International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 17, Issue 1, 2023

Criminal Protection of Communications via Social Media

Lec. Maitham Mohammad Abd AL Nomani, Al-Furat Al-Awsat Technical University, Babylon Technical Institute, Legal Management Technologies Dept., Iraq, Email: inb.mth@atu.edu.iq

Nowadays, society lives in a machine controlled by advanced technology, which has occupied all aspects of the lives of its members through various social media. Many companies have started working on the design of many applications that allow the user to communicate with others via the Internet through computers or mobile phones to accomplish daily work quite easily. Millions of people use social media applications for chatting and sending pictures and videos, such as Facebook, Facebook messenger, Viber, WhatsApp, Telegram, Instagram, and others. However, some may resort to violating these rights in various ways, such as hacking to see the personal conversations of others or to steal studio files such as photos, videos, audios, etc. without the consent of the owners for various purposes, such as defamation, revenge, or blackmailing girls to pay money in order to avoid the scandal. Therefore, the topic of user privacy in social media is one of the most important topics worth being studied. To protect personal communications, a law criminalizing serious violations should be enacted because of its close connection with the issue of confidentiality of human life and dignity.

Keywords: *Protection, criminal, crime, communication.*

Introduction

Electronic crimes are new crimes that arose with the emergence of social media as a result of the development of technology in society. These crimes differ from traditional crimes. The electronic information network has raised the level of traditional crimes to a higher level than the level of traditional crimes. The phenomenon of blackmailing victims of social media from the young people of both genders in Iraq and many countries of the world spread with the frequent use of these sites. Recently, social media turned from innocent interest and pleasure into aggressive amusement, extortion, and threat with the aim of obtaining benefits or social subjugation as a result of personal enmity or political subjugation for the purpose of reaching the seats of government . Legislators should pay attention to this phenomenon through penalties that are commensurate with the degree of these crimes.

The crimes committed through social media have exceeded the effects of the individual interest in order to reach the level of prejudice to the security of the state and the stability of society. Today, calls may be made for demonstrations by a few on social media and the majority respond.

The problem of study

The problem of the present study is focused on answering the following questions:

1. What is meant by communications and what are social media ?, their types ?, the crimes committed using them?, and what are the means used in committing these crimes?

2. What is the extent of the applicability of the traditional texts of ordinary crimes of blackmail to the crimes of hacking communications and electronic blackmail. Does the Iraqi legislator criminalize the act of hacking and electronic blackmail?

The aims of study

The present study aims at:

1. Defining social media and communications through them.

2. Identifying the legal guarantees of the confidentiality of personal communications as attacking privacy and personal freedom of people is the greatest risk they may be exposed to.

3. Identifying the way in which crimes that violate the sanctity of communications are committed on social media.

The significance of the study

Electronic crime in general and the crime of electronic extortion in particular has become one of the most serious topics in the field of study and scientific research as a result of the seriousness of these crimes. This seriousness is the source of the significance of the present study. The present study is an attempt to find appropriate legal solutions to address the legislative deficiency resulting from the lack of an Iraqi e-crime law. In light of the widespread of electronic crimes, criminalizing the act of piracy and hacking of communications and electronic extortion by referring to the traditional texts of the Iraqi Penal Code of extortion is an urgent need.

Previous studies

Despite the novelty of the topic and the lack of legal studies that dealt with it, the researcher could find some studies as follows:

1. Ziyush, Saeed, (2017); The phenomenon of electronic blackmail and ways of prevention: A sociological reading and theoretical opinions, No. 22, Journal of Social Sciences, University of Chlef, Algeria.

2. Hussein, Muhammad Abduldhahir, (2004), legal responsibility in the field of the Internet, Arab Renaissance House, Cairo, Egypt.

The methodology

The researcher adopted the analytical method to analyze the legal texts related to the subject of the study in order to reach solutions for the problems with a discussion of jurisprudence opinions and judicial solutions.

The design of study

The present study is divided into three sections. Section one addresses communications and social media. Section two is devoted to the crimes of electronic communications. Section three presents the legal provisions.

Section one

What are communications and social media?

Before defining the concept of communications, social media should be defined as communications are done through them. Therefore, researching this topic requires dividing it into two subsections. The first is devoted to the definition of social media. The second discusses the types and characteristics of social media.

First: The definition of social media

Social communication is defined in general as increasing the number of the person's friends by establishing relationships with others (Marwan, 2020: 1). It is also defined as the process of communicating with a number of people; relatives, colleagues , Friends, ...) through electronic sites and services that provide fast delivery of information on a large scale. They are sites that do not only give information, but they also coincide and interact with the subscriber while supplying that information in the scope of his/her network (Al-Miqdadi, 2013: 24) and (Mekawi, 2006: 3939- 398). As for social media, it is a technology used across the global Internet using multiple types of devices, such as computers, tablets, or even smart phones. This means allows its users to interact with other users such as family and friends through what is shared via these means, such as pictures, blogs, videos, and other things provided by social media such as games, for example. The use of these means is not limited to individual and personal use. Companies use these media For the purpose of reaching customers and interacting with them, placing advertisements through these means, or providing various support services. These means are based on the principle of exchanging ideas and information and building virtual societies (Al Dwikat, 2019: 1). It is a system of electronic networks via the Internet. It allows the subscriber to create a private site and link it through an electronic social system with other members who have the same interests and hobbies (Rami, 2003: 23). It is also defined as those social sites that allow their surfers to share files, pictures, and exchange video clips. It also enables them to create blogs, conduct instant conversations, and send messages (Al-Mansur, 2012: 3). As such, it is a means of exchanging information immediately through the Internet (Alyan, 2003: 127).

The emergence of social media allowed users to communicate with each other via the internet, whether through video calls, audio clips, or conversations. These sites have become a means of establishing relationships between individuals. Thus, social media can be defined as interactive social sites that allow users to communicate with other users of the same sites by creating personal accounts; a virtual reality to meet friends, relatives, and families of different ages, genders from all parts of the world united by common interests and activities despite their different awareness And their thinking and culture to express the joys and sorrows in people's minds, through which they exchange experiences, knowledge, information, files, pictures, and videos. In addition, they provide many other services to their users such as e-mail, private means, instant chats, and others.

Second: Types of social media and their characteristics

This section clarifies the types of social media and their characteristics as follows;

1.Types of social media

Social media has many types, including Facebook, Facebook Messenger, Skype, Viber, Instagram, WhatsApp, Twitter, YouTube, Google Drive, and Telegram. These applications have been widely used by users and followers of social media.

It also recently spread in light of the current situation due to the spread of Corona virus and the imposition of a curfew. Some applications are used in electronic education in order to continue the educational process. Professors use them to deliver lectures, attend virtual conferences, or to hold seminars, workshops, and training courses. These applications are Google Classroom, Free Conference Call, Zoom Cloud Meetings, and Google Meet.

2.The characteristics of social media

It is undeniable that social media has returned to the whole world with many positive returns. These positive returns have facilitated the process of getting to know new friends. These sites have also provided an opportunity for the individual to express him/herself. Moreover, The communication process has become easy and very fast due to the social networking sites.

Social media has made the world like a small village as the user of these means can communicate with anyone else anywhere around the world with ease. Social networking sites have provided the user with an opportunity to meet new people who share the same interests to form new relationships With them (Marwan, 2020: 2).

University professors can also take advantage of social media to attend scientific conferences, seminars, training courses, and workshops as they can attend them electronically while they are at home, even if they are in another country far from them, without the need to bear the hassle of traveling, incurring expenses, and wasting time.

It is also possible to take advantage of the various social media to develop the teaching and learning process by making use of educational programs that are shared through social networks and providing learners with adequate experience by communicating with people who are specialists in specific topics and following them through these means. Any search can also be searched within these sites.

Social media also provides many benefits to business owners, including increasing the proportion of sales, reducing the costs of marketing and advertising, increasing the number of visits to the website of the project or company, developing the ability to access the product to

international markets, and developing communication with customers or other companies (Al-Dweikat, 2019: 2).

Despite these positive returns, they have reduced the productivity of the individual. They cause employees to be distracted from their work. Facebook alone reduced the productivity of the individual by 1.5%. Moreover, British companies lose approximately 2.2 billion dollars annually due to the distraction of their social networking sites (Marwan, 2020: 2).

Having clarified the role of social media that allow surfers to share files, photos, video clips, and audio clips, and enable them to make instant calls and send messages, the researcher believes that communications are everything that is exchanged and sent between Different Parties (Nataga, 2011: 1).

Section two

Crimes against social media communications

The phenomenon of blackmailing social media victims; young males and females in Iraq and many countries of the world has spread recently with the abundance of these methods and the remarkable acceleration in the number of different chat programs and the growing number of their users, which recently intensified and attracted attention to turn Social media into aggressive amusement, extortion, and threats.

The blackmailer may directly penetrate the personal accounts of well-known figures such as politicians and officials in the Iraqi government or artists known by means of hacking to take some information about this character, such as family photos, conversations, and private videos in the victim's mobile phone or personal computer. Electronic communications may directly be blackmailed from the target person's mobile phone by establishing a friendship with the target person. The blackmailer may hack the conversation and enter all the communications of the victim to take some private information to obtain material benefits or social projection as a result of personal enmity, or political fall for the purpose of reaching the seats of government. In both cases, the victim may be threatened by requesting transferring money, waiving the nomination for certain elections, forging an official document, or establishing an auction if the victim is an employee in exchange for not defaming the victim or publishing his/her photos or conversations. The degree of extortion may amount to a request for sex with the victim if she is a woman, taking advantage of the surrender of the victim and ignorance of the methods used To deal with such situations.

The term Hacker historically refers to intelligence and deductive thinking. It was not only associated with computer systems and the Internet. In the world of computers and the Internet, piracy is any technical effort made to manipulate and control the natural functioning of the

system for networks or Hardware. Therefore, the hacker is the person responsible for the hacking process and manipulating the workflow of devices and networks. Attacks on sites, programs, and others are related to piracy and piracy operations (Al-Shawabkeh, 2018: 1).

The penetration of accounts and access to personal conversations of other persons constitutes an attack on human freedom in the communication, postal, telephone and electronic communications protected under the text of Article (40) of the Constitution of the Republic of Iraq for 2005, Article (12) of the Universal Declaration of Human Rights issued by the Assembly General of the United Nations on 10/12/1948, and Article (17) of the International Covenant on Civil and Political Human Rights issued by the United Nations General Assembly on 16/12/1966.

Electronic crimes are considered to be among the newest crimes that differ from traditional crimes. The electronic information network has raised the level of traditional crimes more than the level used in books and references for traditional crimes. The legislators should issue penalties that are commensurate with the degree of these crimes by developing some legal aspects related to investigation, evidence gathering, judicial seizure, and the type of jurisdiction concerned.

Section three

Legal provisions for crimes against social media communications

To tackle the legal provisions of the crime of piracy, hacking of communications, and electronic threat, this section is divided into two subsections. The legal elements are discussed in the first subsection. The second subsection is devoted to the penalties imposed on the perpetrators as follows;

First: Elements of the crime of hacking and extortion electronic communications

The pillars of this crime are the material and the moral pillar.

1.The material pillar

The material component of any crime is embodied in the underlying psychological state inherent in the same offender into material acts in the external world that have a criminal characteristic (Al-Hayari, 2010: 109). Law does not punish abstract ideas unless they are combined with material acts. The materiality of each crime is the criminal behavior, criminal consequence, and causal relationship.

1. The criminal behavior; It is represented by the sum of the criminal acts that constitute the crime, which may appear in a positive activity when the perpetrator performs an act

prohibited by the law. It may appear in the form of a negative attitude when the perpetrator refrains from carrying out an act required by the law Article (28) of the Iraqi amended Penal Code No. (111) of 1969.

The criminal behavior of the crime is the penetration of the perpetrator into the electronic account of the victim to enter into his/her personal conversations and then bargaining with him/her to request transferring money, waiving the candidacy for certain elections, falsifying an official document, or establish a bid or public tender in exchange for not defaming the victim or posting pictures or conversations. In some cases, the degree of extortion may amount to a request for sex with the victim if she is a woman.

2. The criminal result; The criminal result is also considered to be one of the elements of the material pillar. It means the material change that takes place in the external world as an effect of criminal behavior. It is he effect of criminal behavior (Mahmoud, 2002: 61). With regard to the crime of extortion, It is achieved by achieving the criminal result or without achieving it. In other words, the criminal result is not required to be confirmed, but it should only be possible. This is due to its danger on society. The criminal legislator has not only limited protection of social interests to the extent of protecting them from harm, but also includes protection against any danger that may befall them or threaten them. It included criminalization and punishment deficiency of aggression on this interest. Thus, these crimes take one of Two forms; They are either crimes of danger or, they are crimes of harm.

   Dangerous crimes are those crimes that do not cause tangible harm, but they rather have a danger that threatens the interests protected by law" since the seriousness of their actions is so great that they must be fought before happening because if they were committed, they would lead to very serious results. The crimes of harm mean those crimes that have tangible criminal effects (Mahmoud, 2002: 79).

   The crime of hacking and extortion is realized as soon as the criminal behavior is achieved without the need to achieve the criminal result. Once the criminal behavior is achieved, this threatens the lives of people and their property leading to defaming the victim or harming him/her. In other words, the crime of electronic extortion occurs once the perpetrator threatens The victim's defamation, whether he/she carries out his/her threat or not.

3. The causal relationship; It is evident that the material element of the crime does not exist except when the causal relationship between criminal behavior and the criminal result is realized. If the causal relationship is not established, this leads to the absence of the material pillar of the crime and consequently to the fall of the whole crime.

The causal relationship must be verified in the crime of blackmail when the harm is achieved with no condition being required when the harm is not achieved.

2. The moral pillar

It is not sufficient for the crime to occur that its material pillar is available, but it must also have its moral pillar with its two elements; the criminal qualification and the criminal sin.

1. The criminal qualification; It is defined as a set of characteristics that a person must have in order for the crime to be attributed to him/her as consciousness and willingness (Alia, 2002: 298). The criminal qualification is the criminal responsibility that is available to those who hack and blackmail when they possess the awareness and the will.
   Perception or discrimination is understood to mean a person's willingness or ability to understand the nature and character of his/her actions and estimate their consequences (Rasool and Ahmed, 1982: 96). The will or freedom of choice is defined as the ability of a person to direct him/herself to a certain action or to refrain from it (Mustafa, 1983: 416).

   There is no criminal responsibility for those who are not eligible to bear it as eligibility lags behind cognition or will, or both (Article (60) of the Iraqi amended Penal Code No. (111) of 1969). As a result, there is no responsibility for the insane, drunk, narcotic, or young; Everyone lacks the qualification to form a criminal perception because their mental perceptions are not complete, which greatly detracts awareness. The same applies to those who are forced to commit a crime or are forced by circumstances to do so as they are deprived from freedom of choice due to the pressure of coercion or the necessity of his/her will, which leads to the fall of the moral pillar.

2. The criminal sin; It is the will of the perpetrator to actually do the component of the crime, which may take the form of willfulness; a criminal intent. It may take a form of the mistake; non-intentional error (Sorour, 1981: 524).

Because hacking and blackmailing is an intentional crime requiring the criminal intent, there is no unintentional error.

Criminal intent is defined as directing the will to create an order that is already punishable by law knowing that it is criminalized legally (Al-Haidari, 2012: 309). The Iraqi legislators in Article 33/1 of the Penal Code define criminal intent as that the perpetrator directs His/her will to commit the act constituting the crime that took place or any other criminal result. The general criminal intent is achieved by the offender's will,, criminal outcome, and knowledge of the crime. The normal intent itself, which is in the direction of The will of the perpetrator is to deny the account of the victim and enter his/her communications and then bargain over that

knowledge of criminalizing what he/she does legally, knowing that the element of knowledge is presumed against the perpetrator (Mahmoud, 2002: 67).

Second: The penalty of hacking and extortion

The punishment is defined as a sanction prescribed by law for the crime stipulated in it for the benefit of the community that has been harmed. The judge imposes it on the perpetrator (Ibrahim, 2008: 298).

The Iraqi legislators did not issue a law on cybercrimes. But, reading the texts of the Iraqi Penal Code No. (111) for 1969, the researcher found some texts that apply to ordinary crimes of blackmailing, which can also be applied to crimes of hacking and electronic blackmailing. Article (328) states that every employee in the postal, telegraph, and telephone departments, and every employee or person charged with a public service who has opened, destroyed, or concealed a message or telegram deposited or handed over to the aforementioned departments, facilitates it to others, or discloses a secret, shall be punished with imprisonment for a period not exceeding seven years. The same punishment shall be imposed on those who disclose a phone call or whoever facilitates this. Article (430) also states that; "1.Any person who threatens another person with a felony against him/herself, his/her money, against the property of others, or entrusting or abusing matters that are insulted with honor, shall be punished with imprisonment for a period not exceeding seven years. 2.The same penalty shall be applied if the threat is in a letter devoid of the name of its sender or if it is attributed to its issuance to an existing or alleged secret group". Likewise, Article (438) stipulates that "a penalty of imprisonment for a period not exceeding one year and a fine not exceeding one hundred dinars, or one of these two penalties ... 2. Whoever is not aware of those not mentioned in Article 328 of a letter, telegram or phone call, and divulges it to someone who has been charged with it if that would cause harm To anyone".

Article (452) stipulates that: "1. A penalty of imprisonment for a period not exceeding seven years or with imprisonment for another period is imposed on the threat of delivery of money or other things ...".

It is clear that the offender and the blackmailer have two punishments according to the Iraqi Penal Code; the punishment that deprives the perpetrator from freedom and the fine. The researcher finds that the aforementioned law differentiates between two cases. In the first case, the crime is considered a felony and therefore the penalty prescribed for it is imprisonment. In the second case, the crime is considered a misdemeanor and the punishment for it is imprisonment, a fine, or both.

As for the position of the Iraqi judiciary, It did not remain idle in the face of threatening cyber - crimes; Because there is no legal provision to punish it, so it employed the punitive texts for the

regular crimes of threat or defamation and reflected them on this new crime through the texts of articles (328, 430, 438, 452) from the Iraqi Penal Code, thus, the blackmailers missed the opportunity to take advantage of the legislative vacuum, or that they stick to the rule "There is no crime and no punishment except by the text".

The Iraqi judiciary stipulated many decisions concerning electronic threat crimes as follows:

1. The Babylon Criminal Court sentenced one of the defendants to a severe prison sentence for three years after being convicted of extorting a girl electronically by hacking her page on social networking sites "Facebook", by sending a link in the Messenger application, withdrawing pictures and content from her phone, and bargaining her financially. The ruling was issued according to the provisions of Article (430) of the Iraqi Penal Code, which was ratified by the Federal Court of Cassation (Muhammad, 2019: 60- 63).

2. The Central Criminal Court at the Presidency of the Baghdad / Al-Rusafa Federal Court of Appeal issued a seven-year prison sentence against a convict who broke into a girl's account on Facebook and obtained her personal photos, and then began bargaining for money in exchange for not publishing her pictures. The judgment was issued according to the provisions of Article (430) Of the Iraqi Penal Code (Muhammad, 2019: 5679).

3. The Wassit Criminal Court / First Instance issued prison sentences (21) years in three cases, with a prison term of seven years for each of them, against a person convicted of threatening and blackmailing three citizens by assigning things that violated honor with the abuse of their personal pages on social media. The judgments were issued according to Article (430) of the Iraqi Penal Code (Muhammad, 2019: 5991).

4. The Muthanna Criminal Court issued a five-year prison sentence and one month in accordance with the provisions of Article (430) of the Iraqi Penal Code, against a convicted person who broke into a personal account via Facebook for a citizen and obtaining family photos threatening to publish them through the communication sites in the event he did not pay money . The ruling was ratified by the Federal Court of Cassation (Muhammad, 2019: 5820).

The results

The results of the present study are as follows:

1. Electronic crimes are considered new crimes that differ from traditional crimes. The network of electronic information made the level of traditional crimes higher than the level in books and references for traditional crimes. Electronic crimes may be through a push of a button, not spreading to certain regions, but rather sweeping all countries Being intercontinental crimes.

2. The failure of the victim to submit to the demands of the blackmailer pays the latter to defame the victim. This constitutes a threat to family and social security.

3. The crimes committed through social media outlets have exceeded the individual interest in order to amount to prejudice to the security of the state and the stability of society. Today, it is sufficient for calls to go out in demonstrations by a few pioneers of these means so that the majority respond.

Conclusions.

The crimes committed through social media outlets have exceeded the individual interest in order to amount to prejudice to the security of the state and the stability of society. Today, it is sufficient for calls to go out in demonstrations by a few pioneers of these means so that the majority respond.

The victim's disobedience to the demands of the blackmailer pays the latter to defame the victim. This poses a threat to family and social security.

Suggestions

In light of the previous results, the researcher presents some suggestions to combat the phenomenon of hacking, piracy, and extortion as follows:

1. Protecting the right of personal communications and enacting a law criminalizing serious violations committed against it to develop some legal aspects related to investigation, gathering evidence, judicial control and the type of jurisdiction to try the perpetrators with penalties that are commensurate with their degree due to their close association with the issue of confidentiality and its impact on human life and dignity. Therefore, the Iraqi legislator should issue a law on cybercrime, or amend the articles of the penal code on ordinary extortion to include cyber extortion crimes within its scope.

2. The Iraqi Ministry of Interior, through its media bodies, should have an effective role in conducting educational and awareness seminars to demonstrate the dangers of piracy and electronic hacking to clarify how to properly use social media.

3. Strengthening international cooperation to confront cybercrimes.

References

Al-Dweikat, S. (2019). "The Importance of Social Media", available on the website: https://mawdoo3.com

Al-Haidari, J., (2012). "Al-Wafi explaining the provisions of the general section of the Penal Code", 1st edition, Al-Sanhoury Library, Baghdad.

Al-Hiary, M., (2010)." The material pillar of Crime", 1st Edition, Al-Halabi Human Rights Publications, Beirut, Lebanon.

Alia, S., (2002)." Explanation of the Penal Code - General Section", A Comparative Study, University Foundation for Studies, Publishing and Distribution, Beirut, Lebanon.

Al-Mansour, M., (2012)."The Impact of Social Media Networks on the Audience of the Recipient", A Master Thesis in the Faculty of Arts and Education, The Arab Academy in Denmark.

Al-Miqdadi, K., (2013)."The Social Networking Revolution", 1st edition, Dar Al-Nafees Publishing, Jordan.

Al-Shawabkeh, M., (2018)." What is Hacker?", available on the website: https://mawdoo3.com

Alyan, R., (2003). "Communications and Educational Technology", 2nd edition, Safaa House for Publishing and Distribution, Amman.

Ibrahim, A. (2008). "General Rules in the Comparative Penal Code", 2nd edition, Al-Sanhoury Library, Baghdad.

Mahmoud, D., (2002)." The Simple in Explaining the Penal Code - General Section", 1st edition, without a publishing house, Baghdad.

Marwan, M.,(2020). "Search for social media", available on the website: https://mawdoo3.com.

McCawy, H., (2006)." Communication and Contemporary Theories", 6th edition, The Lebanese Egyptian House, Cairo, Egypt.

Mohammad, A., (2019)." Judicial Decisions, Iraqi Supreme Judicial Council website", Judicial Media, available at https://www.hjc.iq/view.

Mustafa, M. (1983)." Explanation of the Penal Code - General Section", 10th edition, Arab Renaissance House, Cairo, Egypt.

Nataga, (2011)."Definition and Importance of Administrative communications", available on the website: https://www.droit-dz.com/forum/threads/6915/

Rami, Z., (2003)." Using Social Media in the Arab World", No. 15, Journal of Education, Al-Ahliyya Amman University, Amman.

Rassool, K. & Ahmed, K., (1982)." Principles in Psychology", without a publishing house, Baghdad.

Sorour, A., (1981)."The Mediator in the Penal Code - General Section", Part 1, without a publishing house, Cairo, Egypt.

Laws and regulations

- The Universal Declaration of Human Rights issued on 10/12/1948.
- The International Covenant on Civil and Political Human Rights, issued on 16/16/1966.
- The Iraqi amended Penal Code No. (111) for 1969.
- The Constitution of the Republic of Iraq, 2005.