THE INCREASE OF CYBERCRIME AMIDST THE COVID-19 PANDEMIC: A SPOTLIGHT ON THE MOROCCAN CONTEXT

AIRAJ, S.

Faculty of Letters and Humanities, University of Mohamed First, Oujda, Morocco.
e-mail: soumia.airaj[at]outlook.com

(Received 10th January 2024; accepted 05th April 2024)

Abstract. Amid the COVID-19 outbreak, the entire world has been turned upside down. Daily practices such as work and education have shifted to the online and remote model at homes. This transition from in-person to online transactions has increased the prevalence of electronic crimes, commonly known as 'cybercrimes'. These types of crimes are among the most significant types of crimes for the entire world and Morocco is no exception. Cyber-attackers have seized the opportunity of the pandemic to multiply their digital crimes and take advantage of individuals who were extremely frightened by the virus and bombarded with a significant amount of constant updates, including fake news, related to the Coronavirus outbreak. They have also exploited the increased use of people's virtual communication particularly via social media platforms and the online vulnerabilities to target victims with low digital and media literacy. The current paper seeks to investigate the kinds of cybercrimes that have been committed online during the pandemic notably false promotion of products claiming to protect against COVID-19, online fraud operations, extortion, identity theft, threats, abuse, harassment, defamation, among others. Moreover, the researcher attempts to suggest proper ways to address these types of crimes and enhance cybersecurity that involve promoting digital literacy, implementing legal deterrence, and engaging multiple parties.
Keywords: *cybercrimes, COVID-19, cybersecurity, digital literacy, legal deterrence*

Introduction

In contemporary society, it is challenging to envision how an individual could navigate daily life without relying on online tools and systems. The digital realm plays a ubiquitous role in various aspects of society, facilitating communication, entertainment, and business interactions for users on a daily basis. During the COVID-19 pandemic, there happened abrupt and profound alterations in the everyday routines of individuals in most of the countries around the world that have undergone a set of precautionary measures to cope with the virus outbreak. The day-to-day routines, including work and education, have transitioned to an online and remote format within the confines of homes. Meanwhile, there has been a noticeable increase in the rate of online criminal activities, commonly referred to as "cybercrimes". At a time when the international community is racing against time to curb the spread of the Coronavirus, "cybercriminals" are intensifying and expanding their activities, diversifying their forms under the guise of electronic commerce, attempting to exploit the disruption caused by this global health crisis. Thus, what is a cybercrime? What are the types of cybercrimes that have emerged during the COVID-19 pandemic in Morocco? What are the legal procedures in Moroccan legislation to deter cybercriminals? What is the role of digital literacy in mitigating the exacerbation of cybercrimes? These are questions and more that we will try to answer in this paper.

What is a cybercrime?

A cybercrime refers to "any malefactor or other crime involving electronic communications or information systems, including any device or the internet or both."

(Tiwari, 2022). In other words, it is any criminal act that is held online using a technological device such a computer or a phone. This kind of crimes takes various forms and targets both individuals and organizations. Bunga (2019) asserts that a cybercrime "is a very serious threat faced by many countries. The loss of this case is not only related to financil losses but also related to moral and behavioral degradation" (p. 71). Therfore, cybecrime the repercussions of such criminal incidents extend beyond financial losses to encompass moral and behavioral deterioration.

As for cybercriminals who commit these crimes "illegally access information systems to steal, misuse and compromise the integrity of information for personal financial gains" (Chigada and Madzinga, 2021). They deceive vulnerable people who are unaware of the dangers of sharing their private information online and lack strategies to deal with the digital world appropriately. Moreover, a cybercrime is considered "a new phenomenon in crime due to a direct impact of the development of information technology" (Kusuma et al., 2022). It is perceived as a modern trend because of the great impact of technology on criminal activities. Many experts and researchers in the field of cybersecurity accentuate the correlation between the development of information technology and the rise of cybercrime.

Types of cybercrime emerging during the COVID-19 pandemic in Morocco

According to Khweiled et al. (2021), "Although traditional crime rates decreased due to curfews' imposition, cybercrime rates have witnessed a remarkable increase since the beginning of the pandemic". Thus, despite the measures that accompanied the COVID-19 pandemic, such as lockdown and quarantine, leading to a decrease in traditional crimes, cybercrimes have risen tremendously. In fact, these cybercrimes cover a wide range of illegal activities that involve the use of computers, networks, and the internet. Lallie et al. (2021) distinguish between two main types of cybercrime: (1) Cyber-dependent crime that includes Hacking, Malware, and Deniale of Service, and (2) Cyber-enabled crime that involves Fianancial Fraud, Phishing, Pharming, and Extortion. The following are some common types of cybercrimes that have emerged amidst the COVID-19 pandemic in Morocco.

The proliferation of the illegal sale of medications claimed to treat the Coronavirus on the internet

Immediately after the announcement of the spread of the novel Coronavirus in some countries, illicit sales of medicines and medical supplies proliferated online at the global level and Morocco was no exception. According to a web portal, The International Criminal Police Organization (INTERPOL) announced the seizure of counterfeit masks, inadequate hand sanitizers, and unlicensed antiviral drugs during the COVID-19 outbreak. Other online businesses disappeared as soon as they received payment from customers. In fact, cybercriminals have been directing efforts towards healthcare entities "that are at the forefront of dealing the COVID-19 pandemic, especially hospitals, research organisations, laboratories and pharmaceutical companies" (Chigada and Madzinga, 2021). Moreover, the INTERPOL stated that phishing websites, which are electronic messages purportedly from national agencies or global health organizations, have emerged aiming to deceive victims and make them provide personal information, payment details, or open an attached file containing malicious software. As for sending phishing emails during the pandemic, Plachkinova (2021) states the following scenario:

"*Individuals receiving emails disguised as coming from a hospital informing them that they may have been in contact with someone who tested positive for COVID-19. The email instructs the recipient to download a file, fill it out, and bring it to the nearest hospital for further testing. As in the previous example, here the attackers have embedded malicious code in the file and their goal is to steal login credentials, lookup cryptocurrency wallets, discover open shares on the network, and obtain the IP address*".

The EUROPOL headquartered in The Hague, noted that online fraud has become an ideal strategy for cybercriminals claiming to sell products that purportedly protect against or cure the novel Coronavirus. The Confederation of Pharmacists in Morocco noted that the public prosecutor's office has initiated legal proceedings after receiving a complaint regarding the sale of drugs for the Coronavirus online. The confederation stated that the judicial investigations conducted by the cybercrime unit in Morocco led to the arrest of individuals and the seizure of 20,000 boxes of "Vitamin C" medication and approximately 3,500 units of "Zinc" medication were confiscated, along with other unregistered and unknown-source medications. Other cybercriminals contact victims, pretending to be employees of medical clinics, hospitals, or other healthcare facilities, claiming that a person's relative has been infected with the virus and demanding payment for medical treatment. Mohamed Lahbabi, the president of the Confederation of Pharmacists in Morocco, had previously warned about the proliferation of the illegal sale of medications claimed to treat the Coronavirus on the internet. He emphasized that some drugs are being sold online illegally and from unknown sources, often at higher prices than those in pharmacies. Lahbabi cautioned that taking such medications without a doctor's prescription or consultation with a pharmacist could pose health risks.

The spread of fake news during the Coronavirus

During the COVID-19 pandemic, there has been an observed misuse of modern technologies and the evolution of communication channels by some social media users. Among the significant issues during that period were the dissemination of fabricated information, malicious rumors, and the spread of false news related to the Coronavirus pandemic that aim to create anxiety, instill worry and panic among citizens, disrupt public security, and cast doubt on the state's ability to confront the crisis affecting the entire world. The tracking of several audio recordings and videos circulated through social media applications and platforms, containing rumors and inaccurate information about COVID-19 infections, which caused panic and fear among citizens, impacting social security and public order. In fact, these misleading narratives resonate strongly with recipients due to the severity of the subject matter and its direct impact on them. According to The Economic, Social and Environmental Council in Morocco, which has released an Opinion entitled "Fake News: From Global Deception to Reliable and Accessible Information" in 2022, the number of legal cases presented to the courts in Morocco regarding fake news reached 226 legal files during the period from 2019 to the end of August 2022. And they are distributed in *Table 1*. It should be noted that the fake news that have gone viral during the Coronavirus outbreak targeted various issues; namely, causing anxiety and panic among individual, inciting hatred and discrimination, and affecting the discipline of the military.

Table 1. *Descriptive statistics for artificial intelligence adoption.*

The nature of false news that is spread with malicious intent	The number of cases in which judgments have been issued
News that affects public order or instigates panic among people.	175
News that directly incites hatred or discrimination.	42
News that affects the discipline or morale of the military.	9
Total	223

In the time of the COVID-19, scams and fraud on social media platforms

During the Coronavirus outbreak, certain groups were created by particular entities claiming to have humanitarian and social purposes (*Figure 1*). They claim to contribute as an initiative to confront the economic and social repercussions of the COVID-19 pandemic in Morocco. The founders of these groups created virtual spaces and turned them into traps to deceive individuals with compassionate hearts and charitable intentions. They mislead them into donating money and other resources, which are then supposedly collected and distributed to benefit the poor and needy people. On the other hand, the recipients are asked to provide their complete personal information under the guise of camouflage procedures and promised financial assistance within 10 days; however, this assistance is never actually provided leaving the individual clinging to the illusion of fraud and exploitation of their needs.

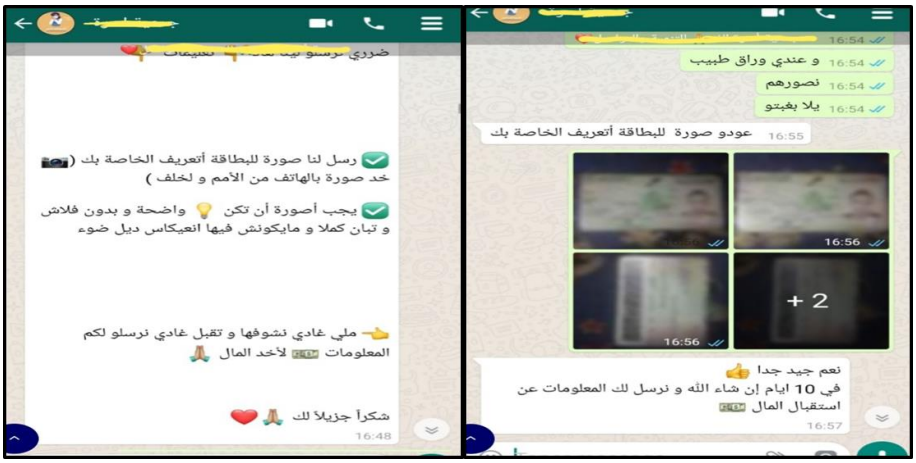

Figure 1. *A deceiving WhatsApp Group.*

The above picture showcases a screenshot of a deceiving WhatsApp group in which the founder of the group asks group members to send a picture of their identification card (take a photo with their phones, front and back). They request the image should be clear, without flash, and show the complete card without light reflections. Once the founder receives and verifies it, he/she promises to provide them with the information to proceed with the payment in few days. The admin of the group takes advantage of the vulnerability of the victims who have financial issues. Thus the poor individuals send their personal information without knowing the dangers of that as they might use them for criminal purposes. Actually, victims were easily manipulated due to the fact that a large number of people have lost their jobs during the health crisis that necessitated the shutdown of a number of job providers. In this regard, Khweiled et al. (2021) note, "most companies requested their employees to work from home, students moved to online studies, online shopping increased, and social networking activity increased, leading to an increase in Internet users significantly". These criminal groups

intentionally manipulate the emotions and sentiments of the poor and needy people and weave virtual scenarios on social media platforms in order to gain the trust of well-intentioned individuals and solicit their compassion. They then redirect the money generously given by sincere and kind-hearted donors into the pockets and accounts of criminals who hide behind the masks of piety and enjoining good.

The growing exposure of Moroccan children to electronic crimes in the middle of the COVID-19 pandemic

Amidst the unprecedented increase in the time children spend in front of electronic device screens, exacerbated by the COVID-19 pandemic that altered the traditional education pattern with the adoption of remote learning. During the peak of the health crisis, it has been noted a significant increase in materials involving the online sexual exploitation of children. Thus, the dissemination of such content has 'become more popular' due to travel restrictions. In this regard, a scientific guide was conducted by a Moroccan association named "Sesame Citizen Engagement Association" and targeted middle and high school students from eight Moroccan cities. It has warned of various risks posed to children in the digital world such as: phishing, cyber-bullying, digital harassment, cyber intrusions, digital extortion, defamation, psychological harm, and exposure to violent or sexual content. The study revealed that 62% of the participants are exposed to risks while using the internet, with 30.6% stating that they do not feel safe while browsing the internet or using social networks. The study found that 30.6% of the participants were victims of cybercrimes including unauthorized use of images and personal information, threats using personal data, and account breaches. Unfortunately, most victims talked about the cybercrimes they experienced with acquaintances, but only two out of ten reported the incidents to law enforcement. As stated in the previous web portal, in a report on the growing cybercrime during the COVID-19 era, The European Police Agency (EUROPOL) warned of another type of cybercrime specifically targeting children. This vulnerable group becomes more susceptible to exploitation (sexual harassment, abuse, exposure to inappropriate content) by some cybercriminals due to children's isolation during long periods of quarantine and limited supervision by parents.

The increase of defamation and extortion of women during the Coronavirus health crisis

Defamation and extortion are among the most dangerous cybercrimes that have held the forefront for years. In the year 2020, more than 560 defamation cases and over 370 extortion cases were recorded in Morocco. The perpetrators of these criminal acts take advantage of human nature, credibility, and the trust that the victim places in the unknown person with whom they interact online. However, in many cases, the majority of women prefer not to file complaints, so the police do not know what is happening and these criminals who may be active in gangs and mafias are not searched for it. In an interview with Amine Raghib, a Moroccan cybersecurity expert, claims that there are diverse ways in which victims are deceived. One method involves individuals working with groups that have no issues with nudity as the crucial point is to send them money. Yet, these women are then subjected to threats and extortion if they do not provide them with money. The other way involves recording the victims or hacking their computer, and taking their private pictures and videos from them to use them in crimes of

extortion and defamation. In this regard, Eaton et al. (2023) refer to “sextortion”, that is a combination of ‘sexual’ and ‘extortion’, “as the act of threatening to expose or distribute sexually explicit materials unless a victim complies with certain demands”. As for ways of executing sextortion, Eaton et al. (2023) explain : “sextortion can occur when perpetrators hack into victim’s electronic devices, accessing stored images and webcams. Sextortion may also be perpetrated as the result of sexual acts (consensual or forced) that are nonconsensually-recorded” (Eaton et al., 2023). However, it is important to mention that the majority of female victims do not contact the police; thus, the criminals are never caught and punished. Interestingly, it is worth noting that both women and men can be victims of online defamation and extortion.

Legal deterrence

Legal deterrence presupposes the use of laws and regulations to discourage individuals from engaging in illegal activities. The goal of legal deterrence is to guide individuals' behavior and maintain order within a society through penalties and punishments. In the context of cybercrimes, these penalties may involve the imprisonment and fines of cybercriminals who commit illegal activities online, serving as examples to others. Undoubtedly, electronic crimes that harm the private lives of individuals witnessed a massive response during the quarantine period accompanying the Coronavirus pandemic in Morocco, which made the rate of complaints rise. Accordingly, during the year 2020, 373 cases were registered regarding infringing on private life, publishing fake news, photographing people without their consent, and broadcasting and distributing a composition of people consisting of statements or pictures of people in order to infringe on their private lives and defame them. 454 people were followed up under chapters 447-1 and 447-2, which shows the increased impact on private life during the COVID-19 pandemic, quarantine, and health emergencies.

Penalties

In fact, penalties for committing cybercrimes can vary significantly depending on the jurisdiction and the specific nature of the offense. Cybercrimes may encompass a wide range of illegal activities, including hacking personal accounts, identity theft, fraud, defamation, extortion, fake news, sexual exploitation, and more. Penalties are typically outlined in the Moroccan constitution (legal framework) and legislation (laws), which are regularly amended to keep pace with ongoing technological developments. Common penalties for cybercrimes may include as discussed followed.

Article 447-1 of the Penal Code

"Any person intentionally capturing, recording, broadcasting, or distributing statements or information of a private or confidential nature, through any means including information systems, without the consent of the concerned parties, shall be punishable by imprisonment for a period ranging from six months to three years and a fine ranging from 2000 to 20000 dirhams”.

Article 447-1 of the Penal Code

"Any person using any means, including information systems, to broadcast or distribute a composition consisting of a person's statements or image without their consent, or spreading false claims or facts with the intention of infringing on the private life of individuals or defaming them, shall be punishable by imprisonment for a period of one to three years and a fine ranging from 2000 to 20000 dirhams".

Article 72 of the Press and Publication Law

"Anyone who maliciously publishes, broadcasts, or transmits false news, allegations, untrue facts, or manipulated documents attributed to others, causing a disturbance to public order or panic among people, by any means, especially through speeches, shouts, or uttered threats in public places or gatherings, or through writings and publications offered for sale, distributed, or displayed for sale or exhibited in public places or gatherings, or through posters displayed to the public, or through various audiovisual or electronic media, and any other means used for this purpose, shall be punished by a fine ranging from 20,000 to 200,000 dirhams".

According to Al Mazhari Ibrahim, Chief Clerk of the Public Prosecution at the Criminal Court of First Instance in Casablanca, when talked to the chief, "When a citizen submits a complaint to His Majesty the King's Undersecretary and the Deputy King's Attorney receives it, Mr. Deputy King studies it, takes a decision, gives his instructions, and sends it to the judicial authority, whether security or gendarmerie, so that they can investigate the subject of the complaint. The judge's discretion plays a pivotal role in determining sentences". The standard for taking these penalties is subject to the discretion of the judge by taking into account the social circumstances of the accused, the reasons and motives for committing these acts, and then most importantly, the extent of the damage resulting from this crime.

The public prosecution office in Morocco

Ahmed Taheri Alaoui, Judge and Head of the Unit for Organized Crimes and Modern Crimes under the Public Prosecution, when interviewed, he asserted that special attention has been given to this type of crimes by the Public Prosecution Office in Morocco since its establishment in October 2017 by taking a set of measures: (1) A special unit was created to track cases and information crimes at the level of the Public Prosecution; (2) Appointing judges for the Public Prosecution in charge of information crimes at the level of various courts in the country; (3) Giving important attention to specialized training in the field of information crimes; and (4) Giving special attention to cooperation with service providers at the national level as well as at the international level.

Digital literacy

According to Eshet (2004), digital literacy can be defined "as survival skill in the digital era. It constitutes a system of skills and strategies used by learners and users in digital environments". This means that it involves the ability to effectively use and understand digital technologies, tools, and platforms, enabling individuals to engage, communicate, and make informed decisions in the context of the digital world. Furthermore, "Digital literacy means that you understand how to use digital information" (Kusuma and Muslikhah, 2022). This highlights the importance of the ability to effectively navigate, comprehend, and utilize information in the digital realm.

Thus, being digitally literate is of paramount importance in the present era. Additionally, digital literacy entails "the ability to use and understand information in many formats from various sources when it is presented on a computer" (Kusuma and Muslikhah, 2022). This implies that it is the proficiency and capability of individuals to effectively utilize and comprehend information that is presented in diverse formats and originates from various sources, particularly when accessed on a computer (*Figure 2*).

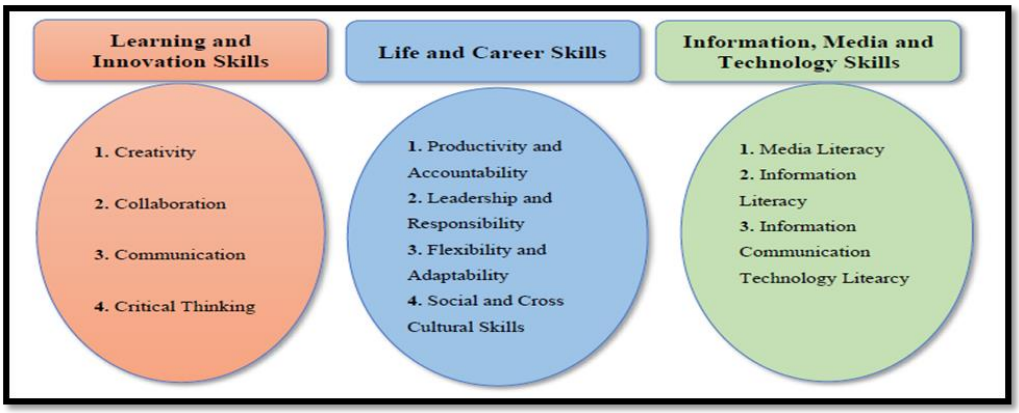

Figure 2. *Categorization of 21st century skills.*
Source: Agaoglu and DemİR (2020)

It could be assumed that digital literacy is essential for effectively using digital media interchangeably as both literacies are crucial in today's information age, where digital and media platforms play significant roles in our daily lives. Based on figure 3, media literacy is one of the main 21st century skills that are of paramount important in the current era. It belongs to the third category entitled 'Information, Media and Technology skills'. According to Kusuma and Muslikhah (2022), there are ten benefits of digital literacy: save money; always up to date; save time; more secure; learn faster; always connected; make better decisions; provide a job; makes happier and influence the world.

Some of the recommendations to address the challenges associated with the lack of digital literacy, and consequently, mitigate the exacerbation of cybercrimes include the following: don't click on links or open files shared online without knowing their sources; don't reveal your personal information to the public; don't accept anonymous friend requests; don't trust people who ask for sensitive and personal information; don't hesitate to contact the police if deceived online; and use antivirus software.

Conclusion

Digital literacy is emerging as an indisputable starting point that can be the most effective means of combating such malicious cyber activities. It is the responsibility of various stakeholders to alleviate the exacerbation of cybercrimes. Parents, in particular, should keep a close eye on their children and monitor their interaction in the digital world. Also, schools play a significant role in raising students' awareness about the threats and dangers of the cyber space. Additionally, the government is responsible for organizing sensitizing programs and training to make people aware of these types of crimes and ensure cybersecurity. Finally, one may wonder, "How did modern

technology turn from a blessing into a curse that violates the honor of some and causes economic, social and psychological crises for others that sometimes lead to suicide?"

Acknowledgement

This research study is self-funded.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Agaoglu, O., DemİR, M. (2020): The integration of 21st century skills into education: an evaluation based on an activity example. – Journal of Gifted Education and Creativity 7(3): 105-114.
[2] Bunga, D. (2019): Legal response to cybercrime in global and national dimensions. – PADJADJARAN Jurnal Ilmu Hukum (Journal of Law) 6(1): 69-89.
[3] Chigada, J., Madzinga, R. (2021): Cyberattacks and threats during COVID-19: A systematic literature review. – South African Journal of Information Management 23(1): 1-11.
[4] Eaton, A.A., Ramjee, D., Saunders, J.F. (2023): The relationship between sextortion during COVID-19 and pre-pandemic intimate partner violence: A large study of victimization among diverse US men and women. – Victims & Offenders 18(2): 338-355.
[5] Eshet, Y. (2004): Digital literacy: A conceptual framework for survival skills in the digital era. – Journal of Educational Multimedia and Hypermedia 13(1): 93-106.
[6] Khweiled, R., Jazzar, M., Eleyan, D. (2021): Cybercrimes during COVID-19 pandemic. – International Journal of Information Engineering and Electronic Business 13(2): 1-10.
[7] Kusuma, C.S.D., Muslikhah, R.I. (2022): Strengthening of Digital Literacy to Support Student Community Service to Prevent Hoax and Cybercrime. – In 9th International Conference on Education Research, and Innovation (ICERI 2021), Atlantis Press 10p.
[8] Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021): Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. – Computers & Security 105: 20p.
[9] Plachkinova, M. (2021): Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic. – International Journal of Cyber Forensics and Advanced Threat Investigations 2(1): 50-62.
[10] Tiwari, S. (2022). A Study on Social Media Literacy and Cybercrimes against youth in Kumaon and Garhwal Regions of Uttarakhand. – IMS Unison University 44p.