users, and enables the public authorities in the country to be notified about electronic content that violates the law (Naqrouz, 2017 : 16).

Second: the obligations of the information supplier the supplier is the person who has real authority to monitor the information material transmitted over the network for cyber security; Because he is the one who collects or authors, and therefore it is his responsibility to supply legitimate and real information material, and accordingly, the supplier of information, or any other activity, which falls under his obligation to practice his work transparently (first). Also, the information provider must allow the public to exercise the right of reply (II).

1- Commitment to transparency:

This person works to publish information, so he bears primarily responsibility for the content of the messages, information, and images that he transmits. He is committed and the content of this information is consistent with the nature of his work as an electronic publisher of the information material. (Habbour, 2018, 25). - If the information supplier is a natural person, he must provide his data, the nature of the activity and the center of management. - He also appoints a publishing director or editor-in-chief, as confirmed by the French legislator in Article 6-3/1 of the French law.

2- Obligation to allow the right of reply:

According to what was stated in French law in Article 6-3/2 that natural or legal persons have the right to respond to information published on the network that harms honor, reputation or rights by submitting that to the publication director within a period of three months, and the information resource must also: He is obligated to secure every necessary technical and informational means so that the person who has been harmed can exercise his right to that in general (Qasim, 2007: 11).

The Second Requirement

Cyber Security in Jordanian Laws

Cyber security in Jordan is somewhat recent, and many legislators have organized this issue that is related to cyber security, including the Jordanian law on cyber security, which was approved in the year (2019) after the issuance of the royal decree approving a system for the National Center for Cyber Security (Ababneh , 2020: 231).

We find that the Hashemite Kingdom of Jordan has paid great attention to the issue of cyber security, as Jordan realizes that there are several risks that may affect cyber

security, which prompted the legislator to put in place a cyber security law in the year (2019), which was approved after it was presented to the House of Representatives.

The importance of this law is highlighted in the fact that there are many attacks that affect cyber security. Therefore, Jordan has found that there is a need to update its information systems to face any cyber threats that the systems may be exposed to.

There is no doubt that the law issued in the year (2019) No. (16) was the result of several legitimate reasons indicated by the Jordanian authority, which aimed through this law to create necessary protection for cyber security, after the law took its constitutional stage by submitting it to the House of Representatives and then approval The Senate and then the approval of His Majesty the King, as this law became an effective law aimed at achieving many goals.

The researcher believes that there are many objectives behind the development of the law, which are:

1- There is a guarantee that cyber incidents or threats will not occur that affect the information systems in Jordan.

2- The existence of protection for the infrastructure and the electronic services provided to citizens from any penetration in general.

3- Creating a stimulating and attractive environment for investment.

4- Creating a strong economy away from any penetration.

5- Ensuring that the strategy and law are implemented as set.

6- Monitoring and supervising the implementation of the law.

7- Work to create oversight for cyber security and cyberspace.

8- Finding a reference committee that can implement all the cyber security law related matters.

9- Create an effective alarm system.

This is what appeared through the text of the law, which showed how the law was set, the committee responsible for this, and the members of the committee who carry out this process, so that there is a clear guarantee to protect cyber security in the Hashemite Kingdom of Jordan (Ababneh, 2020: 239).

The Third Requirement

Compensation for the Obligations of Information Service Providers

Whoever provides the shelter service on cyber security, shelters on the site that he created, manages information and private messages, and gives them the opportunity to enter the network to be available to those who wish to view them, and this generally goes beyond the technical role of the service provider as one of the carriers of information (Hegazy, 2020, p. 12).

On the one hand, it undertakes the management process for information activities on the network. It also provides technical means that help individuals to reach the sites where the information is located, as the provider must provide all techniques and capabilities so that the information content is traded via the Internet and here the information becomes Available by users in general, and this will be addressed through the following branches:

Subsection One: Compensation, the obligations of the contractor for accommodation

The shelter contractor provides the information activities circulating through the network, and if it appears that the content of the content is illegal, this raises a number of legal problems and requires compensation for the mistakes committed (Al-Shoubaki, 2017, p. 14):

First, the shelter operator must monitor what is provided of information content through the cyber-security network, so it is or is important to him, and then the second must specify the obligations that he bears in relation to the information and its content. What the French legislator referred to.

First: The position of the judiciary on the compensation process:

In the absence of legal texts related to compensation for the responsibility of the shelter operator, the judiciary in France has shown a degree of leniency with regard to this responsibility, as well as the nature of compensation for the resulting errors (Hegazy, 2012, p. 12).

Second: The legislator's response to compensation for cyber security errors:

It appears from the general tendency of previous judicial rulings, such as the ruling of the Court of First Instance (Nanterre), that they tend to obligate shelter operators to exercise the necessary care to prevent the circulation of illegal content or information, through vigilant efforts that are commensurate with their capabilities. However, the content and extent of these efforts remain ambiguous (Hegazy, 2020, 200).

The text of Article 6-1/7 of the French law on "trust in the digital economy", which was in accordance with the text of Article 15-1 of the European Directive on "electronic commerce" prevents the imposition of a general obligation on the accommodation provider "to monitor the information that he transmits or stores, or the active search for facts and circumstances that reveal illegal activities. Under this text, the shelter operators find themselves exempted, alike, from exercising prior control over illegal information content, and from the technical and economic difficulties that accompany this control, some of which have questioned its effectiveness.

Subsection Two: Compensation for the Information Supplier's Obligations:

The supplier of information is the real authority to control the information material transmitted through cyber security; Because he is the one who collects or authors, and therefore it is his responsibility to supply the information material that is legitimate and real (Hijazi, 2003: 353)

The researcher finds that the information resource must adhere to caution and caution, otherwise he must be compensated for the errors that occurred because of the responsibility that was issued due to the error in transmitting the content of the information.

The responsibility, and consequently, compensation is also based on the information resource, due to his inability to secure the necessary technical means to identify the owner of the illegal content. Hence, this does not cause a problem for the information resource, as there are identification codes that can be identified through the cyber security network (Mansour, 2003, p. 5).

The researcher believes that the information resource should not disclose the information except when necessary and when needed so that there is clear confidentiality.

Fourth Requirement

Basis of Responsibility for Cyber security Service Providers

When we examine the legal texts set by most of the legislation that regulates the responsibility of cyber security service providers, it becomes clear to us that the establishment of this responsibility depends on the service providers' knowledge of the illegal electronic content, and the results obtained from informing them of its existence. The basis of responsibility, then, is the constant error represented in the intervention and participation of service providers in the violation, or their passivity by taking the necessary measures to withdraw the illegal electronic content, or to prevent access to it. Establishing the responsibility of cyber security service providers on the consistent error

finds justification for it, in that in the decentralized world of cyber security, in which every intruder works for his own account without being subject to a gradual administrative organization prepared in advance for the distribution of roles and tasks, a person can be responsible only for what he can control on him.

Therefore, there is no room for research, at the time of the injury, about the responsibility of the executor or the responsibility for guarding things according to the text of Articles: 1384 of the French Civil Code and 289, 291 of the Jordanian Civil Code, or, with the exception of the responsibility of the information provider, for the responsibility in the sequence applicable in the field of The press and the audio-visual media, which are based on taking risks and dependence, but must identify who is personally responsible, and prove that he committed the error in the sense stated in the texts of Articles: 1382 and 1383 of the French Civil Code, which stipulate for liability for personal action a fixed error, damage, and a causal relationship that brings them together . (Hegazy, 2012, 30).

Accordingly, the French judiciary decided in the case of the afore mentioned model Estelle Holyday, not to exempt the service provider from his responsibility unless he proves that he has fulfilled all the obligations imposed on him. This judiciary also declared that the service provider's activity is not limited to the technical role of transmitting information, and in the event of a breach of his obligations, he can assume his responsibility on the basis of a consistent error, according to the text of Article 1383 of the French Civil Code. Exempting him from exercising general and accurate control over the content of the information network does not prevent him from taking the legal and reasonable measures that every careful and vigilant professional is supposed to take in order to know the electronic information that is characterized by apparent legitimacy. This balanced solution is consistent with the legal regime of responsibility for cyber security providers established by the European Directive on “E-commerce” and the French Law on “Trust in the Digital Economy” which tend to set a general standard of consistent error, which is the service provider committing a breach, or its passivity in Ending it (Mansur, 2003: 188).

With this openness and the entry of the digital age and the transition of societies from the actual physical reality to the cyber reality, we are witnessing the emergence of cyber crimes and their encroachment on the individual and society, in a noticeable and increasing manner. For this reason, the law stipulates the protection of cyber security and the fight against cybercrimes. Article (16) of the Cybercrime Law stipulates:

1- Whoever intentionally sends through the electronic network or an information technology means everything that is audible, readable, or visual that includes pornographic acts for those over eighteen Gregorian years without their consent, shall be punished by imprisonment for a period of no less than three months and not more than two years. , or a fine of no less than two hundred Jordanian dinars, and not more than one thousand Jordanian dinars, or its equivalent in the legal currency of circulation, or with both penalties.

2- All information that has been intentionally published through the electronic network or sent to a technological means in an audible, readable or visual way that includes pornographic acts for those who have not completed eighteen Gregorian years or related to their sexual exploitation, shall be punished by imprisonment for a period of no less than one year. Or a fine of no less than one thousand Jordanian dinars and not more than three thousand Jordanian dinars, or its equivalent in the legally circulated currency, or with both penalties. 3. Anyone who intentionally uses the electronic network or an information technology means to create, prepare, save, process, display, print, publish or promote pornographic activities or works for the purpose of influencing a person who has not completed eighteen years of age or a person with a disability , shall be punished with imprisonment for a period of no less than two years, or a fine of no less than one

thousand Jordanian dinars, and not more than three thousand Jordanian dinars, or its equivalent in the currency of circulation, or with both penalties.

## Conclusion:

The responsibility of service providers is related to many matters related to the content of information and its protection and non-disclosure of secrets. It is also necessary to achieve criminal or civil liability in the event of errors and risks, as the establishment of a mistake against them generally arranges the existence of civil or penal liability. The judiciary had an imprint in this, and the study reached a number of conclusions and recommendations, namely.

First, The Results:

The study reached the following results:

1- Internet Service Provider: A company that enables customers to access the network (the Internet) and its related services in return for paying a subscription to it.

2- Cyber security has become an issue of global importance and importance. Already more than 50 countries have officially published some form of strategy document outlining their official position on cyberspace, cybercrime and/or cyber security.

3- The concept of cyber security, which has gone through successive stages of development, has been of great importance. In the sixties, computers and their work were the occupation of workers in the information departments, and their concern was how to implement computerized programs and activities, and they were not preoccupied with information security as much as they were preoccupied with the work of the devices. Access or view data by preventing any stranger from tampering with the devices, so the term computer security appeared

4- The Jordanian legislator has regulated the Cyber Security Law No. 16 of 2019, but it did not regulate the procedural rules that are based on the protection of cyberspace.

5- The Jordanian legislator did not limit the measures taken to protect information systems, networks and critical infrastructures from cyber security incidents and the ability to restore their work and continuity, whether access to them without a permit or misuse or as a result of failure to follow security procedures or exposure to deception that leads to this, in what determines international legislation.

Second: Recommendations:

The researcher can make the following recommendations:

1- The need to work on coordinating efforts in different countries, where special legal rules are created that regulate civil and criminal liability for cyber security services, so that this is reflected in encouraging investment and increasing the benefit obtained by the national economy through protection through the cyber security network.

2- There must be harmony between international legislation with regard to protecting cyberspace from any attacks or penetrations and prosecuting all countries in the event of a cyber security network penetration to preserve privacy.

3- The necessity of the various legislations to avoid any deficiency in the texts of the articles related to determining the legal status of service providers so that all the roles that these providers must play in relation to cyber security are defined.

4- Working on following up the cases related to the transmission of information so that actions are taken to withdraw this content by the users of the network.

## References

Ahmed, Al-Hilali (2013). Inspection of computer systems and information guarantees for the accused, 1st floor, Cairo, Arab Renaissance House.

Ibrahim, Khaled (2019). Information Crimes, Dar Al-Fikr University, Alexandria, 1st Edition.

Al-Janayi, Mounir and Al-Junayhi, Mamdouh (2016). Internet and computer crimes and the means of combating them, Alexandria, Dar Al-Fikr Al-Jamii, 1st Edition.

Rostom, Hisham (2017). Penal Code and Information Technology Risks, 1st Edition, Modern Machines Library, Assiut.

Rostom, Hisham (2012). Procedural Aspects of Information Crimes, 1st Edition, Modern Machines Library, Assiut.

Hegazy, Abdel Fattah Bayoumi (2020). Combating Computer and Internet Crimes, Dar Al-Fikr University, Alexandria

Hegazy, Abdel Fattah (2012). Criminal Evidence in Computer and Internet Crimes, House of Legal Books, Cairo.

Al-Ababneh, Muhammad (2020). Computer crimes and their international dimensions, Dar Al-Thaqafa, Amman, 3rd Edition.

Abdullah, Abdullah (2011). Information and Internet Crimes - Electronic Crimes, Al-Halabi Human Rights Publications, Beirut, 1st Edition.

Al-Shoubaki, Muhammad Amin (2019) Computer and Internet Crimes, Information Crime, House of Culture for Publishing and Distribution, Amman

Mansour, Mohamed, (2003) Electronic Responsibility, New University Publishing House, Alexandria, first edition.

Al-Naqrouz, Ali (2017) Information Systems Crimes, Dar Al-Sana Publishing, Jordan, Amman

Jabbour, Mona Al-Ashqar, (2018). Cyber, Obsession of the Age, League of Arab States.

Al-Qahwaji, Ali Abdel-Qader (2013). Criminal protection of electronically processed data, research presented to the Conference on Law, Computer and the Internet, which was held during the period from 1-3 May, College of Sharia and Law, United Arab Emirates University.

Younes Arab, Khaled (2012). Computer Crimes, Master's Thesis, University of Jordan.

Kora, Naila Adel (2015). Economic computer crimes, published PhD thesis, 1st edition, Dar Al-Nahda Al-Arabiya, Cairo.

Kassem, Ahmed Farah (2007) The Legal System for Internet Service Providers

Analytical comparative study - Department of Legal Studies, College of Jurisprudence and Legal Studies, Al al-Bayt University

Maashi, Samira (2011). The nature of information crime, research published in the Journal of the Legal Forum, Issue Seven, University of Mohamed Khider Biskra, Algeria.

Zhang Y. (2013) "Audit Committee Quality, Auditor Independence, and Internal Control Weakness, "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327.

Oqab, R, (2012) The Role of the Audit Committee in Raising the Efficiency of the Internal Control System to Combat Money Laundering in Jordanian Banks. "Journal of Accounting and Public Policy", Volume 26, Issue 3, p: 300 – 327

Gion Green, (2016). Introduction to Security, Fourth Edition, Revised by Robert J. Fischer , Butterworth's.

Clasessens, J., Dem,V., De Cock and Van de walle, J. (2002) on the Security of Today's Online Electronic Banking System, Computer and Security. 253-265.