DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

Electronic Blackmail in Iraq

Asst. Lect. Mustafa Lutfi abdul jaleel ALdalle
Southern Technical University, Nasiriyah Technical Institute, Iraq

ABSTRACT

The importance of addressing this topic from a scientific and scientific point of view lies in the fact that electronic extortion as a crime is one of the newly developed crimes that are linked to the methods of subterfuge practiced by individuals in society and are affected by the modern technological development in the field of communications, which was in conjunction with the development of human life, as it opened a new window for unknown types of crimes to be carried out. Using modern means, these crimes are hidden from view of the perpetrator, who carries out his crime from one place, targeting a person who may be located in another place, by means that are difficult to discover and not easy to deduce. A person initiates it at will Another person to compel him to commit a particular crime is that threat and intimidation to the victim by publishing pictures or film materials or leaking confidential information about the victim, provided that this is in return for payment of money or exploitation of the victim to carry out illegal acts for the benefit of extortionists such as disclosing confidential information about the business or other illegal business. Victims are usually trolled by e-mail or various social media such as Facebook, Twitter, Instagram, WhatsApp and other social media due to its wide spread and great use by all segments of society. Electronic extortion is increasing in light of the growing number of social media users and the remarkable acceleration in the number of different conversation programs and the human development in the use of these programs, so the legal position of it in Iraq compared to Arab countries has been clarified and how the legislative treatment of it has been done in the absence of explicit legal texts.

Keywords: Electronic Blackmail, Iraq.

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

Introduction :

Electronic extortion is one of the most important risks facing internet users and smart devices who do not have any knowledge about the security of information, as it leads to problems affecting the psychological situation of the person who is blackmailed, especially in our society and because of our customs and traditions. With the rapid technological development reached by the majority of the countries of the Arab and Western world, anyone sitting at home can get what he wants at the touch of a button. We can browse hundreds of news sites, thousands of electronic stores and many other social networking sites that are now used by the young before the big one, and hence the problems of the Internet are increasing due to the exploitation of some electronic gangs. These accounts and the extortion of their owners in order to raise money and children are the large target group of these gangs.

The importance of this research:

Is highlighted in terms of scientific and practical aspects and the scientific importance is that the crime of electronic extortion through social media sites is a serious crime developed that is directly related to the lives of individuals in society and therefore this research is a scientific addition in terms of discussing the shortcomings of Iraqi legislation and this type of crime developed from an ongoing development that has emerged with the emergence of modern technological developments in the field of communications and on the other hand comes the practical importance of this research in the statement of methods and extortion methods that These crimes are among the most widespread in Arab societies in general and Iraqi societies in their own form as a result of the ease of communication between all races where this crime is committed and represents an attack on the sanctity of the private lives of individuals in order for the perpetrators to obtain personal information of interest to individuals and their relatives through social media and then blackmail them into disseminating this information in order to obtain material and moral benefits for the perpetrators. (Al-Saghir, 1992, p. 4)

The concept of electronic extortion

Among the cybercrimes whose danger has recently worsened is the crime of extortion to which a person is subjected by a person or a certain group if there are many forms of extortion and its forms, including what is the extortion of women by men or vice versa, but the perpetrator of this crime is characterized by being unknown in terms of actual existence, which would pose a major challenge to the criminal and judicial authorities. The definitions differed and their collection was one basic line: the use of technology and virtual sites as a crime scene (Hasser, 2015, p. 8)

As well as the perpetrator with skills and characteristics distinct from the traditional criminal, and it was very important to blame the causes and motives of extortion that have negative effects on society and deterrence this crime was necessary to identify the ways in which it is committed and the means used to commit it. There is no doubt that the recent development in technology resulted in illegal practices and the opening

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

of doors to new ideas in the commission of crimes, electronic blackmail is a picture of information crime that has its features clear in light of the spread of social media sites and technical countries in all walks of life.

Electronic extortion is a traditional crime in its methods, which can be committed by the blackmailer through the information system in general, with the aim of getting another person to do an act or refrain from it, whether it is legitimate or illegal by entering multiple images into the computer by a person, website or email using various means of information technologies, including mobile phones equipped with a camera. Extortion is the practice of blackmailing the victim using a method of pressure and coercion with the aim of infringing on his private life and compromising it by defaming him of information such as personal photographs or family statements. (Al-Rasheed, p. 194)

The first requirement "The concept of electronic blackmail in Iraq"

Among the electronic crimes whose danger has recently worsened is the electronic extortion of a person by another person or a certain category, as there are many forms of extortion and a picture, including the extortion of some people who hack into the computers belonging to other people (hacker), and may be in the form of blackmailing some employees to the reviewers to force them to pay money in exchange for facilitating their transactions and many more, Electronic extortion has become a globally classified crime crime and may be punished by the maximum penalty in international law for up to 20 years, according to the legislator of each country, and the victims of electronic extortion in the world have 150 million cases of extortion of women. (Shadid, p. 44) The crime of electronic extortion is one of the forms of electronic crime has become a phenomenon that violates the body of society and infects it with weakness and disorder and women often fall victim to such crimes as a result of its association with an emotional relationship with Rajab it is clear that he uses it to obtain documents, documents and pictures of the victim to threaten her and blackmail her by asking for cash or doing illegal acts, and the victim is forced to comply with the desire of the perpetrator to prevent defamation and expose them in front of her parents, relatives and husband if she is married, especially the nature of Arab societies The victim carries out the threats of the criminal to get what threatens her and if she has enough money, she may have to commit suicide, as happened in some cases presented, but the Iraqi judiciary is no less heinous or dangerous than murders and kidnappings. (Aladdin Zaki Morsi, 2013, p. 146) Cybercrime begins when you commit these crimes individually or collectively through organized networks working in the areas of spreading rumors, spreading deviant ideas, spreading incorrect news that spreads very quickly, spying, money laundering and terrorism.

The crime of cyber-extortion begins when it is committed individually or collectively through organized networks working in the fields of spreading rumors, spreading deviant ideas or spreading incorrect news spreading very quickly, espionage, money laundering and terrorism, and the criminal who commits these crimes usually enjoys

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

high skill using computers and new technologies, where it is difficult to control the inputs of the Internet, which hinders the speed of discovering this crime or identifying its source.

The perpetrator may use a pseudonym to hide, which makes many of these crimes restricted against an unknown person. It may be difficult to reach conclusive evidence of the criminal because he uses many technical protections such as password, coding or encryption to hinder the necessary security attempts to access, access or copy these sites (Khalil Yusuf Jundi, 2021, p. 65)

The reason for the recent spread of this phenomenon is the development of electronic media, its abundance and ease of entry, exit and to it, as well as the weakness of the moral reasons among some, which leads them to perform immoral practices under many motives and names, the most important reasons for extortion are due to the woman herself without her failure to give the blackmailer pictures, videos, etc. when the man could find what he blackmailed her with, She responded to it from the beginning. (Abdullah, Blackmail of girls, its rulings and punishment in Islamic jurisprudence, n.d., p. 9)

In addition, the lack of family control for girls, as most of those who fall victim to extortion of young ages, the family has a major role in building the culture and morals of its children and its negligence in controlling them leads to their moral and intellectual deviation, in addition to this lack of experience and dealing with electronic means and ignorance of its pros and cons, and this is what is exploited by the blackmailer in carrying out his actions, he is often experienced and knowledgeable with computer and Internet technologies, In addition to the weakness of the law in addressing this phenomenon and the lack of legislation regulating such crimes and imposing deterrent penalties for criminals, as well as the rise in unemployment in societies led some to blackmail girls in order to get money from them, as well as the difficulty of tracking these crimes, the blackmailer may enter under an imaginary name or page and leave no indication of his personality so that tracking him becomes difficult for the security men, Especially since he has the skill, knowledge, intelligence and ability to contact people, he is social in nature (Al-Ajami, 2014, p. 33)

The lack of experience of security personnel in computer and Internet subjects is due to the fact that dealing with these crimes is not traditional but modern, which has made some countries unable to deal with these crimes. (al-Baghdadi", n.d.)

This requires subjecting them to continuous courses to raise their eligibility in this aspect and for these reasons the electronic extortion of women has spread and affected the reputation of many women at the hands of the weak souls, which often led to the killing of the victim and the destruction of her family life and destroyed her future and these crimes contributed to the spread of mental illness, chaos, fear and disorder due to the fear of using electronic media and this crime is one of the crimes that the jurists did not address in the past, especially with the weakness of the existence of electronic means in the past (Ba'ayoi, n.d.)

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

"The definition of electronic extortion is a language and a term" The crime of electronic extortion is a modern crime that arose with the introduction of technology to the whole family, through their use of smart devices, and for the purpose of outlining what this crime is, we know it as follows: "Extortion": - is to threaten to disclose certain information about a person, or to do something to destroy the person threatened, if the person threatened does not respond to certain requests, and this information is usually embarrassing or of a socially destructive nature as he was known as the many illegal demands to reach the target that was drawn for him and this goal is often destructive to social life and may be used in any dirty game to inflict the victim without fear of God or religious scruples that make him hold himself accountable before falling In error, he also knew the way of coercion from a person, persons, or even institutions, and that coercion would be by threatening to expose a secre (Aleid, 2021)

Electronic extortion is one of the electronic crimes known by some as (violations committed against individuals, or groups of individuals motivated by crime, with the intention of harming the victim's reputation or physical or mental harm to the victim directly or indirectly using communication networks such as the Internet, chat rooms, e-mail and mobile) (Badayna, 2014) It is also known for exploiting other methods for financial or sensual purposes by keeping electronic recordings to threaten them and the images are an important means in the hands of blackmailers, after which the voice and blackmailer do not stop there, but may photograph situations and situations that may be shameful and therefore the threat increases and the situation worsens if he still asks for money (Hamid Salih Ibn Abdullah Ibn Muhammad, 1432)

If we may provide a definition of electronic extortion, we believe that it is (the blackmailer's exploitation of his electronic skills or his social proximity to the victim for the purpose of stealing the secret information of that victim as well as her personal photographs and documents of any kind, and forcing her to pay money or comply with his requests contrary to sharia and law) Electronic extortion is known as "threat": one or more people try to set up another person by posting pictures, conversations, video footage, documents, documents, etc. of that victim, which are often disclosed to that information or images on the Internet, social networks and chat rooms in particular without realizing the intentions of the blackmailer (Radi, 2022, p. 73) Cybercrime according to the expanded concept that accommodates sufficient criminal acts is all forms of illegal conduct committed using a computer or is any criminal activity in which the computer system plays a role to complete, with this role of importance As for the electronic threat (extortion): it is a term consisting of two words (extortion) meaning obtaining money or benefits from a person under threat of exposing his secrets or otherwise, and the second word (electronic) i.e. the act of threatening the use of means and electronic media does not mean that extortion occurs by other means such as telephone communications, letters, paper telegrams or faxes and other means (Ghanem, 2019, p. 5)

"Methods of electronic extortion" Extortion methods vary depending on the general situation of both the blackmailer and the victim, and by tracking cases of electronic

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

extortion through the websites of the security agencies specialized in combating this type of crime we found several ways followed by the blackmailers to reach their sordid purpose and these methods are: First: - The strong friendship between girls through social media sites, where through these sites the girl talks to her friend about all her personal secrets, and sends her pictures and videos of her, such as taking opinion in some models of clothing, or hairstyles etc., making her an easy prey in the hand of the blackmailer where the latter has a fatty material for extortion after a long period of time. Second: - Many cases of electronic extortion occur in case a young man hides the personality of a girl through social media, and then the relationship between the blackmailer and the victim develops to communicate together through emo, Skype and Instagram applications, so that the perpetrator records and saves some pictures and videos that are sent by the victim and then begins blackmailing and threatening to publish these pictures and videos through networks and send them to relatives and friends and often the victim in such cases is a public figure who has public opinion A major impact on her working and social life. (Ibrahim, 2022)

Third: - One of the methods of electronic blackmail is what happens from luring some girls by university students and seducing them by marrying blackmailers and photographing them in some intimate moments, and then exploiting these pictures and videos to hunt them down if they do not comply with their orders and requests. Fourth: - One of the new methods of electronic extortion, what is happening from the exploitation of some plaintiffs (e-extortion fighters) where the blackmailer communicates with the victims and lures them through the establishment of a website under the title (fight against extortion) and asks the victims their data and photographs to then blackmail them and threaten them for money, and this was confirmed by the Court of Investigation of Al-Karkh through the website of the judiciary by certifying confessions to fight electronic extortion, After blackmailing and threatening girls on social media, all measures were taken against him in accordance with article 456 of the Iraqi Penal Code. (Ibrahim, 2022)

Also, one of the methods of electronic extortion targeted at the category of children and adolescents and their sexual exploitation and documentation of video clips of them and threatening them if they do not comply with their orders and requests and start blackmailing and threatening to publish these pictures and videos via networks and send them to relatives and friends (Hussein Abdul Karim Younis, 2021, p. 55)

And the victim's understanding to go to the competent authorities is the right decision and that is part of solving the problem, in these cases the distinction between men and women is not made in dealing with cases to consider this regardless of the sex of the victim, so things are analyzed and the victim is directed in the same way and not to request contents and pictures from the victim unless the party is competent in solving these cases, The circulation of content may cause it to leak and spread without paying attention to the victim's psyche, and cutting off communication with the means in which the crime was used is necessary that may make the criminal put more pressure on the victim and threaten him in ways. Documenting all conversations and evidence

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

helps arrest the criminal to get his punishment. Dealing with extortion cases in a humane manner guarantees the dignity of the victim to take the legal course of action, it may take time so that the victim's right is not lost (Involved, 2021)

The second requirement

"Reasons and methods for getting rid of extortion through social media"

Section 1: - The reasons for extortion through social media"

In this demand, we address the causes of cyber-extortion that may be behind these crimes, and then we address the means used by the perpetrators in their crimes to blackmail their victims. Reasons: To commit the crime of extortion through social media, there are many reasons that the perpetrators seek to achieve through blackmailing victims, and these reasons may be either financial or immoral (sexual) or hostile (retaliatory) and to address these reasons in some detail as follows (Al-Badayna, 2021)

Financial reasons: - One of the most important reasons for committing cybercrime is the desire of the perpetrators to obtain financial resources and is done through the perpetrators threatening the victim in order to hand over money or other items of material value, whether the extradition directly or indirectly and achieve the direct method of electronic extortion by asking the perpetrators to hand over money to them or others on an ongoing basis. As for the indirect method, it is done through the blackmailer asking the victim to pay the money he borrowed from a bank or by paying the credits due to the blackmailer or paying his mobile phone bill, and the blackmailer here uses all the sexual content belonging to the victim in order to obtain money in exchange for his silence on the publication of this content, and here is the use of the progressive method of extortion, The operation starts with pictures of the victim for a certain amount. (Marei, 2016)

Immoral reasons (nationality):

This situation is achieved when it is intended to force the victim to perform immoral acts regardless of the status of the perpetrator (male or female) and refers to this last type of criminal behavior in the western youth circles, when the blackmailer moves his emotional relationship with the victim or coerces her to engage in such acts in exchange for not publishing information, conversations or images acquired by the crimes of using social media. Regardless of how these things are obtained or how they are viewed, whether by legitimate means through the availability of the element of consent by the victim, but often it is illegally acquired to select consent by the victim, such as being under puberty or by unauthorized access to the victim's electronic account, which is called "sarcasm", or by exploiting the blackmailer's job status as a public servant who can access all information from (Telegrams or communications via phones or the national internet network) as well as by the employee who works in the queries that are deposited the phones of their reviewers and others or to exploit his technical and professional status as a repairer or stores of devices and smartphones or equipped with internet service in addition to cases of theft or forgetting phones in public places (Ahmed, 2011)

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

Here lies the importance of rapid communication with legal bodies and specialized centers such as the community police and that what guarantees the victim a quick solution to his problem and complete secrecy without fear of disclosing any information belonging to her to the public, which contributes to ending the case without access to the family of the victim or one of the people in his social circle, the criminal in this type has obtained chats, videos or sexual images belonging to the victim, the blackmailer asks the victim some immoral things Such as pornographic things or sexual acts he does in exchange for the criminal not carrying out his threat and posting these pictures or videos on various websites or social sites. This is one of the most dangerous types of electronic extortion because it directly affects the victim and his family significantly (Marei, 2016)

Reasons for revenge (hostile):- This case is represented by the blackmailer threatening his victim in intangible ways and the moral side has an active role in this type of blackmail where the victim lives in a state of internal conflicts because of his expectation that the blackmailer will carry out his threat to him, which pushes the victim to implement these requests to avoid the threat he has made, and achieves this motivation The blackmailer enjoys harming the victim and enjoying his pain and crying What makes it worse is that the blackmailer deceives the victim and photographs him and forces him to mention his full name Or all his data and details that relate to his private life, and the motive of revenge of the offender can be to harm the victim and take revenge on him by discrediting him by publishing his privacy from photos or videos on the Internet sites or through social networking sites (Facebook - Twitter - Instagram) which is one of the fastest spreading and latest ways at present. (Hammadi, 2019, p. 83)

Or the blackmailer puts pressure on the victim (the woman) in order to prevent her from marrying in order to take revenge and harm her Some seek by virtue of previous social relations or by virtue of competition in a place such as a workplace or in the field of scientific or commercial success to try to influence another person in a negative way that degrades his social status or harms him in his reputation or work or anything else through which the offender wants to take revenge on that person for the purpose of what he achieves in the same offender and makes him feel that he has taken his right that he believes exists from the victim and follows this feeling either out of revenge or jealousy Which pushes the offender to blackmail the victim in order to achieve the interest he wants (Aleid, 2021, p. 3)

"Methods of getting rid of blackmail through social media" A person in his life may be subjected to blackmail by someone one day, and unfortunately many do not know how to behave, and what steps to follow to get rid of the crime of threat and extortion, many of those who have fallen into the trap of extortion obey the orders and desires of the blackmailer and thus drop themselves in the mud of extortion and be a victim of cybercrime.

The fact that the reason for the victim's confusion is the situation of the problem that has afflicted him, the majority of victims of extortion do not expect one day to be blackmailed by people who have been trusted and therefore we find some of them

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

may develop a state of depression and psychological collapse as a result of what happened to them, believing that it is over and that they are heading for a scandal and a harsh life full of obsessions and psychological pressures (Al-Sanad, 1439, p. 34)

One of the most important means to combat all forms of electronic extortion is: Combating electronic extortion on a personal level: Make sure to erase all sensitive photos and files before selling your mobile phone using Super Easer for Android, for example, or reformat the device, store unimportant files, and not send personal and private photos to any unknown individual on social networking sites and activate the role of censorship in prisoners.

Combating electronic extortion on an institutional scale: notifying the employee to the management in the event of an extortion related to the company or institution and training employees on how to deal with the technology correctly and the proper disposal of garbage and old computers so as not to exploit and reveal their secrets .

Initial self-disposition: Keeping calm, doesn't react quickly, or stress even though it's a normal feeling, but it doesn't help make sound decisions. Know the type of relationship with the criminal, how he reaches you and how your contents reach him, if it is by hacking the computer, you must act wisely and speed up the disconnection of the Internet from the suspicious device, whether it is a computer or a phone and delete any private content. If the criminal's arrival is through a dating relationship or sending photos or contents with your consent, security measures must be taken such as downloading a computer protection program. Determine the extent to which the criminal knows about you and your privacy, if the criminal does not know about you any private information such as your name or official electronic computers, the right action is to block him and stop dealing with him for fear of any information reaching him Dealing with the criminal: - How to avoid falling into the trap of extortion:- It only takes awareness, knowledge and electronic culture that enables you not to fall into the trap of one of the criminals who trolls the victim by their ignorance of some simple things and is almost very simple as you just need to check a few things and when you make sure that they are not true you should immediately stay away from taking any action by you. Knowing what the demands of the criminal are, responding to a small demand of the criminal may open his appetite to a larger demand, so he calculates not to respond and submit to the requests of the criminal but to act with great wisdom and make firm decisions Not to insult the criminal or provoke him or talk about things that provoke his anger so as not to be a motive for a retaliatory action Gain more time and try to access any information about the identity of the criminal and his place of residence, he may be outside the country and this thing helps in acting legally, knowing any real information about the criminal is a very important issue. (Al-Sanad, 1439, p. 35).

The demands of the blackmailers (criminals) of the victim: It is expected that the blackmailer will ask the victim for sums in exchange for covering up the documents, information or contents he possessed that would take the victim out or threaten his psychological and social stability or expose the victim to serious danger and may request sexual images or clips in order to tighten his grip, especially if the victim is a

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

girl, and may ask for information related to a specific person and this extortion is very dangerous because those who commit it sometimes belong to suspicious groups and the scientific reality of this crime says: The demands of the blackmailer do not end with the victim achieving what he wants, but they are like a case of addiction to blackmail that is matched by the speed of their implementation by the victim for fear of scandal.

This blackmailer will turn into a broken monster in order to achieve his sexual and financial desires and become a tyrant over the victim to do whatever he wants with it The reality confirms that more than 99% of the cases of extortion do not end with the fulfillment of the request of the blackmailer to larger and more requests, and the relationship of extortion relations has not ended with the achievement of the rare thousand demands, which ends only through interference, whether from the family or through the blackmailer's communication with the presidency, the tragedy ends.

While the role of the designated authorities in revealing its circumstances and circumstances and those involved in it appears, after the crime was carried out in secret, after reporting it becomes a visible reality, and here comes the role of the Code of Criminal Procedure No. 23 of 1971 and moves from a state of silence to movement because of the role it plays in detecting the occurrence of the crime of electronic extortion in order to protect the interests of individuals when the crime occurs, the Code of Criminal Procedure. (Sorou, 1996, p. 10)

should be detailed and regulated To conduct the detection of the crime and investigate all the evidence and information necessary to reveal the details of the crime and to know the perpetrators, there may be many means by which the victim will be blackmailed, it may be an e-mail containing information, whether it is writing, photo or even video, and it may be an audio communication containing what the offender wants from blackmailing the victim with it (Chalhoub, 1432, p. 21)

The second section I "Legislative Position on Electronic Extortion" The fact of the matter is that there is no legislative text in Iraq that explicitly punishes the commission of cybercrimes, and this is a clear failure by the Iraqi legislator in his delay in enacting such important laws as of this writing, where the Iraqi government has prepared a draft law

(Cybercrime) was referred to the House of Representatives in 2011 and was read first in the House and is still under legislation. Through our tracking of the cases of electronic extortion, we find that their legal adaptation at present varies according to the fact of extortion, by scamming the blackmailer and defrauding the victim for the purpose of reaching the end of the subject of extortion, and here the legal adaptation of such cases is under the text of paragraph (1) of article (456) of the Iraqi Penal Code in force.

Because of the seriousness of this crime and its repercussions, these crimes have been addressed by the Iraqi judiciary by relying on the general principles in the Iraqi Penal Code and considering the crime of electronic blackmail through social media as crimes of threat and fraud for the purpose of cheating the victim up to blackmailing him.

ISSN Online: 2709-071X
ISSN Print: 2709-0701
DOI: https://doi.org/10.33193/JEAHS.28.2023.405
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

The Iraqi legislation dealt with the crime of threat in general in articles (430-431-432) of the Penal Code No. 111 of 1969, where the first paragraph of article (430) of the Iraqi Penal Code stipulates that "Anyone who threatens anyone to commit a felony against himself, his money or others or to assign or disclose things that are detrimental to honor shall be punished by imprisonment for a period not exceeding seven years or by imprisonment and the second paragraph of the said article shall be punished by the same penalty if the threat is an empty speech. From the name of the sender or was attributed to an existing or alleged secret group. Article (431) "Anyone who threatens another person to commit a felony against himself, his money or others or matters that are contrary to honor or consideration or disclose them other than the cases specified in Article (430) shall be punished by imprisonment. Article 432 stipulates that anyone who threatens another by word, deed, or by referring to a euphemism or verbally shall be punished by imprisonment for a period not exceeding one year or a fine. (Al-Shukry, 2008, p. 56)

Any word or writing that would throw terror into the heart of the person threatened by the commission of a crime against the offender or money or the disclosure or attribution of things that are detrimental to honor shall be considered a threat, and the threat may be carried under the influence of that fear to answer the offender to what he wanted whenever the threat is accompanied by the request for a threat in general as an expression of the will of the accused to inflict harm on the victim or a person of interest to him affects his psyche or freedom of will and this will is supposed to be intended The threat must also be serious. (Al-Ghalbi, 2009, p. 14)

On this condition, the law punishes the threat because of the impact it has on the psyche and freedom of will of the victim and would not do so unless it was serious.

It does not matter whether the threat intends or does not intend to execute the threatened order, as well as the crime of threatening, even if it is an oral or written insinuation. (Mamdouh Rashid Al-Anazi, 2017, p. 33)

Article (433) refers to extortion in some way by saying "defamation is the attribution of a certain fact to others in one of the public ways that, if true, would require the punishment of the person entrusted to him or his contempt for the people of his homeland" and "If the defamation occurs by publishing in newspapers or publications or by one of the other methods of information, this is considered an aggravating circumstance", while Article (434) stipulates (insulting anyone who throws at others what violates his honor or consideration or hurts his feelings, even if this does not include attribution of an incident). Certain . If the insult is committed by publishing in newspapers or publications or by one of the methods of information at other times, this is considered an aggravating circumstance, while Article (438) states that "The penalty shall be imprisonment for a period not exceeding one year and a fine not exceeding one hundred dinars. 1- Publishing in one of the public ways news, photos or comments related to the secrets of the private or family life of individuals, even if they are true if their publication is to offend them. (Code, 1969)

Section II "Judicial Position on Electronic Extortion" The noble Iraqi judiciary has not remained idle in the face of the crime of electronic extortion because of the lack of a

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

legislative text that punishes this despicable act as it missed the opportunity for blackmailers to take advantage of this legislative vacuum, or to adhere to the rule (no crime and no punishment except by a text), where our esteemed judiciary had a firm role in addressing this imbalance, and judging the extortionists and perpetrators according to legal adaptations. Through the follow-up of the judicial authority, we were able to find a set of judicial decisions related to many crimes of electronic extortion, including the following:

1. The Karkh Investigation Court specialized in terrorism cases at the presidency of the Baghdad – Karkh Federal Court of Appeal has confirmed the confessions of members of a network specialized in hacking social media sites by taking photos, copying electronic conversations, bargaining with their owners and threatening to publish them in all sites when not paying with the intention of defamation and extortion, and legal procedures have been taken against the defendants and referred them to the competent court in accordance with the provisions of Article (430) of the Penal Code (writer, 2009)

2- Recording confessions by the Muthanna investigative judge to a group of criminals who extort citizens through social networking sites (Facebook) from fake pages by threatening to publish photos or pay money and were arrested for the crime of witnessing where they confessed to their crime and were referred to the competent court in accordance with Article (430) of the Iraqi Penal Code (1). There are many legal measures taken by the Iraqi judicial authorities to attack the crimes of electronic extortion, and for the legal and information benefit of viewing the websites of the Ministry of Interior and the website of the judiciary regarding the review of all cases of electronic extortion.

It should be noted that the procedures followed in the detection and investigation of the crime of electronic extortion must be legal and follow the controls set by the law by those who collect evidence and search even those extracted from the information network, and the extraction of this evidence is not legitimate unless the process of putting it to the judiciary was carried out in accordance with the law and otherwise if evidence is obtained without the consent of the competent authority, it is not considered no matter how strong, For example, if the concerned agencies monitor the phone of the blackmailer without obtaining the approval of the judiciary or monitor him in his residence or workplace without the prior approval of the judiciary, all these procedures, although they have led to strong and fruitful results in the investigation, are not reliable and illegal are not considered illegal. The Iraqi Ministry of Interior / Directorate of Combating Baghdad Crime has set a hotline for the purpose of communication by women who are subjected to extortion, which is (533), in the event of a call on this line, the competent department of the complainant to come to initiate a lawsuit against the blackmailer with all the information and evidence on how to extort it, or to visit the nearest office of the said Directorate for the said purpose, after the victim submits the complaint, the physical evidence available to it from (phone number) is investigated. Correspondence on one of the social media), after which the blackmailer is monitored based on the decision of the judge, to arrest him in flagrante

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

delicto, and the technical department and the investigative unit of the above directorate are competent to collect all information through phone numbers or social media to reach the offender.

Conclusion

Conclusions After we finished our research tagged "Electronic blackmail in Iraq", we have reached a number of conclusions and recommendations, perhaps the most important of which are the following:

1- The crime of electronic extortion is achieved through social networking sites using the offender as a single or multiple behavior, as there is no indication of the means resorted to by the blackmailer to commit his crime in blackmailing the victim, as it is possible to commit this crime through chat rooms or any other method aimed at getting the victim to produce a certain result of doing or refraining from doing an act .
2- The crime of electronic extortion is one of its distinctive features that it requires expertise in computer technology, as computers and smart devices are its tool
3- Cybercrime has no geographical boundaries and its theater is virtual, non-field, and bright, difficult to detect and soft that does not require much effort to commit it, only experience in the field of computers.
4- The crimes of electronic extortion have produced many legal problems and revealed the legislative inadequacy of penal laws in criminalizing these crimes introduced through the absence of Iraqi legislation from a direct law dealing with cybercrimes.
5- The crime of extortion represents a process of intimidation and a threat to social and family security by placing the personal matters of the victim with a high degree of confidentiality in full view of everyone in the event that the victim does not submit to the requests of the blackmailer

Recommendations

At the end of this research, it is useful to make some recommendations, hoping that the Iraqi Sharia will observe them, including:

1- We recommend that the Iraqi legislator expedite the enactment of the Cybercrime Law, provided that this law is compatible with the special nature of the new cybercrimes or the amendment of the Iraqi Penal Code to include these crimes within a legal framework and criminalize all that includes them from the process of extortion, fraud and penetration of the electronic devices of others
2- We call on the hands of the Iraqi legislator to develop a complete strategy in which all relevant security and judicial agencies participate and to discuss ways to develop them materially and humanly to help the investigative bodies in accomplishing their work at this level.

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

3- Establishing an integrated security system in the Ministry of Interior to combat cybercrime similar to the security systems for ICT-related crimes in developed countries
4- Intensifying efforts to conduct regular training courses for the judiciary, members of the judicial police and even lawyers specialized in dealing with the crimes of electronic extortion and how to properly use social media accounts among young people
5- Supporting and supporting victims of electronic extortion through social media sites by urging victims who have been blackmailed to inform the security authorities and arrest the perpetrators and bring them to justice to receive their punishment
6- We recommend the establishment of competent courts to try the crimes of electronic extortion or the creation of competent judicial bodies whose membership includes judges with a high degree of technical and technical qualification in the field of information technology because of the importance of this type of crime at the national level
7- Supporting the media effort in all relevant state institutions and in partnership with all civil society organizations and working to perform intensive and organized awareness campaigns targeting age groups at various stages of study starting from the university stages and preparatory studies and warning the age groups of young people of the dangers of drifting behind emotions and victims of this type of criminal acts and spreading the values of moral commitment between the individual and society

References

1. Al-Saghir, J. A.-B. (1992). Modern Criminal Law. In J. A.-B. Al-Saghir, *Modern Criminal Law* (p. 4). Cairo: Al-Nahda-AlArabiya.
2. Hasser, O. S. (2015). *Research published in the Journal of Police Thought*, p. 28.
3. Al-Rasheed, M. R. (n.d.). "Criminal Protection and Criminal Protection of the Victim from Extortion. , *Arab Journal of Security Studies*,, p. 194.
4. Shadid, A. A. (n.d.). Extortion seminar research", concept, causes, treatment. *preparation of the Center for Women Researchers for Saudi Women's Studies*, p. 44.
5. Aladdin Zaki Morsi. (2013). Assault Crimes on Show. In A. Z. Morsi, *Assault Crimes on Show* (p. 136). Egypt: Publishing House.
6. Khalil Yusuf Jundi, H. A. (2021). Electronic Extortion and Cybercrime - Concept and Reasons. In H. A. Khalil Yusuf Jundi, *Electronic Extortion and Cybercrime - Concept and Reasons* (p. 65). House of Knowledge Competencies.
7. Noura bint Abdullah .*Blackmail of girls, its rulings and punishment in Islamic*
8. Blackmail of girls, its rulings and punishment in Islamic : https://unis.imamu.edu.sa

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

9. Abdullah, N. b. (n.d.). *Blackmail of girls, its rulings and punishment in Islamic jurisprudence*. Retrieved from Research submitted to the College of Sharia: https://unis.imamu.edu.sa
10. Al-Ajami, A. D. (2014). "Scientific and Legal Problems of Cybercrime". In A. D. Al-Ajami, *"Scientific and Legal Problems of Cybercrime"* (p. 33). Jordan: Middle East University, Amman.
11. al-Baghdadi", A. B. (n.d.). *Means of research and investigation,*. Retrieved from Najah.edu: Najah.edu
12. Ba'ayoi, S. S. (n.d.). *Cyber Extortion Crime"*. Retrieved from researchgate.net: researchgate.net
13. Aleid, N. A. (2021). *Nawal Abdulaziz Aleid*. Retrieved from http://nawalaleid.com/cnt/lib/768: http://nawalaleid.com/cnt/lib/768
14. Badayna, D. M. (2014). (a scientific lecture entitled "Cybercrime – Concept – Reasons. (p. 7). Jordan:), the Scientific Forum at the College of Strategic Sciences and Targeted Crimes in the Light of Regional and International Changes and Transformations).
15. Hamid Salih Ibn Abdullah Ibn Muhammad. (1432). *Extortion Symposium Research, its concept, causes and treatment.* Riyadh: Research Center for Women's Studies,.
16. Radi, A. M. (2022). (Principles of Criminal Investigation in Electronic and Information Crimes via the Internet and Ways to Address It. In (. o. It. Baghdad: Books and Documentation House.
17. Ghanem, Y. M. (2019). "Electronic extortion - a study from a legal point of view within the author of electronic extortion - the crime of the modern era. In ". e.-a.-t. era, *"Electronic extortion - a study from a legal point of view within the author of electronic extortion - the crime of the modern era* (p. 5). Baghdad,: House of Books and Documents.
18. Ibrahim, H. H. (2022, 6 30). *The Supreme Judicial Council*. Retrieved from The Supreme Judicial Council: https://www.hjc.iq/view.69769/
19. Hussein Abdul Karim Younis, D. K.-J. (2021). (electronic extortion and cybercrime, concept, reasons). In D. K.-J. Hussein Abdul Karim Younis, *(electronic extortion and cybercrime, concept, reasons)* (p. 55). Cairo: , Dar Al-Qafdat,.
20. Involved, E. e. (2021, 10 25). *Electronic extortion Lack of awareness of the intervention of victims with the prohibited and the law deters those involved*. Retrieved from Electronic extortion Lack of awareness of the intervention of victims with the prohibited and the law deters those involved: https://www.ina.iq/139500--.html
21. Al-Badayna, T. M. (2021). Created crimes in light of regional and international changes and transformations. *Scientific Forum at the College of Strategic Sciences,* (p. 51). Jordan: College of Strategic Sciences.
22. Marei, I. J. (2016, 8 9). *Cybercrime "Aims – Causes – Methods of Crime and Processing"*. Retrieved from Arab Democratic Center : https://democraticac.de/?p=35426

DOI: https://doi.org/10.33193/JEAHS.28.2023.405
ISSN Online: 2709-071X
ISSN Print: 2709-0701
مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (28) October 2023
العدد (28) أكتوبر 2023

23. Ahmed, A. S. (2011). *criminal responsibility for mobile phone abuse,*. Iraq: research of graduation requirements from the Judicial Institute.
24. Hammadi, K. A. (2019). Electronic Fraud, The Art of Penetrating Minds (Social Engineering). In K. A. Hammadi, *Electronic Fraud, The Art of Penetrating Minds (Social Engineering)* (p. 85). Baghdad: Iraqi Ministry of Interior.
25. Al-Sanad, A. R. (1439). The Crime of Extortion. In A. R. Al-Sanad, *Abdul Rahman Abdullah Al-Sanad* (p. 49). Riyadh: Kingdom of Saudi Arabia, King Fahd National Library for Publishing.
26. Ahmed Fathi Sorou) ..Mediator in the Code of Criminal Procedure .(Ahmed Fathi Sorour*) ،Mediator in the Code of Criminal Procedure (*Cairo :Arab Renaissance House.Chalhoub, M. '.-M. (1432). (The crime of extortion, comparative study). In M. '.-M. Chalhoub, *(The crime of extortion, comparative study)* (p. 23). Saudi Arabia: Master's thesis, Imam Muhammad Ibn Saud Islamic University,.
27. Al-Shukry, A. Y. (2008, 7 6). Information Crime and the Crisis of Criminal Legitimacy. *Journal of the Kufa Studies Center*, pp. 117-120.
28. Al-Ghalbi, R. A. (2009). The crime of electronic extortion and the mechanism of combating it in the Republic of Iraq, . In R. A. Al-Ghalbi, *The crime of electronic extortion and the mechanism of combating it in the Republic of Iraq,* (pp. 14-18). Bahdad: House of Books and Documents.
29. Mamdouh Rashid Al-Anazi. (2017). Criminal Protection of the Victim of Extortion. *The Arab Journal for Security Studies*, 58-101.
30. Code, I. P. (1969, 7 1). https://www.rwi.uzh.ch/dam/jcr:00000000-0c03-6a0c-ffff-ffff96be3560/penalcode1969.pdf. iraq, Baghdad.
31. writer, L. t. (2009). https://al-ain.com/article/electronic-blackmail-iraq-victims-escalating-laws. Iraq, Bahdad, Bahdad.