CIVIL LIABILITY ARISING FROM THE ZERO CLICK ATTACK

MURTADA ABDALLA KHEIRI ABDALLA
Associate Professor Civil in LAW- **A'sharqiyah University**

Abstract
We are now in the twenty-first century, and this coincided with the high-speed development in information and communication technology and the widespread and remarkable spread of the Internet, this resulted in the presence of many websites, and most of the official transactions are now carried out through many different websites such as buying, selling, or shopping, not to mention The multiplicity of social media and its sites, the most prominent and widespread of which are: (Facebook, Twitter, and WhatsApp).
This technological development was also accompanied by the development of electronic devices, and as a result, the release of digital devices, including laptop computers and smart phones, and the emergence of software science, and electronic programs that can be installed on personal computers and mobile phones, and there is no doubt that all of this is considered of the positives produced by the massive technological development. in the field of the Internet
However, on the other hand, many negative aspects appeared, including the increase in cybercrime rates that we had not heard of before, such as systematic intrusions and spying on people using programs developed by rogue programmers who were called hackers and crackers with the intent to harm. Many people, and even countries, were subjected to these attacks, which caused them huge losses of money and violation of privacy, as well as inflicting great risks on the economy, national security, and the lives of individuals, so the Internet turned into an arena of conflicts and settling scores, and after the crimes were taking place on the ground, these crimes of Piracy, terrorism, money laundering crimes, forgery, counterfeiting, spreading racism and pornography, spying on others, and unlawfully stealing money to the virtual reality that exists in the Internet arenas in a way that is compatible with the characteristics of the Internet, which prompted many countries to enact strict legislation to confront these cyber crimes[(1)]

Keywords: *widespread, legislation, pornography, counterfeiting, forgery*

INTRODUCTION

Recently, electronic attacks have increased and have taken many forms , but these attacks agree to take a certain natural form, which is that the hacker exploits the weaknesses of government agencies, organizations and individuals and not to renew their security system and follow the electronic security system and use programs that protect them from these attacks, so the hacker (hackers) by sending encrypted messages carrying a program that was specially created to open a loophole in the victim's device, whether it is an individual, a company, or a government agency. He can even turn on the victim's camera and record videos without anyone knowing about it, and also access the audio of the hacked device and record everything that goes around it at a distance of approximately ten to twenty meters, depending on the quality of the device used, as long as the device is connected to the Internet.

(1) The following is meant by cybercrimes. It is a type of crime committed against individuals or groups with a criminal motive and an intention to harm the victim's reputation, body, or mentality. Whether directly or indirectly. And this is done using modern means of communication such as the Internet and chat rooms, email, or groups. For more information, see Dr. Abeer Shafiq Rahbani. Electronic crimes and their risks. Dar Al-Thaqafa for Publishing and Distribution, Jordan.2021. p. 29. See also Dr. Mohamed El-Desouky El-Shahawy, Criminal Protection of the Sanctity of Private Life, PhD thesis, Cairo University, without year, p. 52..

In a remarkable development of these electronic attacks, a new type of attack appeared, more dangerous than the regular attacks that were observed in the past years, as the regular attacks always depend on the use of fraudulent means to lure the victim, such as sending spam e-mail that contains a link or a file, taking advantage of the victim's ignorance of computer matters or The Internet or depends on deception by forging an electronic link or an application of unknown origin used by the victim or sending him fake offers in the form of files, and the program built inside is activated immediately after the victim opens those files or links, which makes the hacker's access to the victim's device easy and accessible

As for the modern method, which appeared recently, it is known as the zero click attack in which the hacker does not need to send a message to the victim, a forged email, or any link at all, and here lies the absolute danger, as the hacker can access any device Without any reaction from the victim, taking advantage of security holes in the operating systems of the computer or smartphone used by the victim, he does not need.

The hacker only needs to know simple and available information about his victim, such as his own phone number, the places he frequents, the operating system he uses, or the wireless network (WiFi) he uses, and he exploits the gaps in this system directly to install spyware without the knowledge of the victim or without any positive behavior.

In fact, the zero-click attack puts us in direct confrontation with a new type of cyberattack that resulted in cybercrime that was condemned by various legislations, including the Egyptian legislator, the Saudi regulator, and the French legislator, as they set a special system to combat information crimes.(2)

RESEARCH PROBLEM

Are the rules of civil liability defined by national legislation - such as the Egyptian legislator, the Saudi regulator, and the French legislator - in their laws sufficient to compensate those affected by the new crimes that resulted recently from the zero-click attack, which differ in their characteristics from those that existed before?

We find that the person who has been exposed to this attack has suffered great harm in addition to his unawareness of it, and his lack of attention to it in the first place, so it is necessary to enact a law that accurately defines the criminal penalty prescribed for the wrongdoer of the zero-click attack, as well as a law that compensates the victim for the serious damage he suffered. As a result of that attack, whether it was physical or moral damage.

RESEARCH IMPORTANCE

The importance of the research lies in the definition of the crime of the zero click and the statement of the risks resulting from it, such as a violation of privacy and the assault on established rights approved by the law for the victim, and clarifying the legal protection approved by the civil law for such crimes, while shedding light on the possibility of just applying the objective general rules defined by the civil law or not, and if These have been implemented, so does the zero-click attack fall under them?

RESEARCH METHODOLOGY

This research is based on three methodological axes: descriptive, analytical, and comparative. So, we first uncover the nature of the zero-click attack, trying to measure the power of comparison

(2) For more information, you can see the Royal Decree on Combating Cybercrime issued No. M/17 dated 8/3/1428, where the last entry was on 5/5/1443 AH:

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010- a9a700f2ec1d/1

And also the Egyptian Anti-Cybercrime Law No. 175 of 2018, where the last entry was on 5/5/1443 AH: 31487/https://manshurat.org/node France enacted Law No. 19-88, which added to the Penal Code computer crimes and the penalties prescribed for it. .

between each of the laws issued by the Saudi regulator issued by Royal Decree No. M / 17 dated 3/1428 8 on combating information technology crimes, and between Egyptian Law No. 175 of 2018 on combating information technology crimes, in light of French Law No. 88-19, which added computer crimes to the Criminal Penal Code, Then analyze the legal texts for each of them in order to determine the legal system for the zero-click crime, as well as to determine ways to compensate those affected by the losses that befell them.

RESEARCH PLAN

Chapter one: the nature of the zero-click attacks crimes.
Chapter two: the legal basis for civil liability arising from the zero-click attack crimes.
Chapter three: the effects of civil liability for damages arising from the zero-click attack.

The first chapter

zero-click attacks nature.

Before we start talking about zero-click crimes or zero-click attacks, we must first talk about cybercrimes, then explain their characteristics, and then show everything related to zero-click crimes.

The first part

The concept of cybercrime

Electronic crime is considered one of the modern phenomena because its emergence was linked to the emergence of modern technologies such as the computer and the Internet, and therefore no specific definition was agreed upon. Many jurists have argued that it is not defined as a specific crime, and their argument was that it is just an ordinary crime, but electronic means were used to implement it.

First, definition cybercrime

To define cybercrime, two approaches emerged from jurisprudence, one of which narrowed the concept of cybercrime and defined it as an illegal activity aimed at copying, changing, deleting, or accessing information stored inside a computer or that is transferred through it.(3) *And the French jurist "Parker" defined it through his publication as a deliberate act associated with any aspect using computers, causing the victim to suffer a loss."*(4)

As for the broad approach, he defined cybercrime as "every criminal behavior that takes place with the help of a computer.(5)

" Cybercrime was also defined as "one of the criminal activities that represent an attack on computer programs and data".

The Saudi regulator defined it as "any act committed involving the use of a computer or information network in violation of the provisions of this system."(6)

(3) See "Dr. Naila Adel Mohamed Farid, Economic Computer Crimes, Al-Halabi Human Rights Publications", 2005, p. 28, and for more information see Dr. Khaled Mamdouh Ibrahim, Internet Governance, Dar Al-Fikr University, Alexandria, 2019, p. 357. See also Dr. Jamil Abdul Baqi Al-Saghir - Criminal Law and Modern Technology, Book One, Crimes Used on the Use of Computers, Fourth Edition, 2002, Dar Al-Nahda I Arabic, p. 47.

(4) Casey, E,Dijital Evidence Computer Crime 2005 San DI-ego ACADMIC PRESS, P 5.&" David Bainbridge- Introduction to computer law-third edition-Pit Man publishing2004" p.14.

(5) Dr. Khaled Mamdouh Ibrahim, op. cit., p. 358. See also: "Chriss Reed, Internet Law-CAMPRIDGE UNIVERCITY PRESS". 2004.p 13

(6) - For more information, you can see the Royal Decree on Combating Cybercrime issued No. M/17 dated 8/3/1428, where the last access was on 5/5/1443 AH: "https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/"12.

As for the Egyptian legislator, he did not set a specific definition for it, and only referred to the penalties resulting from electronic crime, such as violating the sanctity of private life, and crimes of defrauding banks and bank cards, etc.

It is noted through these definitions previously mentioned that cybercrime emerged because of the digital revolution and its cross-border activities, which thus violated all the laws that were set by governments for traditional crimes. These crimes are carried out in different ways, whether directly or indirectly, targeting individuals, organizations, and governments. It aims to penetrate sensitive information and espionage, and without the presence of electronic guarding, the matter evolves to eventually reach electronic terrorism. Second, the characteristics of cybercrime: Cybercrimes are characterized by many advantages not found in traditional crimes, for example, that they are cross-border crimes, due to their dependence on the Internet, which is also cross-border.

Thus, the cybercriminal can commit the crime in one country and be a resident of another country, just like infringing on company databases, stealing credit cards, or violating the sanctity of private life and threatening individuals.[7]

One of the characteristics of cybercrime is also the difficulty of proving it and the difficulty of discovering it, as most of these crimes do not leave a trace after their commission[8]*, and it is also very difficult to determine the location of their occurrence due to the wide spatial scope and the large amount of data that you deal with, in addition to the speed of committing the criminal act, where the cybercriminal can in a few moments steal all passwords on the hacked device is not only that, but it can also delete all the important data on the device, all within a few seconds*[9] *.*

cybercrime is one of the new crimes that were not used before, and therefore there is no common concept between countries, whether in defining it or in the penalties resulting from it, and the dispute occurred in defining a unified concept for it, and as a result, there was not enough international cooperation in the field of cybercrime. Although there have recently been many successful projects in this field, for example, the European Convention on Computer Crime.

Third: Pictures of electronic crimes at the present time

- Many crimes that take place electronically have appeared, including crimes that target existing data stored on the computer illegally. This data may be for individuals, companies, or governments, and it is stolen, deleted, or disclosed.

- There have also been crimes in which computers are hacked and their only goal is to destroy all the data stored on the computer, and the goal is mostly to destroy important files for commercial companies, and these files are either administrative files or financial files or planting malware programs that hide all the data on the computer and are known as (Ransom) where the hacker encrypts all the data on the computer and asks for a sum of money in exchange for decryption

- Multiple crimes, including email theft, stealing usernames and passwords, and threatening Individuals and investors and disclosing their trade secrets.

<u>The second part</u>

<u>The concept of the zero-click attacks crime.</u>

Cyberattacks have become alarmingly widespread lately, and they often follow a uniform approach. Which is relying on the failure to update the security system of the victim, whether the

(7)See Dr. Abdel Aal Al-Duraibi, Mr. Muhammad Sadiq Ismail, Cybercrime, National Center for Legal Publications, First Edition, Cairo, 2012, p. 54 .

(8) "Johan Eaton& jermy smithers A Managers Guide to information Technology ,London ,Philip Allan" 1982,p263.

(9) See Dr. Khaled Mamdouh Ibrahim, Internet Governance, op. cit., p. 363, and also Dr. Hisham Mohamed Farid, research presented to the Conference on Law, Computer and the Internet, which was held in the United Arab Emirates, United Arab Emirates University during the period from 1 to 3 May 2000. .

victim is an individual, an organization, a company, or a government agency that does not observe electronic safety and security procedures. By providing the latest anti-virus and anti-spyware programs. The cybercriminal sends an unreliable link or an e-mail that contains files that draw the attention of the victim, such as making the e-mail appear as if it is from one of the managers in the company, or it appears as if it is from giant companies or the multinational ones, or sends him pictures or data, so curiosity pushes him to click on this file. Or the spam link, and as soon as the link is entered or the file is opened, a loophole is opened in the victim's device, and the hacked person's device becomes fully controlled, so he can control literally everything, for example, entering the internal storage and copying all its contents, as well as knowing all the passwords on the device Knowing the passwords for all the bank cards on the device (10).

Not only that, but the hacker can record all of this even in the absence of the hacker on his own device. The malicious program used to open loopholes on the victim's device records everything even if it happens that the hacker is not on his device and the victim logged in at another time. By saving all movements, commands, pictures, and passwords in the form of a record, the hacker can access them again if he happens to be absent at the moment the victim opens his device, and even records all the sounds that occurred, and the calls made by the victim at all times as long as the device is connected to the Internet.

Some may ask, what is the use of anti-virus software that costs a lot of money and why does it not stop such attacks?

To answer this question, we must know that the cybercriminal has intelligence and craftsmanship, because he uses a method called the encryption method. (11)

What is meant by encryption method?

Cybercriminal uses programs such as Biofrost or pison ivy to prepare the hacker file, and combines it with an image, link, or. Then he sends it to the victim, and as soon as the victim opens it, the hacker can immediately open the electronic hole in the victim's device, but if the victim has an anti-virus program such as Kaspersky, he will discover directly that the file sent to him is a malicious file and refuses to open it, so what to do? (12)

The hacker understands very well the way anti-virus software works and how it detects the malicious program or what is known as (patch) the malware file, so he performs a process called

(10) See Dr. Ahmed Khalifa Al-Malt, Information Crimes, Cairo, Dar Al-Fikr Al-Jamia, 2005, p. 539. For more information, see also Dr. Esraa Jibril Rashad Marei, Cybercrime: Objectives, Causes, Methods of Crime and its Treatment, published by the Arab Democratic Center The last accessed was on 23/8/1443. http://democraticac.de/?=35426.

(11) In cybersecurity, encryption means converting data from a readable format to an encrypted format. Encrypted data cannot be read or processed until it is decrypted, and hackers use the same method, but in a reverse way by hiding the spyware in an illegible format that makes virus programs unable to detect it For more information, you can see this website, where the last accessed was on 23/8/1443: Day.

https://me.kaspersky.com/resource-center/definitions/encryption

(12) For more clarification of the idea, you can access this website, where it has approximately twenty free trial versions of the most famous antivirus programs for free, and there are trial versions on each 60 program, anyone can free scan his computer, as do hackers when he displays the encrypted program with which he wants to penetrate the victim to see if it will be discovered or not and keeps repeating the matter until he is completely sure that all antivirus programs will not detect it, so it is done The encryption process is successful and the spyware is ready to be sent to the victim: https://afdal10antivirus.com/best-free-antivirus

.

encryption, which is to change the properties of the malware file that is sent to the victim in what looks like a fraudulent maneuver on the anti-virus program to make it believe that it is a normal file that does not contain any malicious files through merging it to a regular path that does not have any problem. Once the anti-virus program scans the file, it sees it as a normal file that does not have any problem, so the victim is allowed to open it. Once it is opened directly, it is activated by integrating a file with the malicious program inside it, and the loophole is made in the victim's device, which allows the hacker to directly enter the victim's computer or mobile phone.

But the question remains, how does the hacker know that the victim is using an anti-virus program or not? Or how does he ensure that his fraudulent cryptographic maneuver will pass the anti-virus software during a scan and not be detected? To answer this question, we must know very well that not all anti-virus programs are as strong as they can detect the program sent to the victim the same way. Some of them can, and some cannot, so what is the solution then?

The solution, unfortunately, is that all anti-virus programs, without exception, place links on their sites for free scans on devices to encourage people to buy them, especially when some harmful viruses are discovered on users' devices. They show them this and ask them to buy the program if they want to remove harmful viruses and malicious files on the device.

So, what does the hacker do? After the hacker prepares the malicious program that he intends to penetrate the victim, he proceeds to encrypt it in order to deceive the anti-virus , so he displays it on all anti-virus software sites, and if he is discovered by these sites, he repeats again and encrypts it in a different way until he finally reaches the satisfactory result, which is his success in the test after the examination of his file from all anti-virus programs , and it was not discovered at that time, so he sends it to the victim, and he is completely certain that even if the victim has an anti-virus program, the malware program will not be discovered, and the victim will not be alerted to it, so the victim falls easy prey for hackers.

Some may think that this process takes a lot of time, but in fact, the encryption and examination process take only a few minutes, so it never takes long for the victim to fall prey to the hacker.

You can imagine, dear reader, that all these previous and long steps in hacking the victim ,encryption ,and trying to send malicious programs to the victim who may enter the malware files or not until he finally falls prey to the hacker are completely unnecessary and that there is a modern way that shortens all this effort And time, besides it never venture to discover that there is an attempt to penetrate or spy and does not require positive intervention from the victim in any way, so there is no need to send him a deceptive link or a mined file that has been encrypted or any of the methods used by ordinary cybercrime to hack the victim.

This method is known as the zero-click attack, so what is meant by this modern method? And what is the mechanism of its work to clarify the civil liability for it, and who is responsible in the end for the compensation due to the victim resulting from the harm incurred by him because of such a crime that was not usual before? We will explain all this in detail in the coming parts.

<u>Definition the crime of zero click attack.</u>

The crime of a zero-click attack is defined as "an attack that takes place remotely on an electronic device and does not require any action from the users of these electronic devices. This attack is carried out by air (OTA), and it is only sufficient for the user to be within the range of the wireless communication channel [(13)]*."*

(13) We find that there are companies specialized in searching for the vulnerabilities that are used for the zero-click attack, which they are looking for and buying for millions of dollars and selling these vulnerabilities on the black market and getting millions of dollars for them because once anyone gets the vulnerability, he can easily exploit it and enter the victim's system, and in order to bring the image closer to the reader, the vulnerability is in the operating system itself, meaning that the vulnerability is discovered in the Windows 11 operating system (11) WINDOS),

It is clear from the definition that all the procedures used by the hackers until the victim is harmed do not exist in this crime, as the victim is not required to take any action at all, it is only enough that the victim to be within the range of the communication channel, meaning that he uses the wireless network used by the hacker.

How is the zero-click attack crime done?

We must first know that both mobile phones and laptops contain wireless communication channels such as GSM, LTE, Wi-Fi, Bluetooth or NFC) It is enough just to have any of these channels open, which are already used by millions of people on a daily basis so that the hacker can pass data through these channels, taking advantage of the loophole in the operating system that was discovered before, and sends through it a spy program specially designed for that in order to be compatible with this method of hacking, as the program once enters through the loophole.

previously discovered through one of the communication channels by installing itself directly and the victim's device becomes under the full control of the hacker practicing all the malicious means that were mentioned in the regular electronic crime of accessing the files in the device and images, stealing passwords, hacking e-mail, transferring it completely, deleting its content, and even recording all What is going on the victim's device of voice calls or calls via video technology, in other words, the hacker has become in full control of the victim's device[(14)].

Do their documented cases of zero-click attack crime?

Some may think that what was mentioned above is just a fantasy of the researcher, and I do not blame anyone for that. Is it conceivable that a person passes through a commercial market, uses a network of wireless communication networks, or is it sufficient to know the wireless network that he uses in his home or at work, and then finds himself directly a victim of the unethical cybercrime known as the zero-click attack?

In fact, the answer is yes, although the hackers who use this method do not usually use it for easy targets or with the public, but rather they use it for senior public figures such as ministers, heads of giant companies, political opponents, and journalists, but this does not preclude that each of us is subject to a zero-sum attack whenever the hacker decides to do so.

Indeed, there are many cases that have been documented by specialized experts, for example, a few days ago, Apple announced that it had made a security update for all its devices, after a loophole was discovered that was used in a zero-click attack. The Israeli NSO , which uses the spyware program called Pegasus or the Pegasus Monitoring Tool, has been accused of this act ,Pegasus is program developed by the Israeli company (NIO) used in the zero-click attack, where the Israeli company exploited a vulnerability in the Apple system through an application that is used for chatting called (I MESSAGE), which is a program that is installed within the operating system for (Apple) users, so everyone has this application , and so it is directly in the crosshairs of the zero-click attack.

---

which is an operating system for devices Computer This means that anyone who uses Microsoft's operating system can be hacked easily and without any action from him because the vulnerability already exists in the operating device that he and millions of users use and in the application on smart mobile devices You can imagine that the vulnerability is in the Android operating system that millions of people use in our time This means that all smartphones that use the And Red system have this vulnerability and are easily penetrated and from these companies Which looks for these loopholes and sells them on the black market a company called Zerodium.

(14) For more information, you can see this article entitled "Zero Click Attack" The attack published on the following website The last accessed was on 23/8/1443"

https://www.computer-wd.com/2021/10/zero-click-attack.html"

.

Technical researchers at Apple found traces of the zero-click attack on Apple devices, known as FORCEDENTRY, from last February and were not discovered until recently. Therefore, everyone who uses Apple devices, before the security update, was vulnerable to hacking according to the zero click-attack technique from the Israeli company NSO.

Among the documented cases is also what was discovered in the well-known software development company, Citizen Lab (15) *last September, in which the monitoring tool (Pegasus) was used through a zero-click attack on some targets where a PDF file was developed that can install itself automatically.*

Also, the same method was used in 2019 via the WhatsApp application using a zero-click attack, where the spyware was installed on the devices, and it is activated immediately upon contact with them and without any action from the victim.

Is there a way to be protect against zero click attack?

Until now, given the malicious method pursued by hackers based on exploiting vulnerabilities in the operating systems of electronic devices, it is very difficult to be certain of protection from these attacks, but there are several very important tips, including:

- Being careful when buying software, try to buy original software as much as possible, and not using cracked software, as well as be careful when transferring programs and files from people, as they may contain spyware

- Using anti-virus software and updating it permanently, because it is considered a wall against hackers and vandals, even if it is proven to be useless with the zero-click attack, but in light of the updates, it may be able to detect the attack before it gets into the victim's device.

- Do not use unreliable public networks because they are considered one of the easiest ways to hack smart devices through a zero-click attack.

-There is another thing that is more important, which is constantly maintaining the security updates that companies send to their users, such as Apple and Microsoft, because these updates - often - fill discovered gaps that hackers may use in a zero-click attack, so it is necessary to make security updates periodically.

-Also, use programs that change the IP address or that hide your address on the Internet, such as VPN programs that hide your identity over the Internet.

The second chapter

The legal basis for civil liability resulting from the zero click attacks crimes.

Preface

The law obliges liability in general, whether it is a contractual liability or a tort liability, to compensate the harmed party for the damage incurred, but each of the two responsibilities differs in the reason for the emergence of each of them. The contractual liability arises from the breach of a contractual obligation, while the tort liability arises from the breach of a legal duty or a public duty, and given the specificity of the zero-click attack crime, we must first clarify several points so that the picture becomes clear to the reader (16)*:*

(15) One of the laboratories located at the University of Toronto in Canada and specialized in information controls and monitoring issues of spying on companies that affect the security and safety of the Internet and threaten human rights through technical researchers specialized in the field of computer under the leadership of Professor Robert Debert and this institute has won many international awards for its ethical role in the field of the Internet

(16) For more information, see Dr. Farouk Ali Al-Hefnawi, Encyclopedia of Computer Law and Information Systems, Book Two, Part One, Software Contracts, Dar Al-Kitab Al-Hadith, 2009, p. 980.

First: We previously mentioned the hacker's mechanism of action considering the zero-click attack and explained that he opens a loophole in the victim's operating system and then sends the malicious spyware to the victim's personal computer or smartphone.

Second: What is meant by the operating system here is the program that was installed on the device, whether it is a personal computer, an example of this is the copy of Windows that is purchased from Microsoft which includes important programs that enable the computer to perform its functions, It is known as the Windows operating system that is installed on the computer whether it`s personal or office.

Or the program that was placed on the smart devices to operate them, for example, the smart phone operating system in Apple (APPLE) which is called iOS [17]*where the company's devices work with it, such as the iPhone, iPad and iPod or the operating system for phones running Android (Android)* [18] *that other companies use it on their mobile phones such as Samsung and Xiaomi.*

Third: Among the forms of infringement on operating systems is the exploitation of weaknesses in them opening loopholes that allow hackers to access and install their malicious malware programs, also enter data that did not exist before, or destroy the data contained in these programs and files. And with the development of modern technology, hackers' methods have also evolved in this matter.

The first requirement:

contractual liability for zero-click attacks damage.

The contractual liability is based on the breach of one of the parties to his commitment arising from a contract between both the creditor and the debtor. For the contractual liability to be valid, a set of conditions must be met, namely:

- That the contract concluded between the two parties be a valid contract that fulfills all the terms and conditions, and that both parties abide by it, and it is also required that the contract be between the one responsible for the damage and the harmed party. itself." [19]

-And if one of the parties to the contract breaches his commitment in the contract [20]*.*

- Based on the aforementioned, if the harmed party has contracted with one of the companies that owns the operating systems for the personal computer, such as Microsoft, which sells the Windows system, or the person bought a mobile phone on which one of the operating systems was installed, which Apple sells with its mobile phones known as the IOS system, or The company (Samsung) that

(17) The system (IOS) is an operating system where it was initially known as (iPhone OS) and this was the previous name of the system and this system appeared in 2007 as an operating system made by Apple for its iPhone phone. For more information, you can see this website, where the last accessed on: 24/8/1443

"https://mawdoo3.com/%D9%85%D8%A7_%D9%87%D9%88_%D9%86%D8%B8%D8%A7%D9%85_IOS"

(18) It is an operating system for mobile devices based on a modified version of the nucleus of the famous Linux operating system, and some open source programs; they are programs whose developer allows any other developer or technical community to modify the writing of its code or add new lines of code to it, as long as several predetermined conditions are adhered to, such as not using the system for criminal purposes or exposing any individual to danger. For more information, you can access this website, where the last access was on 24/8/1443. https://www.alrab7on.com

(19) See Dr. Anwar Sultan, Sources of Commitment in the Jordanian Civil Code: A Comparative Study of Islamic Jurisprudence", Dar Al-Thaqafa for Publishing and Distribution, 2007, p. 286..

(20) See Dr. Salal Hussein Ali Al-Jubouri, Compensation for Moral Damage in Civil Liability, A Comparative Study, Dar Al-Fikr Al-Jamia, 2014, p. 43..

sells with its mobile devices the Android operating system. each of these companies is obligated periodically, in accordance with the conditions of service and the terms of the contract between it and the users, to send security updates to fill the loopholes that are discovered to protect both personal computers and mobile phones from hacking, then the contractual liability is active if One of the parties breached his obligation.

-If damage occurs based on these systems to the person affected by loopholes in these systems, then manufacturer of these systems has breached the terms of the contract between them and the users, and therefore it is responsible for compensating them for the harm incurred by them.

First section

conditions of contractual liability First,

first: the contractual error:

The contractual error contents the failure of one of the parties to the contract to fulfill its commitment stated in the contract.

As the French law stipulates that the debtor's non-fulfillment or delay in fulfilling his commitment is a contractual error, regardless of the reason that led to the non-fulfillment." (21)

The Egyptian law dealt with it, as it stipulated that: "If it is impossible for the debtor to implement the obligation, he shall be ordered to pay compensation for failure to fulfill his commitment, unless it is proven that the impossibility of implementation arose from a foreign reason that he had no control over."(22)

The Saudi regulator did not define the contractual error, but according to the legal rulings in effect within the "Kingdom of Saudi Arabia, the Saudi judiciary relied in its rulings on the provisions of Islamic law in the principle of adherence to contracts and non-violation of their terms by both parties, relying on his saying ,Allah said , "O you who believe, fulfill (all) contracts." (23) *Therefore, it is obligatory that the parties to the contract must fulfill their obligations in the contract, otherwise, in the event of non-implementation, the one who violated his commitment would be liable for the guarantee. This is what the Saudi Court of Appeal went to in its rulings, as it stated that:*

The contract is the law of the contracting parties and the Muslims on their terms (24) *and in the event of a breach by one of the parties, he is obligated to indemnify the other party. This is also what the Saudi Supreme Judicial Council went to in its ruling issued in 1425 AH in a case in which a person rented a car and committed an accident, the damage to the rented car was estimated at 30,000 Saudi riyals, so it obligated him to pay compensation because the accident was due to his fault* (25)

(21) Article 1147 of the French Civil Code.".

(22) Article No. (215) of the Egyptian Civil Code, which is a fundamental article in both contractual and tort liability, and therefore it was placed in the section dedicated to the effects of the obligation For more information, see Counselor / Mounir Riad Hanna, Civil Responsibility of Doctors and Surgeons in the Light of the Egyptian Judiciary and Jurisprudence, Dar Al-Fikr Al-Jamia, 2014, 113-112.

(23) The Holy Quran, Surat Al-Ma'idah - any number 1.

(24) Judgment of the Saudi Court of Appeal issued on 4/11/1434 AH, No. (34349104), in the lawsuit issued on 22/8/1434 AH, No. (33683430), and deed No. (34302116), Collection of Judicial Judgments of 1434 AH, Volume VII, p. 153.

(25) Judgment of the Saudi Supreme Judicial Council issued on 23/10/1425 AH, No. (33/151), Code of Judicial Judgments, First Edition, Issued by the General Directorate for Codifying and Publishing Judgments at the Ministry of Justice, 1428 AH - 2007 AD, p. 106..

It was also dealt with in Kuwait Document [26]*, where it stipulated that "the rights stated by the contract are also established immediately after its conclusion, and each of the parties must implement what the contract required of it." Also, in the same document it stipulates that: The contract must be executed in accordance with what it includes and, in a manner, consistent with what is required by good intention*[27] *.*

One of the forms of contractual error, and based on what was previously mentioned about the hackers' work mechanism according to the zero-click attack, is that the companies that produce and manufacture operating systems should, in accordance with the terms of the contract between them and the customer, deliver these programs to him free of defects, capable of doing their work perfectly, and that they do not contain viruses Or malicious software or loopholes that give hackers the ability to access these systems, exposing users' privacy to violation, whether by stealing the contents of their devices, deleting their contents, exploiting and extorting them, stealing the contents of e-mail, deleting its components, or stealing their passwords or their bank account. . etc

Second: contractual damage

The contractual liability is based on several pillars, the first of which is the contractual error, and the second is the damage, which is the cornerstone for the establishment of the contractual liability, without which there is no contractual liability, no matter how serious the error. [28]

However, we must note that sometimes the debtor does not fulfill his commitment and at the same time the creditor does not suffer any harm. The lesson here is that the actual harm has occurred, and the burden of proof is on the one who claims that the damage occurred, which in this case is the creditor.

The harm may be physical harm or moral harm. physical harm is what befalls a person in his body or money, and moral harm is what befalls a person in his reputation.

This is what was stated in the Egyptian Civil Code regarding damage, as it stipulated that "every mistake causes harm to others, the person responsible for it is obligated to pay compensation." [29]

It also discusses what is included in the compensation for the damage, and the compensation includes the loss suffered by the creditor and the lost gain[30]

It also provided for compensation for moral damage. Compensation includes moral damage, but in this case, it is not permissible to transfer it to a third party unless it is determined by virtue of an agreement, or the creditor demands it before Judiciary [31]

And the French law spoke about harm, as it stipulated that every act, whatever it was, that occurred from that person and caused harm to others, obliges the one who committed this act through his fault to compensate the harm.[32]

And based on what was mentioned above about the mechanism by which hackers operate according to the zero-click attack, we find that there is great damage to the user or customer who contracted with the company to buy the operating system for his personal device or mobile phone,

(26) Article 237 of the Kuwait Document For more information, see Kuwait Document for the Unified System of the Cooperation Council for the Arab States of the Gulf, Riyadh, General Secretariat, Third Edition, 1432 AH-2011, p. 47.

(27) Article (238) of the Kuwait Document.

(28) For more information, see Dr. Amjad Muhammad Mansour, The General Theory of Obligations (Sources of Commitment, 1st Edition, Dar Al-Thaqafa, Amman, 2009, p. 225).

(29) Article 163 of the Egyptian Civil Code.

(30) Article 221 of the Egyptian Civil Code..

(31) Article 222 of the Egyptian Civil Code..

(32) Article 1382 of the French Civil Code..

thus he found himself a victim as a result of the company's failure to implement its commitment to keep the program free of loopholes exploited by hackers using zero click attacks to carry out their plan.

The damage may be physical if they harm his personal device, which results in deleting its contents, damaging it, restricting the data on it and asking for the ransom (33)*, stealing the passwords on his device that he uses for his bank accounts, or stealing his bank account. All of these are physical damages to the person, also the damage may be moral as it affects the victim`s reputation by violating his privacy and leaking news about him based on what they found on his device and phone and publishing his secrets.*

Third: the causal relationship between the contractual error and the damage

The causal relationship is considered the third pillar in the contractual liability so that the contractual liability does not exist without the causal relationship. There may be a contractual error and their damage happened, but there is no causal relationship between the contractual error and the damage, and therefore there is no contractual liability.

So, for the establishment of contractual liability, the creditor must prove the existence of a contractual error committed by the debtor and that there was damage caused to him as a result. Once the creditor proves the existence of the contractual error and proves the damage, the causal relationship here is assumed, meaning that the original is that there is a relationship between the error and the damage, unless the debtor proves otherwise.

If we apply the matter to the zero-click attack, the debtor, who is the user, must prove that a contractual error occurred, and this comes first by proving that there is a loophole in the operating system that enabled the hacker to

Access the victim`s device according to the zero-click attack, and then proving the damage the victim has suffered due to the presence of such vulnerabilities in the operating system with which his devices operate, whether the personal computer or the smartphone

It should be noted that the issue of proving the causal relationship in the zero-click attack is one of the difficult and complex issues, as the process of accessing and the implementing of all the malicious tasks of the hacker may be completed without the user even realizing that he is under the influence of the zero-click attack due to the dangerous mechanism by which it operates, and as soon as The hacker of has finished of his crime, he can delete the spyware and the file that enabled him to access the victim`s device without leaving any trace of his crime.

Second section

The legal basis of contractual liability for damages arising from a zero-click attack.

First, we must know that the electronic programs that customers use and put on their devices, whether personal computers or mobile phones, are the subject of a contract between the two parties to the contractual relationship. The first party may be the producer or distributor of these programs, or he may be a seller for them, and the second party corresponding to him in the contractual relationship is the customer, and this results in obligating both parties to corresponding obligations, as the first party (producer, distributor, seller) is committed to delivering a quality product that is not defective, and the second party (the customer) is obligated to pay the price of the product on the date agreed upon in the electronic contract.

If the user purchases these electronic programs from the producing company or distributors approved by the company or its sellers, and then discovers that this product is defective, contains gaps, or was hacked due to loopholes in this product of the company, then the contractual responsibility arises and he has the right to return to the company or any A person affiliated with

(33) The ransomware virus is one of the worst malicious programs ever and is known as Ransomware, where if it infects the user's device, it encrypts all the files in it and prevents the user from accessing them except after paying a physical ransom, and when it infects the device, the ransom request message appears and how to pay it until the hacker decrypts the device and enables the user to restore his important files again

it (such as the producer, distributor, supplier, seller) who have sold this defective program to him based on his breach of the obligations stipulated in the contract. Accordingly, the responsibility rests with the seller of the electronic operating system or program in several aspects, including:

First: Electronic drivers and hidden defects guarantee:

Among the obligations imposed by the sale contract on the seller: That the sold object be free of Defects so that the buyer makes the best use of the sold object that enables him to obtain all its advantages, but if there is something that prevents this by the presence of a defect in the sold object that prevents the buyer from using the sold object, detracts from its value, or causes damages, This is considered a warranty-positive defect, and it is also considered a hidden defect that if the buyer had known about it before purchasing, he would not have purchased this product. The Civil Code has dealt with this problem and established legal provisions for it, including:

The French law which stipulates that the seller is obligated to hand in the buyer a product identical to the product sold, in accordance with the stipulated conditions. At the agreed time and place." (34)

And also what the Egyptian Civil Law went to, as it stipulated that "the seller is obligated to guarantee if the object sold at the time of delivery does not have the qualities that the buyer guaranteed its presence in it, or if the object sold has a defect that reduces its value or benefit according to the intended purpose, drawing on what is indicated in the contract." or what is apparent from the nature of the object, or the purpose for which it was prepared, and the seller warrants this defect if he was not aware of its existence. There are several conditions that must be met for the defect, including that it is hidden and not known to the buyer. Also, the defect is old and influential.(35)

Undoubtedly, if the electronic operating program has loopholes that allow hackers access the user`s devices causing damage to the user's devices, it is considered a hidden defect that is difficult for the user to detect, and this defect is not a spur of the moment, but rather it is old and influential, because it exposed the user to fall as a victim of an zero click attack by hackers, and thus the company is obligated to compensate the user for what he suffered from the damages, and if all these conditions are met, the buyer has the right to return the object sold or to demand a reduction in the price with compensation for the damage incurred if the conditions of contractual liability are met.

Second: Electronic driver programs and the principle of pure intention in contracts:

The general principle in all contracts, whether ordinary or electronic, is that they are based on the principle of good faith, and therefore each party to the contract must implement its obligations according to the principle of good faith, and then the provider of electronic operating programs must be honest with the user who purchased the programs to use and obtain Despite its advantages, it must be free of loopholes that hackers may exploit in carrying out their zero-click attacks on users, causing them many damages. If the aggrieved party proves that the software-producing company dealt in bad faith, then he has the right to claim compensation and so there is contractual liability.

Third, electronic driver programs and "consumer protection" laws:

It is possible to establish contractual liability based on consumer protection laws "organized by many countries, for example the French, Egyptian and Saudi legislators." The French Consumer Protection Law stipulates that "every professional seller of goods or provider of services must, before concluding the contract, enable the consumer to know the basic characteristics of the good or service." (36)

(34)Article 1604 of the French Civil Code: .

(35)The text of Article (447) of the "Egyptian Civil Code".

(36) Article 111-1 of the French Consumer Protection Act of July 26, 1993.

The French Consumer Protection Law issued in 1993 also provided for provisions combating fraud and deception by the producer to make the consumer fall into error or make the consumer vulnerable to fraud."(37)

This is what the Egyptian Consumer Protection Law went to, urging it to stipulate that "the producer shall be liable for any damage caused or caused by the producer if it is proven that the damage is due to the supplier's failure to take sufficient care to prevent the occurrence of damage, or to warn of the possibility of its occurrence."(38)

The Saudi regulator also went to protect the consumer if he was deceived by the producer according to "Cabinet Resolution No. (119) dated 4/22/1429 H (39)

And if we look closely at the previous legal texts, we will find that most of the legislations of the countries of the world have issued laws that protect the user if he is exposed to damage from a defective product, and he may claim compensation for the product. That a security vulnerability has been exploited in the program, this means that the program is defective, and therefore, according to consumer protection laws, he can refer to the company producing the program for compensation.

Second requirement

In tort liability for zero-click attack damages

We mentioned above that the contractual liability is based on a breach of a contractual obligation, so the contractual liability is established if one of the parties to the obligation breaches his obligation in the contract, but sometimes there may not be a contract linking the aggrieved party to the wrongdoer of the harmful act, and then how will the aggrieved party be compensated?

For this reason, the law created another type of liability known as tortious liability, which is intended for a person to violate a duty imposed by law or a public duty, and because of this breach, damage is caused to others that requires compensation for the damage he suffered.

It was also defined as the obligation of the debtor to compensate the damage that resulted from a breach of an obligation that falls on him. The source of this obligation is the law, as it is independent in determining it and how to compensate for it(40) .

The general principle is that every person freely practices his life guaranteed by the law without harming others. If this person commits a mistake and this mistake results in harming someone, then he is obligated to compensate him for the mistake he committed against him, and this is the

(37) See the text of Articles 121 et seq. of the French Consumer Protection Act of July 26, 1993.

(38) Article 27 of the new Egyptian Consumer Protection Law No. 181 of 2018

(39) The following shall be deemed to be in violation of the provisions of this Law: 1. Deceives, or attempts to deceive, in any way in one of the following matters:

(a) The subjectivity, nature, sex, type, elements, or essential characteristics of the product; B - The source of the product.

c. The amount of the product, whether in weight, measure, size, number, energy or caliber -2 Cheated - or proceeded - to cheat the product

3. Sells or displays an adulterated product

4. Possesses a counterfeit product with the intention of trading

5. Manufacture, produce, acquire, sell or display products contrary to approved standard specifications

.

(40) Dr.| Essam Ahmed Al-Bahiji, Guaranteeing the Right to the Sanctity of Private Life in the Light of Civil Responsibility and Human Rights, New University House, Egypt, 2005, p. 43

basis of tort liability, and there are several legislations that talk about tort liability, including For example:

What the French Civil Code stipulates is that "every act that causes harm to a third party obliges the person through whose fault the damage occurred to compensate him." (41)

This is also covered by the Egyptian Civil Code, as it stipulates that every mistake that causes harm to others requires the person who committed it to pay compensation."(42)

This is what was decided by the Kuwait Document, in which it was stated that every harm to a third party obligates its wrongdoer, even if he is not discerning, to be liable for the damage (43). *The same document stipulates that the damage is direct or caused, and if it is direct, it is necessary to guarantee and there is no condition for it and if it is caused, then it is required that the act was infringement or intentional, or that the act led to "harm."*(44)

Based on what has been mentioned, if a person commits a mistake and this mistake results in harm to others, then the perpetrator of the mistake is obligated to compensate, but in light of the development that we are witnessing now and the technological progress and the emergence of the Internet, new types of errors have appeared that can be committed not in reality, but rather through the Internet. These actions are illegal and cause harm to others. Are the general rules of liability capable of dealing with this new type of breach of legal obligations that cause harm to others via the Internet?

With this development that we are witnessing, what is known as electronic tort liability has appeared, which depends mainly on the general rules in tort liability and is also based on its elements of error, damage, and causal relationship, but there is a difference between it and traditional tort liability as the electronic tort liability is wrong Assumed (45)

The first section

Elements of tort liability

If we reflect on the reality of the matter, we will find that tort liability is based on a personal act that causes harm to others, although the general duty and the law both call for not causing harm to others(46) *. Thus, three pillars are necessary for the establishment of tort liability: first: the error, second: the damage, and third: the causal relationship between the error and the damage, and we will discuss each of them in detail.*

The first pillar: error

Error is considered one of the most important elements of tort liability, and although most legislations did not address its definition, many jurists defined it, and all jurists' definitions revolved around "being a breach of a legal duty protected by law or legislative texts" (47)

This is what the Egyptian Civil Code referred to, as it stipulated in its article 163 that "every mistake that causes harm to others is obliged to pay compensation." (48)

(41) Article 1382 of the French Civil Code"

(42) Article 163 of the Egyptian Civil Code..

(43)Article 261 of the Kuwait Document .

(44) Article 262.127.

(45) See Dr. Khaled Mustafa Fahmy, The Civil Responsibility of the Journalist, Dar Wael: Amman, 2007, p

(46) We will suffice to study the personal act in tort because it is more general and comprehensive and is considered the general origin of liability as tort liability is fully based on a wrongful act issued and caused damage to others.

(47) Dr. Abdelkader Al-Arari, "The General Theory of Obligations in the Moroccan Civil Code", Sources of Obligation, Book Two: Responsibility for the Injurious Act, 1988, p. 11.

Thus, we find that the Egyptian legislator established the error and made it a basis for tortious liability, in contrast to what some other legislations went to, where they made the act of damage a basis for tortious liability, such as the Jordanian legislator and the Emirati legislator The Supreme Court in Amman also agreed with this, as it began to move away from the idea of error as a basis for tort liability and issued its decision "that error is not a basis for the responsibility of the custodian of things, which Do not assume wrongdoing in a harmful act." (49) We find that this is considered one of the provisions of Islamic law, which does not Presume fault in the harmful act.

And if we look at the level of the Gulf Cooperation Council, we will find that the Kuwait Document in its Article 261 stipulates the following: "Every harm to a third party requires the perpetrator, even if he is not discerning, to guarantee the damage."(50)

However, the question that arises is whether the error or the act of damage and its definition according to the traditional rules is sufficient to determine the responsibility according to the electronic transactions, which contain many risks?

In fact, many jurists have developed a separate definition of an electronic error or an error that causes damage due to the use of the Internet, as it has been defined as "the harmful act committed via the Internet"(51)

It was also defined as "every use of Internet devices in a way that causes harm to others while the perpetrator is aware of that."(52)

Based on the previous definitions, we will find that the electronic tort caused by the zero-click attack is based on distinct elements, the first of which is: the infringement element, which is the physical element in the electronic error, and the electronic hacker has crossed the limits, deliberately deviated, and transgressed against others in several ways.

Among these methods, for example, is the violation of the victim's privacy and unauthorized access to third-party devices, whether it is a personal computer or a mobile phone.

Also, manipulating the information on the hacked person's device according to the zero-click attack, and all of this is done by the hacker exploiting a loophole in the operating system of the victim's device without his knowledge. To copy all available data on the device and know all the passwords used by the victim, whether for social media accounts such as Facebook, Twitter, Telegram, and personal email. (53)

---

(48) Article 163 of the Egyptian Civil Code.

(49) Decision No. 30 Appeal No. 483/2008, First Civil Chamber, Saturday 12/4/2008, Publications - Technical Office of the Omani Supreme Court.

(50) Article 261 of Kuwait's Common System Document for the GCC States.

(51) Dr. Samir Hosni Al-Masry, Tort Liability arising from the use of the Internet", A Comparative Study of Anglo-American Law, PhD Thesis, Faculty of Law, Ain Shams University, Egypt, 2016, p. 32 .

(52) Dr. Fares Boubacar, Civil Responsibility in the Field of Electronic Transactions, PhD Thesis, Faculty of Law and Political Science, University of Hajj Lakhdar Batna 1, Algeria, 2021, p. 19.

(53) Dr. Mohamed Rashad Al-Qatani, Criminal Protection of the Right to the Sanctity of Personal Communications, Second Edition Al-Fath for Printing and Publishing, Alexandria, 2015, p. 103 According to one of the rulings issued by a court in the United States of America, in order for e-mail correspondence to be characterized by privacy, two basic elements are required: 1- An objective element related to the content of the message, and his unwillingness to disclose it by another person. Referred to the judgment Dr. Omar Muhammad Yunus in writing the most famous principles related to the Internet in the American judiciary, Dar Al-Nahda Al-Arabiya, Cairo, 2014, p. 580.

Not only that, but he can also know all the data of the bank and bank accounts, as well as record a voice and image of the victim and use these recordings to blackmail him later, and the most dangerous thing is that he can hack all the existing users who deal with the victim and exploit the victim as a Trojan horse and exploit their trust in receiving The messages are from the victim, so the hacker can impersonate the victim and send the malicious encrypted program to them, and through it he can open a loophole in their devices, so everyone falls into an easy victim for the hacker within moments.

The second pillar: damage

Damage is considered one of the important pillars for the establishment of tort liability, so liability does not exist without it, but the important question remains: Does the damage differ according to the traditional tort liability from the damage in the electronic tort liability? There is no doubt that damage is a very important element in the traditional tort liability, so there is no compensation without its existence, and this is what the Kuwait document approved that "every damage to others.

Every damage to a third party is obligated by an actor, even if he is not distinguished, to guarantee the damage" (54) *as it stipulates that "the owner may not use his property in a way that causes harm to others."* (55) *Thus, its utmost importance is also evident to us in transactions that take place electronically, due to the huge physical and moral losses that may be possible to infect a person from using the Internet.*

Before we delve deeper into electronic damage, we must first touch briefly on the definition of damage according to traditional tort liability, as some have defined it as "the harm that befalls a person as a result of a violation of one of his rights or a legitimate interest that he has, whether the right or that interest is related to the safety of his body, his passion, or money, freedom, honor, or otherwise."(56) *Some also defined it as "the harm that befalls a person in respect of one of his rights or in a legitimate interest, whether that right or that interest has a financial value or not.* (57)

According to the previous definitions, we find that the damage that befalls a person in his financial responsibility is known as physical damage and affects the person because of the illegal act committed against him, whether in the form of a physical assault that threatens human health and safety, as well as every violation of one of the rights related to a person, such as his personal freedom, freedom of work and freedom of opinion if it results in a loss such as his imprisonment or travel ban. As for the moral harm, it is what afflicts a person in feeling and honor, and whether the person commits physical or moral harm, the wrongdoer of the harmful act is obligated to compensate them for the damage they suffered.

As for the damage caused by electronic means, it can be defined as "the damage caused by dealing with modern computers through the use of the Internet ". (58)

Through this definition, we find that electronic damage may cause damage, whether materially or morally, and several conditions must be met, including that the damage is certain to occur, and

(54) Article (256) of the Kuwait Document for the Unified System of the Gulf Cooperation Council.

(55)Article No. (953) of the Kuwait Document for the Unified System of the Gulf Cooperation Council .

(56) See Dr. Yousef Muhammad Obeidat, Sources of Commitment in the Civil Code, First Edition, Dar Al-Masirah for Publishing, Distribution and Printing, Jordan, 2009, p. 219.

(57) Ramadan Abu Al-Saud, Provisions of Commitment, University Press, Egypt, 1998, p. 240.

(58) See Dr. Nael Ali Al-Masa'a, The Pillars of Electronic Harmful Acts in Jordanian Law, Journal of Sharia and Law Studies, University of Jordan, Volume 32, Issue 1, 2005, p. 55.

the electronic damage must also be a direct "damage" that affects the person in a right or legitimate interest. (59)

The electronic damage caused by the zero-click attack has several forms, including: violating the privacy of the person or the company, leaking their data and personal accounts, tampering with the content of the personal email, recording a sound and image of everything that goes around the victim's personal computer and exploiting everything that is recorded against him to blackmail him later.

And if we analyze the damage resulting from the zero-click attack, we will find that the harm afflicted the victim in a right protected by law, and then he has the right to seek refuge in the judiciary and resort to it to claim compensation because preserving the privacy of the individual is a right that is guaranteed by law, as well as not being subjected to extortion, and all damages, whether they are physical damage or moral damage, and it should be noted that the interest protected by law must be a legitimate interest, If it is illegal in the sense that the owner of the device uses it for immoral acts, or exploits it in acts of sabotage, whether it is his personal device or the website, such as a pornographic site, or if this person exploits his device and website for the benefit of terrorist organizations, then in all of these cases is not covered by legal protection at all.

The third pillar: the causal relationship between error and damage Among the very important elements that represent the third pillar in tort liability: the causal relationship between the error and the damage, as if there is no causal link between the error and the damage, both of them become useless, so if the error is not the cause of the damage, then the tort liability does not exist.

We find that most of the legislations called for the causal relationship through their legal texts, for example what the Egyptian legislator went to, where he stipulated that "every mistake causes harm to others, the one who committed it is obligated to compensate." (60)

Likewise, what the Kuwait document went to, as it stipulated that "every harm to others is obligatory for its wrongdoer, even if he is not discerning, to be liable for the damage" (61).

As for the French law, we find that the causal relationship is present in its texts, as it stipulated in more than one place this matter, as it stated that "every act, whatever it may be, that causes harm to others, requires the one whose fault this harm occurred to compensate it (62). *In another place, it mentioned every person who is responsible For the damage he causes, not only by his action, but also by his negligence and lack of foresight."* (63)

It is noted that the majority of legislations relied on the establishment of liability on the establishment of a causal relationship between the error or the harmful act and the harm caused to the person. But the question that arises in the case of multiple causes is what is the criterion used to determine the causal relationship.

In this case, we find that most of the legislation adopted the theory of the effective cause or the productive cause, and the meaning of this theory is that if there is interference with more than one cause in causing the damage, then we must distinguish between the less powerful accidental causes and the productive causes that are a direct cause of the occurrence of damage.

And if we apply the matter to the zero-click attack, we will find that all the elements of tort liability are available. There is a mistake that was committed, which was the illegal access into

(59) Dr. Ahmed Kamal Sabry, Civil Responsibility for Traffic on Information Networks, PhD Thesis, Faculty of Law, Cairo University, 2010, p. 205.

(60) See Article 163 of the Egyptian Civil Code.

(61) Text of Article 261 of the Kuwait Act.

(62) Article 1382 of the French Civil Code.

(63) Article 1383 of the French Civil Code.

the victim's device without his permission, and a loophole was opened in his device, violating the victim's privacy by installing malicious programs on his device, using it for infamous purposes, including exploiting it and stealing the content of the existing data. And we find that this access was the direct cause of material and moral harm to the victim, and thus we find that the productive or effective cause of the damage was achieved directly because of the zero attack.

Although the rules for tort of error, damage, and causal relationship are easy to adapt legally to traditional crimes, however, if we take a closer look at the zero-click attack crime, contemplating its nature, we will find that the wrongdoer of the error or illegal act represented by the hacker, saboteur, or cracker exploiting the loopholes in the User`s devices are like a ghost literally, as they can enter the victim's device without realizing it, committing all illegal acts, and leaving without anyone knowing, and the victim is surprised after the passage of time that he is threatened with audio recordings of him, or inappropriate video clips that were recorded without his knowledge, or that the content of his device has been leaked. Without knowing exactly who did it or when he did it, so the zero-click attack is considered one of the most serious crimes due to its extremely dangerous impact and the inability to discover the wrongdoer, as the matter is extremely difficult from two aspects, the first of which: that the wrongdoer may be outside the country in which the victim resides, Second: The difficulty of discovering this attack until it is too late due to its accuracy and the use of high techniques in stealth and penetration. However, if the person responsible for this is discovered, then he is obligated to compensate the victim for the physical and moral harm suffered.

Third requirement

The effects of civil liability arising from the zero click attack.

If the elements of liability are available, represented as error, damage, and a causal relationship that results in that the wrongdoer is obligated to compensate the harm suffered by the victim in order to redress this damage, and we will discuss in this requirement about the compensation arising from the zero-click attack, but before this, we will first discuss how Obtain this compensation by judiciary. Whereas, the Civil Code has guaranteed the victim protection from attack, whether from violating his privacy by hacking his personal devices, or attacking his data and accounts using the zero-click attack.

The first section is a lawsuit claiming compensation for the damages of the zero-click attack.

It should be emphasized that the civil law has provided the victim with protection from attack, whether from violating his privacy by hacking his personal devices or attacking his data and accounts using the zero-click attack, by filing a lawsuit before the competent court to obtain compensation for the damage he suffered because of this attack. And we will - first of all - identify the parties to the lawsuit, and then clarify after that the competent court to hear the case.(64)

The parties to the lawsuit

Liability is generally based on compensating the harm suffered by the victim, but contrary to what is usual, the harmed person here is the plaintiff and not the defendant.

The person who sustained damage resulting from the zero-click attack is called the plaintiff, and this particular person is the one who goes to the judiciary to claim compensation for the damage he suffered, as well as bears the burden of proving the damage he suffered, it is normal that he fulfills the general conditions for accepting his claim so that he has a known Legitimate interest from filing the lawsuit and filing it on the specified dates for that and not after the lapse of time as the reference to these general rules where the limitation period is 3 years from the time of knowing who hacked his devices according to the zero attack or 15 years if he did not know who carried out this attack or the damage caused with it.

(64) See Dr. Ayed Reda Al-Khalayleh, Electronic Tort Liability (Liability arising from the use of computers and the Internet: a comparative study), Dar Al-Thaqafa for Publishing, Amman, 2009, p. 212.

The other party, who is the defendant, is the one who carried out this attack on the plaintiff, and he is obligated to compensate the plaintiff for the damages he committed, even if the defendants were more than one person.

But in fact, and in view of what we have already explained of the dangerous nature of the zero-click attack crime and the extent of the professionalism of its wrongdoer, and the mechanism that is used that completely conceals the identity of the hacker so that the victim does not feel at all his presence or his attack, we find that it is very difficult to determine the identity of the defendant (the hacker) and so, It is difficult to prove the incident which make it difficult for the victim to resort to the courts to claim compensation.

The court having jurisdiction over the case.

In order to designate the competent court in the lawsuits filed by the plaintiff to claim compensation for the damage he sustained as a result of the zero-click attack , the path that the plaintiff takes to claim compensation must first be determined, If there is a contractual relationship between the victim and the one who caused the damage, then we are in the process of contractual liability, so if the victim used one of the programs that he purchased from a global company such as Microsoft, and these programs contained loopholes that facilitated the exploitation of the hacker using such loopholes to carry out the hacking process, At that time, the company must adhere to the guarantee, and this is in various ways, because the product was purchased under a contract between the affected person and the company, or through protecting the consumer from defective products, because the program in this The case is considered defective, and then the competent court is the court of the domicile or residence of the defendants.(65)

In the absence of a contractual relationship, the court competent with tort liability in accordance with the provisions of the law - then it is the court of the home of the defendant or the hacker, but as we mentioned above, the place of the zero-click attack crime is the Internet and it is possible that the damaged plaintiff (the victim in a country and the wrongdoer of this attack in Another country, and as we have shown, it is very difficult to determine who committed this crime or harmful act, and because of such crimes, many legal scholars have called for the enactment of unified legal principles that settle such disputes, especially since the Internet is considered a virtual world that has no specific place.

The second section is compensation for the zero clicks attack.

After the elements of liability are available for a mistake committed against the victim by the hacker and it was a direct cause of damage to the victim or the plaintiff, then he goes to court demanding compensation for the damage through the liability claim, demanding compensation for the damage he suffered, and we have already said about the lawsuit and its parties, and we will discuss compensation.

Compensation is defined as correcting the imbalance in the condition of the victim because of the occurrence of the damage by restoring the balance to what it was before the occurrence of the damage. (66) *Among the definitions of compensation is also reparation for the damage that befell the injured person.* (67) *If we apply these definitions to the topic we are talking about, which is the zero-click attack, we will find that compensation here is reparation for the damage resulting from the illegal infringement of the hacker on the victim's devices.*

(65) See Dr. Abbas Al-Aboudi, Explanation of the provisions of the Civil Procedure Law - A Comparative Study, Dar Al-Kutub for Printing and Publishing, University of Mosul, 2000, p. 203

(66) . Cf. Dr. Ibrahim Al-Desouki Abu Al-Lail, Civil Responsibility and Enrichment Without Reason, Dar Al-Kitab and Publishing, Kuwait, without year of publication, p. 212

(67) Dr. Nabil Ibrahim Saad, The General Theory of Obligations, Sources of Commitment, Knowledge Foundation, Alexandria, 2011, p. 436.

Compensation in this case may be monetary compensation, or it may be compensation in kind, or by performing a specific matter, but the best way to compensate is to restore the situation to what it was, and this is what is known as compensation in kind, but the issue of restoring the matter to what it was in the issue of arising damages For a zero-click attack or via the Internet in general is very difficult, and we find that monetary compensation is inevitable until the damage is removed or at least mitigated.

One of the advantages of monetary compensation is its flexibility and validity, whether for physical damage or moral damage, although compensation for moral damage may sometimes be more valuable, especially if the person who was subjected to the zero-click attack has a high social status and enjoys a good reputation, as It gets worse if the hacker publishes things that affect the victim or his reputation, and these things spread widely through the Internet and social networking sites.

We find that many legislations, including the French, Egyptian and Kuwaiti legislators, and the Saudi regulator, have spoken extensively about compensation for damage.

The compensation resulting from the zero-click attack raises many legal problems, especially with regard to the issue of the time in which the damage is assessed, as the damage suffered by the victim at the time of filing the lawsuit can be variable and other damages may appear later, therefore it is difficult to fully determine the time of pronouncement of the judgment, so It is possible for the judge to specify the compensation at the time of issuing the judgment with the right for the aggrieved party , within a certain period, to demand a reconsideration of the compensation estimate.[68]

Also, due to the special nature of the zero-click attack and its recentness in terms of implementation, the method used, and the use of the latest technologies and modern software for hacking, it may be difficult for the judge to get acquainted with its details in a great way, so this does not prevent the judge from seeking help from experts and engineers to benefit from their experience in order to estimate the compensation accurately, however their opinions are certainly not binding to the judge.

CONCLUSION

Through our study of the subject, we have demonstrated to what extent science has advanced in the field of modern technology and how humans can benefit from this technology for their own interests. Despite this progress, which has brought physical and spiritual well-being and comfort to humans, it was not imagined existing one day, but at the same time, it brought many damages that did not previously exist and left damages that require compensation. We spoke about the crime of cyber-attacks, which is one of the most dangerous crimes and the latest in this modern age due to the significant damage it causes to the person, both physically and morally. We explained the mechanism of this crime, how it works, and the extent of the physical and morally harm that affects the person as a result of this attack.

Through the pages of this research, we also dealt with the appropriateness and adequacy of the general rules in liability, both contractual liability and tort liability to address the legal problems raised by the zero-click attack crime, especially in the absence of texts regulating it, and whether the general rules would be sufficient if resorted to - to keep pace with this type of modern crimes.

The subject of the study crystallized in clarifying the nature of this crime and an explanation of how it occurred with an explanation of its privacy from the rest of the electronic crimes, which is

(68) Cf. Dr. Mohamed Hussein Mansour, Electronic Responsibility, New University Publishing House, Egypt, 2003, 345. .

Dr. Mohamed Hussein Mansour, Electronic Responsibility, New University Publishing House, Egypt, 2003, 345.

represented in the fact that it is difficult to detect on the one hand, and on the other hand the unique and dangerous method used by the hacker to access the victim's device without any role for the victim in this matter and the consequences On that of catastrophic damages, then we explained after that the contractual liability resulting from the zero-click attack, then went to the clarification of the tort liability as well, and finally, we explained how the victim can obtain compensation for the damages he suffered as a result of this illegal attack on one of his rights that is guaranteed to him by the law .

Through our study of the research topic, we reached several results, the most important of which are:

1- The zero-click attack is one of the very modern crimes that were not known before and arose due to the high development in the use of modern technology and programs, and it is characterized by its unique way of accessing the victim's devices without any participation from him or even resistance.

2- The legal nature of the violations caused by the zero-click attack crime represents a flagrant violation of one of the personal rights protected by law.

3- The error in the contractual liability resulting from the zero-click attack is based on a breach of one of the parties to his contractual obligations, while the error in the tort liability resulting from the zero-click attack is the result of a breach of a legal duty protected by law.

4- The idea of damage resulting from a zero-pressure attack may be physical damage that affects personal devices or operating systems with a defect by opening loopholes in them, and then it can be physical damage, and it can be moral damage if it causes a violation of a person's privacy and damage to his reputation

5- The general principle regarding the court competent to assess the damages resulting from the zero-pressure attack is the court of the plaintiff and not the court of the defendant.

6- The penalty resulting from the tort liability arising from the zero-click attack takes the form of monetary compensation and not compensation in kind, due to the great difficulty in restoring the situation to what it was in this type of damage.

RECOMMENDATIONS

[1] Urging all legislation to issue special laws to combat zero-click attack crimes and not to rely only on general rules in the provisions of liability, whether contractual or tort, as the general rules are not considered sufficient to cover all aspects of liability.

[2] Be careful when buying software, try to buy original software as much as possible, and not buy counterfeit software, as well as be careful when transferring programs and files from people, as they may contain spyware.

[3] Using anti-virus software and updating it permanently, because it is considered a protective shield from attacks by hackers and vandals, even if it proves useless with the zero-click attack, but with updates, it may be able to detect the attack before it gets into the victim's device.

[4] Do not use unreliable public networks because they are considered one of the easiest ways to penetrate smart devices through zero-click attacks.

[5] Another very important thing is always maintaining the security updates that companies send to their users, such as Apple and Microsoft, because these updates - often - fill discovered gaps that hackers may use in a zero-click attack, so it is necessary to make security updates periodically.

[6] Also, use programs that change your IP address or that hide your address on the Internet, such as VPN programs that hide your identity on the Internet.

Holding training courses to educate people about protecting their information and personal data while using the Internet.

References in Arabic

Legal Books:

[1] Dr. Ibrahim Al-Desouki Abu Al-Lail, Civil Responsibility and Enrichment without Reason, Dar Al-Kitab and Publishing, Kuwait, without a year of publication.

[2] Dr. Ahmed Khalifa Al-Malt, Information Crimes, Cairo, Dar Al-Fikr Al-Jamia, 2005.

[3] Dr. Amjad Muhammad Mansour, The General Theory of Obligations (Sources of Commitment), 1st Edition, Dar Al-Thaqafa, Amman, 2009.

[4] Dr. Anwar Sultan, Sources of Commitment in the Jordanian Civil Law, A Comparative Study of Islamic Jurisprudence, Dar Al Thaqafa for Publishing and Distribution, 2007.

[5] Dr. Jamil Abdul Baqi Al-Saghir - Criminal Law and Modern Technology, Book One Crimes Used on the use of computers, fourth edition, Dar Al-Nahda Al-Arabiya, 2002.

[6] Dr. Khaled Mamdouh Ibrahim, Internet Governance, Dar Al-Fikr Al-Jamia, Alexandria, 2019.

[7] Dr. Khaled Mustafa Fahmy, The Civil Responsibility of the Journalist, Dar Wael for Publishing: Amman, 2007.

[8] Ramadan Abu Al-Saud, Provisions of Commitment, University Press, Egypt, 1998.

[9] Dr. Salal Hussein Ali Al-Jubouri, Compensation for Moral Damage in Civil Liability, A Comparative Study, Dar Al-Fikr Al-Jamia, 2014.

[10] Dr. Ayed Reda Al-Khalayleh, Electronic Tort Liability (Liability arising from the use of computers and the Internet, a comparative study), Dar Al-Thaqafa for Publishing, Amman, 2009.

[11] Dr. Abdelkader Arari, The General Theory of Obligations in the Moroccan Civil Code, Sources of Obligation, Book Two: Responsibility for the Injurious Act, 1988.

[12] Dr. Abbas Al-Aboudi, Explanation of the provisions of the Civil Procedures Law - a comparative study, Dar Al-Kutub for Printing and Publishing, University of Mosul, 2000.

[13] Dr. Abeer Shafiq Rahbani, Cybercrime and its dangers, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2021.

[14] Dr. Essam Ahmed Al-Bahiji, Guaranteeing the Right to the Sanctity of Private Life in the Light of Civil Responsibility and Human Rights, New University House, Egypt, 2005.

[15] Dr. Farouk Ali Al-Hefnawi, Encyclopedia of Computer Law and Information Systems, Book Part One, Software Contracts, Dar Al-Kitab Al-Hadith, 2009.

[16] Dr. Kars Boubacar, Civil Liability in the Field of Electronic Transactions, PhD Thesis, Faculty of Law and Political Science, University of Hajj Lakhdar Batna 1, Algeria, 2021.

[17] Dr. Mohamed Hussein Mansour, Electronic Responsibility, New University Publishing House, Egypt, . 2003

[18] Counselor / Mounir Riad Hanna, Civil Responsibility of Doctors and Surgeons, in the Light of the Egyptian Judiciary and Jurisprudence, Dar Al-Fikr University 2014.

[19] Dr. Nabil Ibrahim Saad, The General Theory of Obligations, Sources of Commitment, Knowledge Foundation, Alexandria, 2011. .

[20] Dr. Nael Ali Al-Masa'a, Elements of Electronic Harmful Acts in Jordanian Law, Journal of Sharia and Law Studies, University of Jordan, Volume 32, Issue 1, 2005.

[21] Dr. Yousef Mohammed Obeidat, Sources of Commitment in Civil Law, First Edition, Dar Al-Masirah for Publishing, Distribution and Printing, Jordan 2009.

<u>Doctoral Theses: -</u>

1- Dr. Ahmed Kamal Sabry, Civil Responsibility for Traffic on Information Networks, PhD Thesis, Faculty of Law, Cairo University, 2010, p. 205.

2- Dr. Mohamed Mohamed El-Desouky El-Shahawy, Criminal Protection of the Sanctity of Private Life, PhD Thesis, Cairo University, without year of publication.

3- Dr. Samir Hosni Al-Masry, tort liability arising from the use of the Internet, a study Compared to Anglo-American Law, PhD Thesis, Faculty of Law, Ain Shams University, Egypt, 2016

<u>References in English</u>

1- David (W) e.commerce strategy technolocies and application. Engalnd 2001

1- David Bainbridge- Introduction to computer law-third edition-Pit Man publishing 1996

2- Casey, E,Dijital Evidence Computer Crime 2005 San DI-ego ACADMIC PRESS,

3- Chriss Reed, Internet Law- CAMPRIDGE UNIVERCITY PRESS. 2004

4- Johan Eaton& jermy smithers A Managers Guide to information Technology ,London ,Philip Allan 1982.

Websites

https://laws.boe.gov.sa/Boelaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

https://www.computer-wd.com/2021/10/zero-click-attack.html

/https://alkhabaralyemeni.net/2021/07/22/137272