

---

## Combating Cyber Sextortion Crimes in International Law and National Legislation

Duha Suleiman Ibrahim Nazzal<sup>(1)</sup> , Prof. Abdelsalam Hammash<sup>(2)</sup>

<sup>(1)</sup> PhD student in law, University of Islamic Sciences  
[Lawyer.dnazzal88@gmail.com](mailto:Lawyer.dnazzal88@gmail.com).

<sup>(2)</sup> Professor of International Law, University of Islamic Sciences, Department of Law.  
[Hammash23@gmail.com](mailto:Hammash23@gmail.com)

doi: <https://doi.org/10.37745/gjplr.2013/vol11n63259>

Published December 04, 2023

---

**Citation:** Nazzal D S.I and Hammash A. (2023) Combating Cyber Sextortion Crimes in International Law and National Legislation, *Global Journal of Politics and Law Research*, Vol.11, No.6, pp.32-59

---

**ABSTRACT:** *Cyber sextortion, the malicious act of coercing individuals into providing sexually explicit content through online means, has emerged as a pervasive threat in the digital age. This article explores the challenges of combating cyber sextortion crimes through the lens of international law and national legislation. Analyzing the existing legal frameworks, jurisdictional complexities, and gaps in enforcement, the article proposes comprehensive strategies to address and mitigate the impact of these crimes on individuals and society. By examining recent case studies and legal precedents, it sheds light on the evolving nature of cyber sextortion and emphasizes the need for collaborative efforts at both international and national levels.*

**KEYWORDS:** cyber sextortion, international law, national legislation

---

### INTRODUCTION

There have been different attempts by the legislator and the judiciary in different countries to determine criminal responsibility for electronic crimes, including electronic sexual blackmail. These attempts have taken the form of legislative intervention to set controls for the Internet or expansion on the part of the judiciary in interpreting existing criminal texts to include these actions or applying existing texts to sexual blackmail crimes. Electronic because its texts allow it.

Unlike traditional crimes, electronic sexual blackmail crimes are committed for various reasons, most of which target networks and systems that are linked to bank accounts and financial transfers. Perhaps the most important of them is the motive of greed and avarice, obtaining the largest amount of money with the least effort and the shortest time, or the desire for revenge against the institution in which he works, or To demonstrate his ability and show off his muscles in front of

all his colleagues and friends, or for various other motives such as defamation, slander, defamation, etc.<sup>1)</sup> but rather; The incident in the crime of electronic sexual blackmail may harm the honor of the victim, degrade his status, or harm his honor or the honor of his family or one of his relatives, as long as it results in material or moral damage to the victim of the crime.<sup>2)</sup> That is, in the crime of electronic sexual blackmail, he threatens to expose something, which in its essence is a threat to harm the victim in order to pressure his will, achieve what the perpetrator demands, and reach his goal, which makes the victim disturbed to the point of being unable to do his usual work, which affects the person. In his security and personal freedom, that is why the legislator included this crime within the scope of crimes affecting human freedom and sanctity.

Whereas modern constitutions and legislation stipulate the principle of legitimacy of crimes and punishments, which confirms that there is no crime or punishment except based on the law. We cannot say that this or that act is sinful by law unless there is a provision prior to its occurrence that prevents its commission and imposes a penalty for it. The legislator had to precisely define the criminal activity and its elements so that the judge would not be left with a controlling authority that would allow him to interfere in determining these elements, so it is permissible to do so. The legislator's place.

In fact, criminal penalties represent the important effect that results from the criminalization of aggressive behavior, and therefore the penal legislator regulated every act or omission that violates its established texts, and made a penalty in exchange for this criminal act or omission, in order to achieve general deterrence for society as a whole, and achieve specific deterrence for the perpetrators. Punishment has two aspects: the first is therapeutic by imposing punishment on the perpetrators and the other is preventive by deterring those who are tempted to commit the crime in the future. Criminal systems and legislation differ from one country to another, depending on the punitive policy taken by the legislator, whether mitigating or tightening the penalties.<sup>3)</sup> Then comes the role of the criminal judiciary in applying these legislative texts to criminal behaviors and imposing penalties that are commensurate with the crime committed by the offender.<sup>4)</sup>

---

<sup>1)</sup>Jamil Abdel-Baqi Al-Saghir, *Criminal Law and Modern Technology*, Dar Al-Nahda Al-Arabiya, Cairo, 1992, 1/62.

<sup>2)</sup>Mahmoud Naguib Hosni, *Explanation of the Penal Code, Special Section*, 8th edition, Dar Al-Nahda Al-Arabiya, Cairo, 1984, p. 197.

<sup>3)</sup>Fakhri Abdul Razzaq Salbi Al-Hadithi, *Explanation of the Penal Code (General Section)*, Al-Zaman Press, Baghdad, 1992, pp. 36, 37.

<sup>4)</sup>Emil Jabbar Ashour, *Criminal Liability for the Crime of Electronic Blackmail on Social Media Sites (Comparative Knowledge)*, Maysan Research Journal, Volume 16, Issue 31, June, 2020 AD.

The perpetrator may threaten the victim by attributing to him a specific incident that degrades his value or the value of others or affects his honor or the honor of his family or someone dear to him. The law does not care whether the incident with which the perpetrator threatens the victim by attributing to him is true or false, and it also does not matter whether the harm was The victim shall be harmed personally or by another person, such as his wife, one of his children, or one of his relatives.

Accordingly, the criminal liability for the crime of electronic sexual blackmail and its effects can be studied through two sections, as follows:

**The first topic: combating electronic sexual blackmail crimes in international law.**

**The second topic: combating electronic sexual blackmail crimes and its effects in national laws.**

**The first topic**

**Combating cyber sextortion crimes in international law**

Crimes committed via the Internet, just as they occur at the national level, are also committed at the international level. Electronic sexual blackmail crimes are usually committed remotely, such that the perpetrator is not present at the crime scene, and thus the distances between the action and the result are wide, and these distances do not stop at the borders of the state, but may extend to the territorial scope of another state, which doubles the difficulty of detecting or prosecuting them.<sup>1)</sup>

The perpetrator may commit a crime in one country and its effects may occur in another country, which raises many difficulties, such as the extent to which electronic communications are tracked by investigative authorities, in order to establish evidence of these crimes. and then adjust it<sup>2)</sup>. Criminal laws across countries still adopt the idea of territoriality defining jurisdiction, which makes these laws unable to keep pace with the developments brought about by modern technology, and thus the problem of detection and search for evidence emerges. This is on the one hand, and on the other hand, the inadequacy of international agreements concluded between... Countries

---

<sup>1)</sup>Al-Shahat Ibrahim Muhammad Mansour, *Cybercrimes in Islamic Sharia and Man-made Laws*, 1st edition, Dar Al-Fikr Al-Jami'i, Alexandria, 2011, pp. 193-194.

<sup>2)</sup>Osama Ahmed Al-Manasa, *Computer and Internet Crimes, "A Comparative Analytical Study,"* 1st edition, Dar Wael for Printing and Publishing, Amman, 2001, p. 292.

regarding the mechanism for searching for perpetrators and seizing evidence in this regard are also among the difficulties facing international efforts made in this context.

The crime of electronic sexual blackmail is committed in a theater that cannot be geographically determined, but it includes the largest human gathering characterized by complex connections and interconnections. Its most important characteristic is the creation of special mechanisms to impose obligations and comply with them, such as cutting off contact with those who violate some rules or expelling them from forums. However, this human gathering The huge lacks common moral standards.

Hence, the international community realized that the problem of cybercrime is not an individual problem that concerns only one country, but rather concerns the entire international community, as criminal groups in information systems have begun to extend their influence throughout the world thanks to the power, influence, and influence they possess. Hence, the international community took the initiative to Taking necessary measures aimed at combating electronic crimes, including electronic sexual blackmail.

Accordingly; The international response to the crime of electronic sexual blackmail can be studied through two demands, as follows:

**The first requirement: The role of international organizations and agreements to confront cybercrime.**

**The second requirement: The role of regional organizations and agreements to confront cybercrime.**

**The first requirement is the role of global organizations and agreements to confront cybercrime**

The means of combating cyber sextortion crimes are not limited to the national side only, as the danger of these crimes is a danger with an international dimension as well. Cybercrimes are committed most of the time by people from outside the country's borders, as they pass through international communication networks until they reach the desired result. Among them, inspection and seizure procedures that extend beyond the state's territory require cooperation and a coordinated international effort among the countries affected by these crimes, in order to be able to eliminate them, and this in turn requires the establishment of joint security services and the conclusion of bilateral agreements to eliminate and reduce them.

Investigating cybercrime and prosecuting its perpetrators emphasizes the importance of mutual judicial assistance between countries, as it is impossible for the state alone to eliminate these cross-border crimes. Combating it can only be achieved if there is international cooperation at the criminal procedural level, as it allows direct communication between police agencies in different countries, through the establishment of specialized security agencies in the field of research,

investigation, and collecting information about cybercrime perpetrators. In electronic sexual blackmail crimes, the perpetrator may have the nationality of one country, and the viral attack is launched from computers located in another country, and the effects occur in a third country. It is natural that border problems stand as an obstacle to discovering these crimes and punishing their perpetrators. Because the police force in this or that country is unable to track down and prosecute criminals except within the borders of the country to which this criminal belongs.<sup>1)</sup>

Therefore, there has become an urgent need for concerted international efforts, which undertake this task for countries free of cybercrime, and this is undoubtedly not achieved except through the establishment of a device or organization that takes into account finding effective means to combat the crime of cybersextortion. This is what we will explain in more detail through this requirement, which we have divided into two sections as follows:

**Section One: The role of international organizations in confronting the crime of electronic sexual blackmail.**

**Section Two: The role of international agreements in confronting the crime of electronic sexual blackmail.**

**First branch**

**The role of the International Criminal Police Organization (Interpol) in confronting the crime of electronic sexual blackmail**

The study of the role of international organizations in combating electronic sexual blackmail crimes comes through the following paragraphs:

The International Criminal Police Organization (Interpol) is the largest international police organization, which was established in 1923 and is headquartered in Lyon, France.<sup>2)</sup> The establishment of this organization dates back to when the “International Criminal Police Committee” was established. The goal of this committee was to coordinate between the national security services of European countries in the field of combating crime, especially cybercrime. It is considered one of the specialized international organizations concerned with international cooperation among its member states in the field of combating crime and tracking down criminals

---

<sup>1)</sup>Youssef Hassan Youssef, International Internet Crimes, 1st edition, National Center for Legal Publications, Cairo, 2011, p. 144.

<sup>2)</sup> Muhammad Al-Shennawi, Strategy to Combat Human Trafficking, National Center for Legal Publications, Cairo, 1st edition, 2014, p. 433.

who are able to cross the borders of the state in which they committed their crimes and flee to another state.<sup>1)</sup>

The initiatives of this organization have increased due to the rapid development in communications and information systems; The success of this organization depends on the effective use of its criminal database. The effectiveness of exchanging important information depends not only on the complex computer system owned by Interpol, but also on the national communications network. One of Interpol's most important activities was the circulation of international notes that provided information related to photographs and fingerprints.<sup>2)</sup>

The organization undertakes a number of specializations to achieve its goals, which can be explained as follows:

**First/Objectives of the organization:**

The most important objectives of this organization, according to Article Two of the Charter, are to achieve the following:<sup>3)</sup>

1. Cooperating with member states in apprehending fugitives and those wanted or against whom judicial rulings have been issued, or arrest warrants and summons to appear before investigative authorities, through issuing designated international bulletins.
2. Working to support police efforts in combating cross-border crime, and providing services in the field of forensic evidence, such as fingerprints and DNA.DNA.
3. Collecting and providing information related to crimes and criminals, through the information that the organization - with its main office in Lyon - receives from the national central offices of the criminal police in member states, and this is done through modern technologies and communications networks.

---

<sup>1)</sup>The activity of this committee stopped completely when the Second World War broke out (1939-1945 AD) due to the armed conflict that broke out between European countries.Except thatThe work of this committee was revived again when the war ended in 1945 AD, through the international conference that was held specifically for this purpose in the Austrian capital, “Vienna,” from the sixth to the ninth of June 1946 AD. All the countries that were present at this conference signed the document to revive this International Committee, and these countries considered that document to be constitutional for this international organization “the International Committee.”For more details see:Montaser Saeed Hamouda, Interpol, International Criminal Police Organization, Dar Al-Fikr Al-Jami’i, 2nd edition, 2013, p. 11.

<sup>2)</sup>Ahmed Fathi Sorour, The Legal Confrontation with Terrorism, Al-Ahram Center for Publishing and Translation,2nd ed, 2008, p. 430.

<sup>3)</sup>Adel Abal Ibrahim Kharashi, Problems of International Cooperation in Combating Information Crimes and Ways to Overcome Them, New University Publishing House, 2010, pp. 26-27.



4. Establishing and developing mutual cooperation on the broadest scale between all criminal police authorities within the framework of existing laws in various countries, and in the spirit of the Universal Declaration of Human Rights.

Accordingly; Interpol's strategy in combating cybercrime is to reach a safe global country. In 2004, it established a special unit to combat technology crimes. The organization also cooperated with the Group of Eight major countries (G8) to develop strategies to confront this type of crime through:<sup>(1)</sup>

- Using modern means to combat crimes, such as using a central database of pornographic images transferred from party countries, which uses a program **Excalibur** For automatic analysis and comparison of images.
- Establishing a security communications center that operates 24 hours (7) a week at the level of police departments in the States Parties.
- Providing the police of States Parties with guidance manuals on cybercrime and how to train to combat and investigate them.<sup>(2)</sup>

We note that the International Police Organization (Interpol) is a global organization that exchanges information in combating cross-border electronic crime between countries.

### **Second: The powers of the International Criminal Police Organization.**

The International Criminal Police Organization is responsible for coordinating all efforts made by police departments in member states in the field of crime prevention and prevention and international security cooperation. The organization carries out its activities in the following two axes:

#### **1. Exchange of information:**

This includes the information axis; It includes reports, correspondence, or communications carried out by police officers in a member state with other member states of the General Secretariat regarding criminal activities and their perpetrators. This includes descriptions of criminals, their

---

<sup>(1)</sup> a. Nabila Heba Harwal, research titled Procedural Aspects of Internet Crimes in the Evidence-Gathering Stage - A Comparative Study, Dar Al-Fikr Al-Jami'i, 2007, p. 153.

<sup>(2)</sup>As an example of Interpol's role in...oppositeH thecrimeseThis operation was carried out by the US Federal Bureau of Investigation in conjunction with Interpol, related to pursuing the person who spread the love worm.Love Bui online in Philippines,And so onThat operation, in which a young German man was arrested on charges of distributing a virus through coordination with Interpol between the American Federal Bureau of Investigation and the German police, was achieved by dismantling the website on which pictures were published.aBahia in association with Orpol on 2/5/2005M.

fingerprints, photographs, and descriptions and photographs of the objects involved in the crimes.<sup>1)</sup>

In the same context, some international agreements are concerned with exchanging information, as Article 1 of the Riyadh Arab Agreement for Judicial Cooperation stipulates the necessity of exchanging information between state parties with regard to applicable legislative texts and legal and judicial research. The Sixth United Nations Conference on the Prevention of Crime and the Treatment of Offenders also addressed the need to develop the systematic exchange of information, as it is an effective element in the international plan of action to prevent and combat crime, and also recommended the commitment of the United Nations to establish an information base to inform States Parties of global trends in the field of crime <sup>(2)</sup>. Paragraph (c) of Article Seven of the Arab International Organization for Social Defense Against Crime Convention stipulates that: “Information, data, statistics and publications shall be exchanged.”<sup>3)</sup>

In the same context, Article (21-21) of the judicial agreement between Jordan and Syria regarding the exchange of the criminal record stipulates the following:<sup>4)</sup>

1- The two countries’ judicial registry departments exchange information on misdemeanors and felonies adjudicated in one of them against nationals of the other country.

2- Each of the two administrations gives the second administration free of charge the information it requests from the criminal record. Accordingly, the international community is very interested in exchanging information between countries in the field of combating cybercrime, because correct and reliable information provides support to law enforcement agencies in all fields, including following up on the emergence of cybercrimes. Criminal organizations and sources of

---

<sup>(1)</sup> Hussein Fathi Al-Hamouli, *International Security Cooperation in the Implementation of Criminal Judgments*, Cairo, 2015, p. 521.

<sup>(2)</sup>See Muhammad Karim Ali, *Combating Organized Crime under International Treaties*, Master’s Thesis, Faculty of Law, Mansoura University, 2016, pp. 86-87.

<sup>(3)</sup> The organization includes three specialized offices And It is: the International Criminal Police Bureau And The Arab International Bureau for Combating Crime and the Arab International Bureau for Narcotics Affairs, and the three offices cooperate with international bodies that investigate the purposes it aims to achieve by exchanging research, scientific studies, and practical experiences, and participating in seminars, conferences, and other aspects of cooperation, And for more details look: The Jordanian Gazette published on 7/16/1970, issue 2250, p. 963.

<sup>(4)</sup>This agreement was signed in Damascus in 1953, and the Jordanian judicial agreement was issued under Law No. (32) of 1960..

For more details see: Ali Hussein Al-Tawalba, research on international judicial cooperation in combating cybercrimes, Faculty of Law, University of Applied Sciences, undated, p.6.



funds, and the necessity of concluding bilateral or collective agreements or treaties to extradite criminals and exchange information between countries to reduce the danger and harm of cybercrimes.

## **2. Personal investigation:**

This axis is one of the most important aspects of international security cooperation.<sup>1)</sup>There is a large number of these criminals who use pseudonyms or impersonate personalities behind which they hide their real names in order to mislead security personnel and avoid prosecution and surveillance procedures. However, revealing the true identities of these people who are adept at impersonating names and personalities is mostly done through comparing fingerprints. If it is easy for a criminal to change his name, then changing his fingerprints is impossible. It is sufficient, therefore, to collect his fingerprints from the criminal once, and to record them in a specialized central department until his true identity is restored to him and his identity is revealed every time he wants to hide it. No matter how much effort he makes to change his name or alter his external appearance, fingerprints remain decisive evidence to prove his identity and reveal (His identity)<sup>2)</sup>Interpol has contributed to combating crime by providing its member states with important information about criminals wanted by justice.

Recently, Interpol's focus has been primarily on organized crime and related criminal activities such as money laundering.<sup>3)</sup>

## **3. Transfer actions:**

It means that a state, based on an agreement, takes criminal measures for a crime committed in the territory of another state and for the benefit of this state, under certain conditions.<sup>4)</sup>

---

<sup>(1)</sup> Aladdin Shehata, International Cooperation in the Field of Combating Crime, A Vision for a National Strategy for International Cooperation in the Field of Combating Drugs, Cairo, 2000, p. 178.

<sup>(2)</sup>See Hassan Al-Tawalba, International Procedural Cooperation in the Field of Extradition, University of Applied Sciences, Bahrain, pp. 13-14,<http://www.policemc.gov.bh>.

<sup>(3)</sup>Sabrina Adamoli and others (Organized Crime Around The World. op cit p124 Dr.. Kurkis Yusuf Daoud, Organized Crime, International Scientific House, 2001, p. 110. Akram Abdul Razzaq Al-Mashhadani, Interpol and the pursuit of wanted persons (blurring understanding of the tasks of the...thatTarbol), article published in Katabat newspaper, November 23, 2011,<http://www.kitabat.com/ar>

<sup>(4)</sup>Salem Muhammad Suleiman Al-Awjali, Provisions of Criminal Liability for International Crimes in National Legislation - A Comparative Study, PhD thesis, Ain Shams University, Cairo, 1997, p. 27.

- That the act attributed to the person constitutes a crime in the requesting state and the requested state.
- The action required to be taken should lead to arriving at the truth, such as if evidence of the crime exists in the requested country.<sup>1)</sup>.

## **Second section**

### **The role of international agreements in confronting the crime of electronic sexual blackmail**

International treaties are the basis on which international cooperation in the field of combating cybercrime is based. Many treaties have been concluded that work on international cooperation in the field of combating cybercrime, including the Budapest Treaty, the European Treaty, the Berne Treaty, and the TRIPS Treaty.

#### **First: The Budapest Convention against Cybercrime.**

---

<sup>(1)</sup>for example: A criminal rose from theaArgentine in 1995 by accessing the computer network at the Naval Surveillance Command Center for Oceanic Reconnaissance in California.In a wayUnlawful to what no Less than367A site across the world and over836Suitable and include12circleaAmerican marine sites and targeting138Signed in23Town, and modified some files, but the majority of criminal activity focused on installing Exploration's filesaZalaaSky and the user's personal passwords, and estimated material losses as a result of this in the NASA networkaMore than one hundred thousand dollars. Several parties cooperated to pursue the information criminal, and as a result of the investigations, a judicial order was obtained from the competent court allowing her to enter and eavesdrop on electronic communications. Her computer was linked to Harvard University, which made her able to determine the identity of the criminal. The criminal is among16500Account from user accounts and through the use of the shrinkage process Automation, at that time these methods were not usedaformeraAfter investigations, it was foundaNot a young manaRegini, and according to the information provided to the Argentine authorities, sheaIssuing a warrant to search and seize a headquartersaThe accused's height and his personal computer equipment were seized with the help of the criminal policeaInterpol International, and a criminal warrant was issued by the US government accusing him of violating computer-related laws. The accused confessed and was sentenced to probation for 3 years and a fine of \$5,000.

The Neis, Argentine Computer Intersection Investigation - FBI - Law Enforcement Bulletin - 0 ct 1928, VOL 67. Issue 10, p9.

Dr.. Ali Hussein Al-Tawalba, research on international judicial cooperation in combating cybercrime, Faculty of Law,University of Applied Sciences, pp. 7-8

In late 2001, the Hungarian capital, Budapest, witnessed the birth of the first international agreements combating cybercrime, which crystallized international cooperation and solidarity in combating and reducing them.<sup>1)</sup> Where cybercrime is committed in a location that cannot be geographically determined, the European Council held the Budapest Convention for the year 2001 on electronic crimes)<sup>2)</sup> Convinced that this agreement will provide what is necessary to deter any action directed against confidentiality in information and the availability of computer systems, networks, and data, and to take measures to combat crimes via the Internet. The agreement stressed the need to take legislative measures to combat cybercrime and its dangers to countries, especially in light of the huge and expanded development and progress in Information networks and the Internet, which called for combating all criminal activities targeting information security, ensuring the prosecution and detection of the perpetrators of these crimes, and providing all appropriate means for investigation, investigation, inspection and trial, focusing on the importance of cooperation at the local, regional and international levels.<sup>3)</sup>

This international treaty aims to unify international efforts in the field of combating cybercrime, which has moved from an initial stage of innocent infiltration attempts carried out by amateurs in most cases and without any criminal purpose, to a new stage carried out by professionals with the highest degree of specialization. Such as the electronic sexual blackmail crimes in question, which are issues that endanger the lives and property of many Internet users, are the first step in the field of forming international solidarity against those crimes that take place on the Internet and their worst use. The signing of this agreement by officials in European countries is an addition to America, Japan, Canada and South Africa are the result of discussions and negotiations that took more than four years until the appropriate final version of that agreement was reached until it was signed by all parties without finding any objection from any of them. On the contrary, it found acceptance from new parties so that the circle of countries was expanded. Which agrees to join that agreement, and the International Federation and international solidarity in the field of combating cybercrime will be expanded (<sup>4)</sup>.

This agreement stipulates that each party may take legislative and other measures to determine its jurisdiction with respect to every crime that occurs in accordance with what is contained in Articles

---

<sup>1)</sup>Munir Muhammad Al-Junaibi, and Mamdouh Muhammad Al-Junaibi, Internet and Computer Crimes Lee and means of combating it, Dar Al-Fikr University, 2004 edition, p. 96.

<sup>2)</sup>Abdullah Daghsh Al-Ajmi, Practical and Legal Problems of Cybercrime - A Comparative Study, Master's Thesis, Middle East University 2014, p. 100.

<sup>3)</sup> Mahrous Nassar Ghayeb, Information Crime, published in Al-Technical Magazine, Volume 24, 2011, p. 18.

<sup>4)</sup>Munir Muhammad Al-Junaibi, and Mamdouh Muhammad Al-Junaibi, previous reference, p. 96.

2 to 11 of the current agreement when the crime occurs.<sup>1)</sup>: a. Within the local scope of the state b. On board a ship carrying the flag of that country c. On board an aircraft registered in this country d. By one of her subjects H. If the crime is punishable by a criminal offense in the place where it was committed, and. If the crime does not fall within any jurisdiction of any other country.”

Each party has the right to make a reservation and not apply the rules of jurisdiction stipulated in the first paragraph (b and d) of this article, and that will be in special conditions and cases. This is because the Model Arab Law did not classify cybercrimes based on any rules to determine jurisdiction, so if criminal jurisprudence today goes to Accepting the idea of applying foreign law to confront crime at the national level, which has been shown to go beyond the idea of inseparability of criminal and legislative jurisdiction. It is a fortiori to accept this idea and delve into it in crimes committed in the virtual space that cross borders and continents. Thus, we determine the necessity of resorting to setting criminal attribution controls to determine jurisdiction. Substantive and procedural classification of these crimes into categories that include the interests that must be protected at the global level and refer to the applicable law.<sup>2)</sup>

Therefore, these rules must be formulated within the framework of international agreements, as the crime of electronic sexual blackmail is an international crime that cannot be confronted and combated unless there is international cooperation. This has been made clear by many countries alone that they cannot confront these crimes committed over the Internet, no matter how much they issue laws or how severe the penalties are, because These crimes cross borders.<sup>3)</sup> It is not limited to a specific country, but rather the criminal infiltrates many countries before accessing the computer system. The most important thing is the Budapest Agreement in a way that allows for the exchange of cooperation, whether at the level of collecting evidence or extraditing criminals. This indicates that the international world is on the verge of an expansion in cooperation. It is

---

<sup>1)</sup>Article (22) of the aforementioned Budapest Convention.

<sup>2)</sup> keyaBu Bakr Al-Matroudi, Cybercrime, paper presented to the Third Conference of Chiefs of Supreme Courts in Arab Countries, Sudan, September 22-23, 2012, p. 27.

<sup>3)</sup>In this context, it can be pointed out incident I mentioned it one Studies on Crimes that Done via Internet when Take control One of them on System Computer private At an airport American And he rose By turning off Lamps Lighting existing on Corridors Landing and this is maybe that Lead to Dropp off Planes And death Preparation from people, And after Investigate Show that behind the incident a job terrorist teenager from California, And for this He should that Complete cooperation international For example This is amazing Crimes, and for more detailslook:Lawyer Mounir Muhammad Al-Junaihi and Lawyer Mamdouh Muhammad Al-Junaihi, previous source, p. 182.

assumed that judicial and security cooperation will take place together and directly, because the time factor in cybercrimes requires speed and accuracy in completion.<sup>1)</sup>

Therefore, although there is international cooperation in reducing electronic sexual blackmail crimes; However, there are still obstacles and difficulties facing it because there is no agreement between countries on the general concept of electronic crimes and then electronic sexual blackmail crimes, and also there is no agreement on criminal procedures between the laws of countries in investigating and investigating these crimes.

### **Second: The European Convention against Cybercrime.**

Commissioned by the European Council, the Special Committee on Crime Issues signed the final draft of a comprehensive treaty aimed at helping countries combat cybercrime, amid criticism from advocates of protecting personal freedom. After it is ratified by the Council Presidency and signed by the countries concerned, the agreement will oblige the signatory countries to enact The minimum necessary laws to deal with high-tech crimes, including electronic sexual blackmail crimes.<sup>2)</sup>

The provisions of this treaty include paragraphs that guarantee governments the right to monitor and obligate states to help each other in collecting evidence and enforcing the law, but the new international powers will come at the expense of protecting citizens from governments misusing the powers given to them by that agreement, which they may misuse.<sup>3)</sup>

### **The second requirement is the role of regional organizations and international cooperation to confront electronic sexual blackmail crimes**

The means of combating information technology crimes are not limited to the national aspect only. The danger of these crimes is also a danger with an international dimension. Information crimes are most often committed by people from outside the borders of the state, as they pass through international communication networks until they reach the desired result. Inspection and seizure procedures that extend beyond the territory of the state require cooperation and a coordinated international effort among the countries affected by these crimes, in order to be able to eliminate them, and this in turn requires the establishment of joint security services and the conclusion of

---

<sup>(1)</sup> Muhammad Amin Al-Bishri, Investigation into Computer Crimes, Dar Al-Kutub Al-Lawaniyya, Egypt,2009, p. 178.

<sup>(2)</sup>Saeedani Salami, Development of International Legislation and Agreements in the Field of Information Crimes (Facts and Approaches), Al-Ustad Al-Researcher Journal for Legal and Political Studies, Issue Ten, Volume One, Publication Date 6/4/2018, p. 5.

<sup>(3)</sup>Munir Muhammad Al-Junaibi, and Mamdouh Muhammad Al-Junaibi, previous reference, p. 101.

bilateral agreements to eliminate and reduce them, and this is what we will do. By clarifying it in detail in this requirement, we divided it into two sections, the first in which we discuss international cooperation in the field of confronting information crimes, while we leave the second section to talk about international efforts in confronting information crimes, as follows.

**Section One: The role of regional organizations and agreements in confronting the crime of electronic sexual blackmail.**

**Section Two: International cooperation in confronting the crime of electronic sexual blackmail.**

**First branch**

**The role of regional organizations and agreements in confronting the crime of electronic sexual blackmail**

Regional organizations are considered a manifestation of rapprochement and cooperation between different countries in the era of international organization. In regional organizations, membership is limited to several countries linked to each other by specific ties due to geographical, political, historical or economic circumstances.

**First: The role of the European Union in confronting the crime of electronic sexual blackmail**

The European Council was established in 1949 at the regional level. It is older and more comprehensive than all other European political organizations, as it covers all fields. Its headquarters are in the city of Strasbourg, France, and it consists of forty European member states until the end of April 1997. <sup>(1)</sup> The role of the Council and the European Common Market was highlighted on September 17, 1980, with the signing of the Council of Europe Treaty on the Protection of Persons from the Risks of Automated Processing of Personal Data, Especially Threats.<sup>2)</sup> The threat in light of electronic sexual blackmail crimes consists of sending messages that would affect the victim's psyche and create terror, panic and fear in himself, making him disturbed to the point of being unable to carry out his usual activities because of that threat, and it is a threat that affects a person's security and personal freedom and for this reason. The legislator included this crime within the scope of crimes affecting human freedom and sanctity.<sup>3)</sup>

---

<sup>(1)</sup> Aziz Ali Abdul Aziz Jamadar, Organized Crimes between Scientific Progress and Security Control, Ras Al Khaimah National Press, 1st edition, 2012, p. 277.

<sup>(2)</sup> Lawyer MuhammadaWho? aHamad Al-Shawabkeh, Computer and Internet Crimes (Information Crime), 2004, p. 73.

<sup>(3)</sup> Abdul-Ilah Al-Nawaisa, Information Technology Crimes, previous reference, p. 113 et seq



The Council of Europe has issued a number of recommendations emphasizing the expansion of the scope of protection, to include sectors of private activities such as personal research data. Among the efforts made at the regional level, several resolutions have been issued by the European Parliament, including the resolution of April 8, 1979 on protecting the individual in the face of the technical development of information technology, and the resolution Issue No. (13/81).R) 1980 on the exchange of legal information relating to data protection)<sup>1)</sup>As well as Recommendation No. (1/81R) in 1981 regarding the organization of automatically processed medical data in information banks, and Recommendation No. 10/R83 in 1983 regarding the protection of personal data used for scientific research)<sup>2)</sup>.

The European Council has paid attention to the crimes of electronic sexual blackmail, which is a crime that essentially depends on the victim's loss of choice. This is what the European Council has given special protection to, as the threat resulting from blackmail has a psychological content, represented by warning the threatened person that he will harm him personally or A person dear to him, whether this harm is physical, affecting the victim's body or money, or moral, affecting his honor, reputation, and family.<sup>3)</sup>The threat here is achieved in the crime of electronic sexual blackmail by threatening the victim with exposing his situation and publishing pictures, videos, audio recordings, information and personal data affecting the victim himself or someone dear to him, in order to force the victim to do an act or abstain from it, even if doing this act or abstaining is whether lawful or unlawful)<sup>4)</sup>The perpetrator may threaten the victim by attributing to him a specific incident that degrades his worth or the value of others or affects his honor or the honor of his family or someone dear to him. The law does not care whether the incident with which the perpetrator threatens the victim by attributing to him is true or untrue, and it also does not matter whether it is The harm befalls the victim himself or another person, such as his wife, one of his children, or one of his relatives.

The European Council plays a prominent role in the field of electronic crimes, especially in the field of preserving individual data and everything related to private life, and then combating what is called the phenomenon of electronic sexual blackmail. The reason for this is that the countries belonging to this Council are among the scientifically and technologically advanced countries,

---

(1) Abdel Wahed Muhammad Al-Far, International Organizations - General Theory - The United Nations - Specialized Organizations - Regional Organizations, Dar Al-Nahda Al-Arabi, Cairo, 2008, p. 326

(2) Lawyer MuhammadaWho? aHamad Al-Shawabkeh, sourceformer, p. 74.

(3) Ramses Benham, Penal Code, "Special Section Crimes," Mansha'at al-Ma'arif-Beirut, 1999, p. 1195

(4) Mamdouh Rashid Musharraf, Criminal Protection for the Victim of Blackmail, Arab Journal for Security Studies, Volume (33) Issue (70), Riyadh, 2017, p. 208

which makes Prompting it to make recommendations and make agreements that require internal legislation that addresses everything that is new in the field of scientific progress, which in turn affects the diversity of means of committing crimes. Personal information is that information related to a specific - specific - individual, with the intention of information files, that is, a group of information that is processed automatically by a computer, and by processing is meant The mechanism for storing information in a computer, transferring and exchanging programs, changing or deleting information, or distributing it as well. This agreement defines the so-called file controller or person responsible for it as every natural or legal person, public authority, agency, or any body authorized in accordance with the law of the country to determine the purpose of collecting information and the method or purpose of processing it.

It is worth noting that one of the efforts that established the principles of confronting electronic sexual blackmail and protecting privacy is that of the Organization for Economic Cooperation and Development **OECD**, which was scientifically concerned with protecting privacy across borders, and was known as the Guiding Rules on the Protection of Privacy and the Transfer of Personal Data, which are guiding rules whose provisions are not legally binding and are limited only to natural persons.<sup>1)</sup>

Harmony is essential for substantive and procedural laws, and all States should reassess and revise the rules of evidence, searches, arrests and electronic eavesdropping to include digital information, modern computer systems, telecommunications systems and the global nature of the communications network.<sup>2)</sup> It is essential to form specialized law enforcement units to deal with issues related to this type of crime at the level of the country concerned. They can provide a basis for international cooperation based on networks of trust between law enforcement officials in different countries to achieve successful cooperation between different countries.

### **Second: The role of the Arab Council of Ministers of Justice in reducing the crime of electronic sexual blackmail**

---

<sup>(1)</sup> And I have Rules approved OECD guidelines 22 Member states of the organization: Austria, Belgium, Canada, Denmark, Finland, France, West Germany (formerly), Greece, Iceland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States, For more look: Lawyer Muhammada Who? a Hamad Al-Shawabkeh, source former, pp. 74-75.

<sup>(2)</sup> Younis Arab, Developing Legislation in the Field of Combating Cybercrimes, Working Paper "Legislative Trends in Cybercrimes", Telecommunications Regulatory Authority/Muscat - Sultanate of Oman, 2-4a Brill 2006, pp. 29-30.

The idea of establishing a Council of Arab Interior Ministers emerged.<sup>1)</sup> During the first conference of interior ministers of the Arab countries, which was held in Cairo in 1977 AD, it was decided to establish this council. The Council of the League of Arab States approved the statute of the Council of Arab Interior Ministers on December 15, 1982. The council represents the supreme body for joint Arab action regarding combating crime and achieving internal and regional security among others. Arab countries, and the Council has replaced the Arab Organization for Social Defense against Crime in exercising the powers related to the field of Arab security in its comprehensive sense and combating crime. The Council's powers that enable it to achieve its goals include the following:

1. Reporting on means of cooperation with international bodies.
2. Establishing the necessary bodies and devices to implement its objectives.
3. Supporting Arab security services with limited capabilities.

At the end of 2010, the Arab Ministers of Interior and Justice signed five agreements with the aim of strengthening and documenting Arab action. Among these Arab agreements is the Arab Agreement to Combat Transnational Organized Crime, which stipulates combating the crimes of human trafficking and trafficking in human organs. The matter was not limited to this point, but the Arab Convention to Combat Information Technology Crimes stipulated the criminalization of electronic crimes related to human trafficking and human trafficking.<sup>(2)</sup> All countries have taken an interest in the field of international cooperation to combat cybercrimes, including combating cyber-extortion crimes, because of the damage it causes to their economies and the depletion of their human resources, which any country depends on for its economic progress.<sup>(3)</sup>

At its second session in Baghdad in 1982, the Council of Arab Interior Ministers approved the Arab security strategy, which aims to combat crime in all its old and new forms in Arab society, achieve Arab security integration, preserve the security of the Arab world, and protect its institutions, bodies and public facilities from all aggressive attempts. From inside and outside, preserving the security of the individual in the Arab world and ensuring the safety of his privacy, freedom, rights and property)<sup>(4)</sup>.

---

<sup>(1)</sup>Aladdin Muhammad Ahmed Shehata, The National Strategy for International Cooperation in the Field of Combating Crime, an applied comparative study, to combat drugs in both the Arab Republic of Egypt and the United States of America, Cairo, 1999, p. 198.

<sup>(2)</sup>Muhammad Al-Shennawi, Strategy to Combat Human Trafficking Crimes, previous reference, pp. 442-443.

<sup>(3)</sup>See lawyer Munir Muhammad al-Janabahi and lawyer Mamdouh Muhammad al-Janabahi, previous source, p. 199.

<sup>(4)</sup>Gorkis Yusuf Daoud, Organized Crime, previous source, p. 123.

To activate international cooperation, it is necessary to focus on three main topics and maximize their presence, which are as follows:<sup>1)</sup>

1. Finding international cooperation in harmonizing the laws of various countries to combat cybercrimes; The act committed and considered a crime in one country must be punished by the laws of the other country. In the absence of this coordination among countries, criminals find safe haven without any considerations for the crimes they committed.
2. All countries cooperate in extraditing criminals or those wanted by security forces to countries that request them for committing cybercrimes.
3. Joining international treaties that work to increase cooperation and coordination between the efforts made by countries in the field of combating cybercrime.
4. Bringing these international treaties into effect and implementing what is stipulated in these agreements without any delay.<sup>2)</sup>

### **Third: The efforts of the International Criminal Police Organization (Interpol).**

The first beginnings of international police cooperation date back to the year 1904, when the International Convention against White Slavery was concluded in 1904.<sup>3)</sup>

After that, international police cooperation began to take the form of international conferences, the first and most historically precedent of which was the Monaco Conference of (1914 AD), which included police, judiciary, and law officers from (14) countries, in order to discuss and lay the foundations for international cooperation in some police matters, especially with regard to the extent of the possibility of establishing International Office for Criminal Registration and Coordination of Extradition Procedures<sup>4)</sup>.

---

<sup>1)</sup>See lawyer Munir Muhammad al-Janabahi and lawyer Mamdouh Muhammad al-Janabahi, previous source, p. 197.

<sup>2)</sup>Muhammad Ahmed Amin Al-Shawabkeh, Information Crime, House of Culture, Amman, 2004, p. 120.

<sup>3)</sup>(Article text(The first)Of theseaAgreement on: "All Contracting Governments undertake to establish or designate an authority to collect information concerning the use of women and girls for the purpose of prostitution abroad, and this authority shall have the right to address directly the corresponding administration in all Contracting States Parties." See: Youssef Hassan Youssef, **International Internet crimes**, 1st edition, National Center for Publications legal,Cairo ,2011, p. 145.

<sup>4)</sup>However, as a result of the outbreak of World War I, the conference did not achieve any significant practical results. After the end of World War I, specifically in 1919 AD, Colonel Van

---

Publication of the European Centre for Research Training and Development -UK

This organization aims to confirm and encourage cooperation between the police agencies in the States Parties in an effective manner in combating crime, by collecting data and information related to the criminal and the crime, through the national central offices of the International Police located in the territories of the countries joining it, and exchanging them among themselves and providing them with the information available to them. on its territory, especially with regard to information crimes.

Similar to this organization, the European Council in Luxembourg established in 1991 AD a European police to be a link between the national police services in the organized countries, and to pursue perpetrators of cross-border crimes, including, of course, crimes related to the Internet.

At the Arab level, we find that the Council of Arab Interior Ministers established the Arab Criminal Police Office, with the aim of securing and developing cooperation between police agencies in member states in the field of combating crime and prosecuting criminals within the limits of the laws and regulations in force in each country, in addition to providing assistance in the field of support and development. Police services in member states)<sup>1</sup>.

---

Houten, a Dutch police officer, tried to revive the idea of international police cooperation by calling for an international conference to discuss this issue.,However, he was not successful in his endeavor, and at the end of 1923, Dr. Johanno Sowira, Director of the Vienna Police, succeeded in holding an international conference, considered the second at the international level of criminal police, which resulted in the birth of the International Criminal Police Committee (ICPC).International Criminal Police Commission) AndIts abbreviation (ICPO) shall be based(Vienna)It works on coordination between police agencies,In order to cooperate in combating crime; Except that BaWith the outbreak of World War II, the committee stopped its work until the war ended in a year(1946 AD),soIt was held in Brussels, Belgium during the period(6-9/6/1946 AD)An international conference with the aim of reviving the principles of security cooperation and putting them into practice Implementation at the invitation of the Inspector General of the Belgian PoliceLive(Louvage) , AndWe end theaMeeting to revive the International Criminal Police Commission (ICPOIt moved its headquarters to Paris, France, and changed its name to become the International Criminal Police Organization "Interpol"International Criminal Police OrganizationAs of writing these lines, the number of its members has reached 186. For more details on this topic, see: Adel Rayan Muhammad, computer crimes and data security, an article published on the InternetaInternet on Al Jazeera newspaper website - Electronic Village:<http://www.guiforum.com> .

<sup>(1)</sup> Youssef Hassan Youssef, previous source, p. 148.

## **Second section**

### **Means of combating cyber sextortion crimes at the international level**

The means of combating electronic sexual blackmail crimes are not limited to the national side, as we will see in the second section. The danger of these crimes is also a danger with an international dimension. Electronic sexual blackmail crimes are most often committed by people from outside the borders of the state, as they pass through international communication networks until it reaches the desired result, and inspection and seizure procedures that extend beyond the state's territory require cooperation and coordinated international efforts among the countries affected by these crimes, in order to be able to eliminate them, and this in turn requires the establishment of joint security services and the conclusion of bilateral agreements to eliminate them. And limit it.

If a cross-border electronic crime, such as electronic sexual blackmail, has occurred and is being investigated in order to uncover its circumstances and arrest its perpetrators, there may be a more urgent need for assistance from the authorities in the country in which the crime occurred, or the country through which the criminal activity passed on its way. To investigate the result or location where evidence of the crime is located.

Therefore, it has become necessary for countries that suffer from this type of crime to rush to take a number of matters in the international field in order to combat information crime and eliminate its negative aspects, which have begun to afflict the individual in a very serious way. Therefore, it was necessary to translate this international cooperation into the form of training to confront this crime, or through the existence of joint cooperation in the field of investigation and research. The practical reality has proven that the state cannot, through its unilateral efforts, eliminate information crime, because it is a cross-border crime, and therefore combating it cannot be achieved. Unless there is international cooperation at the criminal procedural level, as it allows direct communication between police agencies in different countries.

The continuing progress in computer and Internet technology requires security services to take steps consistent with the rapid developments witnessed by these technologies. And familiarity with it so that the criminal acts that have accompanied this technology can be addressed and confronted on the one hand, and on the other hand, enforcing the law in the face of electronic sexual blackmail crimes requires taking measures that may go beyond the concepts and principles established in the traditional penal code, due to the modernity and speed of these crimes. In implementation, ease of concealment, and ability to erase its traces.<sup>1)</sup>

---

<sup>(1)</sup> soPractical facts have proven that there are crimes related to computers and networksaInternet mayaIt was committed in full view of the police, and some policemen even provided assistance to the perpetrators of these crimes unintentionally and out of ignorance, or as part of their professional duties required by this law, as happened when one of the police departments in the United States of America asked a company that had been hacked to She stops operating her automated device so



For this reason, these devices, of all types, must have a high degree of competence, knowledge, and ability to uncover the mystery of these crimes, reveal their circumstances, and identify their perpetrators with extreme speed and accuracy in a way that does not lead to delay in seizing the evidence that convicts the perpetrators of this type of crime. This will not be achieved except through the training and qualification that the people in charge of research and investigation receive. The competence of justice personnel to confront these new phenomena and their ability to confront them must be based on how to develop and improve the training process and improve the methods for achieving its desired goals. From this standpoint, the call was urgent for the necessity of qualifying. Educating those in charge of these devices to deal with such purely technical matters, especially in the international field, since no country can succeed in confronting these new patterns alone without cooperation and coordination with other countries in order to combat this category of technical crimes. .

Training is part of the development process, the aim of which is to introduce and bring about fundamental modifications to the behavior of the trainees. As for the training curriculum for these crimes, it must include a statement of the risks, threats, weak points, and places of penetration into the information network and computers, along with mentioning and specifying the type and pattern of electronic sexual blackmail crimes. A statement of the most important characteristics that characterize the cybercriminal, and the motives behind committing electronic sexual blackmail crimes <sup>(1)</sup>.

The bottom line is that encouraging and developing computer and information culture among law enforcement officers and linking it to the legal culture ensures that the security services and authorities achieve remarkable success in confronting electronic sexual blackmail crimes. With the need to raise the awareness of agencies working in the field of investigation, judiciary and law on how to deal with these advanced crimes and confront the problems and difficulties they face during the process of searching for them, in order to avoid falling into common mistakes, because any mistake made by the person conducting the inspection or the expert, even if it is unintentional, It may lead to the evidence obtained from this crime being destroyed and lost, and thus not being used as evidence of its value in proof.

---

that she can put it under surveillance with the aim of uncovering the perpetrator of the crime. As a result, she destroys the files and programs that were delivered, and the destruction of evidence may also occur as a result of a common mistake between the experts and the victim. For more details, see: Youssef Hassan Youssef, previous reference, p. 174.

<sup>(1)</sup>Khaled Mamdouh Ibrahim, Information Crimes, 1st edition, Dar Al-Fikr Al-Jami'a, Alexandria, 2009, p. 411.

With the urge to establish an integrated international investigation body specialized in the field of combating electronic sexual blackmail crimes, working under the supervision of an international committee capable of dealing with cases and disputes that result from the use of computers, the Internet, and other electronic means.

**First: International cooperation in carrying out joint security operations in the field of combating electronic sexual blackmail crimes**

Tracking cybercriminals in general and the Internet in particular, tracking and seizing digital evidence, and carrying out cross-border inspections of computer components, information systems and communication networks in search of any evidence they may contain of the commission of the cybercrime, are all matters that require carrying out some joint security operations by those in charge of Combating information crime<sup>1)</sup>.

The United States of America is considered one of the technologically advanced countries in the field of combating information and network crimes. From this standpoint, we find it keen to provide technical assistance and training to raise the criminal justice capabilities of other governments and to assist their police agencies. The Office of Assistance and Training to develop public prosecution agencies. Abroad, affiliated with the US Department of Justice, is specifically charged with providing the necessary assistance to strengthen criminal justice institutions in other countries, and to enhance the administration of justice abroad, and at present the US Department of Justice provides assistance to develop the judicial sector in a number of countries in Africa, Asia, and Eastern and Central Europe. Latin America and the Caribbean Basin, and the newly independent countries including Russia and the Middle East.

Information crime is one of the largest crimes that raises the issue of jurisdiction at the local or international level, and there is no problem with jurisdiction at the national level as reference is made to the legally specified standards for that. Therefore, these crimes are global and their impact extends to more than one country.<sup>2)</sup>

---

<sup>1)</sup> Youssef Hassan Youssef, previous reference, p. 149.

<sup>2)</sup> In an incident, the facts of which are summarized in the fact that two people residing in Melbourne, Australia, sent between six and seven million electronic messages to addresses in Australia and the United States of America, in addition to placing several messages on the message boards of the main companies providing mobile services. One of the defendants, a shareholder in the company, admitted that he provided false and incorrect information, and when prices rose, he sold his shares in the company, thus achieving a huge profit; Through this incident, it is noted that prosecuting the perpetrators of these crimes and bringing them to justice in order to impose punishment on them requires taking procedural measures outside the borders of the state. The crime or part of it was committed, for more details on this

### **Second: International efforts to confront electronic sexual blackmail crimes**

The effectiveness of research and investigation into information crimes often requires tracking the impact of criminal activity by following procedures that are parallel to the amount of damage caused by these crimes so that the parties conducting the research can detect them and arrest their perpetrators by seizing evidence that convicts or exonerates them.

Therefore, investigating cybercrime and prosecuting its perpetrators emphasizes the importance of mutual judicial assistance between states, as it is impossible for the state alone to eliminate these cross-border crimes. Combating it can only be achieved if there is international cooperation at the criminal procedural level, as it allows direct communication between police agencies in different countries, through the establishment of security agencies specialized in the field of research, investigation, and collecting information about the perpetrators of electronic sexual blackmail crimes. For example, in the crimes of viral broadcasting and publishing, the perpetrator of the attack may have the nationality of a country, and the viral attack is launched from computers located in another country, and the effects are located in a third country. It is natural that border problems stand as an obstacle to discovering these crimes and punishing their perpetrators. Because the police force in this or that country is unable to track down and prosecute criminals except within the borders of the country to which this criminal belongs.<sup>1)</sup>

There is no doubt that concluding agreements between countries is a positive step towards building an international community free of crime.

As we previously explained, cybercrime is a cross-border crime, meaning that its criminal impact is not limited to a specific country, but rather extends to other countries. Given the lack of a unified model for criminal activity, the matter requires unifying these legal systems. Given the impossibility of this matter, there is no escape from searching for another means that would help create international cooperation consistent with the nature of this new type of crime, and reduce the extreme differences between the penal systems involved. This means is represented in two points: the first is updating the local legislation concerned with electronic sexual blackmail crimes; While the second point relates to concluding special agreements that deal with this type of crime. As far as the second point is related to our topic, we will address this matter in the European Convention on Information Crime (Budapest Convention).

The European Convention to Combat Cybercrime, which was held in the Hungarian capital, Budapest in 2003, between member states of the Council of Europe, is considered one of the most important agreements that addressed cybercrime, both substantively and procedurally.

---

topic. See: Muhammad Amin Al-Roumi, computer crimes and...aInternet, University Press House, Alexandria, 2003, p. 136.

<sup>(1)</sup> Youssef Hassan Youssef, previous reference, p. 144.

---

Publication of the European Centre for Research Training and Development -UK

What concerns us in this agreement is the procedural aspect of it, which was well organized. In this agreement, we will discuss the most important rules related to mutual assistance between the member states of this agreement

Article (15) of the agreement requires the state parties to provide each other with the maximum possible extent of mutual judicial assistance with the aim of conducting investigations or procedures related to the information crime stipulated in this agreement.<sup>1)</sup>

It also required the States Parties to take all legislative measures or any other measures to ensure this mutual judicial assistance. The Convention allowed the parties, in order to quickly take measures, to provide assistance in case of urgency through quick means of communication such as fax or e-mail.<sup>2)</sup>

The agreement permitted any party to request another party to make an immediate reservation on data stored in an information system within the territory of that country, which intends to request mutual assistance for the purpose of inspecting or controlling this data.<sup>3)</sup>

This agreement also allows any state party to it to request another state party to inspect information data stored in an information system on the territory of the state from which the inspection is required, with the aim of seizing or disclosing this data, including the data that has been reserved, as this agreement concluded so far is one of The best agreements regarding information crime.

Also, the establishment of an integrated investigation body specialized in the field of combating electronic crimes, working under the supervision of an investigating judge capable of dealing with cases and disputes that result from the use of computers, the Internet, e-mail, and other modern means. It consists of specialists in the computer fields who hold a bachelor's degree in computer engineering. At the very least, they work as technical experts in the field of these crimes, and as investigators and officers who hold a law degree, provided that they have a certificate in computer proficiency testing and are familiar with its priorities so that they have the ability to deal with this type of crime, as the mission of this agency is to investigate crimes that occur or It is committed

---

<sup>(1)</sup>For more details about these crimes, see: Hilali Abdullah Ahmed, The substantive and procedural aspects of information crimes in light of a Budapest Convention, The previous reference, 2003, p. 67.

<sup>(2)</sup> Bruce Middleton, cybercrime investigator fie Guide, Auerbach publications USA, 2002, p.45.

<sup>(3)</sup> so Article (19) of this law stipulates: agreement (that The authority in charge has the right to inspect the computer located within its jurisdiction that It extends in case of a The inspection scope will be expedited to All computer components, if accessed to The information is stored from the computer the original inspection location).

by modern electronic means. As for Article (23) of the Convention, it obliges the parties to cooperate with each other in applying international principles related to international cooperation in criminal matters, and agreements based on similar or analogous legislation and local laws, to the widest possible extent, for the purposes of exploration. Investigation or criminal procedures related to criminal crimes linked to information systems and data or to collect electronic evidence of the criminal crime.

The explanatory memorandum for this agreement indicated that Article (23) established three general principles governing international cooperation mentioned in Chapter Three <sup>(1)</sup>.

**The first principle:** Parties must cooperate with each other on the broadest possible scale. This principle imposes an obligation on the parties to assist each other on a broader scale, and to reduce, as much as possible, obstacles that may hinder the rapid flow of information and evidence at the international level.

The second principle: It clarified the extent of the commitment to cooperation, as it decided that cooperation must extend its scope to include all criminal crimes related to information systems and data.

**The third principle:** It was stated that cooperation must be implemented in accordance with the provisions of this chapter and in application of international principles related to international cooperation in criminal matters, and agreements based on similar or counterpart legislation and local law.<sup>2)</sup>

The bottom line is that in order to activate the role of international cooperation in the field of combating electronic sexual blackmail crimes, it is necessary to join international treaties that work to increase cooperation and coordination between the efforts made by countries to combat these crimes, and to bring those treaties into actual implementation, as well as Working to ensure that there is the greatest degree of consistency and conformity between the laws of different countries related to combating these new crimes.

In conclusion, these are crimes of electronic sexual blackmail that cross borders, and these are the methods of confronting them, and this is the scientific heritage left behind by information technology.

## RESULTS

---

<sup>(1)</sup> CrescentAbdul Ilah AHe praised, Cross-border information crimes,The previous reference, p. 65.

<sup>(2)</sup> Hilali Abdul-IlahaHe praised, Budapest Convention against Cybercrime Crossing borders 1st edition, Dar Al Nahda Al Arabiya, Cairo,2007., pp. 299-302.

1. Legal Landscape Analysis: An in-depth examination of existing international and national laws related to cyber sextortion, highlighting gaps and ambiguities.
2. Case Studies: Real-world examples illustrating the challenges faced by law enforcement agencies in investigating and prosecuting cyber sextortion cases across borders.
3. Jurisdictional Complexities: Exploration of the difficulties in determining jurisdiction and enforcing laws when the crime involves multiple countries or transnational elements.

### **Recommendations**

1. Harmonization of Laws: Advocate for the harmonization of international laws to create a unified approach to combat cyber sextortion and facilitate cross-border cooperation.
2. Capacity Building: Enhance the capabilities of law enforcement agencies through training programs and technological resources to effectively investigate and prosecute cyber sextortion cases.
3. Victim Support Mechanisms: Develop comprehensive support mechanisms for victims, including counseling services, legal aid, and education programs to raise awareness about online safety.
4. International Collaboration: Encourage collaboration among nations, law enforcement agencies, and technology companies to share information, intelligence, and best practices in combating cyber sextortion.
5. Technological Solutions: Promote the development and implementation of technological tools to prevent, detect, and respond to cyber sextortion activities.

### **REFERENCES**

- a. Nabila Heba Harwal, research titled Procedural Aspects of Internet Crimes in the Evidence-Gathering Stage - A Comparative Study, Dar Al-Fikr Al-Jami'i, 2007.
- Abdel Wahed Muhammad Al-Far, International Organizations - General Theory - The United Nations - Specialized Organizations - Regional Organizations, Dar Al-Nahda Al-Arabi, Cairo, 2008.
- Abdullah Daghsh Al-Ajmi, Practical and Legal Problems of Cybercrime - A Comparative Study, Master's Thesis, Middle East University 2014.
- Adel Abal Ibrahim Kharashi, Problems of International Cooperation in Combating Information Crimes and Ways to Overcome Them, New University Publishing House, 2010.
- Ahmed Fathi Sorour, The Legal Confrontation with Terrorism, Al-Ahram Center for Publishing and Translation, 2nd ed, 2008.
- Akram Abdul Razzaq Al-Mashhadani, Interpol and the pursuit of wanted persons (blurring understanding of the tasks of the...thatTarbol), article published in Katabat newspaper, November 23, 2011, <http://www.kitabat.com/ar>



- Aladdin Muhammad Ahmed Shehata, The National Strategy for International Cooperation in the Field of Combating Crime, an applied comparative study, to combat drugs in both the Arab Republic of Egypt and the United States of America, Cairo, 1999.
- Aladdin Shehata, International Cooperation in the Field of Combating Crime, A Vision for a National Strategy for International Cooperation in the Field of Combating Drugs, Cairo, 2000.
- Ali Hussein Al-Tawalba, research on international judicial cooperation in combating cybercrime, Faculty of Law, University of Applied Sciences.
- Al-Shahat Ibrahim Muhammad Mansour, Cybercrimes in Islamic Sharia and Man-made Laws, 1st edition, Dar Al-Fikr Al-Jami'i, Alexandria, 2011.
- Article (22) of the aforementioned Budapest Convention.
- Aziz Ali Abdul Aziz Jamadar, Organized Crimes between Scientific Progress and Security Control, Ras Al Khaimah National Press, 1st edition, 2012.
- Emil Jabbar Ashour, Criminal Liability for the Crime of Electronic Blackmail on Social Media Sites (Comparative Knowledge), Maysan Research Journal, Volume 16, Issue 31, June, 2020 AD.
- Fakhri Abdul Razzaq Salbi Al-Hadithi, Explanation of the Penal Code (General Section), Al-Zaman Press, Baghdad, 1992.
- Hassan Al-Tawalba, International Procedural Cooperation in the Field of Extradition, University of Applied Sciences, Bahrain, pp. 13-14, <http://www.policemc.gov.bh>.
- Hilali Abdul-Ilaha He praised, Budapest Convention against Cybercrime Crossing borders 1st edition, Dar Al Nahda Al Arabiya, Cairo, 2007.
- Hussein Fathi Al-Hamouli, International Security Cooperation in the Implementation of Criminal Judgments, Cairo, 2015.
- Jamil Abdel-Baqi Al-Saghir, Criminal Law and Modern Technology, Dar Al-Nahda Al-Arabiya, Cairo, 1992.
- keya Bu Bakr Al-Matroudi, Cybercrime, paper presented to the Third Conference of Chiefs of Supreme Courts in Arab Countries, Sudan, September 22-23.
- Kurkis Yusuf Daoud, Organized Crime, International Scientific House, 2001.
- Mahmoud Naguib Hosni, Explanation of the Penal Code, Special Section, 8th edition, Dar Al-Nahda Al-Arabiya, Cairo, 1984..
- Mahrous Nassar Ghayeb, Information Crime, published in Al-Technical Magazine, Volume 24, 2011.
- Mamdouh Rashid Musharraf, Criminal Protection for the Victim of Blackmail, Arab Journal for Security Studies, Volume (33) Issue (70), Riyadh, 2017.
- Montaser Saeed Hamouda, Interpol, International Criminal Police Organization, Dar Al-Fikr Al-Jami'i, 2nd edition, 2013.

---

Publication of the European Centre for Research Training and Development -UK

- Muhammad Ahmed Amin Al-Shawabkeh, Information Crime, House of Culture, Amman, 2004.
- Muhammad Al-Shennawi, Strategy to Combat Human Trafficking, National Center for Legal Publications, Cairo, 1st edition, 2014.
- Muhammad Amin Al-Bishri, Investigation into Computer Crimes, Dar Al-Kutub Al-Lawaniyya, Egypt,2009, p. 178.
- Muhammad Karim Ali, Combating Organized Crime under International Treaties, Master's Thesis, Faculty of Law, Mansoura University, 2016.
- Munir Muhammad Al-Junaibi, and Mamdouh Muhammad Al-Junaibi, Internet and Computer CrimesLee and means of combating it, Dar Al-Fikr University, 2004 edition, p. 96.
- Osama Ahmed Al-Manasa, Computer and Internet Crimes, "A Comparative Analytical Study," 1st edition, Dar Wael for Printing and Publishing, Amman, 2001.
- Saeedani Salami, Development of International Legislation and Agreements in the Field of Information Crimes (Facts and Approaches), Al-Ustad Al-Researcher Journal for Legal and Political Studies, Issue Ten, Volume One, Publication Date 6/4/2018..
- Salem Muhammad Suleiman Al-Awjali, Provisions of Criminal Liability for International Crimes in National Legislation - A Comparative Study, PhD thesis, Ain Shams University, Cairo, 1997.
- Younis Arab, Developing Legislation in the Field of Combating Cybercrimes, Working Paper "Legislative Trends in Cybercrimes", Telecommunications Regulatory Authority/Muscat - Sultanate of Oman, 2-4aBrill 2006, pp. 29-30.
- Youssef Hassan Youssef, International Internet Crimes, 1st edition, National Center for Legal Publications, Cairo, 2011.