The Crime of Unlawful Access to Computers and Information Systems:

A Critical Study of the Exciting Legal Provisions in Oman

BY

Amna Al.Mamari **Dr. Saif Al-Rawahi**

مجلة حقوق دمياط للدراسات القانونية والاقتصادية – كلية الحقوق – جامعة دمياط

العدد الخامس يناير - ٢٠٢٢

Introduction:

Unlawful access to information systems is a necessary stage to commit many further information crimes, since most other crimes cannot be committed without first gaining access to the information system.(١) Therefore, it is wise to criminalize the act of unlawful access, which many countries have resorted to by legislating provisions for that in addition to technological security means.

Unlawful access to information systems(٢) or computers includes all the actions that allow access to them without the consent of the administrator of the system, ensuring control over the information it contains or the services it provides.(٣).

Unlawful access is also achieved whenever the access violates the will of the owner of the system or who has the right to

١ Abu Issa, H. (٢٠١٧). Information Technology Crimes (A Comparative Study of Arab Legislation), Amman, P١١.

٢ It is stated in the Unified Model Arab Law regarding the definition of penetration (unauthorized or illegal entry into the system of automatic data processing, by violating security procedures).

٣ Agileh, A. Previous reference, p ٣٠٢.

control it, such as the activities related to state secrets or defenses. It is also achieved when the owner of the system places restrictions on access to that system, but the perpetrator does not respect these restrictions, or if access requires paying an amount of money that was not paid by the perpetrator who made the unlawful access into the system [١].

First of all, concepts of unlawful access, bypassing authorized access and unlawful stay should be considered in order to have a clear understanding of all elements related to the crime Unlawful Access to Computers and Information Systems

The Concept of Unlawful Access:

Most comparative legislations did not address the definition of unlawful access, but some of them, such as the Saudi law in the system of combating IT crimes in Article I/٧ defined it as "a person's access in a certified way to a computer, website,

١ Hijazi, A. Combating Computer and Internet Crimes in the Model Arab Law, p. ٧٩-٨٠.

information system or computer network which that person is not authorized to access it [١]."

The Egyptian legislator, in the recently issued law on IT crimes, adopted the term Hacking and defined it in the first article of it as "Unauthorized access or in violation of the terms of the license, or access in any unlawful way to an information system, computer, information network, and the like." Moreover, most of them did not specify the method used to access, and access takes place by any technical means, whether through the real password when the perpetrator was not authorized to use it, by using a program or special code, by using another person's code, or by accessing through a person who is allowed to access, whether by telephone networks or local or international terminals.

Unlawful access may be done through hacking, and the Omani legislator has stipulated this method in the Electronic Transactions Law [٢]. Hacking is defined as the access of a

١ Abu Issa, H. Previous reference, p. ٣٠,٣٩.

٢ Article (٣/٥٢) of the Electronic Transactions Law

party to the device of another party, regardless of what the former causes to it, unlawfully or without the permission of the hacked party. This generally means reaching a specific goal unlawfully [١].

Hackers are people who have experience in programming and handling networks, and they have the ability to take technological measures to seek to override the barriers established to protect networks. They have developed this ability due to their long practice in understanding programming languages and operating systems [٢].

Hacking methods are varied; it may be done through the use of operating systems, and the most important of which is to do this through the protocols that the system uses to interact with the Internet or intranet of all kinds, so the user passes through several stages and steps. The hacker looks for the (IP) number of the device to be hacked, and the hacker is supposed to be connected to the victim's device via the internet or intranet at a

١ Khalifa, M . (٢٠٠٧) . Previous reference, p٤٠.

٢ AL.Hudhaifi, A. (٢٠١٣). Computer and Internet Crimes. Sudan: Ministry of Justice. p ١٥٧.

certain moment because this number changes with every internet connection.

It may also be done using two programs, one of which is the victim's device and is called (the server program) because it takes orders from the hacker and executes its tasks on the victim's device, the second is a program in the hacker's device called (the beneficiary or customer program). The most popular and most dangerous of these programs is (the Trojan horse [١], which is sent to the victim's device in several ways, the most common of which is sending it by e-mail. Then, when the victim opens it, the program takes its place within the system and begins its espionage tasks. Moreover, it may also be through sniffing and capturing passwords or from known hacking methods [٢].

[١] The Trojan horse is one of the dangerous programs that are used in penetration operations, without the ability to split, track, and eliminate it, and it is named so in relation to the famous Greek myth that tells the story of a large wooden horse with which the invaders were inside. Khalifa,M. previous reference, p٤٣ , Al-Janbihi, M. & Al-Janbihi,M. (٢٠٠٤) .Internet and computer crimes and means to combat them, Alexandria: University Thought House. P٥٥.

[٢] Khalifa,M. previous reference. p ٤٢-٤٣.

This access or attempting to stop that access to the information system may result in material losses, including the loss incurred by a nuclear weapons manufacturing factory in California, USA, which was estimated at about one hundred thousand dollars. It was an experiment conducted to try to stop that access to computer system of said factory [١].

Jurisprudence raised a question, whether or not it is required to secure the data protection system technically in order for a crime - hacking of a computer or information system - to occur or not?

The prevailing opinion in jurisprudence is not to require that; the texts were clear without the requirement to include technical protection. According to the established principles in that, the absolute text may not be restricted unless there is something that restricts it [٢].

It is clear from the above that the point of criminalizing unauthorized access is to protect data and information from

١ Al-Momani, N.(٢٠٠٨). Information Crimes. Amman :House of Culture for Publishing and Distribution. P١٥٧.

٢ Hijazi, A. previous reference. p ٣٥١.

being accessed by people who have no right to do so, i.e. protect the privacy of this information in the face of these people.

The concept of Bypassing Authorized Access:

This case goes to the person who is allowed to access a certain part, then they access another part to which they are not authorized to access or in violation of the authorization or exceeds it.

This point raises research within the limits of the authorization; the perpetrator is authorized to access the computer system, but the perpetrator exceeds these limits, and in most cases the perpetrator is one of the employees of the entity whose computer system was accessed, and use their authorization to access this system in other than the authorized cases. It is difficult to determine whether the worker has actually exceeded their jurisdiction, and whether they did it intentionally or unintentionally because this presupposes that

the specialties of each worker are precisely defined and the areas each worker can access [١].

It is worth noting that overstepping the authorization is the overstepping in the place. As for overstepping the authorized time makes it a case of unlawful stay.

The Concept of unlawful Stay:

The act of unlawful stay is pursuant to a legal access, and this is achieved by overstepping the time range or the authorized intent of staying or connecting to the information system, or access by accident or by mistake and staying in it.

Stay is the failure of the perpetrator to disconnect from the system when they realize that their presence is unlawful. It starts from the moment the person should have changed their status by exiting the system.

Staying inside a computer system means the hacker share control of the computer with access and exit of this system [١].

١ Khalifa,M. previous reference. p ١٤٨.

Staying inside the system takes multiple forms, including staying in the system despite the expiration of the contract and not renewing it, or overstepping the time allowed to stay inside the system. In order for the material part to be fulfilled, it is not necessary for the perpetrator to commit another crime; rather, it is sufficient for them to stay without performing any activity while being able to control the automatic data-processing system [٢].

Unlawful Access and unlawful stay:

unlawful access may coincide with unlawful stay, assuming that the offender does not have the right to access the system, and accesses it against the will of the one who has the right to control it. Then, the offender stays in the system after that, and in this hypothesis the physical aspect is achieved [٣].

=

١ Al-Sagheer, R. (٢٠١٧). Criminal Intent in Internet and Informational Crimes. Giza: Arab Studies Center for Publishing and Distribution. P ٣٦٧.

٢ Agileh, A. Previous reference, p ٣٠٤-٣٠٥.

٣ Abu Hatab, Y . (٢٠١٤). Criminal and Security Protection for Electronic Signatures (Comparative Study). Alexandria: Knowledge facilit

What distinguishes unlawful stay from unlawful access is that it is a continuous crime. The criminal behavior in stay is continuous, and with it the infringement of the legal interest continues. On the other hand, access is a temporary crime, whether in itself or led to a certain result. Therefore, if the law does not explicitly provide for the stay, the access crime provisions cannot be stretched to it [١]. However, the question arises about the time when the state of access ends and when does the crime of stay begin? There is no concurrence in jurisprudence regarding that, as an opinion says that access is achieved at the moment of actual access, while the stay includes a short period of time at which the crime of access ends and is completed. After that moment, the crime of stay begins and ends with its end [٢]. Another opinion specifies that the moment in time when the intruder knows that their stay is unlawful, and a third opinion is that the stay crime begins from the moment when the intruder is warned that their presence is

١ . Khalifa,M. previous reference. p ١٥٤-١٥٥.

٢ . Al-Qahwaji, Ali .(٢٠١٠). Criminal protection for data processed electronically. Alexandria: New University House, p. ٥٦١.

unlawful. If they do not exit, they commit from that moment the crime of staying within the system. A fourth opinion says that the crime of unlawful stay starts from the moment the perpetrator begins to roam within the system, or continues to roam inside it after the end of the specified time because the imposition relates to an unlawful access, i.e. the perpetrator knew that they had no access, and if they accessed and stayed still, it is still an access crime. However, if they start to roam, the crime of stay begins from that moment because they roam in a system they already know that the accessing it is unlawful or that the principle of staying in it is unlawful. Moreover, it is sufficient to achieve this that they stay inside the whole system or part of it. This is the right opinion, as the first opinion does not give a definite definition of the meaning of access and stay, the second opinion is difficult to prove, the third opinion may not be possible to implement it except for large companies.

In summation, unlawful stay is staying after the specified period of time after legal access, or staying after accessing by mistake. It is distinguished as a continuous crime, unlike the unlawful access which is a temporary crime.

Elements of the Crime of Unlawful Access and Overstepping the Authorized Access:

Technically, the act of unlawful access is the first act among computer criminal activities; it may stop there, and it may go further. This technical fact raises controversy on whether unlawful access in itself is criminal (a formal crime), or it must be accompanied by other actions such as editing information, possessing it, using it, or damaging it. This requires knowing the position of Omani legislation and the comparative legislation criminalizing this form and other forms of unlawful stay and overstepping the authorization, the pillars that must be available in each of them, is it punishable to initiate it, and the penalties prescribed for them. We will get to know all of that in this requirement.

- **The Physical Aspect of Unlawful Access and Overstepping authorized Access:**

There is unanimity in the Arab legislation to criminalize unlawful access, but they did not adopt a single approach in that. The greatest majority criminalized abstract access, which means that this crime is a positive crime that requires material

activity from the perpetrator to achieve its components. However, some legislations - such as Saudi legislation - do not criminalize access on its own; rather, it requires it to be associated with another intention (a special intent). Others require the achievement of a specific result of that access. Therefore, we will review the comparative legislation under study. According to the aforementioned, their elements differ, and it is possible to say through reviewing the comparative legislations that they differ among themselves. In the following we detail their trends:

- **Trends of the Legislation**

Legislation trends differ in criminalizing unlawful access, unlawful stay, or overstepping the authorized access, including those who are punished for accessing, staying, or overstepping the abstract permit. Among the legislations are those that require achieving a certain result, and others that require a special intent to punish them. We will learn these trends closely according to the following detail:

- **The First Trend: criminalizing the mere access, unlawful stay, or overstepping the authorization**

without requiring a criminal result or a specific intent

The crime of unlawful access, unlawful stay, or overstepping the authorization is effected by simply accessing the system, staying in it, or overstepping the granted authorization, even if this access does not result in any criminal result. Even if the occurrence of a specific result is considered an aggravating circumstance at times, and after that access can achieve the whole crime or part thereof.

Including what the Omani legislator stipulated in Article (٣) of the IT Crime Law: "A penalty of imprisonment for a period of no less than one month and no more than six months, and a fine of no less than one hundred Omani Rial and no more than five hundred Omani Rial, or one of these two penalties, Whoever intentionally and unlawfully enters a website, information system or information technology means or a part thereof, or exceeds the authorized access to it, or continues to do so after knowing it..." Moreover, Article (٢) of the UAE IT Crime Law stipulates: "Anyone who unlawfully enters a website, electronic information system, information network, or information technology means, without permission or

exceeds the limits of the authorization, or stays in it, shall be punished with imprisonment and a fine of no less than one hundred thousand Dirhams and no more than three hundred thousand Dirhams, or one of these two penalties."

Among the judicial applications of the foregoing, in a case whose facts are summarized as follows: a person used a computer program to break the passwords of some Emirates Telecommunications Corporation staff to access unauthorized sites of the network subscribers, and copy some files of passwords and emails of the institution staff knowingly [١].

Likewise, Article (١٤) of the Egyptian IT Crime Law stipulates: "Anyone who intentionally or by an unintentional error unlawfully accesses and stays on a private website, account or information system to which access is prohibited shall be punished by imprisonment for a period of no less than a year and a fine of no less than fifty thousand Pounds and no more than one thousand Pounds or one of these two penalties.

١ . For more details, see the judgment issued by the Dubai Court of Cassation, at the hearing of ١٢/٠٨/٢٠٠١, in Case No. (٢٣٠/٢٠٠١).

If that access results in destruction, erasure, alteration, copying, or republishing of data or information on that website, private account, or information system, the penalty shall be imprisonment for a period of no less than two years and a fine of no less than one hundred thousand Pounds and no more than two hundred thousand Pounds or one of these two penalties." Article (١٥) of the aforementioned law also stipulates: "Whoever accesses a private website, account, or information system using a right that they are authorized and overstepping the limits of that right in terms of time or level of access shall be punished by imprisonment for a period of no less than six months and a fine of no less than thirty thousand Pounds and no more than fifty thousand Pounds, or by one of these two penalties."

Article (٢٠) of the Law on Combating IT Crimes stipulates: "Whoever intentionally or unintentionally unlawfully accesses and stays or exceeds the limits of the authorized right in terms of time or level of access, or hacks a website, email, private account or information system managed by or for the state or one of the public legal persons or owned by it shall be punished by imprisonment for a period of no less than two

years, and by a fine of no less than fifty thousand Pounds and no more than two hundred thousand Pounds, or by one of these two penalties.

If access was done with the intent of intercepting or unlawfully obtaining government data or information, the penalty shall be imprisonment and a fine of no less than one hundred thousand Pounds and no more than five hundred thousand Pounds.

In all cases, if any of the foregoing acts results in the destruction of that data or information or that site, private account, information system or e-mail, or its destruction, distortion, alteration, changing its designs, copying, recording, altering its course, republishing, or canceling it in whole or part by any means shall be punished by imprisonment and a fine of no less than one million Pounds and no more than five million Pounds."

- **The Second Trend: It requires the accused to have a special criminal intent for the unlawful access, stay, or overstepping the authorization**

The legislator may punish for unlawful access, but it is associated with the condition of having a certain intent including what is stated in the Saudi system. Article (٣) of the

IT Crime Law stipulates: "Every person who commits any of the following information crimes shall be punished with imprisonment for a period no more than one year and a fine no more than five hundred thousand Riyals, or one of these two penalties... ٢. unlawful access to Threaten or Blackmail a Person...٣. Unauthorized access to a website or access to a website to change the designs of this site, destroy it, modify it, or occupy its address." Article (٥) of the same law also stipulates: "Every person who commits any of the following information crimes shall be punished with imprisonment for a period no more than four years and a fine no more than Three million riyals, or one of these two penalties: ١. unlawful access to cancel private data, delete it, destroy it, leak it, destroy it, change it, destroy it, alter it, or republish it ...".

Likewise, Article (٧) stipulates: "A person who commits any of the following IT crimes shall be punished with imprisonment for a period no more than ten years and a fine no more than five million or by either of these two penalties:... ٢- unlawful access to a website or information system directly, or through the information network or one of the computers to

obtain data that affects the internal or external security of the country or its national economy."

The Saudi legislator requested the intent to influence the data or influence the computer system itself, or the intent to obtain data that affects national security or the national economy in order to punish this access, or the intent to threaten or blackmail, while it did not require that the system be password protected [١].

By studying the direction in which the Omani legislator took, it was clear that it punishes unlawful access, stay or overstepping the abstract authorization. However, it has broken that rule and punished for access when there was a special intent in another text and other punishment for certain crimes. Moreover, it found That it is necessary to punish the perpetrator if they entered for a special intent, and that is what is stipulated in Article (٦) of the Law on Combating IT Crime."..... Whoever intentionally and unlawfully accesses a

[١] Taha, M. (٢٠١٣). The legislative confrontation with computer and Internet crimes. Mansoura: House of Thought and Law, p. ٢٤.

website or an information system with the intent of obtaining government electronic data and information that is secret by nature or according to instructions issued for that shall be punished with imprisonment for a period of no less than three years and no more than ten years and a fine of no less than three thousand Omani Riyals nor exceeding ten thousand Omani Riyals, if the criminal act results in the cancellation, alteration, modification, distortion, damage, copying, destruction or publication of electronic data or information." It is clear that the legislator limits it to accessing the website and the information system without the means of information technology, in which the perpetrator is punished for access with the intent of obtaining confidential electronic data and information.

Access may be for the intent of obtaining government electronic data and information, and it is intended to contact the information system without the approval of the authority responsible for the system. That takes many forms, including that the perpetrator operates a government electronic information system or devices without the permission of the owner of the system, and sees what the government agency

that owns the system does or moves between parts of the device to see what information it contains. However, that access does not require the perpetrator to view the files of the system owner or the functions it performs, but it is sufficient for its occurrence that the perpetrator be able to access the system remotely even if he was unable to open the information files that the system contains, and that access must be made with the intent of obtaining government electronic data and information [١].

The law also deviates from the general rule adopted in the IT Crime Law as it requires a special intent in the Electronic Transactions Law. Article ٥٢/١٣ of the Electronic Transactions Law states: "Without prejudice to any more severe punishment stipulated in the Omani Penal Code or any other law, he shall be punished with imprisonment for a period no more than two years and a fine no more than OR ٥,٠٠٠. Five thousand Omani Rials, or one of these two for anyone who: ٣. fraudulently accesses an information system or database for the intent of tampering with electronic

[١] Al-Qahwaji, Ali .previous reference. p ٥٨٠.

signatures.... ".....١٣. unlawfully accesses a computer with the intent of committing a crime or facilitating the commission of a crime, whether by him or by another person .... ".

The material aspect of this crime is the activity of the perpetrator, which is fraudulent access to the information system or database. The concept of fraud is a broad one that includes everyone who is not authorized to connect to the information system and includes all forms [١], and that access is for the intent of tampering with electronic signatures, or with the intent to commit a specific crime or to facilitate the commission of a crime, whether by him or by another person.

Article (٢٠) of the Law on Combating IT Crimes stipulates: "Whoever intentionally or unintentionally unlawfully accesses and stays or exceeds the limits of the authorized right in terms of time or level of access, or hacks a website, email, private account or information system managed by or for the state or one of the public legal persons or owned by it shall be

[١] Fekry, A. (٢٠٠٧). Information systems crimes (a comparative study). Alexandria: New University House. Alexandria. P. ٢٠٨.

punished by imprisonment for a period of no less than two years, and by a fine of no less than fifty thousand Pounds and no more than two hundred thousand Pounds, or by one of these two penalties.

If access is done with the intent of intercepting or unlawfully obtaining government data or information, the penalty shall be imprisonment and a fine of no less than one hundred thousand Pounds and no more than five hundred thousand Pounds..."

The aforementioned article stipulates that if access is done with the intention of intercepting or unlawfully obtaining government data and information, the penalty will be stricter than mere access. It is worth noting in this regard that the above-mentioned Egyptian legislation is recent and no books and jurisprudence have been written on it. This opens the way for the researcher to discuss it without relying on the opinion of jurisprudence on this.

- **The Third Trend: criminalizing hacking with a specific criminal result required**

This trend, which the Omani legislator took in the Electronic Transactions Law as article ٥٢/٢ of said law states: "Without prejudice to any more severe penalty stipulated by the Omani

Penal Code or any other law, it is punishable by imprisonment for a period no more than two years and by a fine no more than ٥,٠٠٠ Omani Rials.

Five thousand Omani Rials, or one of these two anyone who:

٢. Hacks a computer, a computer system, a website, or an internet network, and it caused:

a. Disrupting operating systems of a computer or a computer system.

b. Destroying the computer program or computers and the information they contain.

c. Theft of information

d. Using information contained in computer outputs for unlawful intents,

e. Entering incorrect information. ".

This crime is realized whenever the access is against the will of the owner of the system or the one who has the right to control it, and the punitive hack according to this article is the hack that results in a specific result. This means that the crime

does not take place unless the criminal act results in one of the following results:

(The hacked system or site is malfunctioned, or the computer programs, computers, or information that it has are destroyed, either totally or partially, in a fashion that renders them unusable, stealing information in the hacked system or site or using them unlawfully, and entering incorrect information [١].

Information destruction is defined as "destroying or erasing the instructions of the programs and data themselves, and the destruction is not aimed at merely obtaining a benefit from the computer in whatever form, whether seizing funds or accessing information, but causing damage to the information system and impeding it from performing its function" [٢].

By reading the article, we find that the legislator did not specify a specific means of penetration and access to the system, and then it is permissible to enter by any technical or technological means, except that it requires a specific result of

١ Al-Ghafri, H. (٢٠١١). Explanation of Omani Electronic Transactions Law .Cairo: Arab Renaissance House.p. ١٢٩, ١٣٠.

٢ Fekry, A. previous reference. p ١٥٣.

access, and we also note that it narrowed the scope of unlawful access by using the term hack. Nonetheless, we see, in our humble opinion, the use of the term unlawful access is more accurate, which is used in the Law on Combating IT Crime and also used it in the law itself, which is what most legislations have adopted because hacking by its nature is unlawful access, and latter has a broader scope.

Through the aforementioned texts, it becomes clear to us that the Omani legislator took the expanded direction that combines the information system and websites and any means of information technology for unlawful access. Moreover, it did not specify a specific way of accessing the system, and then it is permissible by any technological or technical means, whether it is access to the system using the real password by the perpetrator if they are not authorized to do so, access was made using special programs or codes, or the offender's impersonation of one of the users of the system, in the systems in which users place passwords. Access may also be done through hidden gates, whether entering from telephone networks or communication networks to local or global terminals, and whether entering all or part of the system.

However, it limited protection against unlawful access to government data on websites and information systems without the means of information technology. Here, a question arises as to whether the unlawful access to a method of information technology for the government agency, the text applied here is Article (٣) and not Article (٦) of the said law.

It is clear from the foregoing that for the material element of this crime to be realized - in its simple form - the need for the act of unlawful access, stay or overstepping the authorized access, as stated above, must be realized. Accordingly, according to the different course of legislation in that domain another question arises about if the initiation is punishable in the previous actions or not, that would be clarified in the next point.

- **Attempting Unlawful Access and Overstepping Authorized Access**

According to the general principles, the attempt is to start implementing one of the apparent acts leading to the commission of the crime, but the perpetrator was unable to complete the actions necessary for that crime to occur for reasons beyond his control.

It is conceivable to attempt the crime of unlawful access and overstepping the authorized access, if the perpetrator has exhausted all his capabilities to access the information system or the computer, but he was unable to access because of strong protection or that the perpetrator found some way, and when he entered it, it was changed, so is he punished for that?

It is noted that the legislations almost concur to punish the attempt of cybercrime, as they contained a general text applied to the attempt. However, they may differ in the size of the penalty [١], and that is what is stipulated in Article (٣٠) of the Law on Combating IT Crimes, corresponding to Article (٤٠) In the UAE IT Crime Law, Article ١٠ of the Saudi Information Crime Law, and Article ٤٠ of the Egyptian IT Crime Law. This includes the arrest of the accused after operating the device and before he can open any file in the device, or being unable to open it because it requires a password [٢].

١ Abu Issa, H. Previous reference, p ٤٥.

٢ Taha, M. Previous reference, p ٣٢.

By extrapolating the texts prescribed for the punishment for attempting the crime of unlawful access and overstepping the authorized access in the above-mentioned articles, we find that there is disparity. The Omani law stipulates that the punishment is half the maximum prescribed punishment for the crime, and in the UAE law half the punishment prescribed for the complete crime, while Saudi law punishes with no more than half the maximum limit of the prescribed punishment and so is the Egyptian legislator. This is in contrast to each legislator's view of cybercrime and its impact on their community.

Moral Element of the Crime:

The crime of accessing or staying in the system is one of the intentional crimes that are based on the general criminal intent, which consists of the elements of knowledge and will. The offender must be aware that they are not entitled to access or stay within the system, and that this is against the desire of the owner of the system or the its controller. However, his will is directed towards taking this act in violation of the law and the will of the owner of the system or the owner of the right therein.

According to the previous determination of the criminal intent, the legal aspect is not available when the access or stay of the perpetrator is permitted, nor does it happen if the perpetrator made a mistake related to their right to access or their right to stay or within the scope of this right, such as if he is ignorant of the existence of the prohibition of access or stay or mistakenly believed to be authorized to access. Moreover, there is no place to count for the motivation to commit the crime, even if the motive is curiosity or proving the ability to win [١].

As for the intention of fraud, it appears through access that is made through hacking the system that protects the device, and which does not require hacking to establish unauthorized access or stay, but it is a sign of bad faith and that access is unlawful. Most legislations tend not to require a specific intent, except the Saudi legislator is not satisfied with the general intent; rather, it requires a special type, which is to be for the intent of threat, extortion, obtaining data that affects the security of the state from the inside or outside, or affects the

[١] Hijazi, A. previous reference. p ٣٥٦-٣٦٦.

national economy, that its intent is to tamper with the system or the data it contains or to change, damage, modify or alter the website's designs [١].

The implication of this is that unauthorized access is not considered a crime punishable by law in the Kingdom of Saudi Arabia. Using hacker programs does not make the act punishable, and yet it punishes espionage. Whoever interferes in others' devices and learns what they are doing without having a special intent is not committing the crime of interference; rather, they are committing the crime of eavesdropping (Article ١-٣) of the Cyber Crime Law [٢].

As for the time when a criminal intent is available, attempting and access are equal, i.e. if a person enters an information system by chance or error and then discovers that his access is unlawful, but they continue to stay within the system, then the crime is considered to exist [٣].

١ Abu Hatab, Y .previous reference. p ١٢٧.

٢ Abu Hatab, Y .previous reference. p ١٢٨.

٣ Abu Issa, H. Previous reference, p ٤٧-٤٨.

It is clear from the foregoing that the crime of unlawful access is an intentional crime because the moral element of it takes the form of the criminal intent, and it is sufficient for it to fulfill the general intent, which is knowledge and will. The perpetrator must be aware that they are entering the crime scene, and that this unauthorized access or in violation of or exceeds the authorization and his will is directed to that.

The Penalties Prescribed for the Crime:

The penalty prescribed for the crime of unlawful access or stay varies according to the each legislation, and according to whether it is in its simple or aggravated form, and its aggravated form is achieved, whenever it entails the unlawful access or stay of a specific result stipulated by the legislator in the texts prescribed in each law, and the legislation differed In that, the most prominent results can be summarized in the following: -

١. Modification: It means changing the data inside the system, and replacing it with other data. This is done using programs that manipulate the data, whether by erasing it in whole or in part or by modifying it by using the cyber bomb of data or

viruses in general, or by others who have no right or authority on the information by modifying it [١].

Among the incidents of unlawful access into databases is the incident that occurred in California, USA, where the data access clerk in an automobile club intentionally and on a prior agreement between her and her friend - a car thief - forged data on car ownership registered on the computer so as to transfer their ownership to her boyfriend, who intends to steal the cars and sell them. When the owner of the car reports the theft of his car, the database search on the computer shows that there are no records of the car being registered to him. After the girl's boyfriend sells the car, she re-registers the car in the original owner's name, and she used to take money in return for that [٢].

٢. Entering data in the information system: This law requires that any data be entered into the computer system that was not

[١] Amin, T. (٢٠١٣). Criminal protection for electronic transactions. Alexandria: Al-Wafa Legal Library. P ٦٤.

[٢] Al-Janbihi, M. & Al-Janbihi,M. . previous reference. p ٩٠.

originally present, with the intention of disturbing the existing data, which may affect its validity [١].

٣. Erasing data: Erasing data means destroying them, completely or partially.

It is worth noting that the technical methods that may be used to destroy computer programs and data are beyond count; even if that is possible at the present time, but the means that technology may use in this regard cannot be predicted. However, the most dangerous of these methods (currently) are called means of logical sabotage, i.e. computer viruses, which are attack software that infect computer systems in a manner that closely resembles the style of biological viruses that infect human beings" [٢].

٤. Cancellation: - It means removing information from the information system, which is the most severe type of damage [٣].

[١] El-Shazly, F. & Afifi, k. (٢٠٠٧). Computer crime, copyright, artistic works, the role of the police and the law. Beirut: Human Rights Publications. P ٢١١.

[٢] El-Shazly, F. & Afifi, k. previous reference. p ٢١٤-٢١٥.

[٣] Fekry, A. previous reference. p ٢١٥.

٥. Change: It means causing modifications in the information, which make it contrary to the original content prior to the act. This is considered a middle ground between cancellation and distortion in terms of damage.

٦. Distortion: It means distorting the information so that it becomes partially inconsistent with the original information stored in the information system. This is considered the slightest type of damage, and the causal relationship is required between this activity and the occurrence of the result (cancellation, change or distortion) [١].

٧. Destruction: Destruction is a form of spoiling, and it is considered to be more dangerous than just making adjustments to the information content. Destruction means any action that prevents or ends the availability of data for the person who has access to the computer or the data storage on which the data is stored.

[١] Fekry, A. previous reference. p ٢٠٠.

Having a causal relationship between unlawful access or stay and the result achieved is sufficient for the aggravating circumstance to be present.

This crime is intentional, for its establishment must provide the general criminal intent of the offender with the elements of knowledge and will. If it was proven that the offender has no causal relationship between criminal behavior - unlawful access or stay - and the criminal result, which is the aggravating circumstance in the crime, such as proving that modifying the erasure of data or The authorization of the system to perform its functions is due to a force majeure or sudden accident, the criminal behavior is negated as well as the criminal intent of the perpetrator [١].

We will look at the position of the Omani legislator and the comparative legislation, and discuss the suitability of legal texts in keeping with the electronic scientific development, as follows:

[١] Hijazi, A. previous reference. p ٣٦٧.

The Position of the Omani legislator:

The Omani legislator handled the unlawful access and overstepping the authorized access, in the electronic transactions laws and combating information technology crimes. We will start by reviewing the criminal texts for it. Next, we will analyze the penalties prescribed for it according to the following detail.

- **A Review of Related Legal Provisions:**

We mentioned previously that the Omani legislator addressed the unlawful access and overstepping the authorized access in the Electronic Transactions Law and Combating IT Crimes Law, but this needs to be detailed. Therefore, we address each of them as follows:

- **Electronic Transaction Law:**

The Omani legislator stipulated the unlawful access without overstepping the unlawful access or stay in the Electronic Transactions Law, and two terms were used for that. The first of which narrowed down its limits (the hack that requires

a specific result) [١],

The other expanded its limits (the unlawful access to commit a crime) [٢], and it also stipulated the unlawful access into the information system of the electronic signature with the intent to tamper with it [٣].

[١] The Electronic Transactions Law as article ٥٢/٢ of said law states: "Without prejudice to any more severe penalty stipulated by the Omani Penal Code or any other law, it is punishable by imprisonment for a period no more than two years and by a fine no more than ٥،٠٠٠ Omani Rials.

Five thousand Omani Rials, or one of these two anyone who:... Hacks a computer, a computer system, a website, or an internet network, and it caused:

a. Disrupting operating systems of a computer or a computer system.

b. Destroying the computer program or computers and the information they contain.

c. Theft of information

d. Using information contained in computer outputs for unlawful intents,

e. Entering incorrect information. ".

[٢] Article ٥٢/١٣ of the Electronic Transactions Law states: "Without prejudice to any more severe punishment stipulated in the Omani Penal Code or any other law, he shall be punished with imprisonment for a period no more than two years and a fine no more than OR ٥،٠٠٠. Five thousand Omani Rials, or one of these two for anyone who: ".....١٣. unlawfully accesses a computer with the intent of committing a crime or facilitating the commission of a crime, whether by him or by another person .... ".

[٣] Article ٥٢/٣ of the Electronic Transactions Law states: "Without prejudice to any more severe punishment stipulated in the Omani Penal Code or any other law, he shall be punished with imprisonment for a period no more than two years and a fine no more =

- **Information Technology Crime Law**

The Omani legislator stipulated unlawful access stay and overstepping the authorized access in the Law of Combating IT Crimes, and distinguished between unlawful access and overstepping the authorized access and mere unlawful stay [١]. Moreover, it has made the penalty more severe if it resulted in a specific result, was of a certain type, or the perpetrator has a title, as stipulated in Article (٣ / second and third paragraph): ".....If what is mentioned in the first paragraph results in the cancellation, change, alteration, distortion, damage, copying, destruction, publication or re-publication of electronic data or information stored in the information system or information technology means; the destruction of that system, information technology or information network; or harm to employees or

=

than OR ٥،٠٠٠. Five thousand Omani Rials, or one of these two for anyone who: ٣. fraudulently accesses an information system or database for the intent of tampering with electronic signatures.... ".

١ Article (٣) of the IT Crime Law: "A penalty of imprisonment for a period of no less than one month and no more than six months, and a fine of no less than one hundred Omani Rial and no more than five hundred Omani Rial, or one of these two penalties, Whoever intentionally and unlawfully enters a website, information system or information technology means or a part thereof, or exceeds the authorized access to it, or continues to do so after knowing it...".

beneficiaries, the penalty shall be imprisonment for a period of no less than six months and no more than a year, and a fine of no less than five hundred Rials and no more than a thousand Rials, or one of these two penalties. If the data or information provided for in the second paragraph is personal, the penalty shall be imprisonment for a period of no less than one year and no more than three years and a fine of no less than one thousand Omani Rials and no more than three thousand Omani Rials, or one of these two penalties."

Article (٤) of the aforementioned law made the penalty more sever if it is committed by a person with an official position: "Whoever commits one of the crimes stipulated in Article ٣ of this law, during or on the occasion of performing their work, shall be punished with imprisonment for a period of no less than one year and no more than three years, and a fine of no less than one thousand Omani Rials and no more than three thousand Omani Rials, or one of these two penalties."

The legislator also singled out a separate punishment for those whose access was intended to obtain government data and electronic information. Article (٦) of the aforementioned law stipulates: “Whoever intentionally and unlawfully accesses a

website or an information system with the intention of obtaining government electronic data and information confidential in nature or according to instructions issued thereto shall be punishment of imprisonment for a period of no less than one year and not more than three years, and a fine of no less than one thousand Omani riyals and no more than Three thousand Omani riyals, or one of these two penalties, and the punished with imprisonment for a period of no less than three years and no more than ten years and a fine of no less than three thousand Omani Rials and no more than ten thousand Omani Rials, if the criminal act results in the cancellation, alteration, amendment, distortion, destruction, copying, destruction or publication of electronic data or information.

Confidential electronic data and information for banks and financial institutions is considered to be classified government electronic data and information within the scope of application of the provision of this article."

- **Criminal Policy Followed in Specifying the Penalty:**

By extrapolating the aforementioned texts, we find that the criminal policy pursued by the legislator in specifying the punishment varies according to whether it is in its simple form or in its aggravated form. The legislator took into account the losses that it might have caused, so the penalty was aggravated if the results were of a certain gravity or were committed by a person with official title or was of a certain type. We explain this in some detail according to the following statement: -

١. The simple crime penalty: the penalty prescribed for unlawful access, overstepping the authorization, and mere unlawful stay is the penalty of imprisonment for a period of no less than a month and no more than six months and a fine of no less than one hundred Rials and no more than five hundred Omani Rials or one of these two penalties, but if that access was done with the intention of obtaining government data or electronic information, the prescribed punishment is imprisonment for a period of no less than one year and no more than three years, and a fine of no less than one thousand Omani Rials and no more than three thousand Omani Rials, or one of these two penalties.

٢. The penalty for aggravated crime: with regard to aggravating circumstances, we find that the Omani legislator stipulated two types of aggravation: -

a. If it led to a certain result: The Omani legislator stressed in Article (٣) of the Law on Combating IT Crimes, if that access entails one of the results stipulated in (canceling, changing, amending, distorting, destroying, copying, destroying, publishing or republishing electronic data or information stored in the information system or IT means, destroying that system or information technology, the information network or harming users or beneficiaries), the minimum penalty is not less than six months and not more than a year in its upper limit and the fine in its minimum is not less than five hundred Omani Rials and not more than one thousand Omani Rials, or one of these two penalties.

The legislator has also aggravated the penalty in Article (٦) if access was intended to obtain secret government electronic data and information results in any of the following results (cancellation, alteration, modification, distortion, damaging, copying, destruction or publication of electronic data and information) with imprisonment for a period of no less than

three years minimum and no more than ten years and a fine of no less than three thousand Omani Rials and not more than ten thousand.

a. If the data and information are personal: The legislator also aggravated the penalty if the data or information that was damaged according to the above statement is personal data, that is, related to data of a personal nature, by no less than a minimum of one year and no more than three years and a fine of no less than one thousand Omani Rials and no more than three thousand Omani Rials or one of these two penalties. The question here arises whether the unlawful access is abstract, i.e. it was not intended to obtain electronic government data and information, but that electronic data and information is governmental and consequently that access entails any of the results mentioned. Are personal data more protected than government data?

c. If committed by a person with an official title: The legislator has aggravated the penalty of the crime of unlawful access, or overstepping the authorized access, or unlawful stay during work or for performing the work, whether the mere access or the consequence of a certain result to be punished with

imprisonment for a minimum of no less than one year and no more than three years, and a fine with a minimum of no less than one thousand Omani Rials and no more than three thousand Omani Rials, or one of these two penalties.

Access or stay during the performance of work means when one is inside the system but the worker exceeds the limits of his work by looking at information that is not within the scope of his work. During the work of the worker it means accessing the computer system, the worker himself is not authorized to access it, such as accessing the information on his director's device [١].

Conclusion:

We deduce from the above that the Omani legislator has criminalized unauthorized access and stay and overstepping the authorized access, and has followed the policy of criminalization for mere act as a general rule, and has aggravated the penalty if certain consequences arise.

[١] Ismail, M. (٢٠١٧). Legal regulation of the crime of unauthorized access to the computer system. Saudi Arabia: Qassim University. P ٥٤٢.

Moreover, the legislator deviated from that rule in unlawful access crimes to government electronic data and information and required special intent (in order to obtain this information), and increase the penalty if it leads to certain results.

The Omani legislator intervened in giving the necessary protection to electronic management in its informational part (data and information) and its physical part (its devices and its belongings) with the enactment of the Electronic Transactions Law and the Law on Combating Information Technology Crimes. The Omani legislator criminalized illegal entry and stay and bypassing the authorized entry, and followed the policy of strengthen the penalty if the crime results in certain consequences.

It becomes clear that the Omani legislator has kept pace with the technological development through different legislations to fight information technology crimes. Under which the protection of government electronic data and information is ensured, and accordingly added confidence in its use.

Researchers urge the Omani legislator to standardize the legal terms that have the same meaning and which are used in the

laws of electronic transactions and fighting information technology crimes (information system, electronic information systems), also the scope of these terms should be standardized.

Moreover, the scope of information forgery should be expanded to include cases other than what is stipulated (addition, deletion and replacement). The protection of electronic documents, data and electronic information from destruction and destruction is a direct original protection in the Omani legislation.

References

١. Legislation and laws

- The IT Crime Law: Issued by the Royal Decree (١١/٢٠١١), and published in the Official Gazette, issue (٩٢٩).
- The Electronic Transactions Law : Issued by Royal Decree No. (٦٩/٢٠٠٨), and published in the Official Gazette, issue No. (٨٦٤).

٢. Sources and references:

- Abu Issa, H. (٢٠١٧). Information Technology Crimes (A Comparative Study of Arab Legislation), Amman.
- Abu Hatab, Y . (٢٠١٤). Criminal and Security Protection for Electronic Signatures (Comparative Study). Alexandria: Knowledge facility.

- Agileh,A. (٢٠١٤). Criminal protection for electronic documents. Cairo :Arab Renaissance House.
- Amin, T. (٢٠١٣). Criminal protection for electronic transactions. Alexandria: Al-Wafa Legal Library.
- Al-Janbihi,M. & Al-Janbihi,M. (٢٠٠٤) .Internet and computer crimes and means to combat them, Alexandria: University Thought House.
- AL.Hudhaifi, a. (٢٠١٣). Computer and Internet Crimes. Sudan: Ministry of Justice.
- Al-Momani, N.(٢٠٠٨). Information Crimes. Amman :House of Culture for Publishing and Distribution.
- Al-Qahwaji, Ali .(٢٠١٠). Criminal protection for data processed electronically. Alexandria: New University House.
- Al-Sagheer, R. (٢٠١٧). Criminal Intent in Internet and Informational Crimes. Giza: Arab Studies Center for Publishing and Distribution.
- Khalifa, M . (٢٠٠٧) .Criminal Protection of Computer Data in Algerian and Comparative Law . Azaytah: The New University House.

- Hijazi, A. Combating Computer and Internet Crimes in the Model Arab Law.
- Taha, M. (٢٠١٣). The legislative confrontation with computer and Internet crimes. Mansoura: House of Thought and Law.