Mohamed Hassan Mekkawi

Ph.D. Candidate – Cairo University

Cyber Blackmail between Threats and Protection: A Study of the Egyptian and American Legislations

Correspondence:

Mohamed Hassan Mekkawi, Ph.D. Candidate, Cairo University

DOI: **https://doi.org/10.54873/jolets.v2i2.71**

E-mail: **moh.mekkawi97@gmail.com**

Citation:

Mohamed Hassan Mekkawi, Cyber Blackmail between Threats and Protection: A Study of the Egyptian and American Legislations, Journal of Law and Emerging Technologies, Volume 2, Issue 2, October 2022, p. 53-116

Cyber Blackmail between Threats and Protection: A Study of the Egyptian and American Legislations

Mohamed Hassan Mekkawi

Abstract

This research paper discusses the threats and the legal protection of the Cyber Blackmail in both the Egyptian and American Legislations. The growth of the Internet has led to the overlap between blackmail and Cybercrime where Cyber Blackmail is increasing, in light of the growing number of social media users, and the acceleration witnessed in the number of various conservation programs. With the phenomenon widely increasing in the Egyptian society in recent times, the researcher, after comparing the Egyptian legislation to the American legislation, seeks to identify the potential threats by analyzing the articles in the Egyptian legislation and identifying the needs to address and provide legal protection for this phenomenon.

Keywords: Cyber Blackmail, Online Harassment, Sextortion, Extortion, Cybercrime, Digital Age

الابتزاز الإلكتروني بين التهديد والحماية
دراسة في التشريعات المصرية والأمريكية

محمد حسن مكاوي
باحث دكتوراه – كلية الحقوق جامعة القاهرة

الملخص:

تتنوع آثار استخدام تطبيقات الإنترنت بين الإيجابي والسلبي، ومن بين الآثار السلبية تفاقم الجرائم الإلكترونية. تناقش هذه الورقة جريمة الابتزاز الإلكتروني باعتبارها إحدى الجرائم الإلكترونية التي تزايدت في المجتمع المصري في الآونة الأخيرة. وتستعرض الورقة تعريف الابتزاز الإلكتروني، وأنواعه، وآثاره المجتمعية، ومقارنة القوانين المطبقة لهذه الجريمة في التشريعات المصرية والأمريكية، مع طرح أحدث القضايا لتلك الجريمة، وموقف الأحكام القضائية منها، بالإضافة إلى البيانات الإحصائية التي توضح قدر توسع الظاهرة في المجتمعين المصري والأمريكي.

كما تستعرض الورقة التهديدات المحتملة من تفاقم جريمة الابتزاز الإلكتروني وأثارها على انتهاك الخصوصية الرقمية، والعقبات التي تواجه القوانين الإجرائية في التعامل مع تلك الظاهرة والتي تتمثل في تنازع الاختصاص، وعبء الإثبات، والدليل الرقمي وغيرها. كما توضح الورقة الاحتياجات المطلوبة لمواجهة تلك الظاهرة وتوفير الحماية القانونية للتصدي لها.

الكلمات الرئيسية: الابتزاز الإلكتروني، المضايقات عبر الإنترنت، الابتزاز الجنسي، الخصوصية الرقمية، الجرائم الإلكترونية، الدليل الرقمي.

Table of Contents

Introduction

The global total of internet users has increased by 7.5 percent year on year though, with an additional 326 million new users over the past 12 months taking the global count to 4.65 billion by the start of April 2022(1). This increment of users of social networking sites especially youths is a direct reason of the tremendous development in the field of modern technological techniques in the treatment of collectables and personal photos of others and the infringement of the sanctity of others' private lives by blackmailing them using sensitive data or fabricated content, which could lead the victim to commit a suicide as a result of the psychological and social pressure.

Cyber blackmail threat actors utilize phishing and blackmail across multiple platforms to get money from their victims, with claims that they have obtained compromising sexual pictures or the sexual browsing history of their victim(2). since Cyber blackmail can be combined with social engineering techniques that seek to research their victims and take advantage of Personally Identifiable Information that victims leave online in social media posts, or from previous data breaches that have been released on either open or Dark-Web forums. Therefore, threat actors use increasingly sophisticated techniques to create personalized extortion messages for each victim.

Cyber blackmail activities have also been detected in apps, where threat actors trick unsuspecting victims, who are usually males, to record or send videos of themselves performing sexual acts to what they believe are females, with the threat actors then threatening to release the footage unless the victim pays a financial sum(3).

(1) More than 5 billion people now use the internet, TNW, April 2022, available at: https://thenextweb.com/news/more-than-5-billion-people-now-use-the-internet#:~:text=The%20global%20total%20has%20still,the%20start%20of%20April%202022. Accessed on 27-6-2022

(2) Bridget Small, Scam emails demand Bitcoin, threaten blackmail, Federal Trade Commission, Consumer Advice, 29 April, 2020, available at: https://consumer.ftc.gov/consumer-alerts/2020/04/scam-emails-demand-bitcoin-threaten-blackmail?page=10 Accessed on 19-3-2022

(3) Trend Micro and INTERPOL, Cybercrime in West Africa; Poised for an Underground Market, 2017. Available at https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf accessed on 11-3-2022

1. Cyber Blackmail

In this part, Cyber blackmail will be defined, the similarities and differences between blackmail and extortion are then demonstrated, and finally, the forms and the consequences of Cyber blackmail are expounded.

1.1 Definition of Cyber Blackmail

Cyber blackmail can be defined as a threat and intimidation of a victim by publishing images or filament materials or leaking of the victim's sensitive personal data for payment or exploitation of the victim to carry out illegal work for the benefit of the blackmailer(1).

The process often begins by establishing a friendship with the target person, and then moves to the stage of communication through social media due to its wide spread and great use by all segments of society. Then the extortionist lures the victim and records the conversation that contains offensive and obscene content of the victim or hack into personal accounts and create fabricated pictures.

From the above, the researcher could define Blackmail as a threat to do something that which might cause a financial loss, or would cause a person to suffer embarrassment, unless that person meets and performs certain demands, such as sexual favors or other benefits to gain power over their victim, whether the action demanded by the blackmailer legal or not.

1.2 Difference between Blackmail and Extortion

It is important to note that extortion and blackmail are related concepts in criminal law in US system but not the same. Some states have only regulated the blackmail, others regulated extortion only and some states have regulated

(1) Dhanya Thakkar, Preventing Digital Extortion Mitigate ransomware, DDoS, and other cyber-extortion attacks Packt Publishing, UK, 2017 page. 82

both. In this paper, special emphasis is laid on the states regulating the blackmail in accordance with the official[1] US government website.

Both extortion and blackmail involve threatening a victim to get something of value and often, both crimes are classified as theft or larceny

Extortion is generally considered a form of theft, which involves the threat of destruction of property or physical harm in order to obtain something of value or compel a person to do something. An extortioner[2] might also threaten to reveal information about the victim that is morally reprehensible or would hurt the victim's reputation. As extortion is primarily a crime based on force, blackmail is a crime based on information. The blackmailer uses threats to reveal information in order to coerce the victim, regardless the information is true or false because Blackmail is always considered as a crime.

Therefore, the researcher concluded that the difference between extortion and blackmail is that blackmail is based on information from which the blackmailer seeks to gain money, property or action from the victim based on this information. However, extortion is based on the threat of destruction or physical harm.

1.3 Forms of Cyber Blackmail

The forms of cyber blackmail crimes vary with the multiplicity of the role of information technology on the one hand, and the multiplicity of traditional crimes on the other hand, such as assault on private life, crimes of extortion with money and request forgery via the computer and the Internet, and the establishment of sites hostile to defamation of the person subjected to extortion, data forgery[3], and desire with sexual blackmail. Therefore, the

(1) USA.GOV An official website of the United States government, available at: https://www.usa.gov/laws-and-regulationsAccessed on 28-6-2022

(2) Dorrian Horsey, I'm Being Blackmailed: How to Deal With Blackmail on the Internet, January 11, 2022, MINC, available at: https://www.minclaw.com/5-tips-combat-online-extortion-sextortion-blackmail/ Accessed on 5-3-2022

(3) Ioana Vasiu and Lucian Vasiu, Forms and Consequences of the Cyber Threats and Extortion Phenomenon, European Journal of Sustainable Development 2020, pages 295-302

researcher distinguishes some forms which have dealt with the crimes of cyber blackmail as follows[1]:

1.3.1 Emotional blackmail:

It means an attitude or speech that the blackmailer takes to cause the other party to feel ashamed or wrong, or to make him bear a responsibility he cannot bear. Emotional blackmail is used to achieve emotional and psychological control over others, and to make the other feel guilty or indebted to the person who is blackmailing him[2].

1.3.2 Financial Blackmail:

It is an attempt to obtain material gains through coercion in order to take advantage of a situation of weakness, and extortion is the weakness and fragility of the relationship between weak souls.

1.3.3 Moral Blackmail:

It is done by threatening through the use of abstract means like the use of harsh language in threatening and promising to reveal the victim's secret, regardless of its type whether pictures, videos etc.[3]

1.3.4 Electronic Blackmail:

It is the exploitation of the other party for material or lustful purposes by keeping electronic records to threaten them. There are number of forms and means by which the criminal blackmails his victim, including[4]:

1. Pictures and video clips: These are the pictures obtained by the

(1) Suliman Al-Ghadian, Yahya Khatatbeh and Ezzeddin Al-Nuaimi, Forms of crimes of cyber blackmailing and their motives and their psychological implications from the point of view of teachers, numbers of committee and psychological counselors, Journal of security research vol 27, issue 69 January 2018, page 173

(2) Rebecca Louise Shaw, A Study of emotional vulnerability and reactions to stress, A thesis submitted to the University of Manchester for the degree of Doctor in Clinical Psychology (ClinPsyD) in the Faculty of Medical and Human Sciences, 2014, page 116

(3) Hiba Abdul Mohsin Abdul Kareem, The Social Risks of Electronic Extortion, Palarch's Journal Of Archaeology Of Egypt/Egyptology, 2021, page 8266

(4) Samir Thakkar, Ransom ware - Exploring the Electronic form of Extortion, research gate, 2015, page 34

blackmailer through hacking the computer of the hacker or illegally entering the victim's computer, as well as through the use of e-mail, chat rooms, and Messenger, which allow more privacy between the two parties. The program also allows the exchange of files, films and documents, from which an opportunity for the blackmailer to exploit these materials to obtain material or moral gains or harm the victim is created.

2. Audio recording: It is what the blackmailer obtains through romantic calls between the blackmailer and the victim, or between the victim and another person who was able to obtain this recording.
3. Electronic and romantic messages: It includes mobile messages, the Internet, e-mail and other means of communication that one deals with today through computer channels, programs and smart phones.
4. Information blackmail: a person stealing information; when a person enters a database of a company or organization, and he steals that information, changes the data, or disables its network until the software becomes unqualified to transfer data.

Among the types of electronic blackmail crimes are advertising prostitution, practicing debauchery and incitement to practice it, sexual exploitation, publishing pictures, films and publications that violate public morals, and infringing on copyright and the rights of artistic classifications through copying and imitating programs and selling them, or copying them from the Internet and then using this technology to protect its members avoid falling into the grip of law enforcement agencies by adding secrecy to their operations[1].

(1) Nasser Al-Shehri, Information Security, Perfect Awareness and Impervious Protection, first edition, Riyadh: Obeikan Library for Publishing and Distribution, 2013, Page 172

1.4 The Consequences of Cyber Blackmail

There are multiple effects and consequences of Cyber blackmail such as:

1.4.1 Psychological Effects

The effects of sexual blackmail are represented in several psychological effects that accompany the victim throughout his life, and may develop to make the continuation of his life impossible, which makes him lose confidence in others and in particular makes the victim a turbulent, eccentric and abnormal personality, and perhaps she suffers from incurable psychological diseases, such as depression, nervous breakdown, chronic anxiety, and sexual blackmail which affects the victim in particular and his family in general, as they suffer from mental illnesses and disorders. Accordingly, this is reflected on society and the relationship of individuals with each other, which amounts in a desire for revenge and develops mental illness which leads to a desire to commit suicide and the desire to get rid of life[1].

1.4.2 Security Effects

Sexual crimes, extortion crimes, and other crimes lead to a disruption of security in societies and turn society into a wild jungle, where the individual is not safe for himself and his family because security and safety are among the most important criteria for judging a healthy society and a crime of all kinds leads to the collapse of values and morals in the community and leads to the destruction of its entity and its destabilization and the spread of vice in it[2].

1.4.3 Social Effects

The spread of this crime is a violation of the civil peace, as it is a risk and a threat to the individual and the family and therefore society. The number of young men and girls who are reluctant to marry because of the secrets revealed to the society by blackmailing has increased. Injustice and oppression have

(1) Hiba Abdul Mohsin Abdul Kareem, The Social Risks of Electronic Extortion, Palarch's Journal Of Archaeology Of Egypt/Egyptology, 2021, page 8265

(2) Mohamed Al-Shanawi, The new fraud crimes. Egypt: Law Books Press, 2008, Page 128

also become common because the victim suffers from difficulties in dealing with others and has an unbridled desire to take revenge on the criminal and herself because she feels insulted and resentful of herself, shame and low self-esteem, in addition to the control of irrational thoughts on her thinking, and the inability to focus and be composed.

2. Cyber Blackmail under US Legal System

Blackmailing is generally classified as a felony which could result in the sentence of multi-year imprisonment and heavy fines. In this part, the following points will be tackled: the federal law, the state laws regulating blackmailing, the most famous types of blackmail and finally the statistics.

2.1 Federal Law

The threat to report or testify against a person for any violation of federal law, along with a demand for money or something else of value is considered a federal crime.

18 U.S.C. § 873, The federal statute defines the crime of blackmail as: «Whoever, under a threat of informing, or as a consideration for not informing, against any violation of any law of the United States, demands or receives any money or other valuable thing, shall be fined under this title or imprisoned not more than one year, or both».

So the conviction could result in imprisonment up to one year, a fine of up to $100,000, or both of the penalties.

It is important also to mention that the Hobbs Act[1] regulates extortion and robbery. Although in order to trigger the Hobbs Act, the extortion must affect interstate or foreign commerce.

This might include threats issued by email or another form of communication

(1) 2403. HOBBS ACT -- EXTORTION BY FORCE, VIOLENCE, OR FEAR, available at: https://www.justice.gov/archives/jm/criminal-resource-manual-2403-hobbs-act-extortion-force-violence-or-fear accessed on 5-3-2022

across state and for the burden of proof of a violation of the Hobbs Act the defendant shall[1]:

- Have induced or attempted to induce the victim to give up property,
- Use or attempt to use the victim's reasonable fear of physical injury or economic loss to convince them to give up property.
- Shall actually or potentially delay, obstruct, or affect interstate or foreign commerce.
- Threat to use force, violence, or fear was wrongful which means that the defendant had no lawful claim to the property they are attempting to obtain through extortion/blackmailing.

2.2 State Laws and Elements of Crime

Each state has its own law regarding the blackmail, some states qualify blackmail as an independent distinct criminal offense, while others qualify it as a form of coercion or extortion.

The states which have an independent act of blackmail are (Kansas[2], Missouri[3], North Carolina[4], South Carolina[5], Ohio[6], Oklahoma[7], Rhode Island[8], Washington D.C.[9], and Wyoming[10]).

Each and every statute of them is discussed as follows:

(1) Dorrian Horsey, I'm Being Blackmailed: How to Deal With Blackmail on the Internet, January 11, 2022, MINC, available at: https://www.minclaw.com/5-tips-combat-online-extortion-sextortion-blackmail/ Accessed on 5-3-2022
(2) Kansas Statutes 21-5428
(3) Missouri Statutes 566.200
(4) North Carolina Code 14-118
(5) South Carolina Code 16-17-640
(6) Ohio Code 2905.11
(7) Oklahoma Statutes 21-1488
(8) Rhode Island General Laws 11-42-2
(9) D.C. Code 22-3252
(10) Wyoming Statutes 6-2-402

2.2.1 Washington D.C. § 22-3252[1]

The statute stipulates that "A person commits the offense of blackmail when that person, with intent to obtain property of another or to cause another to do or refrain from doing any act, threatens to":

1. Accuse another person of a crime;
2. Expose a secret or publicize an asserted fact, whether true or false, tending to subject another person to contempt, hatred, embarrassment, ridicule or other injury to reputation;
3. Impair the reputation of a person, including a deceased person;
4. Distribute a photograph, video, or audio recording, whether authentic or inauthentic, tending to subject another person to ridicule, hatred, contempt, embarrassment, or other injury to reputation; or
5. Notify a federal, state, or local government agency or official of, or publicize, another person's immigration or citizenship status.

The conviction could result in imprisonment up to for not more than 5 years, or fined from $100 to $250,000 under the rules of § 22-3571.01[2], or both of imprisonment and fine.

It is clear from this that this law is exemplary. Despite the article of blackmail cases exclusively, it dealt with both forms of physical and cyber blackmail, as it singled out various penalties according to the gravity of the acts, which are perceived as deterrent penalties.

(1) Washington D.C. § 22-3252, available at: https://code.dccouncil.us/us/dc/council/code/sections/22-3252.html Accessed on 5-3-2022

(2) § 22-3571.01. Fines for criminal offenses. https://code.dccouncil.us/us/dc/council/code/sections/22-3571.01 Accessed on 28-6-2022

2.2.2 Wyoming Statute[1] WY Stat § 6-2-402 (1997)

Wyoming recognizes all the crimes of blackmail, not only that, but also recognizes aggravated blackmail as a greater offense.

The statute stipulates that "A person commits blackmail if, with the intent to obtain property of another or to compel action or inaction by any person against his will if the person":

1. Threatens bodily injury or property damage or;
2. Accuses or threatens to accuse a person of a crime or immoral conduct which would disgrace the person.

Form the above, blackmail occurs if a perpetrator causes bodily injury to another person in the course of committing blackmail. The conviction could result in imprisonment up to a minimum of 5 years in prison, although the maximum sentence can be as much as 25 years in prison. It is clear from this that this law concerned itself with material blackmail and singled out harsh penalties for it, but it explicitly neglected the regulation of digital blackmail.

2.2.3 Ohio Revised Code§ 2905.12[2]

The code stipulates that "No person, with purpose to coerce another into taking or refraining from action concerning which the other person has a legal freedom of choice, shall do any of the following":

- Threaten to commit any felony, or any offense of violence.
- Utter or threaten any calumny against any person.
- Expose or threaten to expose any matter tending to subject any person to hatred, ridicule, contempt or to damage any person's personal or business repute, or to impair any person's credit.

(1) WY Stat § 6-2-402, 1997 available at https://wyoleg.gov/statutes/compress/title06.pdf Accessed on 5-3-2022

(2) Ohio Rev. Code § 2905.12, available at: https://casetext.com/statute/ohio-revised-code/title-29-crimes-procedure/chapter-2905-kidnapping-and-extortion/section-290512-coercion?__cf_chl_rt_tk=hYfJdb8WVltnj9OiAf0kjaXcziSamsk5uRqueQaF3To-1646483429-0-gaNycGzNCf0 accessed on 5-3-2022

It is clear from this that this law has imposed general and loose texts and phrases for blackmail without clearly defining it.

2.2.4 Kansas Statute 2014[1] KS Stat § 21-5428 (2014)

The statute stipulates that "Blackmail is intentionally gaining or attempting to gain anything of value or compelling or attempting to compel another to act against such person's will by threatening to:"

Communicate accusations or statements about any person that would subject such person or any other person to public ridicule, contempt or degradation; or

Disseminate any videotape, photograph, film, or image obtained illegally

So Blackmail is a crime against the person, rather than a property offense as well as, the information could be about the victim or about another person, and it is clear that this law regulates the cyber blackmail in an explicit way.

2.2.5 Oklahoma Statute 2014[2] 21 OK Stat § 21-1488 (2014)

The statue defines the blackmail with all different kinds of methods, as "Blackmail is verbally or by written or printed communication and with intent to extort or gain anything of value from another or to compel another to do an act against his or her will":

1. Accusing or threatening to accuse any person of a crime or conduct which would tend to degrade and disgrace the person accused;
2. Exposing or threatening to expose any fact, report or information concerning any person which would in any way subject such person to the ridicule or contempt of society; or

(1) KS Stat § 21-5428, 2014 available at: https://law.justia.com/codes/kansas/2014/chapter-21/article-54/section-21-5428/#:~:text=(2)%20disseminate%20any%20videotape%2C,a)(6)%20of%20K.S.A. Accessed on 5-3-2022

(2) Oklahoma Statute 2014, Title 21. Crimes and Punishments §21-1488. Blackmail, available at: https://law.justia.com/codes/oklahoma/2014/title-21/section-21-1488/ Accessed on 5-3-2022

3. Threatening to report a person as being illegally present in the United States, and is coupled with the threat that such accusation or exposure will be communicated to a third person or persons unless the person threatened or some other person pays or delivers to the accuser or some other person something of value or does some act against his or her will.

It is important to pay tribute to this text, as it included all kinds of acts, and this is in line with the digital and technological development that facilitates the offender to commit the crime, as the text gives an expansion to the judge and includes many forms and methods of blackmail.

2.2.6 South Carolina Statute 2012[1]SC Code § 16-17-640 (2012)

The statute stipulates that blackmail is "Any person who verbally or by printing or writing or by electronic communications" to

1. Accuses another of a crime or offense;
2. Exposes or publishes any of another's personal or business acts, infirmities, or failings; or
3. Compels any person to do any act, or to refrain from doing any lawful act, against his will;

These actions are with the intention to extort money or any other thing of value from any person.

The conviction shall be fined not more than five thousand dollars or imprisoned for not more than ten years, or both, in the discretion of the court.

It is important to mention that the statute shows the different kind of actions the blackmailer could use, whether verbally or writing or even in printing, and this is in line with the continuous technological and digital development, which transforms many different and innovative methods to commit the blackmail using electronic communications.

(1) South Carolina Code of Laws 2012, Title 16 - Crimes and Offenses, Chapter 17 - OFFENSES AGAINST PUBLIC POLICY, Section 16-17-640 – Blackmail.

2.2.7 North Carolina Code 2005[1] § 14-118

This code was different a bit from other statutes, as it defined blackmail by actions the blackmailer could do, and set a harsh penalty for this crime.

The code stipulates that blackmail could be "If any person shall knowingly send or deliver any letter or writing demanding of any other person, with menaces and without any reasonable or probable cause, any chattel, money or valuable security; or if any person shall accuse, or threaten to accuse, or shall knowingly send or deliver any letter or writing accusing or threatening to accuse any other person of any crime".

Under this code, the punishment by law with death or by imprisonment in the State's prison, with the intent to extort or gain from such person any chattel, money or valuable security, every such offender shall be guilty of a Class 1 misdemeanor.

It is clear from this that this law is considered the most severe among the states in terms of the punishment prescribed for blackmail, which may reach the death penalty.

2.2.8 Rhode Island 2012[2] RI Gen L § 11-42-2 (2012)

The law defines blackmail as "Whoever, verbally or by a written or printed communication, maliciously threatens to accuse another of a crime or offense or by a verbal or written communication maliciously threatens any injury to the person, reputation, property, or financial condition of another, or threatens to engage in other criminal conduct with intent to extort money or any unlawful pecuniary advantage, or with intent to compel any person to do any act against his or her will, or to prohibit any person from carrying out

(1) North Carolina Code 2005, available at: https://law.justia.com/codes/north-carolina/2005/chapter_14/gs_14-118.html Accessed on 5-3-2022

(2) Rhode Island General Laws, Title 11 - Criminal Offenses, Chapter 11-42 - Threats and Extortion, Chapter 11-42-2 - Extortion and blackmail. RI Gen L § 11-42-2 (2012) available at: https://law.justia.com/codes/rhode-island/2012/title-11/chapter-11-42/chapter-11-42-2/ Accessed on 5-3-2022

a duty imposed by law". The Punishment shall be imprisonment in the adult correctional institutions for not more than fifteen (15) years or a fine of not more than twenty-five thousand dollars ($25,000), or both. Despite the clarity of the article, it did not regulate cyber blackmail.

2.2.9 Missouri Revised Statutes(1) 2005 § 566.200

According to sections 566.200 to 566.218 and section 578.475, Blackmail means "any threat to reveal damaging or embarrassing information about a person to that person's spouse, family, associates, or the public at large, including a threat to expose any secret tending to subject any person to hatred, contempt, or ridicule."

It is clear from this that the law has defined blackmail in general and in loose terms in order to expand the range of what falls under blackmail.

2.2.10 New York Statute SECTION 155.05(2)

In New York, Blackmail has the pillars of coercion(3)and larceny, as the statute stipulates that blackmail is to "compel or induce another person to deliver property" in order to make the victim perform/do the following:

- Cause physical harm or injury;
- Cause property damage or Cause an action that harms a person's business;
- Engage in criminal conduct or accuse a person of a crime;
- Expose a secret or publicize a fact or invested the privacy of anyone;
- Withhold or testify a testimony with respect to another's legal claim;

(1) Missouri Revised Statutes Title XXXVIII. Crimes and Punishment; Peace Officers and Public Defenders § 566.200, available at: https://codes.findlaw.com/mo/title-xxxviii-crimes-and-punishment-peace-officers-and-public-defenders/mo-rev-st-566-200.html Accessed on 5-3-2022

(2) Article 155, TITLE J Offenses Involving Theft, PART 3 Specific Offenses, Chapter 4 Penal, Consolidated Laws of New York, available at: https://www.nysenate.gov/legislation/laws/PEN/155.05 Accessed on 5-3-2022

(3) https://law.justia.com/codes/new-york/2021/ Accessed on 5-3-2022

- Abuse or use his position as a public servant;
- Perform any other act that is calculated to harm anyone with respect to his health, safety, career, financial condition, reputation, or personal relationships.

From the above, it seems that the New York statute has great lengths to outline the various threats made by blackmailers.

2.3 Types of Blackmail

The blackmailer might have different types of threat, such as revealing sensitive personal data that is likely to cause embarrassment, accusing a person falsely of crime or even reporting a person's involvement in a crime, and as mentioned before it could cause a financial loss or moral embarrassment.

In this study, special emphasis is laid on some examples of Blackmail which show how the courts deal with them.

2.3.1 Hobbs Act Blackmail[1]

Under 18 U.S.C. § 1951[2] "Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery or extortion or attempts or conspires so to do, or commits or threatens physical violence to any person or property in furtherance of a plan or purpose to do anything in violation of this section shall be fined under this title or imprisoned not more than twenty years, or both".

And in order to prove a violation of Hobbs Act extortion by the wrongful use of actual or threatened force, violence or fear, on the following facts shall be done:

(1) HOBBS ACT -- EXTORTION BY FORCE, VIOLENCE, OR FEAR, available at: https://www.justice.gov/archives/jm/criminal-resource-manual-2403-hobbs-act-extortion-force-violence-or-fear accessed on 5-3-2022

(2) 18 U.S.C. § 1951, Section 1951 - Interference with commerce by threats or violence, https://casetext.com/statute/united-states-code/title-18-crimes-and-criminal-procedure/part-i-crimes/chapter-95-racketeering/section-1951-interference-with-commerce-by-threats-or-violenceAccessed on 8-3-2022

The defendant shall induce or attempt to induce the victim to give up property rights.(1)

- The defendant use or attempt to use the victim's reasonable fear of physical injury or economic harm in order to induce the victim's consent to give up property.(2)
- The defendant's conduct shall obstruct, delay, or affect interstate or foreign commerce in any way.(3)
- The defendant used force, violence or fear wrongfully, and it is important to mention that the Supreme Court(4) also made a broadly worded statement that "wrongful" has meaning in the Act only if it limits the statute's coverage to those instances where the obtaining of the property would itself be "wrongful" because the alleged extortionist has no lawful claim to that property.

A prominent and famous case that involved the Federal Hobbs Act was Sekhar v. United States(5) in 2013.

The defendant was a managing partner at FA Technology. The New York Comptroller who was responsible for New York's State and local government pension fund, was considering investing in FA Technology and if the Comptroller invested in the company, FA Technology stood to gain around $7.6 million in fees. While researching the fund, the Comptroller's

(1) See the following cases
United States v. Tropiano, 418 F.2d 1069, 1075 ,2d Cir. 1969
United States v. Zemek, 634 F.3d 1159, 1174 ,9th Cir. 1980
United States v. Debs, 949 F.2d 199, 201 ,6th Cir. 1991
(2) See the following cases
United States v. Duhon, 565 F.2d 345, 349 and 351 ,5th Cir. 1978
United States v. Gigante, 39 F.3d 42, 49 ,2d Cir. 1994
(3) See the following cases
United States v. Farmer, 73 F.3d 836, 843 ,8th Cir. 1996
United States v. Taylor, 92 F.3d 1313, 1333 ,2d Cir. 1996
(4) https://www.justice.gov/archives/jm/criminal-resource-manual-2403-hobbs-act-extortion-force-violence-or-ear Accessed on 8-3-2022
(5) SUPREME COURT OF THE UNITED STATES, Sekhar v. United States, 570 U.S. 729 (2013), available at: https://casetext.com/case/sekhar-v-united-states-2? Accessed on 8-3-2022

General Counsel was advised by the New York Attorney General that an FA Technology agent was under investigation and this led to a result that the Comptroller decided not to invest in the fund. After few days, the Comptroller's General Counsel received an email threatening to reveal his extramarital affair if he did not reverse his decision and invest in FA Technology. After several more threatening emails, the FBI was able to trace the source of the emails to the FA Technology's managing partner. Petitioner was convicted of attempted extortion, in violation of the Hobbs Act and six counts of interstate transmission of extortionate threats.

2.3.2 Revenge Porn

Revenge porn is not something the average person thinks about on a daily basis; however, this distressing situation happens to roughly one in twelve (8%) people in the United States(1). Revenge porn is a form of cyber sexual harassment; the perpetrator threatens to publish sexually explicit content unless the victim provides him with money or other favors. In 2020, 42 states have specific laws outlawing distribution of revenge porn. However, revenge porn laws are still relatively new and the laws are continuing to develop(2). The pillars of this crime is generally about someone who has an intension to annoy or harass another who publishes electronic or printed pictures or videos that shows a part of his/her body, depicts that person engaged in a sexual act. The conviction could be imprisonment to maximum 10 years or fine about $100,000 in some states. According to a Cyber Civil Rights Initiative survey in 2013, 90% of the victims of revenge porn are women and 57% of those women were threatened by an ex-boyfriend(3). In one chilling report,

(1) Aaron Minc and Alexandra Arko (2021) How to Permanently Remove Content From Revenge Porn Websites, November 12, 2021, available at: https://www.minclaw.com/remove-posts-revenge-porn-websites/ Accessed on 8-3-2022

(2) FindLaw Team, State Revenge Porn Laws, 14 January 2022, available at: https://www.findlaw.com/criminal/criminal-charges/revenge-porn-laws-by-state.html Accessed on 8-3-2022

(3) CCRI's 2013 Nonconsensual Pornography (NCP) Research Results, 2013, https://www.cybercivilrights.org/wp-content/uploads/2016/11/NCP-2013-Study-Research-Results-1.pdf Accessed on 8-3-2022

the predator was choking a cat during a video chat. He threatened to kill the animal if the victim did not send him a nude picture. The underage victim complied and the predator used that picture as a basis for further blackmail(1).

2.3.3 Sexual Blackmail "Sextortion"

Sexual Blackmail is the most common form of blackmail people hear about every day. Perpetrators might create fake accounts "catfishing"(2) and persuade their victim to share nude photos or perform sexual acts on a webcam and once they obtain the explicit material, they start threatening to expose the content unless they are paid, or perform more sexual acts. They may even start sending explicit content to family and friends over social media to heighten the victim's fear. Perpetrators often target their clients who they perceive as having the ability to pay as well as those who have a reputation to uphold(3). In 2020, there were 43,101 known victims of extortion who lost a combined $107.5 million to sextortionists.

2.3.4 Celebrity Blackmail

As mentioned before under the sexual blackmail section, perpetrators often target those with a reputation to uphold and have high estimated ability to pay, celebrities are frequent victims of blackmail. Below are some examples about blackmail cases:

David Schmidt, a computer technician, blackmailed two of the famous

(1) Ivana Vojinovic, More Than 70 Cybercrime Statistics - A $6 Trillion Problem, DataProt, 2022, available at: https://dataprot.net/statistics/cybercrime-statistics/#:~:text=60%20million%20Americans%20have%20experienced%20identity%20fraud%2C%20identity%20theft%20statistics%20show.&text=According%20to%20cyber%20crime%20statistics%20from%202017%2C%2016.7%20million%20consumers,consumers%20in%20a%20single%20year. Accessed on 28-6-2022

(2) Catfishing refers to when a person takes information and images, typically from other people, and uses them to create a new identity for themselves. In some cases, a catfisher steals another individual's complete identity—including their image, date of birth, and geographical location—and pretends that it is their own. The catfisher then uses this identity to trick other people into associating with them or doing business online. More information available at: https://www.fortinet.com/resources/cyberglossary/catfishing Accessed on 19-3-2022

(3) Dorrian Horsey, I'm Being Blackmailed: How to Deal With Blackmail on the Internet, January 2022, MINC available at: https://www.minclaw.com/5-tips-combat-online-extortion-sextortion-blackmail/ Accessed on 19-3-2022

Hollywood stars, namely, Katie Holmes and Tom Cruise. When they got married in 2006, Schmidt got hold of personal sensitive pictures of the couple, and in order not to publish those photos, he demanded them to pay $1.3 million. The perpetrator has a history of trading the celebrities' personal information. The FBI arrested him for his extortion plot and accordingly, he committed suicide in September two weeks before his court appearance(1).

Adrienne Bailon was also a victim of a blackmailing scheme. When someone stole her laptop and tried to leak her personal information and files, including some nude photos and demanded $1000 to bring her the laptop back(2).

In 2009, John Travolta was a victim of blackmail. Two men demanded $25 million in order not to publish and to release a medical document that John signed to not have his son transported when he needed medical attention before he died(3). The perpetrator was arrested and charged with two counts of extortion for his actions.

John Stamos was also a victim of blackmail. A man and a woman attempted to extort $680,000 from John Stamos when they threatened to sell private photos of him allegedly using drugs. The two men were taken into custody for the extortion plot, were faced with convictions of conspiracy and interstate communications to extort money, and were sentenced to four years in prison(4).

A photographer threatened to sell and publish topless photos and videos of the famous actress Cameron Diaz. As photos were taken before she came to

(1) Sultan of Sleaze› arrested in Tom Cruise extortion plot, The Guardian Newspaper, 11 Jan 2008, available at: https://www.theguardian.com/film/2008/jan/11/news Accessed on 19-3-2022

(2) Dincan Riley, Adrienne Bailon, nude pics extortion plot, 12 July 2019, INQUISITR, available at: https://www.inquisitr.com/7781/adrienne-bailon-nude-pics-extortion-attempt/ Accessed on 19-3-2022

(3) Guy Adams, John Travolta ends $25m extortion case linked to death of his son, INDEPENDENT,29 September 2009, available at: https://www.independent.co.uk/news/world/americas/john-travolta-ends-25m-extortion-case-linked-to-death-of-his-son-2072193.html Accessed on 19-3-2022

(4) Michelle Caruso, CNN STAFF, Pair gets four years in Stamos extortion case, 8 October 2010, available at: http://edition.cnn.com/2010/SHOWBIZ/celebrity.news.gossip/10/08/stamos.extortion.trial/index.htmlAccessed on 19-3-2022

fame as an actress, Diaz argued that the photographer tried to coerce her into paying him by threatening to publish the secret content. The photographer was ultimately convicted of attempted grand theft, forgery, and perjury(1).

2.4.Statistics

The FBI's Internet Crime Complaint Center has released its annual report. The 2020 Internet Crime Report(2) includes information from 791,790 complaints of suspected internet crime; an increase of more than 300,000 complaints from 2019 and reported losses exceeding $4.2 billion. The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud(3). According to a report(4) in 2022, two-thirds of cyber blackmail victims are girls under the age of 16. A third of sextortion victims never report the incident to anyone, not even family and friends.

3. Cyber Blackmail under the Egyptian Legal System

It seems that the situation in Egypt is different from the situation in the United States of America. Although there is a Penal Code, a Communications Regulatory Law and Anti-Cyber and Information Technology Crimes Law in Egypt, the shocking fact is that there is no special and independent legislative article regulating the crime of Cyber Blackmail. There are a set of articles in

(1) photographer convicted of trying to blackmail Cameron Diaz, 25 July 2005, available at: https://www.seattletimes.com/nation-world/photographer-convicted-of-trying-to-blackmail-cameron-diaz/ Accessed on 19-3-2022

(2) Internet Crime Report 2020, available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf Accessed on 11-3-2022

(3) FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, March 17, 2021, available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics Accessed on 11-3-2022

(4) Ivana Vojinovic, More Than 70 Cybercrime Statistics - A $6 Trillion Problem, DataProt, 2022, available at: https://dataprot.net/statistics/cybercrime-statistics/#:~:text=60%20million%20Americans%20have%20experienced%20identity%20fraud%2C%20identity%20theft%20statistics%20show.&text=According%20to%20cyber%20crime%20statistics%20from%202017%2C%2016.7%20million%20consumers,consumers%20in%20a%20single%20year. Accessed on 28-6-2022

the aforementioned laws, which are judged in cases, and therefore these texts will be analyzed to their suitability with cyber blackmail, and then the opinion of the Egyptian Court of Cassation will be presented and the legal principles that it issued in this regard, according to the following division:

3.1 The Penal Code No. 58 of 1937

3.2 Telecommunications Regulatory Law No. 10 of 2003

3.3 Anti-Cyber and Information Technology Crimes Law No. 175 of 2018

3.4 The Egyptian Child Law No. 12 of 1996 amended by Law 126 of 2008

3.4 The Court of Cassation Principles

3.5 Statistics

3.1 The Penal Code No. 58 of 1937(1)

The Penal Code legislate threatens, but in general and in broad terms, it also protects the sanctity of private life, such as the right to a photo and protecting it from publication. The articles will be mentioned and elaborated as follows:

Article 326

Whoever obtains by threat to be given an amount of money or any other thing by threatening to get it, shall be punished with detention. Attempted threat to obtain it shall be punishable with detention for a period not exceeding two years.

Article 327

Whoever threatens another, in writing, with committing a crime against one's soul or property which is punishable with execution or permanent or temporary hard labor, or with divulging issues or attributing matters outraging

(1) https://manshurat.org/node/23881 Accessed on 11-3-2022

one's honor, and the threat is accompanied with a demand or instruction for something, shall be punished with imprisonment.

The perpetrator shall be punished with detention if the threat is not accompanied with a demand or instruction for something.

Whoever threatens another verbally, via another person, with something of the foregoing, shall be punished with detention for a period not exceeding two years or a fine not exceeding five hundred pounds, whether the threat is or is not accompanied with instructions to perform something.

Any threat, whether in writing, or verbal, via another person, with committing a crime not reaching the foregoing enormity shall be punished with detention for a period not exceeding six months, or a fine not exceeding two hundred pounds.

By analyzing the text, the following deductions can be made:

The criterion for differentiation in punishment is through behavior in the crime. If the offender's threat is not accompanied by a request or a mandate, the penalty of imprisonment shall be applied for a period not exceeding three years, but if the offender's threat is accompanied by a request or a mandate, the penalty shall be increased to imprisonment for a period of 7 years.

So, in order for the blackmailer to be punished, he must blackmail or threaten his victim either by writing, and the threat is not criminal if it is verbal unless it is made by another person, meaning that when the blackmailer threatens his victim himself, but verbally, he is outside the framework of legal accountability and can be saved by his act.

Article 309 bis

A penalty of detention for a period not exceeding one year shall be inflicted on whoever encroaches upon the inviolability of a citizen's private

life, by committing one of the following acts in other than the cases legally authorized, or without the consent of the victim.

a) Eavesdropping, recording, or transmitting via any instrument whatever its kind, talks having taken place in a special place, or on the telephone.

b) Shooting and taking or transmitting by one of the instruments, whatever its kind, a picture of person in a private place.

- If the acts referred to in the two preceding paragraphs were issued during a meeting within the hearing or sight of those present at that meeting, then their consent is assumed.
- A public official/civil servant who commits any of the deeds defined in this article, depending on the authority of his position, shall be punished with detention.

Article 309 bis A

Whoever discloses, facilitates the disclosure of, or uses, even non-publicly, a recording or documents obtained by one or the methods prescribed in the previous Article, or if it is made without the consent of the concerned party shall be punished with detention.

Whoever threatens to divulge an order obtained by one of the aforementioned methods to force a person to carry out or refrain from carrying out some work shall be punished with imprisonment for a period not exceeding five years.

A public official who commits any of the deeds indicated in this Article, depending on the authority of his position, shall be punished with imprisonment.

In all cases, the court shall rule confiscating the instruments and other equipment that might have been used in the crime, or by which the recordings or documents have been obtained. Also the ruling shall enforce the deletion or destruction of the recordings obtained through the crime

From these articles, it is clear that:

- The blackmailer shall be punished with imprisonment for a period of no less than one year in the event that he takes a picture or publishes it without the consent of its owner, indicating that this is a crime that has been established and that the law punishes this crime, whether to take the picture without permission, or obtain the picture without permission, or to publish it without permission. Every crack is an independent crime in itself.
- Therefore, everyone should know, that there is a big difference between taking a photo and publishing it without the permission of the owner, even if the photo was taken with the consent of the girl, publishing it must be with her consent, and if she is threatened or the photo is published on the Internet without her permission, this will be considered a crime.

3.2 Telecommunications Regulatory Law No. 10 of 2003(1)

The law did not provide for an independent crime of blackmail, but there are two articles of the law that are used in court rulings. An article regulating the penalty for those who work in the field of telecommunications only, and another article regulating the punishment for all individuals which is reviewed as follows:

Article 73

Whoever perpetrates any of the following deeds during the performance of his job in the field of Telecommunications or because of it shall be liable to a penalty of confinement to prison for a period of not less than three months and a fine of not less than five thousand pounds and not exceeding fifty thousand pounds, or either penalty:

(1) https://manshurat.org/node/13787 Accessed on 11-3-2022

1. Annunciation, publishing or recording the content of any Telecommunication message or part of it without any legal basis.
2. Hiding, changing, obstructing or altering any or part of Telecommunication message that he might have received.
3. Refraining from sending any Telecommunication message after being assigned to dispatch it.
4. Divulging without due right any information concerning Telecommunication Networks Users or their incoming or outgoing communication.

Article 76

Without prejudice to the right for suitable indemnity, a penalty of confinement to prison and a fine not less than five hundred pounds and not exceeding twenty thousand pounds or either penalty shall be inflicted on whoever:

1. Uses or assists in using illegitimate means to conduct telecommunication correspondence.
2. Premeditatedly disturbs or harasses a third party by misusing Telecommunication Equipment.

3.3 Anti-Cyber and Information Technology Crimes Law No. 175 of 2018[1]

Despite the issuance of Anti-Cyber and Information Technology Crimes Law no. 175 of 2018, the legislator did not explicitly provide for the crime of cyber blackmail.

Although the following articles are used for the cyber blackmailing matters, the invasion of privacy and any content is inconsistent with the family principle.

(1) https://manshurat.org/node/31487 Accessed on 11-3-2022

Crimes on Infringement of Privacy and Unlawful Information Content were in two articles: article 25 and article 26

Article 25

"Anyone who infringes a family principle or value of the Egyptian society, encroaches on privacy, sends many emails to a certain person without obtaining his/her consent, provides personal data to an e-system or website for promoting commodities or services without getting the approval thereof, or publishes, via the information network or by any means of information technology, information, news, images or the like, which infringes the privacy of any person involuntarily, whether the published information is true or false, shall be punishable by imprisonment for no less than six months and a fine of no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties".

Article 26

"Anyone who deliberately uses an information program or information technology in processing personal data of a third party to connect such data with an abusive content or to display the same in a way detrimental to the reputation of such third party shall be punishable by imprisonment for no less than two years and a fine of no less than one hundred thousand Egyptian Pounds and no more than three hundred thousand Egyptian Pounds, or by one of these two penalties".

There is no doubt that this legal article is very useful in principle, as without it, things may go awry, but there is no objection to mentioning some observations that may be right or wrong:

- The phrases in the legal texts must be clear and not subject to measurement or interpretation. When reading the text, it has to be understood in the same way, and not hold different points of view because it is about taking away the freedoms of others.

- After extensive research in the laws, judicial rulings, and principles of the Court of Cassation, unfortunately, there is no definition of the values/principles of the Egyptian family.
- These articles are used in many different contexts; therefore, a separate and independent article has to be legislated to regulate the cyber extortion more clearly and in terms that do not carry interpretation, and show clearly the pillars of the crime.

It is also important to mention that in Article (22) which regulates the programs and equipment used in committing information technology crimes stipulates that:

"Anyone who possesses, acquires, procures, sells, makes available, manufactures, produces, imports, exports or trades, by any way whatsoever, any devices, equipment or tools, or designed, developed or transformed software, or passcodes, ciphers, symbols or any similar data, without obtaining the permission of Authority or holding a credential in fact or in law, and it is proved that such act was aimed at using any of the foregoing for committing or enabling the commission of any crime provided for in this Law, or for concealing the traces or evidence thereof, or that such use, enablement or concealment took place, shall be punishable by imprisonment for no less than two years and a fine of no less than three hundred thousand Egyptian Pounds and no more than five hundred thousand Egyptian Pounds, or by one of these two penalties".

Looking closely at this article, it could be concluded that it only punishes the use of data or tools to commit or facilitate the commission of one of the crimes stipulated in this law only, and not in the entire Penal Code, meaning that it does not protect the personal data of the victim and does not penalize the violation of the privacy of the user or the use or modification of his data. It also happens with pictures of girls and superimposing them on other pictures

to portray the victim girl as one of the prostitutes, and when the law tried to address the protection of personal data of the user, it came with articles that do not guarantee the real protection of the data or the privacy of users.

3.4 The Egyptian Child Law No. 12 of 1996, as amended by Law 126 of 2008

The law singled out provisions that protect the violation of digital privacy which is related to the sexual exploitation of children through digital applications in Article 116.

Article 116 stipulates that without prejudice to the provisions of criminal involvement, any adult who induces a child to commit a misdemeanor, or trains him to do it, or helps him, or facilitates it in any way, but did not attain his goal, shall be sentenced to half the maximum sentence decreed for this crime. The penalty shall be imprisonment for a period of not less than six (6) months if the offender uses coercive or threatening methods with the child, or if he is related to him, or is one of those responsible for his upbringing or watching over him, or one to whom the child was delivered to by virtue of the Law, or was a servant to any of the aforementioned. In all cases, if the crime is committed on more than one child, even at different times, the penalty shall be imprisonment for a period not less than one (1) year, and not exceeding seven (7) years. Shall be penalized with the penalty set forth for cases of instigating a crime, any adult who induces a child to commit a felony, or prepares the child for this, or helps him, or facilitates it in any way, but did not attain his goal.

Article 116-bis stipulates that the minimum penalty decreed for any crime shall be doubled if the crime is committed by an adult against a child, or if it is committed by one of the parents, or by one of the child's guardians, or by people in charge of supervising or upbringing the child, or by those who have authority over the child, or by a servant to any of the above mentioned.

Article 116-bis (A) stipulates that any one importing, or exporting, or producing, or preparing, or viewing, or printing, or promoting, or possessing, or broadcasting pornographic material using children, or related to the sexual exploitation of children shall be imprisoned for a period of not less than two (2) years and a fine of not less than ten thousand (10,000) Egyptian pounds, and not exceeding fifty thousand (50,000) Egyptian pounds.

It shall also be ruled to confiscate the tools and machines used in committing the crime and the money obtained from it, and to close the places where it was committed, for a period of no less than six months, all without prejudice to the rights of third parties.

All the above shall be undertaken without violating the rights of those with good intentions. Without prejudice to any stronger penalty prescribed in any other law, each of the following shall be subject to the same penalty: a) anyone using a computer or internet or information networks or cartoons to prepare, or save, or process, or display, or print or publish or promote pornographic activities, or induce or exploit children to engage in prostitution or pornographic activities or defame them, or sell them. b) anyone using a computer or internet or information networks or cartoons to induce children to delinquency or use them in committing crimes or engage them in illegitimate activities or immoral acts, even if the crime did not occur.

Article 116-bis (B) stipulates that without prejudice to any stronger penalty in any other law, anyone who publishes, or broadcasts in the media any information or data, pictures, or drawings related to the identity of a child at a time when his case is being examined by the authorities concerned with children at risk or are in conflict with the law shall be penalized by a fine of not less than ten thousand (10,000) Egyptian pounds, and not exceeding fifty thousand (50,000) Egyptian pounds,

It is clear from the articles of the law that it has protected the child from his

participation in crimes by criminalizing anyone who incites the child to commit immoral acts, and may amount in an aggravating circumstance for the crime if it is committed against more than one child, and most importantly, Article 166 bis (a) specifically has Criminalized sexual exploitation of children on the Internet who promote pornographic activities or acts, which is implicit in protecting the child from cyber blackmail.

3.5 The Court of Cassation Principles(1)

The Court of Cassation establishes the threat pillars in the crime of threatening a sum of money does not have a special form. It is a crime of free form that does not require the threat to occur through exclusively specific means or a specific form, but rather the occurrence of the threat by any means is sufficient.

It suffices to achieve the MENS REA to prove to the court that the offender committed the threat and is aware of its effect in terms of inflicting fear on the victim, and that he wants to achieve that effect with what it may entail from the victim's acquiescence to his desires, regardless of whether he intended to actually carry out the threat and without the need to know the actual effect that the threat had on the victim.

The rulings are not nulled; the omission to talk about the effect of the threat on the victim himself, or even if the perpetrator was not serious about his threat.

To further explain this, the legal principles on which the Cassation Court has settled in two of the most recent crimes have been presented as follows:

Criminal Cassation of. 6173 of Judicial Year 89 in 13/10/2020(2)

"Obtaining photographs of the victim in an outrageous situation, and

(1) https://www.cc.gov.eg/ Accessed on 11-3-2022
(2) https://www.cc.gov.eg/judgment_single?id=111613768&&ja=285670 Accessed on 11-3-2022

threatening the offender to publish these photographs if he did not pay a certain amount of money. This would disrupt the will of the victim and intimidate him, leading him to hand over money to the offender, and all pillars of the crime of threatening and abuse of communications are available".

Criminal Cassation of. 22620 of Judicial Year 88 in 9/7/2020(1)

"Proof of judgment sending the appellant threatening statements in writing through modern electronic media with the intent of instilling fear in the victims' souls in order to force them to perform what is required that fulfills the elements of the crime of threat".

"Whereas the felony of threat stipulated in the first paragraph of Article 327 of the Penal Code is available if the threat is made in writing to commit a crime against oneself or money, and the threat is accompanied by a request or commanding an order, and the judgment has given its reasons for the appellant to threaten the two victims through social media. He managed to deceive them and obtain from them pictures and video clips in indecent situations and threatened to publish them, and since the term writing was mentioned in the aforementioned Article 327 by way of clarification in a general form to include all the different means of writing, whether it was by traditional methods or by one of the modern electronic means. With the intent of inflicting fear on the victims in order to get them to perform what is required, then he has memorized the elements of the crime of threat as they are defined in the law, and the denial of the appellant in this regard is rendered unfounded."

3.6 Statistics

There are no recent official statistics on the rate of cyber blackmail crimes, but a study prepared by the Communications and Information Technology Committee of the Egyptian House of Representatives revealed that in

(1) https://www.cc.gov.eg/judgment_single?id=111399002&&ja=277482 Accessed on 11-3-2022

September and October 2018, 1038 cybercrimes were reported including cyber blackmail(1).

"Qawem" Facebook page conducted an opinion poll for its followers and for the victims of extortion and blackmailers it has dealt with over the past year and a half, and they found that the biggest crisis lies in society's ignorance of laws(2).

The survey found that 90% of the victims fully believe that reporting blackmail to the police will be recorded in their civil registry, and may harm their future in terms of work or travel, and they are not aware that the procedures are carried out in strict secrecy, and they are not exposed in society where the blackmailer is followed up and arrested by following his text messages on the mobile phone.

As for extortionists, the survey found that 70% of them do not know anything about the crime of extortion and its legal consequences. They see that what they are doing is just a ploy for material gain, believing that as long as there is no sexual extortion, they will not face any legal accountability, unaware of what will happen to them and their families from scandals as a result of committing the crime of extortion.

The founder of the "Qawem" page to combat electronic extortion, which receives from 700 to 1,000 cases of extortion daily, stated that "The victims of extortion avoid writing records in the police department and prefer to resort to the Qawem page to resolve the matter amicably, as they believe that writing

(1) Eman El-Gendy, Cyber blackmail. A crime that needs more than one law, January 5, 2022, Al-Wafd Newspaper, 2022, available at: https://alwafd.news/%D8%AA%D8%AD%D9%82%D9%8A%D9%82%D8%A7%D8%AA-%D9%88%D8%AD%D9%80%D9%88%D8%A7%D8%B1%D8%A7%D8%AA/4098241-%D8%A7%D9%84%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%89-%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%AA%D8%AD%D8%AA%D8%A7%D8%AC-%D9%84%D8%A3%D9%83%D8%AB%D8%B1-%D9%85%D9%86-%D9%82%D8%A7%D9%86%D9%88%D9%86 Accessed on 11-3-2022

(2) Qawem Page, available at: https://www.facebook.com/qawem.community/ Accessed on 11-3-2022

the report against the blackmailer is a new scandal for them, and the victim feels that it is a new scandal for them. She exposes herself and that her record will be dishonorable when she applies for any job in the future." He also explained that with his experience as a civil page, it has faced more than 400,000 cases of electronic blackmail since its establishment in July 2020, and that there is no awareness in society of the punishment of blackmail, especially when the victim is the one who sends the pictures herself to the blackmailer, indicating that the victim believes she will be subject to legal accountability if she informs the police, in addition to the fear of some victims of slowing down the procedures or keeping the record, so the blackmailer returns in this case to blackmail them again more(1).

4. The Main Difficulties and Risks of Cyber Blackmail

There are many difficulties in cyber blackmail, including the evidence, burden of proof and even the victim himself.

4.1 The evolution and increase of Cybercrime

The spread of the Internet and the rate at which technology is evolving along with the fact that social networking is currently one of the most popular online activities, ensures that cybercrime is likely to increase at a rapid rate(2). Around the world, organized crime gangs use technology to coordinate and conduct crimes, posing several problems for law enforcement and forensic analysts(3).

There is no universally agreed definition of the term 'cybercrime' nor is there

(1) https://www.shorouknews.com/news/view.aspx?cdate=01122021&id=b63927b8-4aef-4f19-8717-7cbf6552d-b7b

(2) Mohamed El-Guindy, Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism. Journal of Law and Emerging Technologies, 1(1), 2021, pages 11–64. https://doi.org/10.54873/jolets.v1i1.32 Accessed on 11-3-2022

(3) Robert W. Taylor, Eric J. Fritsch and John Liederbach, Digital crime and digital terrorism. Boston: Pearson. 2015, page 182

consensus as to what cybercrime actually is. It is a term used to encompass a range of criminal activities that use information and communication technologies (ICTs)(1).

The Convention on Cybercrime(2), Budapest 2001 distinguished between two types of cybercrime(3):

1. Pure Cybercrime: A criminal act committed through the use of information and communication technologies or the Internet, where a computer or network is the target of the crime. An example of pure cybercrime is the spread of malicious software, such as viruses.
2. Cyber-enabled Crime: Any criminal act that can be committed without technology or the Internet, but is supported, facilitated or escalated on a large scale using technology. This includes a range of serious and organized crimes, such as Internet fraud, child exploitation material distribution, and terrorism.

In the Middle East, cybercrime has evolved rapidly over time as the Internet penetration rate in the region is outpacing the rest of the world with low digital literacy rate(4). According to a research by Kaspersky(5), the Russian multinational cyber security and anti-virus provider has shed light on the prevalence of malware attacks in 2021 in the Middle East where 161 million malware attacks were observed; a 17% increase compared to 2020. Egypt witnessed a significant increase in malware attacks which increased by 32%.

(1) David Wall, What is cybercrimes, Journal article,2004, available at: https://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/09627250408553239.pdf accessed on 27-6-2022
(2) Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185, available at: https://rm.coe.int/1680081561 Accessed on 19-3-2022
(3) Oonagh McPhillips, Cybercrime: Current Threats and Responses A review of the research literature Co-Authors Sheelagh Brady & Caitríona Heinl, SAR Consultancy & EXEDEC, 2020, page 21
(4) Mohamed El-Guindy, Cybercrime in the Middle East. ISSA Journal, 6(6), 2008
(5) Malware attacks in Egypt increase to 42 million during H1 2021, Accessed on 19-3-2022 https://dailynews-egypt.com/2021/08/18/malware-attacks-in-egypt-increase-to-42-million-during-h1-2021/

Facts are stubborn, but statistics are more pliable in the following are some statistics proofing the increment of cybercrime every day. A study made in 2003 found that there is an attack every 39 seconds on average on the web(1). Another report in 2019 found that security breaches had increased by 67% over the last five years(2). So in general on average 30,000 new websites are hacked every day(3). The FBI reported a 300% increase in the number of cybercrimes, from about 1,000 cases to between 3,000 and 4,000 cases each day during COVID 19 pandemic(4).

4.2 The Right to Digital Privacy

The crime of infringement and the right to privacy were enshrined in international treaties and conventions from the Charter of the United Nations 1948 to the recent conventions. Digital privacy refers to the protection of an individual's information that is used or created while using the Internet on a computer or personal device. It is important to mention that pictures and videos on the Internet are among the most important sources for learning AI algorithms(5).

A recent report(6) by the Office of the High Commissioner for Human Rights entitled Privacy in the Digital Age in 2021 came to mention the danger of artificial intelligence, including profiling technologies, automated decision-making and machine learning, and its impact in the absence of

(1) Agnes Talalaev, Everything You Need To Know About Password Management, Patchstack,2021 available at: https://patchstack.com/articles/password-management/ Accessed on 27-6-2022

(2) Kelly Bissell and Ryan Lasalle, Ninth Annual Cost of Cybercrime Study, Accenture, 2019 available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study Accessed on 27-6-2022

(3) James Lyne, 30,000 Web Sites Hacked A Day. How Do You Host Yours?, Forbes, 2013 available at: https://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/?sh=686ba2c31738 Accessed on 27-6-2022

(4) Maggie Miller, FBI sees spike in cybercrime reports during coronavirus pandemic, The Hill, 2020, available at: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/ Accessed on 26-7-2022

(5) Dr. Mohamed El-Guindy, TECH TALK, TV show, episode 29 January 2022, available at: https://www.youtube.com/watch?v=4mYAZBQMiCg Accessed on 27-6-2022

(6) OHCHR and privacy in the digital age 2021, available at: https://www.ohchr.org/en/privacy-in-the-digital-age Accessed on 27-6-2022

appropriate guarantees on the enjoyment of the right to privacy. AI systems rely on large data sets that include personal data, and this stimulates large-scale data collection, storage, and processing in private and public spaces, and intermediaries obtain, combine, analyze and share personal data with countless recipients(1), and these activities have wide-ranging implications on privacy and human rights in general(2).

First, the data sets used include information on large numbers of individuals, implying their right to privacy. Second, they can lead to state interventions, such as searches, interrogations, arrests, and prosecutions. Rights affected include the right to privacy, the right to a fair trial, the right not to be subjected to arbitrary arrest and detention, and the right to life. Third, the opacity inherent in AI-driven decisions raises particularly pressing questions regarding state accountability when guided by AI in taking coercive measures, and even more pressing in areas that typically suffer from a lack of transparency in general, such as the activities of anti-terrorism, Fourth, predictive tools have inherent risks of perpetuating or even reinforcing discrimination, reflecting historical racial and ethnic bias built into the data sets used, such as a disproportionate focus on policing among some minorities.

The report issued a set of recommendations, some for countries and some for businesses, the most important of which was to ensure that the use of artificial intelligence complies with all human rights, and that any interference with the right to privacy and other human rights through the use of artificial intelligence is stipulated by law, seeks to achieve a legitimate goal, and complies with adopt and enforce data privacy legislation in an effective manner for the public and private sectors, through independent and

(1) Submissions by Centre for Communication Governance at National Law University Delhi, Derechos Digitales, Digital Rights Watch, Global Partners Digital, International Center for Not-for-Profit Law and Universidade Federal de Uberlândia

(2) Aaron Rieke and others, Data brokers in an open society (London, Open Society Foundation, 2016, page 46, available as a pdf file at: https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf Accessed on 1-1-2022

impartial authorities, as a condition essential to protect the right to privacy in the context of artificial intelligence.

With the spread of information technology, there are many programs that increasingly distort personal sayings and images, and this leads to many violations of privacy and social security and leads to a rise in crimes. For example, the most famous program is Deep Fake(1); a program that makes any user on the Internet make clips. A video for anyone who has his picture and where he shows the features of his destination as he wants and says what he wants, and this is something that cannot be tolerated. It suffices to say that if you have a picture of someone you do not like, you may create a video for him in any position or form you want and it is difficult for others to know that it is fake.

A report(2) in 2019 mentioned an increase in the use of this type of software for revenge, as the number of fake clips that were made reached 14,678 clips, with a percentage of 96% sex clips, which represent a mainstay for cyber blackmail crimes.

In implementation of this, a 51-year-old woman was arrested in Pennsylvania this year and faces a year in prison for using anonymous phone numbers to make inappropriate calls and send hostile messages to three girls, and then used the deep fake application to install some sex clips of girls and blackmail them(3).

Therefore, there are some defects which must be addressed in the digital privacy as follows:

- The need for the international community, through its international

(1) DeepFake, Available at: https://deepfakesweb.com/accessed on 28-5-2022
(2) DeepTrace Report, The State of Deepfakes, Landscape, Threats and impact, 2019, available at: https://regmedia.co.uk/2019/10/08/deepfake_report.pdf Accessed on 27-6-2022
(3) Pat Ralph, Bucks County mom found guilty of harassing daughter›s cheerleader teammates, Voice, 2022, available at: https://www.phillyvoice.com/mom-raffaela-spone-guilty-harassment-cheerleaders-bucks-county-pennsylvania/ Accessed on 27-6-2022

organizations, to implement agreements that expand the international authority to some extent to preserve the right to privacy, and work to impose strict and unified international sanctions to limit online interference, and urge countries to impose sanctions on the violator in order to reduce its expansion.

- The imperative of enacting legal rules to protect digital privacy, in line with the challenges of the modern era, and placing it within a sound legal framework.

4.3 Jurisdiction Conflict

Conflict of jurisdiction is a problem that disturbs the work of the control and investigation authorities because the crime of cyber blackmail is one of its problems that it may cross the territorial borders of the state, so that the perpetrator is from one state and the victim is from another state. Against the offender according to the system included in the penalty and the applicable law, and this in itself is a legal problem that takes time and great effort to solve(1).

Internationally: Budapest Convention(2) of Cybercrime in which the United States signed on stipulates in article 22 that each Party shall adopt legislative and other measures to establish jurisdiction when the offence is committed in its territory; or on board a ship flying the flag of that Party; or on board an aircraft registered in this country; or by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State; or an alleged offender is present in its territory and it does not extradite him or her to another Party.

(1) Wael Shater, The legal framework for the crime of electronic extortion in electronic games, AJSP, Arab Journal for Scientific Publishing ISSN: 2663-5798, 2020, page 440

(2) Budapest Convention of Cybercrime 2001 availabe at: https://www.coe.int/en/web/cybercrime/the-budapest-convention Accessed on 18-6-2022

The Situation is harder in Egypt, as Article 1 in the Egyptian Penal Code no 58 of 1937 stipulates that "The provisions of the present law shall apply to any person who commits in the Egyptian country one of the crimes prescribed in it". Therefore, the Egyptian Penal Code does not apply to a crime that did not occur in the Egyptian territory.

However, Article 3 in Law no 175 of 2018 stipulates that provisions of this law shall apply to any non-Egyptian person outside the Arab Republic of Egypt who commits one of the crimes stipulated in this law, whenever the act is punishable in the country in which it occurred under any legal description, in any of the following cases:

1. If the offence was committed using any of the means of transportation by land, sea or air registered in the Arab Republic of Egypt or flying its flag.
2. If one or all of the victims were Egyptians.
3. If the offence was prepared, planned, directed, managed or financed in the Arab Republic of Egypt.
4. If the offence was committed by an organized criminal group which practices its criminal activities in more than one country including the Arab Republic of Egypt.
5. If the offence is likely to cause detriment to any citizen or resident of the Arab Republic of Egypt, or to endanger the security or any interest of the Republic whether locally or abroad.
6. If the perpetrator is found in the Arab Republic of Egypt after committing the crime and was not extradited yet.

It raises the question how to apply the text of Article 3, as there have been no cases so far in which the Egyptian law has been applied to a cybercrime outside Egypt; this also poses another risk which is the effective International Cooperation.

Therefore, the researcher suggests the presence of a body such as the National Cyber Security Authority that provides work on expanded international agreements that guarantee the eligibility of trials according to a specific law between the two countries in the event of such cross-border information crimes.

4.4 The Burden of Proof in Cyber Blackmail Crime

The Burden of proof of cyber-attack has still obstacles and challenges in the world(1). Cyber blackmail, which is a type of cybercrime which takes place in an unconventional environment, meaning that it falls within an intangible framework because its elements are based between the environment of a computer or a technical electronic device and the use of the Internet as another means, which facilitates the erasure of digital evidence by the perpetrator and increases the difficulties facing criminal and judicial officers(2). The traditional means of proof do not always succeed in proving this type of crime due to its different nature from the traditional crime and the different material elements on which the cybercrime is based because:

1. Cybercrime does not leave material traces.
2. Many people who go to the crime scene and have nothing to do with the crime in the first place, during the time when the crime was committed and investigated and proven, help the perpetrators to hide the traces of the material crime and destroy them.

4.5 The Digital Evidence

The digital forensic evidence is the evidence taken from computers and it

(1) Maskun Maskun, Hasbi Assidiq and Armelia Safira, Cyber Attack -The Burden of International Crime Proof: Obstacles and Challenges Conference: The 2nd International Conference of Law, Government and Social Justice 2021 (ICOLGAS 2020)

(2) Michael Heller, Gathering cybercrime evidence can be difficult, TechTarget, available at: https://www.techtarget.com/searchsecurity/feature/District-attorney-Gathering-cybercrime-evidence-can-be-difficult Accessed on 19-3-2022

is in the form of magnetic fields or electrical impulses that can be collected and analyzed using special technological programs and applications stored on electronic devices and the Internet to prove the required incident in electronic crimes and attributing it to the wanted person(1). Evidence of cybercrimes requires digital evidence as a means to prove cyber blackmail. Taking steps to collect digital evidence requires a criminal investigator and a specialized technician who has the technical skill to extract and collect digital evidence because the resolution of electronic crime cases in general and the crime of cyber blackmail in particular(2).

Considering Egypt, it should be noted that the Egyptian Court of Cassation has affirmed the illegality of evidence obtained illegally(3).

Article 336 of the Code of Criminal Procedure stipulates that "if it is decided to invalidate any procedure, it deals with all the effects that result directly from it."

Law no. 175 of 2018 regulates set of articles treating the digital evidence, as following:

Article 6 stipulates what is known as the Temporary Judicial Writs.

The investigation body concerned may, as the case may be, issue a substantiated writ to the competent law enforcement officer in respect of one or more of the following matters, for a period not exceeding thirty days renewable for one time, if this will help reveal the truth about the perpetration of an offence punishable under this law:

1. Control, withdrawal, collection, or seizure of data and information or

(1) Aju D, Anil Kumar Kakelli and Kishore Rajendiran, A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends, Confluence of AI, Machine, and Deep Learning in Cyber Forensics, premiere reference resource, 2021, page 3

(2) National Institute of Justice, Digital evidence in the courtroom: A guide for law enforcement and prosecutors. U.S. Department of Justice, Washington, DC, 2007

(3) Ahmed Awad Belal, Rule of Exclusion of Evidence Obtained by Illicit Methods in Comparative Criminal Procedures - Third Edition, Dar ElNahda El-Arabyia, 2013, pages 149-162

information systems, or tracking them in any place, system, program, electronic support or computer in which they are existing. Its digital evidence shall be delivered to the body issuing the order, provided that it shall not affect the continuity of the system and provision of the service, if so required.

2. Searching, inspecting, accessing and signing in the computer programs, databases and other devices and information systems in implementation of the seizure purpose.

3. The concerned investigation body may order the Service Provider to submit the data or information related to an information system or a technical device under the control of or stored by the Service Provider, as well as the data of the users of its service and the connection traffic made in that system or the technical system. In all circumstances, the writ issued by the investigation entity must be substantiated. The aforesaid writs shall be appealed before the criminal court concerned, as held in the deliberation room on the dates and according to the procedures stipulated in the criminal procedural law

Article 11 stipulates that "The evidence derived or taken from devices, equipment, media, electronic supports, information system, software, or any means of information technology shall have the same value and force of criminal material evidence in criminal evidence where the technical conditions set out in the executive regulations of his Law are met".

Article 9 in the executive regulations issued by Prime Minister's Decision No. 1699 of 2020 stipulates that the digital evidence of value and concealment of physical forensic evidence may be permitted in criminal proof if it meets the following conditions and controls:

1. That the process of collecting, acquiring, extracting or deriving the digital evidence in question is carried out using techniques that ensure

that no change, update, erasure or distortion of writing, data and information, or any change, update or damage to devices, equipment, data and information. Or information systems or programs or electronic supports and others. These include Write Blocker, Digital Images Hash, and other similar technologies.

2. That the digital evidence be relevant to the incident and within the context of the subject to be proven or denied, according to the scope of the decision of the investigation authority or the competent court
3. That the digital evidence be collected, extracted, preserved and kept by the judicial control officers authorized to deal in this type of evidence, or experts or specialists delegated from the investigation or trial authorities, provided that it is indicated in the seizure reports or technical reports on the type and specifications of programs and tools The devices and equipment that were used, with the documentation of the hash code and algorithm resulting from extracting identical and identical copies of the original from the digital evidence in the seizure report or the technical inspection report, while ensuring the continued preservation of the original without tampering with it.
4. In the event that it is not possible to examine the copy of the digital evidence and it is not possible to seize the devices under examination for any reason, the original shall be examined and all of this shall be proven in the seizure report or the examination and analysis report
5. The digital evidence shall be documented in a minutes of procedures by the specialist prior to the examination and analysis operations thereof, as well as documenting the place of its seizure, the place of its storage, the place of dealing with it and its specifications.

Article 291 of the Code of Criminal Procedure states that "the court may, even on its own, during the consideration of the case, order the submission of any evidence it deems necessary to establish the truth."

Article 302 of the Code of Criminal Procedure stipulates that the judge shall rule in the case according to the belief that he has formed with complete freedom. However, he may base his judgment on any evidence that was not presented to him in the session. Every statement that proves that it was made by one of the accused or witnesses under duress or threat of it is wasted and unreliable.

Hence, the judge can have his belief in any form and to everything that falls into his reassurance, and that means if he does not take the digital evidence as evidence, it will be used as evidence and if the arguments are gathered, evidence can be established from it.

Hence, the researcher suggests that the legislator establish mechanisms for the digital evidence because:

- The Egyptian judiciary relies on the rule that says that in the gathering of evidence, evidence is taken, meaning that digital evidence, due to the difficulty of proving what the law requires, is taken as a presumption that accepts proof of the contrary and loses its strength as evidence.
- It is necessary to enter into international agreements to combat cybercrime and exchange digital evidence because the principle of territoriality remains an obstacle in some cases.
- The difficulty of the required technical tracking and the lack of digital capabilities for that.
- Training law enforcement agencies and judges, without exception, on digital evidence, conducting training courses for them, and preparing accredited scientific diplomas.
- Develop texts that are more appropriate and acceptable for proof, where in light of the massive and wide development in information technology and digital transformation, justice remains restricted for lack of proof.

- Reconsidering the principle of legality of evidence, there is nothing sacred, now we are in a digital world and with the existence of a new republic, we have to catch up with technology and massive transformation and not only look at methods of proving traditional crimes, now crimes are digital and cause great damage, we must prepare now because the situation will become worse and we will not be able to keep up with the world, and justice will become captive to texts covered in dust.

4.6 Failure to inform the victim of the crime

The lack of reporting by the victim and the victim's fear of reporting is a major reason for the difficulty facing police officers investigating this type of crime. Therefore, this reluctance helps to disappear the digital evidence that indicates the offender, and this is a reason for creating an obstacle standing in the way Evidence via Digital Evidence.

To make this clearer, it is necessary to mention the most famous example of this problem in Egypt this year: the suicide case of a female student who was the victim of digital blackmail last January, Case No. 2036 Kafr El-Zayat Felonies.

A 16-year-old girl, Bassant, from Gharbia Governorate, committed suicide against the background of the bullying and cyber blackmail she was subjected to through the social media site "Facebook" by two young men seven days before the girl's death. They blackmailed the girl "Bassant" financially in order to establish a relationship with her by installing an indecent picture of her. The main reason for the suicide was the fear of society not believing her. Before her death, she wrote a letter confirming that she did not commit any of these immoral acts and that she was wronged, but no one took her side, and here she means the family and the community.

The Public Prosecution ordered the pretrial detention of the defendants

pending investigations into the case, by accusing one of them of indecent assault on the girl because she was under the age of 18, and accusing the two young men of violating the sanctity of Bassant's private life.

The decision of referral included directing 6 charges against the accused, which is human trafficking, by exploiting the victim's weakness in front of their threats to publish indecent images attributed to her with the intention of sexually exploiting her and forcing her to engage in immoral acts, accusing some of them of indecent assault with force and threat, and threatening to publish indecent images of her honor, and the threat was accompanied by requests from her. Thus, all of them attacked the sanctity of her private life, and their assault on family principles and values in Egyptian society using the international information network.

The Tanta Criminal Court sentenced the 5 defendants to 15 years in prison for 3 defendants, and 2 others to 5 years in prison.

The main problem is that the judge did not stipulate a text criminalizing cyber blackmail only, but resorted to adapting the case to other crimes so that he could sentence them to a deterrent punishment.

4.7 There is no effective International Cooperation

Egypt did not sign Budapest convention till now, so the rules regulating the cybercrime convention 2001 will not be applied, as the convention set 9 ways to enrich the International Cooperation, such as: extradition, mutual legal assistance, expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored computer data, trans-border access to stored computer data with consent or where publicly available, real-time collection of traffic data, interception of content data and 24/7 Network.

Although the Law no. 175 of 2018 stipulates in article 4 "International

Cooperation in the field of Anti-Cyber and Information Technology Crimes" that in light of the ratified international, regional and bilateral agreements, or in application of the principle of reciprocity, the concerned Egyptian authorities shall cooperate with their foreign counterparts through exchanging information to avoid committing Information Technology Crimes, and to assist in the investigation and tracking down the perpetrators of those crimes. But this article is hard to be applied, as the conventions made the cooperation obligatory but under this Law it is something based on ethics and win-win situation, Therefore, the international cooperation is still a main risk in Egypt.

As the different countries' legislation in criminalizing acts of electronic extortion in general is different from one country to another, and this increases the obstacles in the prosecution of the perpetrators, and despite the call for the need for international cooperation in combating cybercrime, there are obstacles to achieving this which include:

1. The absence of a single agreed-upon model related to criminal activity: the legal systems in the countries did not agree on one specific picture of the misuse of information systems to be followed, and there is no agreed and specific definition of the crime, all countries agreed to criminalize it. The same legislation in all countries of the world and not keeping pace with technical progress
2. The lack of international coordination related to criminal procedures in the matter of cybercrime, such as the work of acacia, investigation and inference, the possibility of obtaining evidence in crimes that occur outside the borders of the state, as well as the technical difficulty in obtaining the evidence in particular.

4.8 Urgent need to develop legislations

Having mentioned the challenges, it is inevitable to elaborate on the

development of laws, as the laws must fit the fourth Industrial Revolution, "Artificial Intelligence", and the risks of metaverse. It should also be mentioned that Article No. 99 of the Egyptian Constitution of 2014 amended in 2019 made crimes that affect the sanctity of private life not subject to a statute of limitations, which is a positive thing.

"Every attack on the personal freedom, or the sanctity of the private life of citizens, and other rights and public freedoms guaranteed by the constitution and the law, is a crime. The criminal case, nor the civil case arising from it, is not waived by prescription. The state guarantees fair compensation to the person who has been assaulted. The National Council for Human Rights may inform the Public Prosecution of any violation of these rights. And he may intervene in the civil lawsuit joining the injured party at his request, and all of this is in the manner prescribed by law".

5. Conclusion

This paper has presented a comprehensive analysis of the Cyber blackmail and threats phenomenon. The paper defines Cyber blackmail, its types, and its societal effects, and compares the applicable laws for this crime in the Egyptian and American legislation, with the presentation of the latest cases for that crime, and the position of judicial rulings on it, in addition to the statistical data that shows the extent of the phenomenon's expansion in the Egyptian and American societies.

The paper showed how the digital transformation has increased the violation of privacy online, and showed the gap between the Egyptian legislations and the tremendous development of information technology and digital transformation, which has emphasized the inevitability and necessity of enacting legislation to confront the types of newly created crimes, in their various forms and ways of committing them. Finally, the paper attempts to set some solutions for the procedural obstacles that influence the applying of the expedited justice and general deterrence.

5.1 Findings

- The tremendous development of information technology and digital transformation has had a negative impact on the widespread and increasing violation of digital privacy.
- Digital transformation and artificial intelligence still present great challenges and increase the imposition of cyber blackmail.
- Cyber threats are exacerbated by vulnerabilities in public cyber security strategies and the economic impacts.
- Lack of awareness prevents a large number of victims from reporting the cyber blackmailing for fear of social or family discontent with them.
- Lack of awareness of the law and penalties increases the perpetrators' commission of the crime and diversifies the methods of blackmail.
- The Egyptian Law needs to establish more articles regulating the cyber blackmail with a deterrent punishment.

5.2 Recommendations for victims

- If someone threatens you, avoid showing any weakness and cut all communication.
- Do not give the demands of the blackmailers' requests, even if they threaten you that they will share your information or photos on social networking websites.
- Avoid deleting any pictures or message used to threaten you, and keep the messages that contains the blackmailing as they are your digital evidence.
- If the blackmailer threatens you through any platform, you can report their account to this platform, and it will close the offending account and prevent the IP of the blackmailer's device from creating any other account.

- Set a hard password and avoid using birthdays, names or even your car number, as these passwords are easily hacked.
- If you really care about your personal information, do not share it on any social media.
- In accordance to Article Three of the Code of Criminal Procedure, remember that filing a report with the incident must be within three months of the incident.
- For any emergency, call 108, a line dedicated to reporting cybercrime operating 24 hours a day.
- Notify the Computer and Information Networks Crimes Control Department at the Ministry of Interior headquarters in the Fifth Settlement, New Cairo.
- Notify the Computer and Information Networks Crimes Control Department at the Ministry of Interior by calling the following phone numbers: 27928484 - 27926071 - 27921490.
- Contact the Internet Investigations headquarters in Abbasiya.
- Contact only people on your social media and in your circle.
- Do not open messages with your name because it contains a virus.
- The scammer is impersonating you; therefore, do not connect with him.

5.3 General Recommendations

1. The researcher suggests the presence of a body, such as the National Cyber Security Authority that provides work on expanded international agreements that guarantee the eligibility of trials according to a specific law between the two countries in the event of such cross-border information crimes.

2. The researcher suggests to legislate an article in Anti-Cyber and Information Technology Crimes Law of 175 of 2018 which regulates the cyber blackmail crime, and to elevate the charge of this crime from a misdemeanor to a felony, as it is worthy of imprisonment as a result to the damage resulting from, such as ending the lives of some victims.

3. Spreading compulsory awareness of youth, and according generalizing the German High Five Project which is based in Berlin, and works to increase the political and cultural awareness among local youth aged 15-25 by organizing weekly workshops throughout the year and summer schools for two weeks (14 days), and attendance at these workshops is mandatory(1).

4. Continuing to spread awareness about cybercrimes and teaching them in law faculties, as traditional crime has become less of a step now than what we see of cybercrimes, and the law's failure to keep pace with technological development warns of the existence of negative economic and social effects.

5. Reconsidering the criminalization of incitement to suicide, whoever reads this recommendation may be surprised now, but it is an idea that must be put forward, if the criminal law does not criminalize the instigator of suicide because the original perpetrator of the crime must be held accountable first in order for the partner to be held accountable, but the pressures exerted on digital platforms and the increasing crimes of extortion have to tighten the legal texts in order to achieve general deterrence in society and private deterrence of the criminal.

6. The researcher sees that there are some defects needed to be cured to

(1) Carlos Kölbl, Historical Consciousness in Youth. Theoretical and Exemplary Empirical Analyses, 2001, University of Bayreuth Germany, Increasing political consciousness among young people in Berlin, European commission, available at: https://ec.europa.eu/regional_policy/en/projects/Germany/increasing-political-consciousness-among-young-people-in-berlin Accessed on 20-3-2022

the digital privacy, such as the need for the international community through its international organizations, to implement agreements that expand the international authority to some extent to preserve the right to privacy, and work to impose strict and unified international sanctions to limit online interference, and urge countries to impose sanctions on the violator in order to reduce its expansion and the imperative of enacting legal rules to protect digital privacy, in line with the challenges of the modern era, and placing it within a sound legal framework.

5.4 List of References

Legislations

Convention on Cybercrime, Budapest, 23.XI.2001

Egyptian Laws

1. Anti-Cyber and Information Technology Crimes Law No. 175 of 2018
2. The Egyptian constitution 2014 amended in 2019
3. The Criminal Procedural law no. 150 of 1950
4. The Penal code no 58 of 1937
5. Telecommunications Regulatory Law No. 10 of 2003

US Laws

1. D.C. Code 22-3252
2. HOBBS ACT 18 U.S.C. § 1951
3. Kansas Statutes Stat § 21-5428 (2014)
4. Missouri Statutes 2005 § 566.200
5. New York Statute SECTION 155.05
6. North Carolina Code § 14-118

7. Ohio Code § 2905.12

8. Oklahoma Statutes § 21-1488 (2014)

9. Rhode Island General Laws § 11-42-2 (2012)

10. South Carolina Code § 16-17-640 (2012)

11. Wyoming Statutes Stat § 6-2-402 (1997)

12. Washington D.C. § 22–3252

Books and Articles

1. Aaron Minc and Alexandra Arko, How to Permanently Remove Content From Revenge Porn Websites, MINC, 2021.

2. Abir Amin, Falsifying the awareness of young people between globalization and new agitators. Egypt: The Egyptian General Book Authority, 2006.

3. Agnes Talalaev, Everything You Need To Know About Password Management, Patchstack, 2021.

4. Ahmed Awad Belal, Rule of Exclusion of Evidence Obtained by Illicit Methods in Comparative Criminal Procedures - Third Edition, Dar El Nahda El-Arabyia, 2013.

5. Aju D, Anil Kumar Kakelli and Kishore Rajendiran, A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends, Confluence of AI, Machine, and Deep Learning in Cyber Forensics, premiere reference resource, 2021.

6. Bridget Small, Scam emails demand Bitcoin, threaten blackmail, Federal Trade Commission, Consumer Advice, 2020.

7. Carlos Kölbl, Historical Consciousness in Youth. Theoretical and Exemplary Empirical Analyses, University of Bayreuth Germany,

Increasing political consciousness among young people in Berlin, European commission, 2001

8. CCRI's, Nonconsensual Pornography (NCP) Research Results, 2013
9. Cisco Talos, Ransomware: Past, Present, and Future, 2016.
10. Daniel S. Harawa, Social Media Thought crimes. Pace Law Review, 2014.
11. Dant Coenen, Freedom of Speech and the Criminal Law. Boston University Law Review, 2017.
12. David Wall, What is cybercrimes, Journal article, 2004.
13. Dhanya Thakkar, Preventing Digital Extortion Mitigate ransomware, DDoS, and other cyber-extortion attacks Packt Publishing, UK, 2017.
14. Digital Blackmail as an emerging, Public-Private analytic change program, 2016.
15. Dincan Riley, Adrienne Bailon, nude pics extortion plot, INQUISITR, 2019.
16. Dorrian Horsey, I'm Being Blackmailed: How to Deal with Blackmail on the Internet, MINC, 2022.
17. Europol, Internet Organized Crime Threat Assessment, 2019.
18. Eman El-Gendy, Cyber blackmail. A crime that needs more than one law, Al-Wafd Newspaper, January 5, 2022.
19. FBI Releases the Internet Crime Complaint Center, Internet Crime Report, Including COVID-19 Scam Statistics, 2020.
20. FindLaw Team, State Revenge Porn Laws, 2022.

21. Gjalt-Jorn Y Peters, Robert A C Ruiter and Gerjo Kok, Threatening communication: A qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals. International Journal of Psychology, 2014.

22. Guy Adams, John Travolta ends $25m extortion case linked to death of his son, INDEPENDENT, 2009.

23. Hiba Abdul Mohsin Abdul Kareem, The Social Risks of Electronic Extortion, Palarch's Journal of Archaeology of Egypt/Egyptology, 2021.

24. Ioana Vasiu and Lucian Vasiu, Forms and Consequences of the Cyber Threats and Extortion Phenomenon, European Journal of Sustainable Development, 2020.

25. Internet Crime Report 2020.

26. Interpol, African Cyber threat assessment report, October 2021.

27. Ivana Vojinovic, More Than 70 Cybercrime Statistics - A $6 Trillion Problem, DataProt, 2022.

28. James Lyne, 30,000 Web Sites Hacked A Day. How Do You Host Yours?, Forbes, 2013.

29. Jilian Peterson and James Densley, Cyber Violence: What Do We Know and Where Do We Go From Here?. Aggression and Violent Behavior, 2017.

30. Kelly Bissell and Ryan Lasalle, Ninth Annual Cost of Cybercrime Study, Accenture, 2019.

31. Kyung-Shick Choi, Tim Scott and Daniel LeClair, Ransomware against Police: Diagnosis of Risk Factors via Application of Cyber-

Routine Activities Theory. International Journal of Forensic Science & Pathology, 2016.

32. Maggie Miller, FBI sees spike in cybercrime reports during coronavirus pandemic, The Hill, 2020.
33. Maskun Maskun, Hasbi Assidiq and Armelia Safira, Cyber Attack -The Burden of International Crime Proof: Obstacles and Challenges Conference: The 2nd International Conference of Law, Government and Social Justice (ICOLGAS) 2021.
34. Michael Heller, Gathering cybercrime evidence can be difficult, TechTarget.
35. Michelle Caruso, CNN STAFF, Pair gets four years in Stamos extortion case, 2010.
36. Mitchell N. Berman, The Evidentiary Theory of Blackmail: Taking Motives Seriously. University of Chicago Law Review, 1998.
37. Mohamed El-Guindy, Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism. Journal of Law and Emerging Technologies, 1(1), 2021.
38. Mohamed El-Guindy, Cybercrime in the Middle East. ISSA Journal, 6(6), 2008.
39. Mohamed Al-Shanawi, The new fraud crimes. Egypt: Law Books Press, 2008.
40. Nasser Al-Shehri, Information Security, Perfect Awareness and Impervious Protection, first edition, Riyadh: Obeikan Library for Publishing and Distribution, 2013.
41. Oonagh McPhillips, Cybercrime: Current Threats and Responses A review of the research literature Co-Authors Sheelagh Brady & Caitríona Heinl, SAR Consultancy & EXEDEC, 2020.

42. Rebecca Louise Shaw, A Study of emotional vulnerability and reactions to stress, A thesis submitted to the University of Manchester for the degree of Doctor in Clinical Psychology (ClinPsyD) in the Faculty of Medical and Human Sciences, 2014.

43. Robert W. Taylor, Eric J. Fritsch and John Liederbach,. Digital crime and digital terrorism. Boston: Pearson, 2015.

44. Samir Thakkar, Ransom ware - Exploring the Electronic form of Extortion, research gate, 2015.

45. Suliman Al-Ghadian, Yahya Khatatbeh and Ezzeddin Al-Nuaimi, Forms of crimes of cyber blackmailing and their motives and their psychological implications from the point of view of teachers, numbers of committee and psychological counselors, Journal of security research vol 27, issue 69, 2018.

46. Sultan of Sleaze' arrested in Tom Cruise extortion plot, The Guardian Newspaper, 11 Jan 2008.

47. Trend Micro and INTERPOL, Cybercrime in West Africa; Poised for an Underground Market, 2017.

48. Wael Shater, The legal framework for the crime of electronic extortion in electronic games, AJSP, Arab Journal for Scientific Publishing ISSN: 2020.