RELAÇÕES INTERNACIONAIS NO MUNDO ATUAL

CENTRO UNIVERSITÁRIO CURITIBA - UNICURITIBA - VOLUME 1 - NÚMERO 39/2023 I e-6434 I JAN-MARÇO I CURITIBA/PARANÁ/BRASIL - PÁGINAS 1 A 14 - ISSN: 2316-2880

CASE LAW REGARDING THE LEGALITY OF SOCIAL MEDIA CYBER-BLACKMAIL

Jasim Mohammed Hussein
dept. of law, AlNoor University College, Ninaveh, Iraq:
jasim.m@alnoor.edu.iq

Suhaba Nizar Nazem
Department of LAW, AlNoor University College, Nineveh, Iraq
suhaba.nazar@alnoor.edu.iq

ABSTRACT

Social media evidence (SM) is a relatively new and rapidly growing area of digital forensics. Criminal investigations may greatly benefit from the digital information trail left on social media if it is correctly analysed, especially in situations involving cyber-blackmail. It can be difficult to gather evidence from social media and show it in court, though. It is important to respect both the law and the individual's privacy while gathering social media evidence for cyber blackmail offences. Forensic investigators can conduct fruitful investigations and quickly gather legally reliable evidence if they are given sophisticated tools for controlling the quantity and variety of social media content. The present state of evidence gathering, admissibility, and jurisdiction on social media is studied in order to penalise individuals who engage in cyber-blackmail. In addition to examining Iraqi laws and regulations, the research also considers the difficulties courts today have while gathering, evaluating, presenting, and confirming social media evidence. Moreover, a review of the key elements of a lawsuit, including the case's purpose, the seriousness of the threats made, and the supporting documentation. A descriptive and analytical technique was used to analyse the issue, explain it in all of its aspects, and provide a diagnosis. As a result, we discovered that, in order to prevent cyber-blackmail, the court investigator may run into difficulties because of a legal loophole and a lack of resources for gathering digital evidence in the social media sector. Important aspects of cyber blackmail, such as its scope and character, were also made clear by this study.

Keywords: Cyber Blackmailing, Social media, Evidence, Investigation, Penal Code, Digital.

I. INTRODUCTION

Due to the fact that crimes using computers and other kinds of information technology can take many different forms and be carried out in many different ways, it might be difficult for investigators to look into crimes such as cyber-blackmail and offer digital proof of these crimes. Because of this, law enforcement must work harder and train more to identify fresh evidence from cyber blackmail crime scenes, especially digital evidence, and verify it in forensic evidence to find the offenders.

This research is crucial because of the law's stringent application and high recognition of digital evidence, especially given these offences' unique nature. Cyber blackmail crime need specific technological skills in order to search for evidence, and the discipline of computer forensics is still

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

young and difficult. Investigators have a hard time convicting these offences since the evidence can be deleted quickly. Due to inexperience in collecting electronic evidence, investigating, and prosecuting individuals, evidence may be lost.

Certain criteria need to be defined in order to demonstrate both the effectiveness of the implementation and the dependability of the digital evidence contained within the evidence.[1]

In order to provide evidence that a crime was committed, the purpose of this research is to identify and assess the challenges that are presented by executive activities. It also seeks to gather evidence of cyber-blackmail. This is due to the unusual character of the crime, which makes it necessary to collect evidence from the exact location where it was done. In order to do this, it is necessary to discuss and specify the many sorts of processes that must be followed for examination, research, and the gathering of digital evidence.

The challenges that must be surmounted include the elusive and complex nature of cybercrime as it manifests online and on computers, the difficulty of obtaining and analysing such evidence, and the questionable authenticity of digital evidence. The gravity of the crime, the magnitude of the damages, the rise in the number of cases, and the simplicity with which they are committed give cyber blackmail a special quality. The scope of executive authority to study and look into the crime of cyber-blackmail is another question.

II. CYBER-BLACKMAIL AND THE IDEA OF DIGITAL EVIDENCE

The term "digital evidence" encompasses a wide range of electronic records used in judicial proceedings “what experts deduce from results based on scientific applications and technical principles that follow several observations and sensory observations and by which these technical results are reached through mental deduction and control of science and its theories.” Another definition of it is "evidence obtained from computers in the form of electromagnetic or electrical impulses that can be collected and analysed using specialised programmes, applications, and technology and presented in the form of evidence that can be approved before the judiciary" or "information accepted by reason and logic and approved by science," produced through ethical and scientific means, such as by transforming existing storage data. Computers are used to establish a legal link between the victim, the offender, and the cyber-blackmail crime so that it may be prosecuted in a court of law.

Based on the description provided, cyber evidence may be thought of as "evidence obtained using software systems." In order to prove the existence of the crime and determine whether a person is innocent or guilty, the judge may also request the submission of written drawings or pictures created using computer programmes or apps in compliance with legal and technological requirements. It takes

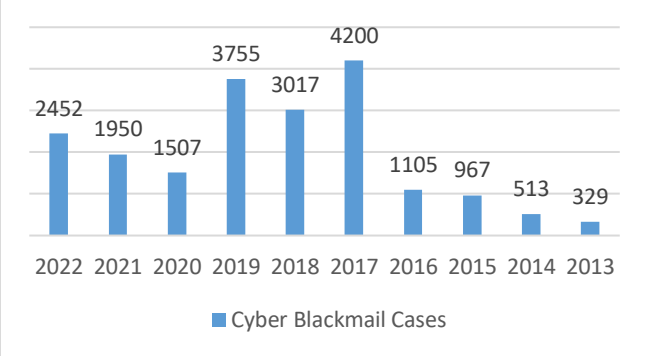
Relações Internacionais do Mundo Atual Unicuritiba.
[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

a criminal a record-breaking amount of time, on a computer or via the Internet, to alter computer programmes. In addition, it is possible for such evidence to be destroyed before it reaches the hands of the law, making it challenging to acquire physical proof because natural processes outweigh technological ones.

A. Cyber Blackmail Threats

When hackers demand money by threatening to release private information, this is known as cyber blackmail. It typically takes the form of distributed denial-of-service (DDoS) attacks and ransomware, both of which can render your company completely powerless. Fear and anxiety might be amplified because of the ease with which technology allows threats to be communicated to large groups of people under the guise of a fake or assumed identity. There are several meanings and variations of blackmail. For instance, among other things, using threats to harm someone's reputation, make someone look bad, or divulge "any secret that affects another person" to force a victim to perform against his will. The phrase "blackmail" is used to describe the illegal use of force, fear of physical damage, or threat of bodily injury to gain a valuable item from another person, as defined by the U.S. Sentencing Guidelines.

TABLE I. CYBERBLACKMAIL INCIDENTS IN IRAQ.



"Items of worth" include things like money, property, advantages, and even romantic relationships. Blackmail occurs when someone uses threats, either direct or implied, to coerce another person into giving them something of value. Threats used by blackmailers must be intended to "grab" or "acquire" something, rather than only deprive the victim of their rights or dispose of them. Threatening another person in order to illegally acquire their property "with his assistance" is known as blackmail. Professor Stephen Shafer, who is the Director of the John M. Olin Center for Law, Economics, and Business at Harvard Law School, said that the threats must be convincing enough for the people being threatened to think there is a good chance the threat will come true if they don't

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

cooperate. However, blackmail victims are more likely to be exposed to repeated demands from perpetrators, resulting in a long-term relationship of dependence and control.

1) Cyber-blackmail as Generally Defined

Cyber blackmail descriptions all include the offender's threat to commit an illegal act of violence against the victim if he doesn't cooperate. Determining what constitutes cyber blackmail as a crime is therefore crucial. Cyber blackmail is a crime that involves employing threats, unlawful methods, such as accessing a computer and collecting images or videos of a person, or the victim may have given the blackmailer the information in the first place. If we examine this term, we may deduce that the blackmailer demands payment in exchange:

"If a person is threatened and forced to pay money, service, or give up property, this is an assault. This explicitly refer to the rights to private property represented in money and property, as well as an attack on the individual's right to security and safety through the use of the threat element, which is supposed to be safe for the individual to his life and private property from assault." "The penetration of mobile phones, obtaining private correspondence, and threatening the person violates the confidentiality of correspondence and the sanctity of the private life of individuals guaranteed by the constitution."

B. *Lawsuit Side*

Cyberthreats and blackmail may take many various forms and contain a number of circumstances, allowing for a wide range of explanations as well as intriguing debates and points of view. The subsections that follow go over several topics related to threat actuality and purpose.

1) *The Role of Intention in Lawsuits*

Since intention spans a wider range and cannot be restricted by a rigorous composition of its meaning, it cannot be adequately described in a strict and limited sense. The conscious application of one's mental faculties to an action with the purpose of achieving a particular end is known as an intention. The concept of "intention" refers to the mental attitude that anticipates and desires the possible outcomes of one's actions. To intend is to have a definite aim of achieving the desired objective. It should be noted that foresight is necessary for intention to exist since a man must make a decision that pleases him and foresee the target of his declared aim. Once more, a man cannot mean to accomplish something that he does not want to. Only when someone is psychologically culpable at the moment of the conduct does criminal liability arise. Four different categories—purpose,

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

knowledge, recklessness, and negligence—are used to describe intent under the United States Model Penal Code (in descending order of guilt).

2) *Actual Threats as a Component of a Lawsuit*

The majority of statutes stipulate that no law limiting free speech may be introduced. Speech that incites crime, employs obscenity or defamation, contains child pornography, conducts fraud, makes genuine threats, or is not a required component of illegal behaviour is not protected. These issues have been carefully examined by several legal professionals. The Public Prosecution Office cannot prosecute speech for being violent or offensive. "Vengeance" doesn't always mean violating the law. The support of a political statement that "threats, nevertheless, must be defended" is one example of how the harm that threats might cause may contribute significantly to the situation's complexity. Individuals are safeguarded against "fear of violence" and "fear-related disruptions," as well as "the potential of the threat of violence" by outlawing true threats.

III. THE CREATION OF SPECIAL INVESTIGATION PROCEDURES

Due to cyber blackmail crime's unique components and tactics, several penal lawmakers in nations have had to rethink a number of procedural concerns, especially those relating to investigation and prosecution, the law's main themes. Because this crime requires technological evidence, traditional investigation and evidence procedures cannot be employed. The conversation that followed addressed modern cyber blackmail investigative methods.

A. *Cyber-Based Infiltration Techniques*

Article 20 of the United Nations Convention against Transnational Organized Crime aggressively includes this strategy, as do the majority of existing cybercrime legislation throughout the world, which call for the disclosure of unique research and investigation methodology. For those "secret efforts" you spoke about, what exactly is the invasion that you mentioned? Most laws describe a leak as "the judicial police officer responsible for monitoring the operation to monitor people suspected of committing a crime or misdemeanour by notifying them that they are an actor or a participant in the operation to monitor them."

In order to actively contribute to the operation of the criminal cell into which they have been infiltrated, it is often necessary for a judicial police officer to help or engage in infiltration, as indicated by the specified requirements. Additionally, it is used to carry out illegal deeds in order to achieve the overall goal of the operation; in certain cases, admittance into the cell may even include performing

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

such deeds. For this reason, neither the officer nor the reported help may be held legally liable for any illegal acts that may have been taken after the leak.

B. ***Communications monitoring and cyber surveillance***

Legislators have lately been aware of the many challenges of expanding traditional interception and surveillance processes to include correspondence due to the extensive use of new communication methods by individuals and organisations and the abuse of information networks. Several countries have added procedural laws to manage this practise due to the expansion of information networks.

The 1991 Criminal Procedure Act was revised by the French lawmaker to include wiretapping and monitoring internet communications in criminal investigations. Following the amendments made to the Federal Procedural Law of the United States in 2000, the American Congress similarly extended the scope of application of the objection and control procedure to embrace all types of communications. The European Convention on Cybercrime 2001 recommended that all Member States incorporate the interception of correspondence and electronic communications monitoring into their procedural laws due to the efficacy of this strategy in locating evidence and demonstrating cybercrime. 16 The European Parliament's Committee of Experts designated communication interception as "technical investigation" during its Strasbourg conference to discuss technical investigation and terrorism “the process of monitoring the confidentiality of telecommunications, as part of the search, investigation of crime and the collection of evidence. Information about persons suspected of committing or participating in the commission of a crime.” Without the knowledge or consent of others who could be impacted, secret technical arrangements may be used to eavesdrop, gather, install, broadcast, and record data transmitted or talks performed by the suspect in specified or confidential in private or public settings.

If eavesdropping telecommunications without owners' consent has proven useful in discovering and establishing numerous nebulous crimes like cybercrime, it is also a major infringement of privacy and a brazen attack on correspondence secrecy. Constitutions and penal codes safeguard their interactions. The objection procedure is limited by legislative limits to prevent public officials from abusing their power and to protect individual freedom. We list the following in summary:

1) ***Getting the appropriate court authority's approval:***

If written and reasoned authorization is acquired from the appropriate judicial authorities during preliminary inquiry or the investigating judge during judicial investigation, the law allows intercepting

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

or monitoring correspondence. Only the judiciary may authorise this process, which guarantees its legitimacy.[13]

2) ***The justification for using correspondence monitoring or interception must be clear:***

It indicates that there is a good reason to monitor or intercept correspondence as well as the pressing need to do so. This is important since it would be impossible to conclude the inquiry and investigation without using this technique. In order to determine whether or not the operation in question violates the principle of the sanctity of private life, a qualified investigating judge must weigh the operation's anticipated benefits against the costs of conducting it, as well as the severity of the underlying causes, the nature of the crime, and the identity of the perpetrators. If the supplied justification is insufficient, the request for authorisation will be turned down.

3) ***Identification of the relevant offences and control:***

Intercepting and monitoring electronic correspondence for investigative purposes is only allowed in drug and organised crime cases. Money laundering, extortion, exchange laws, corruption, and automated processing system crimes were transnational crimes.

4) ***Procedure confidentiality and professional confidentiality:***

To maintain professional confidentiality, the suspect and property owner should not be informed of the interception or monitoring.

IV. DATA INFORMATION PROVIDERS

When conducting an investigation, ISPs must search for and analyse any and all customer-related information data, with the exception of information or materials already in their possession. Article 18 of the Budapest Convention on Combating Information Crimes addressed this technique and included the phrase "Order to furnish information data." It mandated that each Convention party adopt the legislative procedures and other measures necessary to enable his competent authority to order:

1- Data that each individual has on hand, has saved to their computer, or has stored in a data storage device is sent.

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

2- Any service provider that carries on business within the territory of that party for the purpose of transmitting information on subscribers and the services they use that are in such party's custody or control.

V. TECHNICAL EXPERTISE

Investigating cyber blackmail requires a high degree of scientific and technical skills and qualifications since it is committed in an environment that is entirely scientific and technological. As a result, it renders investigators unable on the one hand and exposes their inexperience and lack of expertise in the field on the other. As a result, it is essential that those in charge turn to the hiring of specialists in this technical area. A method called "experience" seeks to leverage a person's scientific and/or technical talents, which the judge or the investigator do not have, in order to find proof of the crime's real commission or proof against the accused.

As a result of recent technological advancements in media and communication, the number of distinct types and models of computers and networks, in addition to the sciences and techniques related to them, have evolved into scientific and technical disciplines. This has led to an increase in the need for specialists to investigate cases of cybercrime. Accurate and sophisticated, and advancements in their sectors happen so quickly and sequentially that it could be challenging for the expert to keep up with and comprehend them. One may even assert that there is still a lack of experts in Iraq who have a thorough understanding of different kinds of networks, programmes, and computers and are competent to handle crimes of all kinds. Legislators therefore grant the investigator total discretion at any point in the probe, and he will hire a technical specialist to supplement his knowledge.

Therefore, one of the contemporary methods of inquiry is to employ investigators with technological competence. It has been proposed that the lawmaker take steps to teach competent officials by sending them to nations with strong standards and effective instruments to combat cyber-blackmail crime and gather digital evidence.

VI. THE IMPORTANCE OF SOCIAL MEDIA-BASED DIGITAL EVIDENCE

The searches and investigations now being conducted by the appropriate authorities are insufficient to produce evidence and present it to the court. A person's guilt or innocence cannot be determined based just on evidence that a crime was committed and that a particular person committed it; rather, the evidence must be convincing enough to be admitted as evidence in court. [17]

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

The legal value of evidence depends on its authority, legitimacy, and persuasion of the criminal court. After identifying cyber evidence, we must determine its legal significance by fulfilling two conditions. The evidence's legality must be established as the first condition. In terms of the second criteria, the judge recognises the comparable laws evidence's authority as proof.

A. ***Evidence from social media used in court cases***

Using social media as evidence in criminal proceedings is increasingly a regular practise. Therefore, online content is increasingly being used as evidence in court cases. OSN data is used by both the prosecution and the defence. The process for requesting a subpoena from social media corporations to obtain access to protected social media data is more difficult for defence attorneys. They therefore primarily rely on the fact that the data is available.[19]

Criminal cases including murder, abduction, and cyber blackmail have been seen to employ social media evidence. In United States v. Abrahams, the defendant remotely controlled the webcams of the victims without their knowledge in an effort to conceal his identity and gather explicit images and videos. In order to get more explicit images or videos from the victims, the offender threatened to publicly disclose the compromising content on their social media accounts. As a result, a court ruling was based on evidence from social media. By printing and exhibiting the photographs in court, the defence attorney showed through social media evidence that Abrahams had posted images on social networking sites.

B. ***The Legality of Acquiring Digital Evidence***

To be accepted as evidence, digital criminal evidence must generally be obtained lawfully, which requires that the party in charge of gathering the evidence follow the rules set forth by the law. When deciding whether or not a piece of criminal evidence is admissible, consideration must be given to human rights declarations, international charters and agreements, standards of public order and good morals in society, as well as other legal precedents.[21]

In addition, procedural legitimacy is the link that guarantees the accused's personal freedom by establishing that the law is the source of procedural regulation, that the accused's innocence is presumed in each proceeding brought against him, and that judicial protection is available throughout the proceedings. Considering that it is the external framework within which the objective norm cannot be successfully applied, it is actually far more dangerous and important than it is.

This shows that procedural legitimacy rests on three pillars: the presumption of innocence for the accused; a provision in the Code of Criminal Procedure; and the Penal Code, which establishes

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

that there are no crimes or punishments other than those set forth in the Penal Code. The second prerequisite for criminal legality is established by the Code of Criminal Proceeding, according to which there cannot be a procedure in the absence of a text.

The necessity that the court oversee all procedures is the third component since it is the legitimate custodian of rights and freedoms. This section's consideration of the legality of the digital evidence will be limited to the reasons behind its gathering. We may assert that due to the distinctive nature of evidence, the legal issues raised by digital evidence in terms of its acquisition are mostly focused on the inspection processes surrounding the legality of seeking for and controlling digital evidence in a virtual environment. More analysis is provided in the parts below, which use this as their starting point:

1) The Legality of Finding Digital Evidence Online and Managing Its Content

In the case of Iraq, The problem of checking computer hardware is not seen as a barrier to the investigation in cyber blackmail crimes, according to the basic provisions in the Code of Criminal Procedure. In accordance with Article 74 of the aforementioned law, the investigating judge was given permission "if it appears to him that there are items or papers that facilitate the inquiry of a person..." We propose altering the wording of the aforementioned article by adding electronic data to the text of article 74 since it is clear from the provisions of this article that the logical components do not come within those requirements. Thus, the text becomes “if the investigative judge finds that there are electronic objects or data or papers that benefit the investigation.”[22]

The study also backs up the first-opinion philosophy, according to which a remedy must be appropriate for the type of online crime. Digital evidence may be trusted to demonstrate that the crime actually occurred, and it can be trusted whether it is presented digitally or on paper. This point of view was taken into consideration by the Iraqi politician who was responsible for drafting the Information Crimes Law for the year 2011, which permitted digital evidence to be submitted to the court in either electronic or paper form.

2) The inspection's legality in light of where the device being inspected is located

When doing a search utilising the Internet as a virtual medium, this virtual medium makes a determination about the location of the device based on rules governing house inspection. However, the concern that emerges in this situation is what would happen if the information system's terminal end extends to a house other than the accused's home? Can it in this situation be searched? By allowing the examination, certain legislation, like the Dutch law, have addressed this problem.

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

According to the analysis, this rule cannot be enforced in accordance with Iraqi law because of the unique character of this examination. As a result, it cannot be employed unless the person performing the search has permission to search someone other than the accused or his residence. In point of fact, it suggested that the significance of the search extended to someone other than the one who was being charged.

C. *Position of the Law Regarding the Integrity of Digital Evidence*

Digital evidence has been categorised and given legal weight by several comparable legislatures, such as the American Legislature. The Iraqi legislature has been applying the main standards of criminal proof to digital evidence in an effort to decipher this manual and make up for the legal gaps it contains. By contrast, the criminal judge in the Latin system actively weighs the reliability and persuasiveness of witnesses before rendering a verdict based on the conviction he has derived from the evidence presented to him.[23]

The Iraqi politician said that the fundamental rules of the Code of Criminal Procedure applied to this type of evidence, rather than being governed by a distinct body of law. According to these regulations, the Iraqi parliamentarians' definition of criminal proof is “The court shall rule on the case based on the conviction it obtains from the evidence presented in any of the roles of the investigation or trial, which includes the confession, witness testimony, the investigation’s minutes, and other official statements, expert reports, technicians, clues, and other legally established evidence.”

Some Iraqi legal scholars argue that the first part of Paragraph A of Article 213 is contradicted by the second part, which states that "The court decides on the basis of its convictions," and thus limits the evidence that can be used to find a defendant guilty. This includes confessions, testimony, investigation logs, other official statements, expert reports, and so on. If that's the case, it's much more obvious considering that the lawmaker from Iraq used the phrase "further legally proven proof" to conclude the piece. Evidence that is required by laws or regulations is referred to here. In addition to the data presented in the preliminary or judicial investigation.

D. *Position of the Judiciary Regarding the Authenticity of Cyber-Evidence*

The Iraqi judiciary's stance on the subject has not been steadfast. The appropriateness of this evidence, its relevance to the decision, and its absence have all been under dispute. What occurred was in accordance with the judgement rendered by the Karkh Federal Appeal Court No. 120/Criminal Code/2011, which upheld the judgement rendered by the Court in the penal file No. 103/c/2011 on March 16, 2011. After the victims begged him to spare them, the Karkh Federal Appeal Court in

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

Baghdad accepted the admissions of an accused who identified himself as a "fighter in cyber-extortion crimes" on a private website for him. He was found to be using social media to threaten and blackmail young women. His computer was searched for digital evidence, including images and chats, and the court accepted the defendant's admission that he had blackmailed a youngster in return for money. According to the guidelines of Article (456) of the Iraqi Penal Code, the competent court has commenced all legal proceedings against him.

VII. CONCLUSION

An extensive investigation of the phenomena of cyber-blackmail has been given in this article. By providing a complete examination of cyber blackmail, its history, the side of the most significant litigation, and the digital evidence produced from them, the article helps the reader better comprehend the issue. This examination covers a variety of subjects, such as the importance of digital evidence in court proceedings, how it is handled by the Iraqi legal system, and novel approaches to the study of cyber-blackmail. The digital evidence gathered by the perpetrator of the electronic extortion crime was taken from the offender's tools of crime or from mobile phone carriers. The judicial investigator's legal acquisition of the digital evidence is required for it to be considered authentic in the evidence. The comparative laws and the legislation from Iraq enabled for the examination of the moral elements. Jurisprudence has disagreed on how to define the word "item," nevertheless, and whether it should be limited to material evidence or also contain moral evidence. The item that incorporates both material and moral proof, however, is what is considered to be the accurate view. In light of the fact that digital data may be physically obtained from computers and used as evidence, we endorse this tendency.

This kind of evidence is not governed by a specific law passed by the Iraqi legislature. Neither Evidence Law No. 107 of 1979 nor its new amendment issued under Law No. 46 of 2000 make any mention of regulating the provision of electronic evidence obtained from social media, with the exception of the fact that it is permitted in both Article 104 of the Evidence Law and Paragraph A of Article 213 of the Code of Criminal Procedure that the judge may benefit from the means of scientific inquiry.

The research found that the insufficiencies of criminal procedural procedures in dealing with cyber-blackmail crimes are linked to gathering evidence and demonstrating crimes done using mobile phone. The efficiency of digital evidence in demonstrating these crimes was also demonstrated, since the difficulties with cyber-blackmail crimes stem from their connection, frequently, to ephemeral data and information that is difficult to recover after deletion. Depending on the circumstances, it may be next to impossible to gather evidence from photographs, recordings of conversations, or videos taken

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

during the commission of such crimes because of the speed and precision with which they are committed and the possibility that the perpetrator will attempt to erase all traces of the crime and conceal any evidence.

In the absence of specific laws against cyber blackmail, improving existing laws, exchanging information and resolving legal issues through specialised investigation and inspection systems, and giving competent authorities individualised training are the greatest answers to the system's problems. To combat crime, better oneself, and improve institutions, all of these things are done via true cooperation. Cyber blackmail investigation and prosecution procedures call for tracing the paths of the crime from its inception to execution and calculating the targeted harm through a number of Internet service providers or businesses that enable such crimes. In order to identify the perpetrator across multiple nations and determine the origin of the crime, services with computer connections to the Internet and competent systems must monitor the impact of communications with source computers, the victim's device, or other devices. They may also work with Internet service providers or telecom service providers.

This article outlined the most important treaties and novel ways in which countries might work together to prevent cyber-blackmail. International or judicial cooperation agreements can be used to help colleagues in other jurisdictions who are involved in cross-border cyber-blackmail offences, which will help reduce crime. The investigation of the crime and the assistance in catching the offender also require cooperation between other police departments. The crime of cyberblackmail, which resulted in the development of a number of international treaties in this field, should also receive special attention from the UN and the majority of international organisations.

REFERENCES

Khaled Mamdouh Ibrahim Muhammad, Information and electronic crimes, a study of information crime in the Knowledge Library, (City: Egypt, 2021), 7.

Kancauskiene, J. (2019). Computer Forensics and Electronic Evidence in Criminal Legal Proceedings: Lithuania's Experience. Digital Evidence & Elec. Signature L. Rev., 16, 11.

Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. Journal of Forensic, Legal & Investigative Sciences, 6(1), 1-8.

Cyber Extortion and Threats: Analysis of the United States Case Law

Robert, E. (2021). Attempting a definition of cyber crime. Available at SSRN 3830589.

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice, 46(6), 837-842.

Eichensehr, K. (2021). Cyberattack Attribution as Empowerment and Constraint. Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper, (2101).

CRIMINAL PROCEDURE CODE 23 OF 1971

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]

Warnock, D. (2010). The Iraqi criminal justice system, an Introduction. Denv. J. Int'l L. & Pol'y, 39, 1.

Drumbl, M. A. (2006). The Iraqi High Tribunal and Rule of Law: Challenges. In Proceedings of the ASIL Annual Meeting (Vol. 100, pp. 79-83). Cambridge University Press.

Dammer, H. R., & Albanese, J. S. (2013). Comparative criminal justice systems. Cengage Learning.

Cyber Blackmail on Social Media and its Authenticity through Criminal Evidence

Kareem, A. F., & Wahidshihab, L. A. (2021). ELECTRONIC EXTORTION AND ITS IMPACT ON UNIVERSITY FEMALE STUDENTS. Review of International Geographical Education Online, 11(10).

Mamade, B. K., & Dabala, D. M. (2021). Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs. Journal of Cyber Security and Mobility, 699-724.

Lazarus, S., & Button, M. (2022). Tweets and reactions: revealing the geographies of cybercrime perpetrators and the North-South divide. Cyberpsychology, Behavior, and Social Networking, 25(8), 504-511.

Agara, E. P., Ojong, F. E., Emeka, J. O., Agba, A. O., Akintola, A. I., & Ogunsola, O. V. (2021). Social media Platforms: Exposing students to cybercrimes. ARRUS Journal of Social Sciences and Humanities, 1(1), 44-54.

Ennin, D., & Mensah, R. O. (2019). Cybercrime in Ghana and the Reaction of the Law. JL Pol'y & Globalization, 84, 36.

Awoyemi, B. O., Omotayo, O. A., & Mpapalika, J. J. (2021). GLOBALIZATION AND CYBER CRIMES: A REVIEW OF FORMS AND EFFECTS OF CYBER CRIME IN NIGERIA.

Thukral, P., & Kainya, V. (2022). How social media influence crimes. Indian Journal of Law and Legal Research, 4(2), 1-11.

Ukwuoma, H. C. (2021). Cybercrime: An Emerging Threat to Economic Development in Nigeria. International Journal of Cyber Research and Education (IJCRE), 3(1), 16-27.

Mahmood, I. S. (2020). Are Cyberbullying Interventions and Criminal Law Prevention Effective?(A Review of Cyberullying Legislation in Iraq). PalArch's Journal of Archaeology of Egypt/Egyptology, 17(7), 16983-16998.

Ambika, T., & Senthilvel, K. (2020). Cyber Crimes against the State: A Study on Cyber Terrorism in India. Webology, 17(2), 65-72.

Kovács, L. (2018). National cyber security as the cornerstone of national security. Land Forces Academy Review, 23(2), 113-120.

Ijeh, A. C. (2021). Is it a Cyber Security Strategy for Social Development?. In Crime Science and Digital Forensics (pp. 202-217). CRC Press.

AbdulAmeer, S. A., Saleh, W. R., Hussam, R., Al-Hareeri, H., Alghazali, T., Mezaal, Y. S., & Saeed, I. N. (2022). Cyber Security Readiness in Iraq: Role of the Human Rights Activists. International Journal of Cyber Criminology, 16(2), 1-14.

[Received/Recebido: Agosto 23, 2022; Accepted/Aceito Dezembro 21, 2022]