Journal of Infrastructure, Policy and Development 2024, 8(13), 8108.
https://doi.org/10.24294/jipd8108

Article

The crime of cyber blackmail in the era of artificial intelligence

Omar Abdulsalam Hussein*, Nazura Abdul Manap

Faculty of Law, Universiti Kebangsaan Malaysia, Selangor, Bangi 43600, Malaysia
*** Corresponding author:** Omar Abdulsalam Hussein, omar_almuooa91@yahoo.com

CITATION

Hussein OA, Manap NA. (2024). The crime of cyber blackmail in the era of artificial intelligence. Journal of Infrastructure, Policy and Development. 8(13): 8108. https://doi.org/10.24294/jipd8108

ARTICLE INFO

Received: 20 July 2024
Accepted: 12 September 2024
Available online: 8 November 2024

Abstract: Cyber blackmail is defined as a transgression which occurs when an individual or group intimidates the victim by threatening to expose his/her personal information on social media. This form of criminal activity, which has emerged with technological advancement, particularly in the artificial intelligence (AI) domain, is not confined to any specific region or nation. The unrestricted reach of cyber blackmail necessitates the constant revision and evaluation of the laws regulating it so that these laws maintain their effectiveness when changes occur in the manner in which this offence is committed. This study comparatively analysed the validity of current cyber blackmail laws in Iraq and Malaysia through discussions emphasizing the association between cyber blackmail and AI, as well as the rules and regulations formulated to curb this crime. The systematic, comprehensive and comparative method employed for this study scrutinized the issue of cyber blackmail from all perspectives. It revealed that the will of Iraqi authorities falls short when it comes to the implementation of effective measures aimed at reining in the prevalence of cyber blackmail. These measures included reviewing the penal code or drafting laws directed at combating IT crimes. The crime of cyber blackmail involves the instilling of anxiety in the victim, with the purpose of compelling him/her to succumb to the demands of the blackmailer. We conclude this study with proposals aimed at curtailing the occurrence of cyber blackmail.

Keywords: artificial intelligence; crime; cyber blackmail; information law; legislation

1. Introduction

While advancements in the field of technology, particularly in the context of artificial intelligence (AI), have served to improve the lives of people worldwide (including in the areas of productivity, social interaction and health), it has resulted in the rise of the threat commonly referred to as cyber blackmail. Taking advantage of technological advancements, the perpetrators of this crime gain access to the victim's confidential as well as revealing information (including in the form of texts or photographs) and threaten to publicize them if he/she does not succumb to their demands. Women are more frequently targeted for cyber blackmailing due to the perception that women are more submissive to extortion, especially when faced with threats that might damage their reputations (Al-Habsi et al., 2024; Alisawee, 2019; Hussein, 2023; Hussein et al., 2022; Mekkawi, 2022).

Though cyber blackmail entails the threat to publicize sensitive private information on social media, sextortion specifically involves the threat to expose the private sexual activities of the victims if the demands of the perpetrator are not met (Edwards and Hollely, 2023; O'Malley and Holt, 2022; Uma, 2017; Wang, 2024). Thus, it can be surmised that cyber blackmail perpetrators misuse AI to conduct their criminal activities in a more

diversified and innovative manner (Al-Najjar, 2024). With this technological advancement, perpetrators can engage in big data and deep learning to garner confidential and revealing information regarding an individual (Dai and Boroomand, 2022; Nienhaus, 2021). Armed with this information, the perpetrators can then develop convincing false details regarding the targeted victim, which serve to promote the realization of the perpetrators' objectives. The threats linked to cyber blackmail escalate proportionally with the technological expertise of the perpetrators. The perpetrator's competence in analyzing an individual's behavior is crucial for achieving a successful cyber-blackmail outcome (Al-khaza and Lahiani, 2023; Hayward and Maas, 2020; Wang, 2024).

Law enforcement agencies can minimize the use of AI by cyber blackmail perpetrators through examining online behavioral patterns and devising effective techniques for detecting and apprehending them.

This investigation highlights the intricate relationship between AI and cyber blackmail while providing information regarding the use of AI to combat cyber blackmail and the exploitation of AI for the development of this criminal activity (Al-Najjar, 2024). This study also covers a comparative analysis of the laws introduced for curtailing cyber blackmail in Iraq and Malaysia and the instances in which AI was successfully applied to combat this crime. The essence of the comparative analysis, is to highlight the fact that while Iraq focuses on traditional existing legislation in dealing with cyber blackmail, Malaysia has gone a step by addressing cyber blackmail within the crime of extortion as done by other advanced countries like the United States. Essentially, this study provides researchers, policymakers and the general public with a better comprehension of the complicated relationship between AI and the crime of cyber blackmail (Hayward and Mass, 2020).

2. Characteristics of cyber blackmail and artificial intelligence (AI)

The features, forms, and concepts associated with cyber blackmail and AI are discussed in this section. The expression 'blackmail' can be linked to several illegal activities. It can involve an attack on the integrity of an individual, the threat to disclose damaging personal information, or actions aimed at compelling an individual to perform or to abstain from performing an activity (Vasiu and Vasiu, 2020; Vasiu and Vasiu, 2020a). Under the US sentencing guidelines (USSG), 'blackmail' is defined as the unjustifiable use of force, fear of physical harm or bodily injury, with the purpose of acquiring something of value from an individual, including money, property or sexual favors (Mekkawi, 2022; Vasiu and Vasiu, 2020).

The act of delivering a threat aimed at convincing the potential victim that his/her status, possessions, social standing, personal/professional safety, or self-worth may be in jeopardy is regarded as the crime of blackmail. However, for such threats to be considered blackmail, they need to extend beyond the removal or eviction of the victim from the property and highlight the acquirement of the property from the victim. In the context of blackmail, a crucial factor is the acquirement of property from an individual, with his/her 'consent', through the issuance of criminal threats (Sulkowski, 2007).

In terms of female cyber blackmail victims, the approaches employed by the perpetrator often include the threat of defamation or the exposure of embarrassing information to the victim's family members. The use of this approach is aimed at compelling the victim to submit to the perpetrator's demands, whether in the form of sexual favours or items of value (Alisawee, 2019; Hussein, 2023; Shafaq, 2023; Spiezia, 2022). More often than not, the victims of cyber blackmail are subjected to repeated demands from the perpetrator, leading to an extended domination-submission relationship. Among the threats issued by cyber blackmail perpetrators to force victims into submission were those associated with damage to property or reputation, the publicizing of slanderous images and videos, as well as the delivery of fabricated allegations (Abdulhameed, 2021; Mekkawi, 2022; Sulkowski and Shea, 2018).

The perpetrators of cyber blackmail are also capable of creating their own methods of acquiring explicit content. In the United States v. Antonio P. Fontana hearing, for example, the defendant, impersonating a juvenile on a chat service, convinced the victim to strip off her blouse. He then proceeded to capture the act on video covertly and threatened to post the video on social media, if she refused to enact increasingly lewd acts, which he also recorded, to consolidate his status as the blackmailer.

In Iraq, the defendant, Ahmed, was put on trial for using malware and other technology to operate a remote control device for the purpose of manoeuvring the cameras of his victims, and capturing lewd images and videos, which he threatened to post on their social media accounts if they refused to deliver more images and videos of a similar genre (Republic of Iraq v. Ahmed, 2021).

Generally, researchers describe AI as the study and design of intelligent systems that understand their environment and initiate actions that enhance their chances of success. John McCarthy, who coined the term AI in 1955, describes it as "the science and engineering of making intelligent machines" (Hayward and Maas, 2020; Scientists, 2022, p. 1).

Over recent years, AI technology has progressed by leaps and bounds, with the concept of deep learning representing its most significant contribution. Deep learning involves the development of artificial neural networks that imitate the manner in which the human brain functions. Put simply, these artificial neural networks come with the capacity to independently experiment, learn, and develop themselves without human assistance.

The proficiency of deep learning technology in the areas of speech comprehension and language translation, among others, has prompted research-related investments from American establishments in Silicon Valley, particularly Facebook and Google, despite alerts that the development of AI may contribute substantially towards the future irrelevancy of a human workforce (Claussén-Karlsson, 2017).

A separate concern is the potential of AI for the future execution of criminal acts. In this context, criminal acts are expressed as all acts (or exclusions) representing a criminal offense under English criminal law, without reduced generality, with regard to the jurisdictions which similarly define a crime.

Proof of AI-crime (AIC) was derived from two previously conducted (hypothetical) research tests. In the initial test, Seymour and Tully (2016), a pair of computational social scientists, utilized AI as a tool to persuade social media users to click on phishing links within mass-generated messages. Each message was fabricated using machine learning algorithms that analyzed individuals' established behaviors and public profiles. The content of each message was personalized for each individual, obscuring the intent of each communication.

In a real-world setting, the clicking on the phishing link and the subsequent completion of the web form by the potential victim would leave his/her personal and confidential information open to extraction by a criminal and exploited for the purpose of embezzlement. In the next test, the simulation of a market by a trio of computer scientists revealed the possibility of trading agents learning and carrying out a lucrative market manoeuvring operation involving a series of fraudulent fictitious requisitions (Martínez-Miranda et al., 2016). As these two tests indicate, the emergence of AI gives rise to AIC (King et al., 2020), which is evidently a workable and basically original threat.

2.1. The effect of artificial intelligence (AI)

2.1.1. Led to the evolution of blackmail crime

The influence of AI is evident in many sectors, including the law enforcement division. Although advanced algorithms and predictive analytics have aided police agencies in their battle against crime, there is a drawback. These technologies may also be exploited by criminals to engage in illegal activities. The capacity of AI to analyze extensive data loads facilitates the identification of patterns, trends and anomalies which may not be perceived by human analysts (Djenna et al., 2023; Oh et al., 2024; Thakker and Japee, 2023). This circumstance can prove to be beneficial for both law enforcement agencies as well as criminal organizations. The prevention and detection of criminal activities are among the main roles of AI in crime management. In this study, the contribution of AI is discussed in terms of crime control, as well as the committing of crimes.

2.1.2. The automatic generation of cyber blackmail messages

A frequently employed cyber blackmail scheme entails the programmed generation of cyber blackmail messages through AI procedures. Following data analysis, the configuration of fruitful messages was learned, and the configuration was subsequently exploited for the generation of personalized messages destined for prospective victims on the receiving end of cyber blackmail. Fraudsters utilized technology such as automatic text creation and deep learning (Djenna et al., 2023a; Djenna et al., 2023b; Kamińska et al., 2021) to create persuasive communications with the intention of exploiting the vulnerability of their victims (Ibrahim, 2021).

2.1.3. Fake threats and confusion

Among AI strategies employed to deceive victims into surrendering personal or financial details is the creation of false identities or accounts (Light, 2021; Velasco, 2022).

Smart technology can also be harnessed for the purpose of confounding protection systems and skirting authorized security installations.

2.1.4. Identify behavioral patterns

Owing to its capacity for online behavioral pattern analysis, AI can be utilized for the identification of factors with the greatest potential, for susceptibility to blackmail. This is a process involving user behavior analysis, the use of the resulting data to target potential victims, and the development of dependable extortion schemes (Chiancone, 2023).

2.1.5. Advanced cyber attacks

AI can be exploited to launch high-tech cyberattacks, which include identity fraud and invasive hacking (Djenna et al., 2023a). Through deep learning and intelligent analysis techniques (Erdélyi and Goldsmith, 2022; Teo, 2023), AI systems learn from user behavior and analyze data to coordinate sweeping targeted strikes.

Generally, the motives for cyber blackmail are materialistic, monetary, psychological or emotional in nature. The targeted victim may be a stranger to the perpetrator, and the latter may not be aware of to the consequences of the crime on the life of the victim. In the context of cyber blackmail, the objective is usually financial gain, although there are also incidences where the perpetrator is driven by the need to cause psychological damage. In situations where the victim is known to the perpetrator such as in sextortion by intimate partners, the motivation for blackmail can be both monetary gain and the urge to cause the victim psychological anguish. According to researchers, victimization is more prevalent in intimate partner relationships (Bailey et al., 2020; Edwards and Hollely, 2023; O'Malley and Holt, 2022; Wang, 2024). Most frequently, this is due to the victim's rejection of the perpetrator's advances or the breaking up of the relationship between the perpetrator and the victim initiated by the victim (Abdulhameed, 2021; Al-Shamari, 2021; Djenna et al., 2023b; Wang, 2024).

The uniqueness of every extortion case calls for their separate management by law enforcement authorities. In terms of the cyber extortion victims, the shared consequence is the devastating and often long-term effects on their lives (Abdulhameed, 2021; Al-Masalha et al., 2020; Sancho, 2017). Cyber-blackmail is a crime that can lead to long-lasting psychological damage, suicides and honour killings, as well as negative effects on the victim's education goals, career prospects, and financial situation (Al-Habsi et al., 2023; Saleem et al., 2022; Salim and Dhafri, 2024).

Numerous blackmail-related crimes involving female victims have been reported by the Interior Ministry. For instance, Iraqi police apprehended 60 individuals who organized gangs to get hold of photos featuring teenage girls in embarrassing situations and blackmailing them into parting with their money or providing sexual favours (Hussein, 2023; Hussein et al., 2022). Cyber blackmail perpetrators frequently use AI to hack social media (Daoud, 2021) accounts (such as Facebook and Instagram) for the delivery of fraudulent messages or to hack smartphones to acquire unseemly photos or videos featuring potential victims of blackmail (Iraqi Council of Ministers, 2011).

In Baghdad, the Karkh investigation court recorded the confessions of members belonging to a set-up focusing on hacking social media sites to illegally capture pictures and duplicate electronic dialogues (Abdulhameed, 2021). This was committed for the purpose of blackmailing the owners of these sites, by threatening to publicize these damaging data on all social media platforms, if their demands were not met. Following the court hearing, these perpetrators of cyber blackmail were dispatched to the competent court in accordance with Chapter (c) 2, Section (§) 3, Paragraph (para) 430 of the Iraqi Penal Code No. 111 (1969).

In Public Prosecutor v. Mohd Zamri Mohd Yunus (2019), the defendant was pronounced guilty under § 507 of the Malaysian Penal Code for delivering a death threat to his former wife, Marina Ibrahim, via a WhatsApp message and sentenced to 3years imprisonment. In Public Prosecutor v. Chang Ye Siong (2019), a case of cyber blackmail was brought against the defendant when he threatened to reveal the lewd videos of his victim if the money demanded was not paid to him. The defendant was pronounced guilty under § 503 of the Malaysian Penal Code for threatening to distribute explicit videos featuring the victim (which he had recorded during a video call in September 2017) to members of her family. He was also found guilty under § 292 for being in possession of lewd videos on two mobile phones belonging to him on the 19th of December 2018 and got 10years terms of imprisonment as punishment.

2.2. The Role of Artificial Intelligence (AI)

2.2.1. Identifying potential victims

Artificial intelligence (AI) can be used to identify those susceptible to exploitation and extortion through the analysis of personal and behavioral data using deep learning schemes. The detection of weak spots in personal security and the analysis of behavior patterns by intelligent systems facilitate the identification of prospective victims and the preparation of personalized blackmail conspiracies (King et al., 2020).

2.2.2. Combating cyber blackmail crime

In terms of its positive impact on cyber security, AI can be harnessed for the development of innovative instruments and strategies, aimed at identifying, detecting and preventing online threats, as well as enhancing predictive analytics.

2.2.3. Enhancing crime prevention and detection

In the context of law enforcement, AI technology is employed to improve the systems associated with the prevention and detection of criminal activities. AI algorithms and machine learning approaches are currently utilized for scrutinizing extensive data loads, for the purpose of identifying crime-related patterns, predicting criminal conduct, and forestalling criminal offensives. The supervision of public spaces using AI-driven surveillance systems facilitates the early detection of illegal activities, and the recovery of crucial evidence for the prosecution of lawbreakers (Chiancone, 2023). Artificial intelligence (AI) technology can be harnessed to scrutinize data from different sources and detect concealed links that may escape the notice of human crime prevention analysts.

Artificial intelligence (AI) systems equipped with advanced algorithms can be applied to enhance criminal activity prediction by unravelling complex dataset correlations (Hung and Yen, 2023; Rajaee et al., 2020). This will serve to assist law enforcement agencies in terms of the allocation of appropriate resources, the identification of high-crime areas, and the proper deployment of personnel. Predictive policing based on AI also facilitates the identification of high-crime locations, paving the way for proactive crime prevention and the early implementation of community safety measures.

2.2.4. AI-based predictive policing

Predictive policing has developed into an effective law enforcement approach for the prevention of criminal activity. Using this approach, the engagement of AI facilitates the analysis of extensive volumes of data for the identification of patterns and tendencies, allowing the effective allocation of resources by law enforcement agencies for the proactive management of likely criminal activities. The emphasis on data analysis paves the way for a more focused and effective placement of police personnel, leading to an elevation in the level of crime detection and prevention (Correia, 2022; Jada and Mayayise, 2024). Among the main advantages associated with AI-driven predictive policing is the capacity to pinpoint the areas where the perpetration of criminal activities is highly likely. Armed with this information, law enforcement establishments can execute preventive strategies, including increased surveillance or targeted investigations, which will serve to curb the occurrence of criminal activities and consequently raise the level of public safety. Predictive policing, with the engagement of AI, has delivered encouraging results in terms of lowering the crime response time, which facilitates the quick intervention and prevention of crimes associated with cyber blackmail (Chiancone, 2023).

2.2.5. AI-powered surveillance systems: Balancing security and privacy

The capacity of the police force to detect potential law-breaking activities in public spaces is considerably enhanced by the employment of AI-driven surveillance systems (Fraga-Lamas et al., 2017; Wehrli et al., 2022). With these systems in place, the use of advanced algorithms and machine learning strategies facilitate the analysis of extensive data loads, covering video footage, audio recordings, and social media feeds. The automatic identification of suspicious activities and subsequent alerting of law enforcement agencies in real-time promotes these systems as effective approaches for the prevention of crime, as well as for the improvement of public security (Ibrahim, 2021).

2.2.6. Improving investigative processes through AI algorithms

The innovative data analysis and pattern identification procedures associated with the use of AI algorithms improve the efficiency and pace of the law enforcement investigation process. Among the significant contributions of AI algorithms in the investigative process is their capacity for analyzing extensive volumes of digital evidence (Djenna et al., 2023a; Hussein, 2023; Østerlund et al., 2021). The importance of this contribution is attributed to the increasing exploitation of digital devices and online facilities for the carrying out cyber blackmail. The need to sift through the massive

amounts of data generated by this activity is overwhelming for those involved in cybercrime investigations.

With their capacity for the quick processing and analysis of extensive data loads, AI algorithms can draw attention to crucial patterns and links which may otherwise escape the notice of cybercrime investigators. Other than reducing the investigation time, AI algorithms can be employed quickly detect vital evidence that can be used in prosecuting cyber blackmail perpetrators. Furthermore, the automation of several aspects of the investigative procedure reduces the impact of human error and partiality, consequently delivering a more precise and non-biased investigation outcome.

2.3. Collaborative efforts: Human and artificial intelligence (AI) partnerships in policing

It is evident that the policing performance of law enforcement agencies is enhanced by the collaboration between humans and AI (Jada and Mayayise, 2024). The merging of the unique traits associated with humans and AI accentuate their respective capacities for the effective curbing of cyber blackmail crimes through quicker response times and increased decision-making accuracy under stressful conditions. AI systems facilitate the effective processing and analysis of extensive data, including those related to surveillance tapes, criminal records, and social media feeds, for the quick identification of criminal activity patterns and possible threats (Ibrahim, 2021).

The findings, derived through the AI data processing and analysis system, are subsequently dispatched to human officials, who make the most of their experience, intuition, and judgement, to deliver informed decisions for the execution of an effective crime prevention response. Other than the time-saving benefit, this combined approach also enables law enforcement agencies to proactively identify and curtail the occurrence of criminal activities, for the realization of a more protected public living space.

3. Analysis

While the use of AI has proven to be effective in the battle against cyber blackmail, there are downsides to this technology that need to be taken into consideration. On a positive note, the engagement of AI, with its advanced algorithms and predictive policing approaches, can considerably improve police operations aimed at stemming the growing and complex threat of cyber blackmail. However, the collection and analysis of large amounts of data using AI systems to improve policing activities raises issues about privacy and confidentiality rights (Krishnamoorthy et al., 2023; Shankar et al., 2023). These concerns are mainly attributed to the possibility that confidential data may fall into the wrong hands and be exploited for blackmailing activities.

The achievement of an appropriate balance between security and confidentiality is essential, in terms of engaging the game-changing services available through AI, without conceding to the potential loss of civil rights and personal information. It should be noted that the theft of personal information can occur under the least likely circumstances. For instance, an Iraqi police officer was apprehended for exploiting the personal information

lawfully surrendered to him by individuals for the purpose of blackmail. He stood trial at the Rusafa criminal court and was charged under Article 456 of the Iraqi Penal Code and was found guilty by the Karkh Investigation Court in Baghdad.

Comparative analysis of the legislative position of Malaysia and Iraq on cyber blackmail crime

In Malaysia, the primary reference to the crime of blackmail is in Act 574 (1936):

> "*[A crime] committed by any individual who intentionally instils fear of harm, either to the individual or another person, and thereby manipulates the victim, in a deceitful manner, to surrender any property, valuable collateral, or anything signed or sealed, which can be converted into valuable security.*" (Act 574, 1936, c. 17, § 383).

While in Iraq, neither the Iraqi Penal Code No. 111 (1969) nor the sections referring to sentencing address the crime of cyber blackmail. However, the Iraqi judiciary, translators, and jurists are in agreement that this crime involves (a) an act of intrusion, which breaches the right to confidentiality (Penal Code No. 111, 1969, c. 3, § 2, para 452) and (b) an act that calls for the execution of an unlawful or immoral activity. The second element of cyber blackmail identifies it as a crime based on the issuance of threats, which is similar to the concept of conventional blackmail (Penal Code No. 111, 1969, c. 3, § 2, para 431). Thus, generally, in the context of threats, blackmail involves (a) the threat of bodily harm or (b) the threat of exposure in terms of issues or materials, which can be detrimental to the reputation of the victim.

As mentioned earlier, Malaysian law registers the crime of blackmail under the same category as extortion, in contrast with the law in the USA, which distinguishes between the two. But in the case of Iraq, the crime of extortion has not been made an integral part of cyber blackmail in any of its existing legislations. This is because, the existing applicable legislation in the country is still the traditional legislation on blackmail which does not recognize modern aspect of blackmail. Hence, it is argued that applying conventional laws for criminal acts that exploit modern technology can prove to be an arduous task. Due to its conception in 1969, the current specifications of the penal Iraqi code are inadequate in meeting the necessary conditions to classify cyber blackmail as a criminal offense.

Furthermore, in Malaysia, the definition of blackmail under the Penal Code Act 574 fails to clarify if the offence of extortion, during which the victim(s) undergoes feelings of fear or anxiety, needs to close with the dispensing of certain belongings, whether in the form of material possessions or documents. Furthermore, the perpetrator of the crime of extortion is liable to a sentence of 10 years in prison, a fine, and whipping, or any one of the last two penalties (Act 574, 1936, c. 17, § 384). Act 574 (1936) segregates the crime of extortion into several provisions (§ 385–389). One section defines extortion as the act of consigning an individual, or individuals, to the fear of death or severe bodily impairment, a crime punishable with up to 14 years in prison and a fine or whipping (Act 574, 1936, c. 17, § 385). On the other hand, in terms of the criminalization of cyber blackmail, the Iraqi penal code, to some extent, addresses this issue by defining the crime

of blackmail as any act that threatens, slanders, violates the privacy, discloses the confidences, smears, or blasphemes any man, woman, or child (Penal Code No. 111, 1969, c. 3, § 2, paras 430, 433, 437, and 452). Similarly, sexual favours, financial gain and revenge are all likely motives applicable for both regular blackmail as well as cyber blackmail. Thus, as the provisions currently stated in the Iraqi Penal Code do not specifically address cyber blackmail, new laws need to be enacted to address this recently detected criminal activity (Penal Code No. 111, 1969, c. 3, § 2, para 433).

In Malaysia, the perpetrator of extortion is any individual who consigns or makes an effort to consign another individual to the fear of death or severe bodily injury. Upon conviction, the perpetrator will be liable to a sentence of not more than 10 years in prison and a fine or whipping, as well as any other sentence deemed fit by the court (Act 574, 1936, c. 17, § 387 and 388). An individual who commits the crime of extortion against another by instilling the element of fear is liable to be sentenced to death, imprisonment of up to 20 years, or imprisonment for not more than 10 years. Any attempt by an individual to coerce another individual into committing a similar offence is liable to be sentenced to not more than 10 years in prison and a fine of not more than 10,000 ringgit.

Another section states that those who commit the crime of extortion or attempt to do so by instilling fear in the victims are liable to face the death sentence, imprisonment for a period not exceeding 20 years, or imprisonment for a period not exceeding 10 years. A conviction can also result in the additional punishment of a fine or whipping. A criminal act of extortion transpires when an individual intentionally subjects another individual to fear for the purpose of inducing him/her to part with his/her belongings, whether in the form of cash, property, or a document (Act 574, 1936, c. 17, § 389).

In Iraq however, the legislative gap on cyber blackmail was closed by bringing into play the penal code, which considers the issuance of threats as a crime as a means for cyber blackmail punishment. This is attributed to the general understanding that cyber blackmail involves the delivery of threats, intending to instil fear in the victim:

> "*Whoever threatens another individual to commit a felony against himself or his money, or against people and their money, or who does so through dishonourable matters or disclosures thereof, shall face a sentence of imprisonment for a maximum period of seven years, as amended by a request or an assignment to order or refrain from performing an act.*" (Penal Code No. 111, 1969, c. 3, § 2, para 430).

Moreover, upon the perpetrator's delivery of a threat, forewarning harm to a victim or a separate person, if the demands for money or a specific act are not met, the perpetrator's threat, as well as the fear instilled in the victim, may pressure the victim to comply with the demands issued:

> "*Anyone who threatens another with committing a felony against himself or his property, or against the person or property of others, by assigning or disclosing matters that are dishonourable or dishonourable in any other manner than those specified in Paragraph 430, shall be subject to imprisonment.*" (Penal Code No. 111, 1969, c. 3, § 2, para 431).
>
> Meanwhile, another paragraph declares:

"*Any individual who threatens another individual through spoken or written words, actions, or signs, or through another individual in any circumstance other than those specified in Paragraphs 430 and 431, shall be penalized with imprisonment for a duration not exceeding one year or a fine.*" (Penal Code No. 111, 1969, c. 3, § 2, para 432).

In terms of the intention of a perpetrator to proceed with a threat, the penal code states that:

"*A felony against an individual or property, or a felony against the person or property of other individuals, or the blaming of certain dishonest or disrespectful acts on an individual, or the revelation of such acts in circumstances other than those described above constitute a felony threat.*"

Additionally, the Iraqi Court of Cassation affirms that:

"*In cases where the threat aims solely at intimidation, without the perpetrator having the intention to commit a specific crime, the situation is governed by the conditions outlined in Paragraph 431 of the Penal Code No. 111 1969 (Iraq), requiring the threat's statements to be sufficiently severe for legal action.*"

The application of the abovementioned regular legislation to criminal activities committed by exploiting cutting-edge technological means can turn out to be a daunting exercise. This can be attributed to the fact that in 1969, when the Iraqi Penal Code was established, the crime of cyber blackmail was yet to make its appearance. Thus, bearing in mind that the current legislation addresses regular, non-cyber infringements, they fall short when it comes to their application for the recently created crime of cyber blackmail. This situation calls for an urgent revamp of the country's legal structure for the establishment of cyber blackmail as a distinctive crime and for the declaration of appropriate consequences.

It can be argued that, legislatively, Malaysia seems to have a more robust provision on dealing with cyber blackmail as compared to Iraq. More so that, both cyber blackmail and extortion are treated as associate crimes while at the same time, punishment varies ranging from 10 years to 20 years imprisonment and even death penalty depending on whether the extortion resulted in fear of injury or serious bodily injury or not. Unlike Iraq, that makes provision for 7years as general punishment with other lesser punishments in other sections of the Iraqi Penal Code and does not cover the crime of extortion which is mostly committed in the course of committing the crime of cyber blackmail by perpetrators.

Although Iraq's information crime draft law was read by the Council of Ministers in 2011, its presentation to parliament was held back until 2020. However, this law was not voted on due to disapproval concerning excessive sentences, fines, and restrictions with regard to freedom of expression on social media. This situation can be attributed to the lack of awareness of the urgent need to bridge the existing cybercrime gaps in Iraqi legislation, particularly in the context of cyber blackmail. The stipulations delineating blackmail felonies are stated in the draft of the Cybercrimes Law 2011. The penalties outlined in Article 11 of this draft law are a prison term of up to seven years and a fine

extending from a minimum of three million dinars to a maximum of five million dinars for the activities listed below (Iraqi Council of Ministers, 2011):

a) The exploitation of computers and the information network to threaten an individual, for the purpose of committing a felony against that individual and his/her possessions, or the lives and possessions of others, with the objective of intimidating or coercing them into executing or abstaining from executing a particular activity.
b) The deliberate delivery or transmission by an individual of any message, document, or news holding threatening content by way of a computer or an information network, with the knowledge that it carries a blackmail bid or threat, to intimidate another individual into executing, or abstaining from executing, a specific activity.

4. Recommendations

The rise of AI in Iraq resulted in a significant increase in cyber threats and extortion. This situation necessitates an immediate enactment of cybercrime legislation, which has been delayed for over a year. The delay in the authorized acknowledgement of blackmail as a crime against freedom is due, according to some quarters. This necessitates the amalgamation of all blackmail-linked transcripts in the draft law into a single all-inclusive transcript, irrespective of the situation or threat type. The growing threat of cyber blackmail also calls for intervention in the form of training programs aimed at providing law enforcement personnel with the required expertise to confront the online perpetration of crimes executed via the exploitation of communication and information channels.

Taking into consideration the threats posed by cyber blackmail, it is essential that the government take steps to educate the public on their moral and official responsibilities regarding the preservation of information confidentiality. Efforts should be made to raise public awareness regarding the dangers involved in the improper application of digital instruments. Hiring personnel who are well-versed in cybercrime, cyber-related issues, and AI should also be considered to raise the efficiency of law enforcement agencies in cybercrime prevention. Professionalism concerning the curbing of cybercrime and online extortion can be enhanced through the relevant authorities' participation in international conferences, seminars and other online-related crime summits. Collaboration between civil society establishments and the Home Ministry may be harnessed to organize nationwide campaigns aimed at increasing public awareness about the risks and dangers of cybercrimes. In addition to the aforementioned measures, it is imperative to implement actions to encourage and facilitate the confidential reporting of cyber blackmail by its unfortunate victims.

In the context of Malaysia, the elimination of data and narratives that infringe upon community guidelines, terms of service, and confidentiality regulations is achieved with the cooperation between the Malaysian Communications and Multimedia Commission (MCMC) and social media sites, including Facebook, Google and X (formerly known as Twitter). Furthermore, the MCMC and law enforcement agencies are authorized to apprehend individuals posting illicit materials on social media, with the convicted

individuals liable to a fine not exceeding 50,000 *ringgit*, a prison sentence not exceeding one year, or both (Act 588, 1998, § 233).

The physical and emotional damage endured by victims of cybercrimes is, more often than not, irreparable. For the public at large, the employment of preventive measures such as the installation of antivirus software or the engagement of a Bring Your Own Device (BYOD) strategy is advisable. In pursuit of this objective, several legislations have been implemented, including both stringent measures and guiding principles. One specific legislation mandates that certain individuals with data access must register, or else they would be subjected to a fine of 500,000 ringgit, imprisonment for a minimum of three years, or both penalties (Act 709, 2010).

5. Conclusion

The widespread reliance on computers to access the internet has exposed many Iraqis to the threat of online extortion. Although the authorities in the country have implemented measures aimed at curbing this innovative crime, the general consensus is that these measures have clearly proven to be wanting in terms of effectiveness. It is becoming evident that alterations to the current laws are in order, as the employment of existing laws and the unenforceable draft law have failed to realize the required objectives.

The findings derived through this study reveal that the crime of cyber blackmail, with the involvement of AI can leave victims in constant distress, leading to psychological issues, trauma, and disruptions in their daily lives.

The criminalization of cyber blackmail, as well as the prosecution and sentencing of its perpetrators, raises complicated and multidimensional challenges. Overcoming these challenges calls for a more wide-ranging comprehension of crime origination and growth, the involvement of threat assessment experts, and updated law enforcement procedures and strategies. In terms of the laws directed at the curbing of cyber blackmail, Iraq needs to develop a more effective legal structure like what is obtainable in Malaysia with the inclusion of extortion as part of cyber blackmail and increasing the punishment for the crime to deter subsequent perpetrators. Iraq must equally move away from the reliance on its penal code in its present form, which fails to fully address the crime of blackmail, as its emphasis is solely on the offence within the threat (Penal Code No. 111, 1969, c. 3, § 2, paras 430 and 431).

The organization of public education campaigns emphasizing issues such as the preservation of personal confidentiality, the risks involved with online interactions, the means for protection against cyber threats, and the prompt reporting of cybercrime perpetration will go a long way towards reducing the occurrences of cyber blackmail. The utilization of AI systems in the law enforcement domain renders the procedures employed for crime prevention and detection more effective, enhances the crime investigation process, facilitates better decision-making, and improves the training and education programmes developed for police recruits.

While this study only explores the cyber blackmail situation in two countries (Iraq and Malaysia), the findings derived may be applicable globally. We are hopeful that these

findings will serve as a source for the development of educational materials to be used in law enforcement training programmes and law school workshops, as well as in the fields of crime analysis and crime victim counselling.

Author contributions: Conceptualization, OAH and NAM; methodology, OAH; software, OAH; validation, OAH and NAM; formal analysis, OAH; investigation, OAH; resources, NAM; data curation, OAH; writing—original draft preparation, OAH; writing—review and editing, NAM; visualization, OAH; supervision, NAM; project administration, NAM. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

Abdulhameed, R. S. (2021). Crimes of threats and cyber extortion through social media: A comparative study. Review of International Geographical Education Online, 11(12): 1022-1033.

Al-Habsi, A., Butler, M., & Percy, A. (2023). Blackmail and the self-disclosure of sensitive information on social media: prevalence, victim characteristics and reporting behaviours amongst Omani WhatsApp users. Security Journal, 37(2), 245–263. https://doi.org/10.1057/s41284-023-00376-3

Al-Habsi, A., Butler, M., Percy, A., et al. (2020). Blackmail on social media: what do we know and what remains unknown? Security Journal, 34(3), 525–540. https://doi.org/10.1057/s41284-020-00246-2

Alisawee, S. (2019). The crime of cyber extortion (A comparative study). University of Al-Qadisiyah.

Al-khaza, M. S., Lahiani, H. (2023). Cybercrime and Harassment: The Impact of Blackmailing on Jordanian Society as a Case Study. 23(3): 117-123. https://doi.org/10.36923/jicc.v23i3.99

Al-Masalha, H., Hnaif, A., Tarek, K. (2020). Cyber-crime effect on Jordanian society. International Journal of Advanced Soft Computing Applications, 12(3): 2074-8523.

Al-Najjar S. F. M., (2024). Criminal responsibilities arising from artificial intelligence crimes. Imam Ja'afar Al-Sadiq University of Legal Studies, 1(7), 80-111. https://www.iasj.net/iasj/issue/321382

Al-Shamari, M. I. (2021). Cybersecurity and its impact on Iraqi national security (in Arabic). Journal of Legal and Political Sciences, 10(1). https://doi.org/10.55716/jjps.2021.10.1.4

Bailey, L., Harinam, V., & Ariel, B. (2020). Victims, offenders and victim-offender overlaps of knife crime: A social network analysis approach using police records. PLOS ONE, 15(12), e0242621. https://doi.org/10.1371/journal.pone.0242621

Chiancone, C. (2023). Smart Government: Practical Uses of Artificial Intelligence in Local Government (Improving Financial Management with AI). Taylor & Francis Online, 126.

Claussén-Karlsson, M. (2017). Artificial Intelligence and the External Element of the Crime: An Analysis of the Liability Problem [PhD thesis]. Örebro University.

Correia, V. J. (2021). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom. SN Computer Science, 3(1). https://doi.org/10.1007/s42979-021-00962-5

Dai, D., & Boroomand, S. (2021). A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. Archives of Computational Methods in Engineering, 29(2), 1291–1309. https://doi.org/10.1007/s11831-021-09628-0

Daoud H. S., (2021). Civil liability for social media hacking. Imam Ja'afar Al-Sadiq University of Legal Studies, 255-283. https://www.iasj.net/iasj/issue/13269

Djenna, A., Barka, E., Benchikh, A., et al. (2023a). Unmasking Cybercrime with Artificial-Intelligence-Driven Cybersecurity Analytics. Sensors, 23(14), 6302. https://doi.org/10.3390/s23146302

Djenna, A., Bouridane, A., Rubab, S., et al. (2023b). Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation. Symmetry, 15(3), 677. https://doi.org/10.3390/sym15030677

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. Journal of Economic Criminology, 2, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Erdélyi, O. J., Goldsmith, J. (2022). Regulating artificial intelligence: Proposal for a global solution. Government Information Quarterly, 39(4): 101748. https://doi.org/10.1016/J.GIQ.2022.101748. https://doi.org/10.1016/j.giq.2022.101748

FindLaw. (2017). United states of America v. Antonio Fontana. Available online: https://caselaw.findlaw.com/court/us-6th-circuit/1872024.html (accessed on 3 May 2024).

Fraga-Lamas, P., Fernández-Caramés, T., & Castedo, L. (2017). Towards the Internet of Smart Trains: A Review on Industrial IoT-Connected Railways. Sensors, 17(6), 1457. https://doi.org/10.3390/s17061457

Hayward, K. J., & Maas, M. M. (2020). Artificial intelligence and crime: A primer for criminologists. Crime, Media, Culture: An International Journal, 17(2), 209–233. https://doi.org/10.1177/1741659020917434

Hung, T.-W., & Yen, C.-P. (2023). Predictive policing and algorithmic fairness. Synthese, 201(6). https://doi.org/10.1007/s11229-023-04189-0

Hussein, J. M. (2023). Case Law Regarding the Legality of Social Media Cyber-Blackmail. Relações Internacionais Do Mundo Atual Unicuritiba, 1, 1-14.

Hussein, O. A., Manap, N. A., Rahman, M. R. A. (2022). Cyber Blackmail Crime against Women - A Case Study. Journal of Positive School Psychology, 6(3), 6882-6893.

Ibrahim, A. A. (2021). Applications of artificial intelligence in confronting cybercrimes. The Legal Journal. 2817.

Iraqi Council of Ministers. (2011). Homepage. Available online: https://iq.parliament.iq/ (accessed on 3 May 2024).

Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Kamińska, D., Aktas, K., Rizhinashvili, D., et al. (2021). Two-Stage Recognition and beyond for Compound Facial Emotion Recognition. Electronics, 10(22), 2847. https://doi.org/10.3390/electronics10222847

King, T. C., Aggarwal, N., Taddeo, M., et al. (2019). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics, 26(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Krishnamoorthy, S., Dua, A., & Gupta, S. (2021). Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. Journal of Ambient Intelligence and Humanized Computing, 14(1), 361–407. https://doi.org/10.1007/s12652-021-03302-w

Laws of Malaysia: Act 574 Penal Code. (2006). Available online: https://icj2.wpenginepowered.com/wp-content/uploads/2012/12/Malaysia-Penal-Code-Act-1936-1997-eng.pdf (accessed on 3 May 2024).

Laws of Malaysia: Act 588, Communications and Multimedia Act 1998. (2004). Available online: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act588bi_3.pdf (accessed on 3 May 2024).

Laws of Malaysia: Act 709, Personal Data Protection Act 2010. (2010). Available online: https://www.kkd.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf (accessed on 3 May 2024).

Light, T. (2021). Data Privacy: One Universal Regulation Eliminating the Many States of Legal Uncertainty. St. Louis University Law Journal, 65(4), 873-896.

Martinez-Miranda, E., McBurney, P., & Howard, M. J. W. (2016). Learning unfair trading: A market manipulation analysis from the reinforcement learning perspective. 2016 IEEE Conference on Evolving and Adaptive Intelligent Systems (EAIS), 36, 103–109. https://doi.org/10.1109/eais.2016.7502499

Mekkawi, M. (2022). Cyber Blackmail between Threats and Protection. Journal of Law and Emerging Technologies, 2(2), 53–116. https://doi.org/10.54873/jolets.v2i2.71

Nienhaus, V. (2021). The digital transformation of the global economy through artificial intelligence: Ethical, Behavioral and Legal Issues (Arabic). Mashura Journal. https://doi.org/10.33001/m011020211591

O'Malley, R. L., & Holt, K. M. (2020). Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. Journal of Interpersonal Violence, 37(1–2), 258–283. https://doi.org/10.1177/0886260520909186

Oh, S. H., Kim, J., Nah, J. H., et al. (2024). Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity. Electronics, 13(3), 555. https://doi.org/10.3390/electronics13030555

Østerlund, C., Jarrahi, M. H., Willis, M., et al. (2020). Artificial intelligence and the world of work, a co-constitutive relationship. Journal of the Association for Information Science and Technology, 72(1), 128–135. Portico. https://doi.org/10.1002/asi.24388

Penal Code No. 111 1969. (2016). Available online: https://menarights.org/sites/default/files/2016-11/IRQ_Penal%20Code%201969%20as%20amended_eng.pdf (accessed on 3 May 2024).

Public Prosecutor v. Chang Ye Siong (2019) 1 MJL 156. https://mjsl.usim.edu.my/index.php/jurnalmjsl/article/view/657 (Accessed 3 September 2024).

Public Prosecutor v. Mohd Zamri Mohd Yunus (2019) MLJU 1501. https://mjsl.usim.edu.my/index.php/jurnalmjsl/article/view/657 (Accessed 3 September 2024).

Rajaee, T., Khani, S., & Ravansalar, M. (2020). Artificial intelligence-based single and hybrid models for prediction of water quality in rivers: A review. Chemometrics and Intelligent Laboratory Systems, 200, 103978. https://doi.org/10.1016/j.chemolab.2020.103978

Republic of Iraq v. Ahmed, 1588/C/2021 (2021). https://mjsl.usim.edu.my/index.php/jurnalmjsl/article/view/657 (Accessed 3 September 2024).

Saleem, R., Hameed, A., Mohammed, T., Aziz, A. (2022). Crimes of Social Media in Iraq. Journal of Positive Psychology and Wellbeing, 6(1), 397-408.

Salim, I. F., Dhafri, M. R. (2024). The Criminal Agreement in Cybercrimes in Iraqi, Emirati, and Qatari Law. Kurdish Studies, 12(2): 4060-4087. https://doi.org/https://doi.org/10.58262/ks.v12i2.300.

Sancho, D. (2017). Digital Extortion: A Forward-looking View. Available online: http://documents.trendmicro.com/assets/wp-digital-extortion-a-forward-looking-view.pdf (Accessed on 3 May 2024).

Scientists, G. (2022). Artificial Intelligence (AI)- Definitions and Applications. Available online: https://gkscientist.com/artificial-intelligence/ (accessed on 3 May 2024).

Seymour, J., Tully, P. (2016). Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter. DEF CON.

Shafaq, N. (2023). What is the current landscape of crime in Iraq? Shafaq News.Com.

Siva Shankar, S., Hung, B. T., Chakrabarti, P., et al. (2023). A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system. Education and Information Technologies, 29(4): 3859-3883.

Spiezia, F. (2022). International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum, 23(1), 101–108. https://doi.org/10.1007/s12027-022-00707-8

Sulkowski, A. J., & Shea, T. (2007). Cyber-Extortion: The Elephant in the Server Room. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.955969

Sulkowski, A. J., & Shea, T. (2007). Cyber-Extortion: The Elephant in the Server Room. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.955969

Teo, S. A. (2023). Human dignity and AI: mapping the contours and utility of human dignity in addressing challenges presented by AI. Law, Innovation and Technology, 15(1), 241–279. https://doi.org/10.1080/17579961.2023.2184132

Thakker, P., Japee, G. (2023). Emerging Technologies in Accountancy and Finance: A Comprehensive Review. European Economic Letters (EEL), 13(3): 993-1011.

Uma, S. (2017). Outlawing cybercrimes against women in India. Bharati Law Review. 5(4): 103-116.

Vasiu, I., & Vasiu, L. (2020). Cyber Extortion and Threats: Analysis of the United States Case Law. Masaryk University Journal of Law and Technology, 14(1), 3–28. https://doi.org/10.5817/mujlt2020-1-1

Vasiu, I., & Vasiu, L. (2020a). Forms and Consequences of the Cyber Threats and Extortion Phenomenon. European Journal of Sustainable Development, 9(4), 295. https://doi.org/10.14207/ejsd.2020.v9n4p295

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. ERA Forum, 23(1), 109–126. https://doi.org/10.1007/s12027-022-00702-z

Wang, F. (2024). Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. International Review of Victimology. https://doi.org/10.1177/02697580241234331

Wehrli, S., Hertweck, C., Amirian, M., et al. (2021). Bias, awareness, and ignorance in deep-learning-based face recognition. AI and Ethics, 2(3), 509–522. https://doi.org/10.1007/s43681-021-00108-6