

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

Nadia Hamouti¹, Abdelaziz Elbouzidi²

¹Doctor Professor, University of Sidi Mohammed Ben Abdellah, Faculty of Legal Economic and Social Sciences, Fez, Morocco.

²Phd, Institution, University of Sidi Mohammed Ben Abdellah, Faculty of Legal Economic and Social Sciences, Fez, Morocco.

ORCID: <https://orcid.org/my-orcid?orcid=0009-0008-4028-0496>¹, <https://orcid.org/my-orcid?orcid=0009-0003-9421-296X>²

ABSTRACT: The subject of cybercrime represents a recent phenomenon that has emerged in the era of the Fifth Revolution, namely the digital revolution. Consequently, with the rise of this type of digital offense, most research and studies have focused on analyzing the crime and the offender. This focus has been to the detriment of the excluded and neglected party in criminal studies (the victim) relying on approaches and schools of thought within criminology.

This article aims to shed light, from a different perspective, on the role of the victim of cybercrime within the criminal justice system, considering that the injured party is no less significant than the other parties in criminal proceedings. Consequently, the authors of this article have addressed all aspects concerning the criminal protection of this category of victims, highlighting the concept of cybercrime, its characteristics, and its legal framework. Finally, they examined aspects of cybercrime perpetrated through social networks and their psychological and social impacts on victims, also exploring the victims' responsibility in the genesis of the crime.

KEYWORDS: Crimes, Cybercrime, Victim, Criminal Law, Cyber Victim

1 - INTRODUCTION

Cybercrime has long attracted significant interest among criminologists as a critical field of research, while also representing a growing concern for policymakers responsible for criminal justice policy. Although numerous definitions of cybercrime exist, the term generally refers to offences committed through the use of computers and computer networks. However, it also encompasses offences that do not primarily involve computers¹ (e.g., mobile phones). It is important to distinguish clearly between cybercrime and traditional offences committed through electronic means.

Consequently, Morocco has followed in the footsteps of advanced countries in developing its legal framework on cybersecurity and cybercrime. At the international level, Morocco acceded to the Budapest Convention on Cybercrime in 2018 and signed a Memorandum of Understanding with the United Arab Emirates in 2023, aiming to join efforts to strengthen cybersecurity. At the national level, Morocco has enacted several laws, including: Law No. 20-05 on cybersecurity; Law No. 20-43 on trust services for electronic transactions; Law No. 05-53 on the electronic exchange of legal data; Law No. 08-31 establishing consumer protection measures, including online consumer protection; Law No. 08-09 on the protection of individuals with regard to the processing of personal data; and Law No. 03-07 amending and supplementing the Penal Code with respect to offences involving automated data processing systems.

At the institutional level, the General Directorate of Information Systems Security (DGSSI) was established to ensure the protection of critical infrastructures. In addition, the Monitoring, Surveillance, and Response Center for Cyber Attacks (Ma-CERT) was created to coordinate efforts in response to cyber threats. These institutions employ artificial intelligence systems to analyze data, detect attacks at their early stages, and contribute to the development of robust encryption solutions aimed at safeguarding sensitive information.

It is worth noting that cybercrime is characterized by a unique specificity that sets it apart from traditional offences, as it is committed within the frameworks of computer and intelligent systems. This particularity facilitates its proliferation and expansion in the digital (or so-called virtual) world, as it constitutes a transnational offence that transcends geographical borders, thereby complicating and hindering the identification of the perpetrators of unlawful acts. Consequently, this situation prompts States to

¹ Fawn T. Ngo & Raymond Paternoster, Cybercrime Victimization: An examination of Individual and Situational level factors, International Journal of Cyber Criminology, Vol 5 Issue 1 January - July 2011, P 773.

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

conclude a series of conventions within the framework of international judicial cooperation in criminal matters, with the aim of locating and extraditing offenders².

As for the victim of a cyber offence, it refers to any individual who suffers harm as a result of an act committed by an expert in the digital field or in one of its components³. Such harm must occur within a digital environment, which is defined as a virtual space comprising computer networks and communication platforms, virtually connecting all forms of interaction and transactions between individuals, institutions, organizations, and States. Through this environment, economic exchanges and transactions are also concluded via network-based payment systems, with all such processes being carried out through internet search engines and various electronic transmission and communication forms⁴.

Despite extensive and growing research on cybercrime, few studies have examined the theoretical causes and correlates of cybercrime victimization (cyber-victim). As a result, numerous offenses can be committed against internet users through or by means of electronic tools, such as computer viruses⁵, unwanted exposure to pornographic material, sexual solicitation, online harassment by a stranger, online harassment by a non-stranger, phishing⁶ and cybercrime, and defamation.

2 - RESEARCH OBJECTIVE

This article highlights victims of cybercrime as a marginalized party in most criminal studies, particularly those concerning these modern offenses. Thus, a comprehensive study of the offense can only be conducted by thoroughly examining both parties in the trial. In this regard, we also propose to address the issue of cybercrime victims by drawing on victimology theories, in order to clarify the overall concept of this type of offense.

From this, several objectives can be highlighted:

- To involve the victim of cybercrime in academic studies and research in order to understand the psychology and motives behind the commission and emergence of this type of crime.
- To grant the victim a major importance relative to their adversary in the criminal trial, which could contribute to their rehabilitation in light of the harm caused by the offense and the resulting moral damages.
- To understand the sources and references of this type of contemporary offenses, which could aid in the development and adoption of new legal texts, while assisting criminal justice institutions in handling these offenses with greater accuracy and care.

3 - RESEARCH PROBLEM

Given the novelty of this type of offense, as well as its current severity, it is difficult for most international legislations to delineate and understand its methods, components, and sources, due to its belonging to the digital or cyber world.

This complicates the possibility of prioritizing the position of the victim over that of the accused, due to the lack of sufficiently qualified experts in this field, notably technical experts operating within the judicial police under the supervision of the Public Prosecutor, or judicial experts responsible for adjudicating cases. Consequently, victims risk losing the opportunity to obtain favorable judgments, thereby resulting in an infringement of their rights.

Accordingly, we pose the following main research problem: **To what extent does the Moroccan criminal legislator adapt to the evolution of offenses, particularly in the field of cyberspace, and what is the impact on the victims?**

This main research problem is divided into a set of questions: **To what extent can the legislator provide adequate protection to victims of cybercrime? To what extent do the stakeholders in this field understand and control this type of offense to ensure the protection of victims? To what extent can the effectiveness and efficiency of the laws enacted in this area of crime be assessed?**

4 - METHODOLOGY & OUTLINE

Nevertheless, it is necessary to undertake an analytical approach to this issue given the importance of the topic. Therefore, in order to grasp the subject, the following outline must be deduced:

² علاء عبد الخالق حسين/ عمار عبد الحليم علي/ مصطفى حسين زوير/ بارق حبيب صادق، الأمن السيبراني: المبادئ والممارسات لضمان سلامة المعلومات، دار السرد للطباعة والتوزيع والنشر، ط 1، بغداد العراق، 2024، ص 12.

³ لخضر سلامي، ضحايا الجريمة الإلكترونية عبر مواقع التواصل: الفايبروك نموذجاً، مجلة دراسات في سيكولوجية الانحراف، المجلد 06 العدد 01 السنة 2021، ص 186-213.

⁴ فريد حمامي، تداعيات الجريمة الإلكترونية من وجهة نظر الضحايا في المجتمع الجزائري، مجلة السراج في التربية وقضايا المجتمع، مجلد 08 عدد 01، سنة 2024، ص 121.

⁵ Infection of the computer system by malicious software.

⁶ Phishing is a fraudulent technique aimed at deceiving the internet user into disclosing personal data (access accounts, passwords, etc.) and/or banking information by impersonating a trusted third party.

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

I. The Notion of Cybercrime

A. Definition of Cybercrime and Its Characteristics

a. Definition

b. Characteristics of Cybercrime

B. The Legal Framework of Cybercrime

II. The Victim of Cybercrime

A. Aspects of Cybercrime via Social Networks and Their Psychological and Social Impacts on Victims

B. Cyber Victims: Protection and Liability of Victims

Results

Conclusion

I. The Notion of Cybercrime

The methods of committing offenses have evolved compared to what was previously known. Attacks no longer target only human life and financial assets, but also include information and data related to users of the digital environment⁷. Criminals can now commit serious offenses against internet victims with ease and without bloodshed, due to the emergence of a new type of crime known as cybercrime⁸.

Consequently, we will identify this new type of crime by addressing its definition and the characteristics that distinguish it from traditional offenses (A), as well as its legal framework (B).

A. Definition of Cybercrime and Its Characteristics

Through this paragraph, we will attempt to address the definition of cybercrime (a), as well as the key characteristics that distinguish it from traditional crime (b).

a. Definition

Like most comparative criminal legislations, the Moroccan legislator has not provided a definition of cybercrime, which is why the definition of general legal concepts remains a doctrinal task rather than a legislative one. Thus, legal doctrine defines cybercrime as "any criminal activity carried out through cyberspace and via the Internet. By extension, it includes any form of electronic malice committed using information and telecommunication technologies. As such, cybercrime is a transnational offense that requires close judicial, technical, and operational cooperation between States in both its prevention and repression"⁹.

It should be noted that there is no unified definition of this criminal phenomenon. Some legal scholars approach the subject from the perspective of the offense itself, while others focus on the means used to commit it. This is evident in the lack of consensus on a uniform definition for this new type of offense, whose terminology has varied over time in connection with the development of information and communication technologies (ICT). As a result, some refer to it as "cybercrime", others as "electronic offenses", while another part of the doctrine prefers the term "misuse of information and communication technologies". References are also made to "computer crimes" and "Internet-related crimes"¹⁰.

In conclusion, cybercrime essentially stems from technological progress and the rapid, ongoing development it entails, particularly in the field of information technology. Legal scholars refer to this as "modern technological offenses," which are linked to technologies primarily based on computers and other technical devices that may emerge in the future. These offenses are also considered modern due to their relative novelty, as they are closely connected to developments arising from modern devices that are expected to possess highly expansive and flexible storage capacities in the future¹¹.

b. Characteristics of Cybercrime

The particular nature that characterizes cybercrime makes it unique, with a set of features that distinguish it from other traditional offenses. This is due to the environment in which the offense is committed, as well as the tool or means used by the digital offender to perpetrate it. These characteristics are reflected in offenses committed through modern technology, primarily the Internet, which is considered a means of commission. Cybercrime is therefore:

- **Cybercrime is an organized form of delinquency:** Initially perceived as a series of threats to network security, it has now evolved into an organized and even mafialike dimension. It has led to the emergence of genuine "black markets"

⁷ Mohamed Karim Missaoui/Abdelaziz Elhila, Le droit pénal et l'éthique à l'épreuve de la cybercriminalité, Journal d'Economie, de Management, d'Environnement et de Droit (JEMED), V 4, N° 2, Mai 2021, P 88-96.

⁸ خالد ممدوح إبراهيم، الجرائم المعلوماتية، مطبعة دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2009، ص 60.

⁹ Sam Lyes, La criminalité électronique et son impact sur la sécurité nationale et la sécurité du citoyen, STRATEGIA Revue des études de défense et de prospective, N° 16 deuxième semestre 2021, P 26. Voir aussi Romain Boos, La lutte contre la cybercriminalité au regard de l'action des États, Hal Open Science, pour l'obtention de doctorat de droit privé et sciences criminelles, Université de Lorraine 2016, P 28.

¹⁰ رامي متول القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية مصر، 2011، ص 17.

¹¹ الموشير تركي بن عبد الرحمن، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة لنيل شهادة الدكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، الرياض 2009، ص 15-16.

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

where hacked information circulates, ranging from identity theft and intellectual and artistic property theft to credit card fraud¹².

- **In terms of purpose:** Cybercrime targets information systems by hacking them with the intent to alter or distort the data and information of users within the digital environment, much like traditional offenses.
- **Flexible offenses:** Cybercrimes are considered flexible offenses due to their subtle nature and the fact that most of them are concealed. The victim may not even be aware that they have been committed, even if they occur while the victim is online. The offender typically possesses advanced technical skills, allowing them to commit offenses with great precision and discretion—such as stealing money or sending destructive viruses to programs and computers.
- **Detection difficulty:** Cybercrime is considered one of the most difficult offenses to detect, as it leaves no physical traces that could help identify the perpetrator, thereby complicating the task of the competent authorities in this environment¹³. Data and information consist of invisible electronic signals, which allows the offender to easily and completely erase such electronic evidence.
- **Cybercrime is a globalized offense:** It is an offense of an international nature. These are transnational crimes or offenses that disregard time and place. They are characterized by the geographical distance and time differences between the perpetrator and the victim. This is due to the information society, which does not recognize geographical borders. It is an open networked society that transcends time and space without being subject to border controls¹⁴.
- **Victim's refusal to report or file a complaint:** In most cases, cybercrimes go unreported, either because the victim is unaware of them or due to fear of defamation. Thus, it is observed that most crimes committed via the Internet are discovered accidentally or even long after they have been perpetrated¹⁵.
- Cybercrimes are considered less violent in their execution: They are characterized by the absence of physical force to achieve their objective. They belong to offenses committed with minimal physical effort compared to traditional crimes, which require some form of muscular effort manifesting as violence and abuse, such as murder and rape. In contrast, internet crimes are discrete offenses that only require the technical ability to operate a computer to commit illegal acts¹⁶.
- Difficulty in controlling and defining cybercrime: Among the challenges faced by judicial police officers and judges, particularly regarding procedures to control cybercrime, is assigning it an appropriate legal qualification. This difficulty may stem from the particular nature that characterizes cybercrime.

Finally, it can also be added that these offenses, under Moroccan legislation, are characterized, on the one hand, by the rigidity of the prescribed sanctions, granting the judge the possibility to mitigate or aggravate the sentence within the prescribed minimum and maximum limits, while emphasizing general deterrence as well as the seriousness of the offense towards individuals and society, without neglecting consideration of prior convictions. On the other hand, they are distinguished by a certain flexibility allowing the offender to benefit from particular judicial circumstances or to be sentenced to a financial penalty, as well as other additional or alternative sanctions.

B. The Legal Framework of Cybercrime

The Moroccan legislator, in its Penal Code as amended and supplemented by Law No. 07-03 governing offenses related to automated data processing systems, as well as Law No. 09-08 on the protection of individuals with regard to the processing of personal data, has not defined cybercrime. Instead, it has enumerated a set of acts the perpetration of which is considered to constitute cybercrime. Accordingly, Moroccan criminal law has been supplemented by a series of acts deemed to be offenses related to automated data processing systems, commonly referred to as electronic offenses.

In this context, it can be stated that the following acts fall within the classification of such categories of offenses, including:

- Fraudulently accessing all or part of an automated data processing system¹⁷
- Modifying or deleting data contained within an automated data processing system¹⁸
- Intentionally obstructing or distorting the functioning of an automated data processing system¹⁹

¹² Farih Omar, Cadre conceptuel et théorique de la cybercriminalité, Revue Maroc Droit, 2014, P 6.

https://www.marocdroit.com/Cadre-conceptuel-et-theorique-de-la-cybercriminalite-Par-Mr-FARIH-OMAR_a5568.html consulted on 07/01/2025.

¹³ عبد المومن الصغير، الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، جامعة محمد خيضر – بسكرة -المجلد 02 العدد 02 2014، ص 201.

¹⁴ Farih Omar, Cadre conceptuel et théorique de la cybercriminalité, AA, P 9.

¹⁵ عبد المومن الصغير، مرجع سابق، ص 75.

¹⁶ صالح بن محمد المسند/عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 29، أبريل 2000، ص 20.

¹⁷ Article 607-3 of the Moroccan Penal Code, as amended and supplemented by Law No. 07-03

¹⁸ Article 607-4 of the Moroccan Penal Code, as amended and supplemented by Law No. 07-03

¹⁹ Article 607-5 of the Moroccan Penal Code, as amended and supplemented by Law No. 07-03

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

- Fraudulently inputting data into an automated data processing system²⁰

The Moroccan legislator has classified such acts as electronic offences and has increased the penalties where they result in the deletion or alteration of data contained in an automated data processing system, in the disruption of its functioning, or in the commission of the aforementioned acts against all or part of an automated data processing system that is intended to contain information relating to the internal or external security of the State or secrets affecting the national economy. The Moroccan criminal legislator has also considered as an offence in the field of electronic crime the act of forging or falsifying information documents, regardless of their form, where such forgery or falsification is likely to cause harm to others²¹.

The legislator has also made reference to both material and moral rights related to the field of information and electronic technologies in the Law on Industrial Property, as well as in Law No. 00-2 on Copyright, particularly with regard to computer programs and databases. Furthermore, Article 218, paragraph 7, of the Moroccan Penal Code provides for offences related to automated data processing systems and classifies them as terrorist crimes when such acts are intentionally connected to an individual or collective plan aimed at seriously undermining public order through intimidation, panic, terror, or violence.

However, despite the proactive approach of the Moroccan legislator within the framework of its criminal policy and in response to developments brought about by the electronic revolution, the considerable and rapid progress in this field reveals that the legislation is striving to keep pace with such evolution. It does so by establishing new rules that seek to strike a balance, on the one hand, between the right to use information technology and the right to innovation, and, on the other hand, the protection of public order and private rights.

It is inevitable to acknowledge that the legislative framework and judicial practice still suffer from significant shortcomings, particularly in the procedural aspect represented by the means of proving electronic crime. Indeed, the tremendous speed of innovation in this field makes it difficult to establish evidence of criminal acts in the absence of specialised experts and due to the challenges associated with relying on traditional means of proof to demonstrate cybercrime.

Indeed, cybercrimes are often committed via the Internet and through the interconnection of various networks at the international level, thereby eliminating the concept of geographical and spatial boundaries. As a result, public authorities face significant challenges in proving the commission of the offence and in accurately identifying both the perpetrator and the place where the crime was committed. Another obstacle to investigation lies in the concealment of identity, either through the use of false identities, the falsification of all identifying information, or registration using stolen or forged information cards, which may be used to purchase goods or to commit serious offences.

Certainly, legal rules alone are insufficient to combat crime in general and cybercrime in particular. Consequently, the discussion on information security requires the development of a comprehensive and clear strategy aimed at fostering a culture of citizenship and human rights through social education. This education should focus on teaching young people to respect others, to use modern means of communication lawfully, and to avoid behaviors that infringe upon the freedom and rights of others, whether individuals or groups.

Similarly, human beings, having reached a state of living in a small village (social networks) thanks to the development of communication means, bear the responsibility, as citizens of the world, to uphold the right to information as a human right and to respect international legal rules that require all countries, including Morocco, to ensure that communication tools are used in a manner that respects privacy, cultures, and the rights to information and human security.

Moreover, referring to the Moroccan Penal Code, it is observed that the legislator has established a range of sanctions for electronic offences that vary according to the severity of the criminal acts. For instance, a prison sentence of one to three months and a fine ranging from 2,000 to 10,000 dirhams is prescribed for fraudulent access to an automated data processing system. Similarly, the penalty is increased to imprisonment of one to three years and a fine of 10,000 to 20,000 dirhams for those who fraudulently access an information system and simultaneously destroy, delete, or alter the data contained therein.

The Moroccan legislator has empowered the judge, taking into account the rights of good-faith third parties, to order the confiscation of tools used to commit offences provided for in the Penal Code concerning electronic crime. The court may also sentence the offender to the deprivation of one or more rights stipulated in Article 40 of the Penal Code for a period ranging from two to ten years. Additionally, the offender may be prohibited from holding any public office for a duration of two to ten years, and the judgment may be made public.

Finally, given the severity of the penalties contained in the Penal Code, which combine imprisonment and fines, the legislator has taken into account the element of good faith. Accordingly, the wording of the Penal Code articles has been cautious and even explicit in protecting the rights of good-faith third parties in cases of erroneous access to information systems.

²⁰ Article 607-6 of the Moroccan Penal Code, as amended and supplemented by Law No. 07-03

²¹ مغار محمد، الإطار القانوني للجرائم الالكترونية في المغرب، المحور: دراسات وابحاث قانونية، الحوار المتمدن-العدد: 2023-7615.

<https://www.ahewar.org/debat/show.art.asp?aid=793305>

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

In conclusion, the role of the scientific and technical police in enhancing its operational efforts to keep pace with the latest international technologies in combating this type of crime should not be overlooked²². This is notably reflected in the coordination between state institutions, represented by the General Directorate for National Security (DGSN), the General Directorate for Territorial Surveillance (DGST), and the General Directorate for Studies and Documentation (DGED), under the supervision of the Public Prosecutor's Office, through the specific procedural framework applied in criminal proceedings against offenders, whether within or outside the national territory.

In any case, after discussing cybercrime and setting out its definition and understanding, as well as highlighting its most important characteristics and legal framework, it is also necessary to examine this offence from the perspective of the victim and their suffering resulting from this criminal phenomenon.

II. The Victim of Cybercrime

With technological advancements, the manner of committing offences has become more sophisticated and complex, leading to a significant shift in the human perspective of the world. Cybercrime constitutes a real threat to rapid technological development. This technological advent has not only redefined human life but has also impacted cybercrime²³. The rapid growth in the number of Internet users - where many users equate to many victims - and their dependence have considerably increased the risks of offences being committed.

Victims of cybercrime vary according to several identified dimensions, notably aspects of vulnerability, psychological perspectives, age-related differences, and attempts by internet users to profile cybercrime victims²⁴. The consequences of being a victim of cybercrime can be significant and are not limited to financial losses alone. Some victims suffer from poor mental health and other adverse effects on their physical health²⁵.

In this study, we will focus on examining aspects of cybercrime through social networks and their psychological and social impacts on victims (A), followed by addressing cyber-victims: protection and liability of victims (B).

A. Aspects of Cybercrime via Social Networks and Their Psychological and Social Impacts on Victims

Social network users are considered among the categories most exposed to the risk of cybercrime due to the lack of awareness among individuals who operate these networks, as well as the widespread growth of e-commerce, which has further exacerbated the problem to the extent that fraudulent offences exceed thousands of criminal acts per day. As for violations of privacy, they have become commonplace, largely due to the vast number of victims affected by such offences.

These offences are reflected among social network users, as they affect them in various ways, notably on the psychological level, which is considered a sensitive nerve and one of the mental (psychological) disorders suffered by victims due to their involvement in such offences. It entails a dysfunctional thought pattern that places victims in a deadlock in understanding and managing situations. This leads to a crisis in social relationships, while these offences also contribute, on the one hand, to diminishing trust among individuals within the same society and, on the other hand, to eroding the individual's trust in themselves²⁶.

According to certain studies, most victims spend a significant amount of time on social networking sites, i.e., more than three hours per day, and do not periodically change their account passwords. Most victims lack antivirus software and, when browsing platforms such as Facebook, tend to perform actions like commenting on third parties' posts and interacting with individuals who are not their friends, thereby extending communication beyond private conversations. They also accept friend requests from unknown persons. These third parties may be of different nationalities, and victims exchange messages and open links they receive without verifying them. These studies confirm that the most vulnerable or exposed to such criminal acts are minors who are not supervised or controlled by their parents²⁷.

The increasing importance of social networks fuels another constantly growing phenomenon, namely the online solicitation of children for sexual purposes (grooming). This offence involves manipulation. An adult exploits a child's vulnerability or weakness to propose, via electronic communication means, a meeting aimed at committing sexual abuse. This practice is characterized by

²² Nadia Hamouti/Abdelaziz Elbouzidi, The importance of artificial intelligence in the field of Moroccan criminal law: What impact on the legal protection of personal data?, *Al-Majd Advanced Scientific Journal*, V 12, N° 12, 2024, P 21.

²³ Vishi Aggarwal, Ms. Shruti, Cybercrime Victims: A Comprehensive Study, Volume 6, *International Journal of Creative Research Thoughts (IJCRT)*, Issue 2 April 2018, P 640.

²⁴ Juraj Sikra Karen V. Renaud and Daniel R. Thomas, UK Cybercrime, Victims and Reporting: A Systematic Review, *Commonwealth Cybercrime Journal*, volume 1, issue 1 2023, P 28.

²⁵ Scott Monteith et All, Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry, *Psychiatry In The Digital Age* (J Shore, Section Editor), 2021, P 1-9. <https://doi.org/10.1007/s11920-021-01228-w>

²⁶ إلهام بودراع، ريان صوالح، تجليات الجريمة الإلكترونية عبر المنصات الاجتماعية وأثارها النفسية والاجتماعية على المستخدمين، مذكرة مكملة لنيل شهادة الماستر، جامعة قاصدي مراح ورقلة، السنة الجامعية 2022-2023، ص 1.

²⁷ Ibid, P 56.

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

gradually gaining the minor's trust, encouraging them to send intimate photos. The minor is then held hostage by the adult, who threatens to send these photos to the child's parents, school, or friends²⁸.

Regarding the relationship between users revealing their identity on social networks and their risk of becoming victims of cybercrime, most people do not rely on the privacy of their personal pages and disclose their true personal information such as date and place of birth, gender, place of residence, personal photos, educational level, family status, workplaces, and relationships with friends. All this important personal information can assist the perpetrator in facilitating their acts, thereby compelling the victim to submit to them, posing a danger and threat to their life. This can directly affect the victim's psychology and may lead to suicide.

B. Cyber Victims: Protection and Liability of Victims

Today, the explosion of the Internet and its multiple uses has profoundly transformed human relationships, particularly through social networks, which have become virtual communities playing a predominant role in the daily lives of nearly all Internet users²⁹. From this perspective, as our dependence on the digital space increases across various aspects of our lives, the risks of cybercrime threatening both individuals and institutions have also risen. Consequently, the criminal protection of cyber-victims has become an urgent necessity to ensure a stable digital environment that strengthens trust and encourages the optimal use of technology.

Accordingly, several laws have been enacted to ensure the criminal protection of victims of electronic offences. By way of example, one may cite Law No. 07-03 supplementing the Penal Code with respect to offences related to automated data processing systems; Law No. 53-05 on the electronic exchange of legal data; Law No. 09-08 on the protection of individuals with regard to the processing of personal data; and Law No. 2-00 on copyright and related rights.

The criminal protection of cyber-victims consists of a set of laws and procedures aimed at safeguarding victims of cybercrime through:

- The criminalisation of harmful electronic acts: such as account hacking, data theft, electronic blackmail or extortion, and the dissemination of offensive content.
- Facilitating the reporting process of cybercrime: by providing clear and secure reporting channels, such as dedicated websites and helplines.
- The investigation and prosecution of cybercrime: with the objective of identifying perpetrators and bringing them to justice.
- Compensating victims for the harm they have suffered: whether material or moral.
- Raising awareness of cybercrime: through public education campaigns and promoting a culture of digital security among individuals.

In accordance with the foregoing, the criminal protection of cyber-victims holds significant importance in today's digital age, where individuals and organisations are increasingly exposed to cybercrime-related threats. This protection ensures the rights of victims, enables them to obtain justice, places them at the centre of attention, and guarantees fair judicial proceedings.

The deterrent effect of criminal protection is an important factor in preventing offenders from committing further crimes, as they become aware of the potential sanctions, particularly in light of recidivism. Likewise, this criminal protection contributes to building greater trust in the digital space, as individuals feel that their data and information are safe and protected. Finally, it helps safeguard the digital economy by reducing financial losses and the negative impact that cybercrime can have on both businesses and individuals.

Moreover, among the challenges facing the enforcement of criminal protection for cyber-victims is the difficulty of prosecuting cybercrime due to its virtual nature and the ease with which it transcends borders. Another challenge lies in the insufficiency of specific legislation on cybercrime, as existing laws may fail to keep pace with rapid technological developments. Additionally, there is a lack of public awareness of this criminal phenomenon, as some individuals may be unaware of their rights or of how to protect themselves against cybercrime. Finally, the limited resources allocated to combating this offence pose another obstacle; the State may lack sufficient means to effectively address cybercrime.

As for the role of the victim in the commission of an offence against themselves, it is highly possible that they may contribute to its occurrence - particularly in emerging offences such as cybercrime - by facilitating the offender's act or even provoking it, due to ignorance or negligence³⁰. Internet users, although sometimes victims of offences, often act as unintentional facilitators, especially when they disclose highly personal information on social networks without realising that such data may one day be used against

²⁸ Mohamad Idris Laena, Riswadi, Legal Protection for Child Victims of Cyber Bullying, ICLSSEE, Semarang Indonesia, 16 April 2022. <http://dx.doi.org/10.4108/eai.16-4-2022.2319752>

²⁹ Charpenel Y, Cybervulnérabilité des usagers des réseaux sociaux, (Article sous la direction de), Prostitutions : Exploitations, Persécutions, Répressions, Ed. Economica, Paris 2016, P 1.

³⁰ لخضر سلامي، ضحايا الجريمة الإلكترونية عبر مواقع التواصل: الفايبروك نموذجاً، م س، ص 195.

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

them. This risk is particularly acute for minors. More than anyone else, minors need to be made aware of digital risks and informed of the actual protection available to them³¹.

Here are some behaviours that may render an Internet user a contributor to the offence committed against them:

- Users trust certain individuals, websites, and emails without verifying their credibility.
- The user neglects to install protection programs against viruses and spyware.
- Failure to update security systems or disabling antivirus and firewall programs.
- Not verifying email addresses that request confidential information such as a credit card or bank account.
- Sharing passwords with others or choosing familiar and easily guessable passwords.
- Storing photo files and personal information on a computer.
- Downloading files or software from unknown sources.
- Failure to file a complaint with the competent authorities in the event of cybercrime.

Based on our analysis, given the rise in cyber threats, maintaining the security of individuals and organisations requires continuous attention and joint efforts by criminal justice authorities - in line with criminal policy - and by society as a whole. Likewise, through the improvement of specific legislation and the development of criminal measures, we can strengthen the protection of cyber-victims and achieve justice in the face of this category of offences.

5 - RESULTS

The motivation behind writing this article lies in the desire to shed light on the weaker party in criminal proceedings. This party (the victim) has rarely been the focus of attention among legal scholars and researchers, particularly in the context of cybercrime. There is no doubt for the reader that we encountered numerous difficulties and obstacles during our research and in the drafting of this article in order to reach the results presented below.

Among the findings reached in this research are the following:

- The absence of a specific legal framework in the form of a comprehensive law that clearly organises and defines cybercrimes.
- The lack of a clear definition of cybercrime by the criminal legislator has left the door open for doctrine to propose multiple definitions, which may sometimes be inaccurate.
- The problem of implementation and enforcement of existing laws constitutes an obstacle to the effectiveness and efficiency of legal texts, particularly regarding their strict and proper application.
- Particular attention is given to enhancing effective coordination between national and international institutions concerned with electronic offences, due to their transnational nature. This has led the State to increase vigilance in light of the seriousness of these offences. Such coordination also contributes to preserving compensation opportunities for victims, thereby ensuring respect for their rights given the gravity and complexity of these crimes, especially in the area of evidence collection.
- This article highlights cybercrime victims, which may help draw greater attention to this marginalised group. It also provides policymakers involved in criminal policy guidance with a different perspective for revising criminal laws, with particular emphasis on victims who suffer in silence, both psychologically and socially.

CONCLUSION

In conclusion, the issue of cybercrime victims holds significant importance today, requiring increased attention and focus due to the emergence of new offences that differ radically from traditional crimes.

It is with this in mind that the Moroccan legislator strives to keep pace with advancements in comparative legislation in this field, in order to respond swiftly and effectively to safeguard the victims of such offences and to guarantee them appropriate compensation for the harm suffered.

EXTERNAL FINANCING?: This article is never funded

CONFLICT OF INTEREST?: This article is not the subject of any conflict or litigation

REFERENCES

In French language

³¹ Robert M., ministère de la Justice, ministère de l'Economie et des Finances, ministère de l'intérieur, ministère des petites et moyennes entreprises, de l'innovation et de l'économie numérique, Protéger les internautes - Rapport sur la cybercriminalité, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014. Charpenel Y, Cybervulnérabilité des usagers des réseaux sociaux, AP, P 5.

Victims of Cybercrime: What Criminal Protection Under Moroccan Law?

- 1) Charpenel Y, Cybervulnérabilité des usagers des réseaux sociaux, (Article sous la direction de), Prostitutions : Exploitations, Persécutions, Répressions, Ed. Economica, Paris 2016.
- 2) Farih Omar, Cadre conceptuel et théorique de la cybercriminalité, Revue Maroc Droit, 2014.
- 3) Fawn T. Ngo & Raymond Paternoster, Cybercrime Victimization: An examination of Individual and Situational level factors, International Journal of Cyber Criminology, Vol 5 Issue 1 January - July 2011.
- 4) Juraj Sikra Karen V. Renaud and Daniel R. Thomas, UK Cybercrime, Victims and Reporting: A Systematic Review, Commonwealth Cybercrime Journal, volume 1, issue 1 2023.
- 5) Mohamad Idris Laena, Riswadi, Legal Protection for Child Victims of Cyber Bullying, ICLSSEE, Semarang Indonesia, 16 April 2022. <http://dx.doi.org/10.4108/eai.16-4-2022.2319752>
- 6) Nadia Hamouti/Abdelaziz Elbouzidi, The importance of artificial intelligence in the field of Moroccan criminal law: What impact on the legal protection of personal data?, Al-Majd Advanced Scientific Journal, V 12, N° 12, 2024.
- 7) Robert M., ministère de la Justice, ministère de l'Economie et des Finances, ministère de l'intérieur, ministère des petites et moyennes entreprises, de l'innovation et de l'économie numérique, Protéger les internautes - Rapport sur la cybercriminalité, Groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014.
- 8) Romain Boos, La lutte contre la cybercriminalité au regard de l'action des États, Hal Open Science, pour l'obtention de doctorat de droit privé et sciences criminelles, Université de Lorraine 2016.
- 9) Sam Lyes, La criminalité électronique et son impact sur la sécurité nationale et la sécurité du citoyen, STRATEGIA Revue des études de défense et de prospective, N° 16 deuxième semestre 2021.
- 10) Scott Monteith et All, Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry, Psychiatry in The Digital Age (J SHORE, SECTION EDITOR), 2021. <https://doi.org/10.1007/s11920-021-01228-w>
- 11) Vishi Aggarwal, Ms. Shruti, Cybercrime Victims: A Comprehensive Study, Volume 6, International Journal of Creative Research Thoughts (IJCRT), Issue 2 April 2018.

In Arabic language

- إلهام بودراع، ريان صوالح، تجليات الجريمة الإلكترونية عبر المنصات الاجتماعية وأثارها النفسية والاجتماعية على المستخدمين، مذكرة مكملة لنيل شهادة الماستر، جامعة قاصدي مراح ورقلة، السنة الجامعية 2022-2023.
- امغار محمد، الإطار القانوني للجرائم الالكترونية في المغرب، المحور: دراسات وابحاث قانونية، الحوار المتعدد-العدد: 2023-7615. <https://www.ahewar.org/debat/show.art.asp?aid=793305>
- تركي بن عبد الرحمن الموشير، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة لنيل شهادة الدكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، السعودية، الرياض 2009.
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، مطبعة دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2009.
- رامي متول القاضي، مكافحة الجرائم المعلوماتية، دار النهضة العربية مصر، 2011.
- صالح بن محمد المسند/عبد الرحمان بن راشد المهيني، جرائم الحاسب الآلي: الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 15، العدد 29، أبريل 2000.
- عبد المومن الصغير، الطبعة الخاصة للجريمة الإلكترونية المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن، مجلة الحقوق والحريات، جامعة محمد خيضر – بسكرة -المجلد 02 العدد 02 2014.
- فريد حمامي، تداعيات الجريمة الإلكترونية من وجهة نظر الضحايا في المجتمع الجزائري، مجلة السراج في التربية وقضايا المجتمع، مجلد 08 عدد 01، سنة 2024.
- لخضر سلامي، ضحايا الجريمة الإلكترونية عبر مواقع التواصل: الفايبيوك نموذجاً، مجلة دراسات في سيكولوجية الإنحراف، المجلد 06 العدد 01 السنة 2021.



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0)

(<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.