

Research Article

The Role of the Law in Protecting Individuals from Electronic Blackmail

Khaled Eid*

Department of Private Law, Giza High Institute for Managerial Sciences, Tomah, Giza

Abstract

The main idea centers on describing the role of the law in defending people against the phenomenon of electronic blackmail by defining the term, outlining its types and characteristics, and outlining the role of the law in combating this phenomenon. This is because laws will inevitably be created to address the enormous advancements in technology and human behavior that have coincided with these advancements. The real problem, which is the incapacity to prosecute those who commit these electronic crimes, has emerged because of the tremendous scientific advancement in the field of technology. This has led to the emergence of new patterns and a new class of criminals who have taken advantage of these sciences and modified them to serve their criminal goals. Crime has gone up, as it has in every nation on the planet. Recent years have seen instances of electronic extortion in Egypt, and judges find it challenging to prosecute these contemporary crimes—especially the offense of electronic extortion. The Egyptian lawmaker demanded prompt action to update the legislation against information technology crimes, include provisions for electronic blackmail, and impose harsh punishments on anyone who engage in such behavior. The psychological and social effects to which individuals are exposed to electronic blackmail were also discussed, and we touch on the impact of these effects on the psychological health and social relationships of individuals. In conclusion, the importance of legal safeguards for victims of cyber extortion in Egypt cannot be overstated, given the ever-changing landscape of cybercrime and the inherent challenges it poses to traditional legal systems. It is necessary to review Egypt's current legal framework. Strict protocols must be established for reporting cases of blackmail against members of society to ensure their protection under Egyptian law.

Keywords

Blackmail, Electronic Blackmail, Electronic Crimes, Electronic Stalking

1. Introduction

The real issue that has arisen because of the enormous scientific advancements in the field of technology is the incapacity to prosecute those who commit these electronic crimes. These advancements have led to new patterns and a new class of criminals who have taken advantage of these sciences and modified them to serve their illicit objectives. Crime has gone up, as it has in every nation on the planet. In

recent years, internet extortion has become more common in Egypt. Judges find it challenging to handle these contemporary crimes, particularly cyberextortion.

The study is important from a scientific standpoint because it explains why people are vulnerable to electronic blackmail, what consequences arise from it, what legislative flaws exist and how to fix them, who is in charge of security, and how

*Corresponding author: keid14064@gmail.com (Khaled Eid)

Received: 5 July 2024; **Accepted:** 7 August 2024; **Published:** 6 September 2024



Copyright: © The Author(s), 2024. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

they are doing their part to curb this crime that has become more common in society as a result of significant technological advancements. The study's scientific value is evident in the legislative and preventive strategies that help address cyber blackmail in a morally and legally responsible manner.

Data from the International Telecommunication Union, a United Nations agency focused on communications technology, showed a phenomenal rise in Internet usage, with 5 billion people expected to use it by 2021. The data also showed that the use of the Internet contributes to the emergence of numerous electronic crimes and legislation-related issues as a result of individual behavior changes that may have led to the development of criminal behavior. One of the most common kinds of electronic crimes that has proliferated throughout the world, particularly in Egypt, is electronic blackmail [1]. In January 2023, there will be 80.75 million internet users in Egypt. In the beginning of 2023, 72.2% of Egypt's population was using the Internet. According to the Kepios study, Egypt's Internet user base grew by 1.2 million (1.6%) between 2022 and 2023 [2]. Due to the high percentage of Internet users in Egypt, a number of electronic crimes have emerged. One of the most well-known of these is electronic blackmail, which involves the perpetrator intimidating and threatening the victim by threatening to publish images, videos, or private information. This is done to coerce the victim into complying with immoral demands and acting in ways that are against the law, morality, and public order [3]. Aliyu made an effort to ascertain the scope and veracity of the contribution methodology used in social group activity. The primary goals of the study are to raise awareness and protect college students from the dangers of cybercrime, which will lessen the impact of electronic blackmail crimes on Al-Azhar University's student body. A variety of themes were used in the study, such as comprehensive impacts, criminality, electronic blackmail, and university youth. A comprehensive survey was also carried out by social workers working in the Youth Welfare Office at the Al-Azhar University branch in Assiut [4]. The goal of Sharifa et al.'s study was to identify the primary social and psychological repercussions that the victim of electronic extortion may experience, as well as its causes. The study employed a qualitative technique in order to meet its goals [5]. Singh talked about the many duties and powers of criminal courts, which are essential for determining what counts as a crime and handling criminal cases [6]. Hiba made an effort to list the most significant social dangers associated with cyber blackmailing females and to emphasize the need for raising social awareness in order to combat it [7]. In addressing the regulation that the UAE legislator had decided upon, Alneyadi decided to start by examining the nature of electronic extortion in the first topic, move on to the second topic's scope to elucidate the fundamentals of the crime of electronic extortion, and conclude with the third topic's explanation of the punishment for the crime of electronic blackmail [8]. In order to reduce other crimes, such as money laundering and bribery in the electronic cash system, Chen et al. changed their scheme

to be offline [9]. The study's objectives are to define electronic blackmail, define its features, and list the most prevalent types of electronic blackmail in society. In addition, it should be made clear that blackmailers have both psychological and social repercussions. I think that a person's overconfidence in others, their lack of religious conviction, and the breakdown of their family are some of the main factors that might lead to blackmail.

2. Definitions

Definition 2.1 [10]: Extortion in language: It is the act of extracting money or benefits from someone by threatening to reveal some of their secrets or otherwise, and it involves blackmailing, robbing, and violently removing money from someone. The act of extortion is akin to stealing, and it is accomplished using illicit means.

Definition 2.2 [11]: The conventional concept to blackmail: According to certain jurists, it is characterized as acquiring electronic records about the victim—such as images and details—and threatening to discredit them.

Definition 2.3 [12]: Procedural definition of electronic blackmail:

According to this perspective, blackmail is the illegal act of taking advantage of another person for one's own financial, moral, or sensual gain with the goal of causing them pleasure or happiness. The victim's emotional modesty is offended, and he becomes a captive to the blackmailer's demands out of fear of scandal, slander, and threats.

3. Types of Electronic Blackmail

Electronic blackmail comes in a variety of forms, which are determined by the intended outcome of the blackmail procedure. Blackmail can take many different forms, such as assaults on one's personal space, financial blackmail crimes, and sexual blackmail offenses. The following is a list of the most common types of electronic blackmail:

3.1. Emotional Electronic Blackmail

Blackmail is any behavior or statement that causes the other party to feel guilty or embarrassed. This kind is applied to gain psychological and emotional control over other people. This is not a morally upright manner of doing business and is a poor approach. A series of steps, including demand, resistance, pressure, threat, acquiescence, and repetition, are associated with emotional blackmail. It's finished now. This kind works by applying emotional pressure, taking advantage of emotions, and counting on the intense humiliation that such pressure causes. It also uses the victim's feelings as leverage to accomplish the blackmailer's targeted outcome [13].

3.2. Electronic Physical Blackmail

In this form, the blackmailer's main goal is to gain monetary advantages by extorting large cash payments or rewards in kind from the victim in exchange for keeping the secrets that the victim fears would be made public. Here, the goal is to take advantage of the victim's vulnerability and use coercion to get financial benefit or to obtain large sums of money by tricking the victim.

Through disclosing certain personal information about him, such as installing the victim's photo using programs and altering it in a pornographic or dangerous way, and then putting the victim in danger to comply with the criminal's demands. Blackmail exposes the flaws in some relationships, turning them into points of vulnerability rather than warmth and affection between the partners.

The Egyptian parliament has made it clear that obtaining money or anything else through threats will result in incarceration, and attempting to do so will result in a sentence of no more than two years. Getting this requires the victim to give up. If the offender takes money from the victim, this behavior is no longer considered blackmail and is instead considered theft. By force, and the blackmailer must exhibit overt behavior that indicates his purpose to blackmail us before we are faced with technological blackmail. He was using several online applications, such as Messenger, WhatsApp, Telegram, or any other online application, to make calls or send messages [14].

3.3. Sexual Blackmail

Here, blackmail is accomplished by threatening to expose him or divulge his secrets to the victim in the event that he declines to engage in sexual relations with him. Threatening the victim to engage in these immoral activities with him or with someone other than the blackmailer is the main tactic used against this type of victim, who is typically a woman. Exploiting people via religion is another form of electronic blackmail, in which the perpetrator poses as a respected sheikh with expertise in legal rayah and engages in conversation with the target. You will have his help in removing the enchantment. The victim is tricked into submitting images and videos, which are subsequently utilized to intimidate and coerce the victim [15].

3.4. Reasons for Electronic Blackmail

Jurists are strongly inclined to believe that the victim is 90% at blame for technological blackmail. The blackmailer would not have been able to obtain the funds necessary to carry out the blackmail procedure if the victims—both men and women—had not replied with images or videos. A person's inability to watch God's actions, the lack of moral standards and values, and the inadequacy of religious morality cause him to perform these illegal and prohibited acts.

Additionally, the main causes of electronic blackmail in-

clude untrustworthy relationships, a shaky sense of security, and a legal system that isn't equipped to handle current technology. With the development of contemporary communication tools, boundaries between the sexes have been removed in the majority of families; yet, users are often unaware of information security terms and regulations. The misuse of contemporary technology, including phones, cameras of various types, and programs already in place, has made it easier for dishonest people to blackmail people. Similarly, a family's emphasis on meeting material needs, disinterest in education, and lax supervision all contribute significantly to the erosion of morals, values, and aspirations. Each of these factors plays a major role in increasing people's vulnerability to cyberbullying. Overconfidence in internet transactions can lead to both material and moral harm if it is not handled properly. Additionally, trust on social media platforms can put a person at risk of being the target of electronic blackmail. Electronic blackmail can take many different forms and have many different root causes. It is a form of crime that requires legislative protection in both the constitution and the law to prevent.

3.5. The Effects of Electronic Blackmail

This issue focuses on the psychological and social repercussions that people who are subjected to electronic blackmail go through. We also discuss how these effects affect people's social relationships and mental health. Cyber blackmail is a form of abusive behavior that takes place online and has the potential to harm the targets' social and psychological well-being.

4. The Effects of Electronic Blackmail

This issue focuses on the psychological and social repercussions that people who are subjected to electronic blackmail go through. We also discuss how these effects affect people's social relationships and mental health. Cyber blackmail is a form of abusive behavior that takes place online and has the potential to harm the targets' social and psychological well-being.

4.1. Psychological Effects of Electronic Blackmail

The symptoms that emerge on the psychological side of a person's personality as a result of their exposure to events or traumas are known as psychological impacts. They are also referred to as the outcomes of social phenomena that a person encounters, impacts his psychological well-being, and manifests itself in his personality. The degree to which an individual suffers psychological and social suffering as a result of being subjected to electronic blackmail is known as the psychological impacts of blackmail. The individual who has been blackmailed is said to experience dread, anxiety, and depression as a

result of which they become hostile and may even consider suicide. Numerous studies have established that psychological ramifications from sexual blackmail follow a victim throughout their life and can even turn their situation into a catastrophe. Impossible, which causes him to lose faith in the people in his life and gives him a confused and aberrant personality. The victim may also be afflicted with debilitating psychological conditions like continuous anxiety and mental breakdown.

When children are exposed to blackmail, we find that the child loses his innocence and dignity, becomes frustrated and depressed, and his academic level is affected.

Cybercrime represents an assault on personal freedom and a violation of privacy. We have explained that the provisions of the Constitution emphasize the protection of privacy and the non-exposure of individuals to violations that affect privacy. The assault on personal freedom by extortion results in serious psychological effects that may push the victim to commit suicide. Among the psychological effects that result from this act is that the victim turns into a criminal because of what happened to him or in reaction to what happened to him, as if he were taking revenge on the entire society because of the psychological effects that he suffers. Examples of this include feelings of guilt, embarrassment, and disgrace, anxiety, stress, and psychological tension, feelings of depression, introversion, and feeling. Isolation leads to a decline in self-confidence and exposure to many psychological diseases.

4.2. The Social Effects of Electronic Blackmail

The social effects that result from electronic blackmail are varied, leading to the destruction of the future for the blackmailed person. This act causes social and family suffering for the victim, and among the social effects that the victim is exposed to are changing social behavior and reducing the level of trust in others, feeling shame, embarrassment, isolation, and not feeling comfortable in society. Deprivation of social activities and social confidence, frustration and tension in social and family relationships. In addition, electronic blackmail has a lot of negative societal repercussions, such as broken families. In certain cases, it results in divorce, and many young men and women are reluctant to get married because they have lost confidence as a result of having many of their secrets exposed as a result of blackmail. Numerous females are subjected to significant psychological and social pressures as a result of the societal repercussions. By utilizing the victim as a tool for the crime, such as coercing someone into stealing or doing evil actions that have unfavorable outcomes, it can be used to further objectives that compromise the safety and stability of society. There are major repercussions for family and societal security from all of this. The social impacts of electronic blackmail vary and are a number of ranks, according to several studies. There are several repercussions for the offender. For example, if a female is the victim of a crime, her chances of getting married are significantly reduced, if not eliminated. The dread of scandal may

cause her to decline marriage and abstain from it. In addition to feeling humiliated by herself because of guilt and beatings, she also starts to have a different desire for vengeance against the criminal and herself. selfishness, shyness, the power of illogical thoughts over her thinking, and her incapacity to focus, stabilize, and interact with people in a socially acceptable manner.

5. Proposed Solutions to Treat the Psychological and Social Effects of Electronic Blackmail

There are many solutions proposed to treat the psychological effects of electronic blackmail, including:

1. Search for psychological support: Those exposed to blackmail and electronic harassment must seek psychological support from those close to them, or search for a center for psychological assistance and training that aims to enhance psychological and social health and improve the quality of life.
2. Communicating with legal authorities: Those exposed to blackmail and electronic harassment must contact the competent legal authorities to report the problem and obtain the necessary support.
3. Enhancing self-confidence: Those exposed to blackmail and electronic harassment can enhance their self-confidence through psychological treatment and training on controlling negative thoughts and dealing with crises.
4. Communication with society: Those exposed to blackmail and electronic harassment must communicate with society and participate in social and volunteer activities, which helps improve mental health.

6. Main Results

It takes a complete approach to address the legal and societal aspects of cyber blackmail challenges. Legally speaking, nations must enact stringent laws that make cyber extortion illegal and stipulate suitable punishments for the offenses committed. This law should provide victim protection while keeping up with technological advancements. From a social perspective, governments and society must raise awareness about cyber bullying and blackmail and offer victims the support they need. In addition to giving victims the assistance they need in the form of therapy, psychological counseling, and legal assistance, organizations tasked with preventing cybercrime must also receive the resources they require.

7. Conclusion

In conclusion, considering the dynamic nature of cybercrime and the inherent difficulties it presents to established

legal systems, the significance of legal protections for victims of cyberextortion in Egypt cannot be emphasized. A review of Egypt's current legal system is required. To guarantee that people are protected by Egyptian law, strict procedures must be put in place for reporting cases of blackmail against members of the community. Cybersecurity precautions are also helpful in preventing people from becoming victims of online extortion. Using smartphone security software, following policies that restrict camera use, and staying away from dubious links can all help to drastically lower the chance of online victimization.

Furthermore, the creation of cyber police stations that offer victim aid can help persons impacted by cyber extortion get justice. Because the judicial system maintains secrecy and offers assistance during the legal process, victims are more likely to report occurrences of cyber blackmail when they have confidence in it. The establishment of case law concerning cyber extortion will be essential for successfully negotiating this changing legal environment. It is possible to better safeguard victims of cyber-extortion in Egypt by implementing policy reforms by addressing these challenges and shortfalls.

Egypt has to take a holistic strategy to addressing electronic challenges and giving victims of electronic extortion legal protection. This approach should include creating and upgrading electronic security standards, support services, attempts to create confidence, and ongoing policy improvements. By placing the security and welfare of victims first, we can make Egypt's internet a safer place for everyone.

8. Future Work

Based on the information and results collected and analyzed from available sources, there are a number of recommendations that can be followed to combat electronic blackmail, including:

1. Improving cultural awareness among individuals and communities about the importance of confronting electronic blackmail, as well as increasing awareness that appropriate legal measures will be taken against those responsible for these acts.
2. Develop strong policies and procedures to combat electronic blackmail in institutions, organizations and companies, and provide the necessary training to employees to enhance awareness and protection.
3. Strengthening legislation related to electronic blackmail, providing deterrent penalties for those responsible for these acts, and strengthening law enforcement mechanisms to hold violators accountable.
4. Providing more resources to achieve the best technologies and programs to detect and combat electronic blackmail, including modern software and techniques to evaluate and address related problems.
5. Support academic research and studies in this field to enhance our understanding of related problems and develop effective solutions.

Abbreviations

EB	Electronic Blackmail
ES	Electronic Stalking
SB	Sexual Blackmail

Author Contributions

Khaled Eid is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

References

- [1] Aznan, A., Viejo, C. G., Pang, A., & Fuentes, S. (2023). Review of technology advances to assess rice quality traits and consumer perception. *Food Research International*, 172, 113105, <https://doi.org/10.1016/j.foodres.2023.113105>
- [2] Kortam, W., Ibrahim, M., & Ibrahim, M. (2024). Examining the Impact of Social Media Advertisements and Consumers' Perception on Consumers' Trust: Evidence from Egyptian public healthcare campaigns. *The Academic Journal of Contemporary Commercial Research*, 4(1), 60-73, <https://doi.org/10.21608/ajccr.2024.216236.1066>
- [3] El-Kady, R. (2024). Examining and Combating Corruption in Egyptian Criminal Legislation. In *Examining Corruption and the Sustainable Development Goals* (pp. 112-143). IGI Global, <https://doi.org/10.4018/979-8-3693-2101-0.ch008>
- [4] Ali Ibrahim Aliyu, A. (2024). contributions, method the social group work in mitigation the severity of the consequences on crimes electronic blackmail for university youth. *Journal of Faculty of Education-Assiut University*, 40(3), 1-42, <https://doi.org/10.21608/MFES.2024.349480>
- [5] Alsuwaidi, S. M., & Noufal, Z. M. (2023). The Causes of Electronic Extortion and Its Psychological and Social Effects: A Qualitative Study. *AL-ADAB JOURNAL*, (146), <https://doi.org/10.31973/aj.v1i146.4008>
- [6] Singh, P. (2021). Concepts of Crime and Criminology. *International Journal of Innovative Research in Engineering & Management*, 8(6), 763-766, <https://doi.org/10.55524/ijirem.2021.8.6.168>
- [7] Kareem, H. A. M. A. (2021). The social risks of electronic extortion. *PalArch's Journal of Archaeology of Egypt/egyptology*, 18(4), 8263-8273.
- [8] Alneyadi, M. S., Alkrisheh, M. A., Alhajaya, N., & Al-Tkayneh, K. M. (2022, November). The Crime of Electronic Blackmail in the Emirati Law. In *2022 International Arab Conference on Information Technology (ACIT)* (pp. 1-6). IEEE, <https://doi.org/10.1109/ACIT57182.2022.9994165>

- [9] Sun, D., Huang, X., Mu, Y., & Susilo, W. (2008, October). Identity-based on-line/off-line signcryption. In *2008 IFIP international conference on network and parallel computing* (pp. 34-41). IEEE, <https://doi.org/10.1109/NPC.2008.12>
- [10] Chen, J., Wang, L., Wen, M., Zhang, K., & Chen, K. (2021). Efficient certificate less online/offline signcryption scheme for edge IoT devices. *IEEE Internet of Things Journal*, 9(11), 8967-8979, <https://doi.org/10.1109/JIOT.2021.3119513>
- [11] Altman, S. (2022). Selling silence: the morality of sexual harassment NDA s. *Journal of Applied Philosophy*, 39(4), 698-720, <https://doi.org/10.1111/japp.12590>
- [12] Božić, V., & Nikač, Ž. (2017). Criminal Law and Criminalistic forensic approach to fighting Cyber. In *International Scientific Conference" Romanian educational system of forensic science"(5; 2017)* (pp. 281-290), <https://doi.org/10.18283/C01-2017-X>
- [13] Abbaspour, Z., Amanuelahi, A., & Choubdari, A. (2019). Evaluation of psychometric properties of the Emotional Blackmail Scale (EB). *Quarterly of Educational Measurement*, 9(36), 183-200, <https://doi.org/10.22054/jem.2020.44909.1944>
- [14] Groneman, C. (2003). Sexual Blackmail: A Modern History. *Journal of the History of Sexuality*, 12(3), 500-501, <https://doi.org/10.1353/sex.2004.0007>
- [15] AlGhanboosi, B., Ali, S., & Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. *Computers in Human Behavior*, 144, 107702, <https://doi.org/10.1016/j.chb.2023.107702>