The Protection of Women from cyber blackmail in Arab Countries in the light of International Human Rights Law

DR. MOHAMMED ELSHOBAKE
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Introduction

- The global use of the Internet and social media has increased significantly, as the number of Internet users reached 5,16 billion and the number of social media users reached 4.76 billion social media users in January 2023.
- In the era of digitization, the profound impact of the internet and information technology has resulted in the transformation of nearly every aspect of modern life.
- While these progressions have granted unparalleled possibilities for communication, learning, and empowerment, they have concurrently spawned novel complexities, especially in the field of cybercrime.

Introduction

- Cyber blackmail is an increasingly common form of crime around the world.
- However, it has become particularly prevalent in Arab countries such as Egypt, Iraq, Lebanon, Syria, Morocco, Jordan, and other Arab countries, where women are often targeted.

The Concept of Cyber Blackmail against women

• It is defined as "a threat and intimidation of a woman through the publication of images or videos, or the disclosure of sensitive information about her via the internet network or any other information technology method, with the aim of extorting money or exploiting the woman to carry out illegal acts."

The Concept of Cyber Blackmail against women

The crime of cyber blackmail occurs through several steps:

- Obtaining confidential data and information.
- Direct or anonymous communication with the victim.
- Coercion, Threats, and Intimidation.
- Demanding payment or forcing the victim to perform a specific act.

The Concept of Cyber Blackmail against women

The use of electronic methods to perpetrate blackmail introduces distinctive characteristics that differentiate it from traditional forms of blackmail, such as:

- Heightened opportunity to commit cyber blackmail due to the ease of accessing digitally stored personal data.
- Cyber blackmail often carries a reduced risk of detection and a higher possibility of impunity.
- It is a cross-border crime, as the perpetrator can commit it from anywhere and at any time using information technology methods.
- It is also a difficult crime to prove, as the criminal does not leave a tangible physical trace as in traditional crimes.
- It is usually committed by professional technical criminals.

Prevalence of Cyber Blackmail against women in Arab Countries

- Cyber blackmail against women in Arab countries is a concerning issue that has been becoming increasingly prevalent in recent years. However, it is not possible to provide accurate statistics on the true rates of crimes, as the majority of victims prefer to remain silent to avoid scandal.
- In Gulf countries, the rates of cyber blackmail crimes are high, as approximately 30,000 cyber blackmail crimes are recorded annually, 80% of their victims are women, and most of them are targeted with sexual content.

Prevalence of Cyber Blackmail against women in Arab Countries

- In Syria, cyber blackmail crimes increased by 30 percent during the war years.
- In Lebanon, Internal Security Forces statistics indicate an increase in cyber blackmail complaints during Covid-19 pandemic by 754%.
- In Yamen, the number of cases of blackmail victims who requested assistance during the last three years exceeded 15 thousand cases.
- In Iraq, the number of cases of cyber blackmail is shocking, as Internal Security Forces dealt with 37 cases of cyber blackmail within just one week in different cities and regions of Iraq.

Digital Connectivity and increased use of social media: Social media usage is prevalent in Arab nations, offering an enabling environment for cyber blackmail due to the easy accessibility of personal information and straightforward communication with potential victims.

Country	Mobile phone Users	Internet Users	Social media Users
Bahrin	2.10 M	1.46 M	1.46 M
	(142.1% of Population)	(99% of Population)	(98.7% of Population)
Lebanon	4.69 M	4.70 M	4.91 M
	(86.4% of Population)	(86.6% of Population)	(90.5% of Population)
Oman		4.44 M	4.17 M
	(136.5% of Population)	(96.4% of Population)	(90.5% of Population)
Qatar	4.89 M	29.M	2.62 M
	(180.9% of Population)	(99% of Population)	(96.8% of Population)
UAE	19.05	9.38 M	10 M
	(200.9% of Population)	(99% of Population)	(105.5% of Population)

Cultural and social factors:

- Arab societies traditionally place a great value on reputation, family honour, and personal privacy.
- Cyber blackmailers exploit these cultural and social factors by threatening to reveal sensitive, or confidential information, knowing that victims may be more likely to comply with their demands to protect their reputation.
- The scandal creates a great stigma that affects the victim and the family. Therefore, fear of scandal may make women more vulnerable to cyber blackmail.

Lack of awareness:

Many individuals in Arab countries are not aware of the dangers of using the Internet and social media, which makes them more vulnerable to cyber blackmail.

Deteriorating economic conditions:

Online blackmailers often aim to obtain financial gains. Poverty, unemployment, and deteriorating economic conditions may prompt some individuals to use electronic blackmail as a means of obtaining money. For example, the recent increase in the rate of cyber blackmail crimes in **Syria**.

Political problems:

- Some Arab countries suffer from political problems, conflicts, and instability, which may create an environment in which cybercrimes including cyber blackmail increase.
- Because of political and economic problems, governments may not be focused on addressing these issues. For example, one of the reasons for the prevalence of cyber blackmail against women in **Yemen** is the miserable political conditions that led to the absence of oversight and accountability and the absence of laws specialized in electronic protection.

Weak legal protection

- Some Arab countries lack comprehensive laws that specifically address cyber crimes against women, including the crime of cyber blackmail, as the laws do not impose deterrent penalties for the perpetrators of this crime. For example, in Yemen, Iraq and Lebanon, there is no special law to combat cybercrime.
- In Egypt, there is special law to combat cybercrime, which is Law on Combating Information Technology Crimes No. (175) of 2018. However, this law does not explicitly address the crime of cyber blackmail.

Weak capabilities and complexity of procedures:

- The law enforcement agencies in some Arab countries do not have the resources and technical development to detect and prosecute the perpetrators of cyber blackmail crimes
- For example, the legal procedures in Iraq for dealing with complaints of cyber blackmail against women are complicated and slow, and some officers treat the victims as if they are guilty or involved in relationships with blackmailers.
- One of the victims of electronic blackmail (a29-year-old girl) said: "The complicated and lengthy security and legal procedures that I underwent after being blackmailed made me stop complaining and resort to the help of one of my relatives".

Impact of Cyber Blackmail on Women's Lives in Arab Countries

- Cyber blackmail caused serious effects on the lives of females in Arab countries, affecting their psychological and physical health, their social status, and their economic condition, and it was a primary reason for them committing suicide.
- Electronic blackmail has been a reason for women being exposed to domestic and social violence. A Yemeni study indicates that more than half of the women who were subjected to cyber blackmail and decided to seek help from their families were subjected to some form of domestic and social violence.

Impact of Cyber Blackmail on Women's Lives in Arab Countries

- Unfortunately, several girls have committed suicide in Arab countries due to cyber blackmail. e.g., In Egypt, there were 2,584 suicide cases in one year for several reasons, most notably cyber blackmail.
- In Morocco, a study by the Challenge Association for Equality and Citizenship on digital violence against women in Morocco reported that 87% of female victims of cyber blackmail thought about committing suicide, and that 20% of them attempted suicide, and some of them actually committed suicide.
- To conclude, cyber blackmail usually begins with a conversation and ends with suicide.

Legal framework governing the protection of women from Cyber blackmail under International Human Rights law

- Universal Declaration of Human Rights (UDHR) of 1948.
- International Covenant on Civil and Political Rights (ICCPR) of 1966.
- Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) of 1979.

Legal framework governing the protection of women from Cyber blackmail under International Human Rights law

Relevant Human Rights:

International human rights instruments do not explicitly indicate cyber blackmail, they encompass principles that can be applied to protect women from such forms of blackmail.:

- The right to privacy.
- The right to the preservation of human dignity.
- Prohibition of torture and cruel, inhuman, or degrading treatment or punishment.
- Prohibition of discrimination and guarantee to all persons equal and effective protection.
- The right to life, liberty and security of the person.

1. Legal reforms:

- Arab countries must enact and reform cybercrime legislation, explicitly criminalizing cyber blackmail and providing deterrent penalties against blackmailers.
- A procedural law must be enacted that simplifies reporting procedures and protects victims.
- It should be ensured that the legal framework to protect women from electronic blackmail in Arab countries is consistent with international standards stipulated in international human rights law.

- 2. Developing technical means and training law enforcement agencies:
- Arab countries should develop technical means to track and arrest perpetrators of cyber blackmail crimes.
- As well as provide specialized training to law enforcement agencies on mechanisms for investigating cyber blackmail crimes and dealing with evidence.
- Arab countries should establish specialized units in investigating cybercrimes, including cyber- blackmail crimes, within law enforcement agencies.

3. Establish confidential and safe reporting mechanisms:

- Law enforcement agencies in Arab countries should create easy-to-use, confidential, and safe mechanisms for reporting incidents of cyber blackmail to encourage victims to come forward and seek help without fear.
- It is necessary to emphasize the immediate response to such reports by law enforcement agencies.

4. Providing victim support services:

Arab governments and NGOs should establish support and assistance services for victims of cyber blackmail, in order to provide psychological and legal support, advice and protection to victims, including providing safe shelters for women exposed to domestic violence and at risk due to cyber blackmail.

5. Developing educational curricula for digital literacy:

Arab countries should develop educational curricula for schools and universities on cybersecurity and digital literacy to empower girls and women, raise their awareness, and provide them with the necessary skills to protect themselves from online dangers.

6. Launching awareness campaigns for victims and families:

Official and unofficial institutions should launch comprehensive awareness campaigns for women, families, and communities to educate them about the dangers of electronic blackmail, how to protect themselves, and the mechanisms for families to deal with victims of cyber blackmail.

7. International cooperation:

Arab countries should cooperate among themselves and with other countries and international organizations to combat cyber blackmail crimes, including exchanging experiences in the field of investigating cyber blackmail cases and prosecuting their perpetrators, as well as in arresting and extraditing the accused in accordance with specific agreements.

8. Promoting community engagement and media role:

Arab society must bear its moral responsibilities towards the victims of cyber blackmail by reducing stigma and blaming the victims of cyber blackmail. This could be achieved by promoting community engagement and discussion between officials, community leaders, and influencers through various media in order to raise awareness and protect victims from the consequences of cyber blackmail, including the most dangerous consequences, which is suicide.