PISSN : 2571-9904 - EISSN : 2602-7763

Information crime: analysis of the concept and effects in the digital environment

Nadjette Charaf Eddine [1,*], Fairouz Latreche [2]

[1] Laboratory of Studies in Digitization and Electronic Information Industry in Libraries, Archives and Documentation / Echahid Cheikh Larbi Tebessi University (Tebessa), Email nadjette.charafeddine@univ-tebessa.dz

[2] Echahid Cheikh Larbi Tebessi University (Tebessa), Email fairouz.latreche@univ-tebessa.dz

Received: 01 / 02 / 2024 **Accepted**: 24 / 04 / 2024 **Published**: 30 / 04 / 2024

Abstract:
This research aims to comprehend the nature of Information crime as a social phenomenon, originating from the exploitation of technology and digital tools in committing crimes. Examples include manipulation of digital information, data theft, electronic system breaches, electronic fraud, and other related crimes. The research also aims to understand the motivations that drive individuals to engage in such activities and to analyze their impacts on individuals, societies, and institutions. Additionally, it seeks to identify the methods employed for prevention and protection against Information crime, including the development of security procedures, information technology, awareness initiatives, and training programs

Keywords: Crime ; information ; criminal ; Information criminal ; Information crime ; digital environment.

[*] Nadjette Charaf Eddine

I. INTRODUCTION:

The electronic advancements in the field of computers, information systems, and communication, including the internet, have brought numerous advantages across various domains, making it challenging to dispense with them. However, this progress is not without drawbacks, as it has led to the emergence of new types of crimes known as cybercrimes. These crimes encompass traditional offenses associated with the use of computers and various information and communication systems, as well as newly introduced crimes that were not present originally. The latter now pose a grave threat to individuals, as well as public and private institutions, resulting in significant losses.

Information crime is increasingly becoming a social phenomenon in the era of modern technology. With the continuous evolution and widespread use of the internet and electronic communication methods, digital information has become widely available, forming a vital part of our daily lives. In this type of crime, technology is exploited to manipulate and forge information for the purpose of achieving illegal gains through illegitimate means. This includes altering and manipulating information, whether by increasing or decreasing it, identity theft, forging signatures and seals, leading to damage to individuals' reputations, affecting business operations and institutions, stealing personal and financial information, exposing individuals to electronic extortion, and negatively impacting information security and the stability of digital data.

The increasing prevalence of these crimes has prompted countries to intensify their efforts in enacting legislation and imposing strict penalties to mitigate the risks and spread of cybercrime.

In light of the foregoing, the study's questions revolve around the following:

- What are the components of information crime and what are its most important characteristics?

- What is the difference between traditional crime and information crime?

- What are the motives behind committing a cybercrime?

- What are the elements of information crime?

- What sectors are targeted by cybercrime?

1. Conceptual Framework of the Study:

1.1. Crime:

The concept of crime can be defined as an event that occurs, an incident that takes place, an act that is committed, or an experience that unfolds. Whether intentional and premeditated or incidental and unintentional, the perpetrator in a crime deviates from prevailing customs and traditions or acts outside the legal framework designed to protect individuals from aggression by others. The actor becomes a transgressor of societal norms and legal standards, either challenging established customs or violating statutory laws meant to deter individuals from committing offenses. This deviation is intended to instill a sense of disapproval within society and serves as a deterrent, prompting individuals to refrain from engaging in criminal activities out of concern for the consequences. **(Al-Saati, 2005, p. 23)**

1.2. The Information:

Information clarifies the concept of the thing, providing it with significance. It highlights its features and characteristics, elucidates its uses and functions, or is that which alters the cognitive state of the recipient, be it a reader, viewer, listener, or any sense through which reception occurs in a given subject.

In the field of library and information science, the terminology dictionary defines information as processed data aimed at achieving a specific goal or for a specific use in decision-making. This refers to data that has gained value after analysis, interpretation, or aggregation into a meaningful form. Information can be exchanged, recorded, published, and distributed formally or informally and in any format. **(Tala, 2021, p. 188)**

1.3. Information crime:

is defined as any deliberate act or intentional omission arising from the unauthorized use of information technology. Its aim is to attack both material and moral assets. **(Bin Saud, 2011, p. 24)**

1.4. Information criminal:

is an individual with the ability to convert their language into digital language, store and retrieve it using digital electronic computers, their accessories, and digital communication tools. This involves performing intentional acts or abstaining from them, causing disruptions in the international or local community due to violations of social norms at both local and international levels. **(Khalili, 2017, p. 405)**

1.5. Digital Environment:

The digital environment is a logical extension of technological advancements in computing. It is an environment produced through the use of computers, enabling users to interact with it. Interaction can involve examining the content through visual and auditory senses or actively participating and influencing it by performing modification and development operations. **(Bin Ammar, Bakhoush, 2021, p. 257)**

1.6. The difference between traditional crime and Information crime:

Information crime involves intelligent criminals compared to traditional crime, which tends to be violent. Cybercriminals typically possess high-level technical skills and expertise in information technology **(Maashi, 2018, p. 414)**. Information crime differs from traditional crime in terms of its locus, which is either electronic information or data **(Khilaf, 2021, p. 337)**.

Among the differences that can be inferred are the following: **(Barhoum, 2019, p. 16)**

1.6.1. Difficulty of detection: This is because Information crimes do not leave external traces, and their discovery is often a matter of sheer coincidence. Additionally, perpetrators can quickly destroy evidence in less than a second.

1.6.2. Non-disclosure: Businesses and institutions in the field of operations tend to refrain from reporting crimes committed within their domain. This reluctance is attributed to

2. Defining information crime and explaining its subject:

2.1. The concept of Information crime:

The widespread adoption of modern technology and the astounding development of cybercrime resulting from it have led to increased interest from researchers and experts in various fields such as law, criminology, media and communication, politics, economics, psychology, and others. This has resulted in diverse definitions and terminology, making it difficult to find a comprehensive and universally applicable definition. Some define it from a technical and technological perspective, while others approach it from a legal standpoint. As Van Dijk and Von Hoorn argue, there is a lack of a general definition and a consistent theoretical framework in the field of cybercrime. Often, terms such as virtual, computer, electronic, digital, and informational are used. **(Tala, Salam, 2020, p. 66)**

The term "information crime" is composed of two components: "crime" and "information," combining the general concept of crime with its informational nature. Crime is defined as a violation of the standards and regulations of society, causing harm to individuals and the community. The law, which serves to protect and represent the social entity, prescribes punishment or criminal penalties for such acts. Sociologists view crime as a social phenomenon, emphasizing that criminalization is not solely the domain of legislators or legal professionals but is derived from the social reality with its values and social standards. Crime, from a sociological perspective, involves deviating from societal norms or social rules set by the community, encompassing actions that pose a threat to society and hinder the achievement of harmony and cooperation among its members. Durkheim and Merton, for instance, considered crime as behavior that lacks a normative basis, deviating from the established standards in society. From a legal standpoint, scholars generally agree that a crime or criminal behavior is "any act or failure to act that the legislator criminalizes and for which the law provides a penalty, constituting a legal rule applied to those who violate it. **(Tala, Salam, 2020, p. 67)**

Regarding the definition of cybercrime, there is notable disagreement based on the differing foundations of these definitions. Some legal perspectives define it based on the method of its commission, while others define it based on personal characteristics of the perpetrator, specifically emphasizing the trait of knowledge and technical expertise. Additionally, another group of legal scholars defines cybercrime by focusing on the computer, considering it both the locus of the crime and the means by which it is committed.

a- Definition in terms of the means:

It is defined as all forms of behaviors and actions that harm society, committed using computers and the internet. It is also considered a criminal act where a computer is used as the primary tool in its commission. **(Aliwa, 2021, p. 1213)**

b- Definition in terms of the individual:

It has been defined as any unauthorized act where knowledge of computer technology is essential for its commission, investigation, and legal pursuit. It is also defined as any intentional act related to computers that causes, or has the potential to cause, the victim to incur loss, gain, or the potential for the perpetrator to gain.

c- Definition according to legal standards:

Another aspect of legal jurisprudence defines Information crime based on two legal criteria, considering the computer as both the locus and the means of committing the crime simultaneously. It is defined as a crime in which a computer is used as a tool or instrument in its commission, represents an inducement for it, or is a crime where the computer itself is the victim. It can also encompass a set of legal offenses that can be committed through information with the aim of achieving profit**. (Aliwa, 2021, p. 1214)**

2.2. History of the development of Information crime:

The history of the evolution of Information crime is closely tied to the historical development of technology and its applications. In the initial stage of widespread computer use in the 1960s, discussions focused on articles and journalistic materials that debated data manipulation and the destruction of computer systems. This debate raised questions about whether these crimes were legally defined or emerging criminal phenomena, leading to controversy over whether they were legal crimes or simply unethical behaviors in an information environment. As personal computers became more prevalent in the mid-1970s, legal studies began to address cybercrime, tackling various actual cases. In the 1980s, a new concept of cybercrime emerged, linked to remote computer system intrusions and activities such as the dissemination and planting of information viruses. These activities aimed at destructive operations against files or programs by infiltrators targeting information systems capable of committing acts that either sought financial gain, espionage, or the seizure of sensitive economic, social, military, and political data. **(Souri, 2005, p. 8)**

The 1990s witnessed a massive growth in the field of technological crimes, resulting in changes to its scope and concept. This was largely influenced by the facilitation of system entry and network intrusion through the internet. Information crimes became more active against significant and influential internet marketing sites. Disrupting these sites for hours caused substantial financial losses, amounting to millions or even billions. During the same period and up to the present day, there has been a surge in crimes involving the spread of viruses through internet platforms, taking advantage of their rapid transmission to millions of users simultaneously. Activities involving the publication of written materials or messages on the internet or sent via email have also emerged, often containing provocative content or aiming to undermine the dignity and considerations of individuals. Such activities serve to promote illegal and unlawful materials or actions. **(Souri, 2005, p. 9)**

2.3. Topic of information crime:

The subject of information crime varies depending on the perspective from which the attack against a component of the information system is viewed. On one hand, this component itself may be the subject of information crime, while on the other hand, the information system may serve as a tool for the crime and a means of its execution. Consequently, these crimes are divided into two categories:

2.3.1. The First Category:

When the information system itself is the subject of Information crime, it appears that these crimes, in their technical sense, align with traditional crimes. In this case, the information crime involves an attack on the physical components of the system (such as devices and equipment). This includes crimes like theft and destruction of these components. Additionally, if the attack is directed towards the non-material components of the system (such as data and programs), it includes crimes like tampering with data stored in computer memory or manipulating data transmitted across various communication networks. **(Houhou, Bellourgi, 2014, p. 46)**

2.3.2. The Second Category:

When the information system serves as a tool for information crime, it is undoubtedly a purely traditional crime. In this case, the information system or the computer becomes a tool for committing crimes such as theft, fraud, breach of trust, or forgery of digital documents. The perpetrator may manipulate the computer and information system to carry out these crimes, including using the computer for theft, fraud, breach of trust, or falsifying digital documents**.** **(Houhou, Bellourgi, 2014, p. 47)**

3. Characteristics of information crime:

3.1. Cross-border:

This refers to a type of crime committed across distances where the perpetrator is not physically present at the crime scene. The criminal conducts the offense remotely, eliminating their physical presence at the location of the crime. Consequently, distances widen between the action carried out through the active computer and the outcome, i.e., the data that becomes the subject of the crime.

3.2. Difficulty in detection and proof:

Information crimes are characterized by their stealthiness, making them challenging to discover and trace back to their perpetrators. The nature of these crimes targets intangible elements rather than physical evidence, leaving little material trace that could be used to identify the criminals, unlike traditional crimes. Moreover, conducting investigations and gathering evidence requires significant expertise in information technology, presenting a challenge for law enforcement agencies and legal authorities to effectively deal with such cases**. (Maashi, 2018, p. 414)**

3.3. Distinctiveness of the perpetrator and their motives:

Information crimes are committed through technological means, requiring the perpetrator to possess expertise and specialization in the field of information technology as they interact with computer systems and automated data processing. These criminals have unique characteristics and capabilities, specifically in terms of scientific and informational knowledge. They utilize cognitive resources and professional methodologies in committing their crimes.

Forging activities, therefore, do not occur by chance or through accidental actions; instead, they are crimes meticulously planned by individuals with high technical skills, experience, and intelligence. These crimes have a mental and scientific nature, relying on informational and technical knowledge dictated by the scientific and cultural progress of modern society. **(Brahmi, 2015, p. 195).**

In reality, Information crimes exhibit several distinctive characteristics, among the most prominent of which are: **(Al-Aryan, 2004, p. 53)**

- Underreporting:

Information crimes often go unreported, either because victims are unaware of them or due to fear of public exposure. Consequently, many Information crimes are discovered accidentally and long after they have been committed.

- Theoretical ease of commission:

Theoretically, committing a technically oriented crime is facilitated, and concealing the crime's details is relatively easy, making it difficult to trace the perpetrators.

- Lack of lasting physical traces:

Information crimes do not leave a tangible physical impact, and the technical traces, if any, are challenging to preserve.

- Mystery and intelligence reliance:

These crimes rely on a high level of intelligence, making it challenging for traditional investigators to handle and prove them. Investigating cybercrimes differs significantly from traditional crime investigations.

- Requirement of high-level technical expertise: Unraveling the truth behind Information crime necessitates the involvement of highly skilled technical experts.

- Globalization impact:

The globalization of these crimes leads to the dispersion of investigative efforts and international coordination to track such offenses. Cybercrimes serve as a true reflection of the globalization phenomenon.

- Quiet nature:

Information crimes are often non-violent, yet some liken them to violent crimes. The Federal Bureau of Investigation (FBI) in the United States has drawn parallels between the motives of attackers on computer systems and those committing violent acts.

4. Motives for committing Information crime:

4.1. Achieving financial gain:

The desire for financial gain is a primary factor motivating individuals to commit Information crime. It is one of the most significant and compelling motivations for criminals due to the substantial profits that can be achieved through such illicit activities. Often, the motivation behind these crimes stems from the offender experiencing financial difficulties, being unable to settle their outstanding debts, or facing family issues linked to a lack of financial resources. This may include situations where the offender needs funds for gambling, purchasing drugs, or similar circumstances. In order to extricate themselves from these predicaments, the perpetrator seeks to manipulate the information systems of banks and financial institutions by hacking into their systems and discovering security vulnerabilities.

4.2. Desire for Learning:

Some individuals engage in cybercrimes with the aim of gaining new information and exploring the rapidly growing and evolving field of technology. These individuals conduct research, discover systems, and collaborate within communities, sharing knowledge. These hackers prefer to remain anonymous for as long as possible to ensure their continued presence within systems. Some of them dedicate their time to learning how to hack into restricted websites and understanding the security technologies employed in computer systems. **(Saghir, 2013, p. 39)**

4.3. Psychological or Pattern Motivations:

The motivation for perpetrators of Information crime is often the desire to assert themselves and achieve victory over the technology that provides opportunities for skilled programmers to commit such crimes.

4.4. Political Motivations:

Political motives are among the prominent international attempts to infiltrate government networks in various countries worldwide. Individuals may also manage to penetrate government security systems. Moreover, the internet has become a fertile ground for disseminating the ideas of many individuals and groups. It serves as a means to promote news and other matters that may, in their folds, contain a threat to national security, government systems, or defamation of international or political figures, leading to criticism and defamation.

4.5. Motive of Revenge:

The motive of revenge can be a significant factor in committing these crimes. It is considered one of the most dangerous motives that can drive an individual who possesses significant information about the organization or company where they work. This is often the case if the person is an employee who acts out of a sense of retaliation for being terminated from their job, bypassed for incentives, or overlooked for a promotion. These circumstances may lead them to commit the crime. **(Saghir, 2013, p. 41)**

5. Elements of information crime:

Information crime is based on three pillars:

5.1. The Material Aspect:

The material aspect of this crime focuses on the electronic system that is abused or unlawfully penetrated, with tangible consequences resulting from such usage. This can take the form of destruction of information or intentional damage to data stored on the computer. It is difficult to perceive the criminal behavior in this crime, unlike traditional crimes, as it is committed through information flowing through computer systems in an intangible manner. Similar to electrical current that flows without being seen, the material act here involves unauthorized entry and presence in the processing system, leading to obstruction and disruption of the system. Additionally, it involves intentional attacks on this system by manipulating and modifying the stored data and information. This means that the material aspect of cybercrime is represented by the environment where the crime occurs, referring to the technical aspect relying on the use of computers and the internet. **(Khalaf, 2021, p. 336)**

5.2. The moral aspect:

The moral aspect, in the general context of Information crime, is related to the psychological state of the perpetrator in all its forms. It involves the criminal intent, where the perpetrator is aware of all the elements of the crime committed, knowing that the act targets the automated data processing system, including information and programs. As these are subjects protected by the law, the moral aspect represents the relationship between the material aspects of the crime and the personality of the perpetrator. The perpetrator in cybercrime must be aware that their criminal activity leads to the disruption or corruption of the automated data processing system without the consent of the rightful owner. This makes the crime intentional and based on disregarding the rights of others through unauthorized access, remaining, and deception.

5.3. The legal aspect:

The legal aspect of Information crime is based on the illegitimate nature of actions carried out by individuals. The principle of criminal legality forms the basis for criminalization and punishment in electronic crimes, prohibiting criminal accountability unless there is a specific legal text addressing it. When the legal text is absent in criminalizing these actions, which are not covered by existing legal provisions, accountability is refused. However, applying this principle to some crimes committed online is challenging due to the absence of specific legal provisions capable of addressing issues related to the unauthorized use of the Internet. **(Khilaf, 2021, p. 337)**

6. **The sectors targeted by Information crime:**

Various sectors have entered the realm of information technology, especially with the emergence of the Internet, given the significant services it offers, particularly in terms of speed, time reduction, and cost-effectiveness. However, in return, these sectors have become vulnerable to being victims of cybercrime. Notable among these sectors are the financial sector, military institutions, along with ordinary individuals.

6.1. Financial and Economic Institutions:

The reliance on information networks has become almost absolute in the world of finance and business. This makes these networks, due to their interconnected nature and openness to the world, an enticing target for criminals. The increased allure of economic and financial targets is due to their tangible susceptibility to prevailing impressions, expectations, and skepticism about the accuracy of information. Simple mishandling or storage of this information can lead to destructive results and undermine confidence in the economic system. This type of crime involves causing widespread disruption in network systems that control the activities of banks and global financial markets. It spreads chaos in international trade transactions. Additionally, it can result in partial or complete halting of trade and business systems, causing economic activities to malfunction and come to a standstill. **(Saghir, 2013, p. 22)**

6.2. Individuals:

Ordinary people have become increasingly more targeted victims of cybercrimes due to the continuous and significant growth in the number of internet users worldwide. Cybercrimes are no longer limited to financial and military sectors. Consequently, many individuals are exposed to crimes such as fraud, theft, and destruction. It is natural for the internet to be a fertile ground for committing such crimes.

6.3. Military Institutions:

The information revolution did not confine its impact to the civilian sector alone but was crucial in developing modern warfare systems, leading to the emergence of what is known as information warfare. This type of criminal activity targets military and political objectives. Despite being relatively rare, instances of such crimes do occur. An excellent example is the success of the Englishman Nicholas Anderson in hacking the U.S. Navy's website and stealing the passwords used in nuclear attacks. Additionally, the German Heis Lander succeeded in penetrating the Pentagon's database, acquiring 29 documents related to nuclear weapons.

The state possessing information has become the most powerful, shifting focus to military espionage. The launch of military satellites has become the cornerstone for the development of military equipment and devices, leading to the emergence of new wars known as information warfare between nations. **(Saghir, 2013, p. 24)**

7. Categories of Information Criminals:

Information crime require a specific mental and intellectual capacity from the perpetrator. These crimes do not involve procedures leaning towards violence as much as they demand a unique mental and intellectual capacity from the offender. Donn Parker, an expert in cybercrime analysis at the Stannifere Institute for Research, identified seven (7) categories for the cybercriminal: **(Philippe, 1998, p. 34)**

- Amateurs.

- Enthusiasts: Those who commit crimes using violence that is difficult to imagine in the field of information. The classic case is the mad programmer aiming to disrupt all systems.

- Organized Crime: Computers have become a tool for crime barons and mafia gangs to execute crimes. For example, Gilberto Rodriguez, the leader of a notorious cocaine trafficking family in Colombia, owns a technological base comparable in size and power to the Soviet intelligence network.

- Foreign Governments: They use computer systems for espionage.

- Elites.

- Extremists: This group uses information networks to serve and disseminate their religious, political, or economic ideas. These motives can be found in well-known groups such as the Red Brigades in Italy.

- System Saboteurs: They use this as a means to satisfy their desires.

8. The nature of evidence in information crimes:

One of the challenges associated with electronic evidence is its invisible nature. The evidence resulting from information crimes committed on or through systems is typically comprised of non-visible data that, in most cases, does not reveal the identity of the perpetrator. This data is electronically recorded and often encrypted on optical or magnetic storage media, making it unreadable for humans, even if machine-readable. The manipulation or alteration performed by the perpetrator does not leave a trace connecting the criminal to the crime, thereby preventing the disclosure of their identity. Consequently, the non-visible nature of electronic evidence has a negative impact on the performance of entities dealing with it. The examination and analysis of such data pose significant difficulties for entities still governed by a material culture in handling this type of evidence. However, the situation is different for this type of digital evidence, which requires procedures suitable for its non-visible nature.

This problem is particularly evident in internet-related crimes, including those involving various electronic operations such as e-commerce or electronic banking operations. These crimes may involve ethical aspects related to the automated processing of data, such as theft or forgery through email, making it challenging to determine the source of the sender. **(Fayez, 2010, p. 394)**

9. Mechanisms to combat information crime:

9.1. International mechanisms to combat information crimes:

9.1.1. The efforts of the United Nations in the field of protecting private life:

were directed towards addressing technological advancements and safeguarding individuals and their freedoms from the risks of encroachment. This was highlighted in the First International Conference on Human Rights concerning the impact of technological progress on human rights, held in Tehran in 1968. The General Assembly adopted its recommendations, emphasizing that electronic computers represent the greatest threat to private life and personal freedom, as they are tools of surveillance and modern eavesdropping devices. This is especially true when personal data is stored on computers and analyzed, revealing patterns of behavior and relationships. The United Nations' Seventh Congress on the Prevention of Crime and the Treatment of Offenders, convened in Milan, Italy, in 1985, affirmed the necessity of applying new developments in the field of science and technology. Recognizing that these advancements may give rise to new forms of crime, appropriate measures should be taken against instances of reusing technology. **(Tayar, Hamlawi, 2021, p. 38)**

9.1.2. The United Nations Eighth Congress on Crime Prevention and Criminal:

Justice appealed in its resolution regarding computer-related crimes to the member states to intensify their efforts to effectively combat computer misuse, which requires the imposition of criminal penalties. It emphasized the necessity of:

- Updating criminal laws and procedures.

- Ensuring that existing penalties and laws regarding investigative authorities and the admissibility of evidence in judicial proceedings apply to cybercrimes and introducing amendments if necessary.

- Formulating crimes and procedures related to investigation and evidence.

- Increasing the activities undertaken by member states internationally to combat crimes associated with computers, including, when appropriate, becoming parties to treaties related to the extradition of criminals. **(Tayyar, Hamlawi, 2021, p. 39)**

9.1.3. Resolutions of the Fifteenth Congress of the International Association of Penal Law on Information crime:

This conference was held in 1994 in Brazil, where it outlined criminal activities that can be considered as Information crime, such as fraud and computer-related cheating involving the destruction and erasure of data. It also included what is known as computer forgery, covering the destruction and erasure of programs and data, as well as disabling the functions of the computer and communication (network) system or unauthorized access by violating security procedures. Procedurally, the decision issued by the Fifteenth International Congress of the International Association of Penal Law included a set of procedural rules in the context of cybercrimes, including :

- Conducting inspection and control procedures in the information technology environment, as well as inspecting computer networks.

- Facilitating effective collaboration between victims, witnesses, and information users to enable the use of information for judicial purposes.

- Intercepting communications within the computer system itself and exercising control over them. **(Alzanati, 2017, p. 36)**

9.1.4. The Budapest Convention on Information crime and Telecommunications 2001:

Recognizing the severity of Information crime as a transnational offense, this convention was signed by thirty countries, including European Union member states, as well as Canada, Japan, South Africa, and the United States. Signed in the Hungarian capital, Budapest, this convention aimed to address the international issue of cybercrime and transcend international borders, assisting countries in combating and tracking cybercrime perpetrators. It provides support for gathering evidence and apprehending offenders, outlining the best practices for investigating internet crimes, with the signatory countries pledging close cooperation in the fight against cybercrime. The European Convention on Cybercrime, also known as the Budapest Convention, signed on 23/11/2001, covers five main topics, addressing four types of crimes: **(Alzanati, 2017, p. 37)**

- Crimes affecting the confidentiality, security, integrity, and availability of computer data and systems.

- Crimes related to computer systems.

- Crimes related to child pornography.

- Crimes related to attacks on intellectual property and rights.

- The fifth section deals with responsibilities and penalties.

9.1.5. The European Treaty on Combating Information crime:

The special committee responsible for crime issues, appointed by the European Council, has signed the final draft of a comprehensive treaty aimed at assisting countries in combating cybercrime amidst criticism from advocates of personal freedom protection. After approval by the Council's presidency and signing by the relevant countries, the treaty will bind the signatory states to enact a minimum of laws necessary to deal with high-tech crimes. These include unauthorized access to a network, data manipulation, computer-related fraud and forgery, child pornography, and violations of digital copyright.

The treaty, which has been amended 27 times before approval, includes provisions that guarantee governments the right to surveillance and obliges countries to assist each other in collecting evidence and enforcing the law. However, the new international powers come at the expense of protecting citizens from potential misuse by governments employing the authorities granted by this treaty, which they may misuse. **(Salami, 2018, p. 200)**

9.2. National mechanisms to combat information crimes:

9.2.1. According to the Algerian Constitution:

The Algerian Constitution of 1996, along with any emergency amendments, guarantees the protection of fundamental rights and individual freedoms, emphasizing that the state must ensure the inviolability of human dignity. These constitutional principles have been enshrined in practice through legislative texts included in the Penal Code and criminal procedures, as well as other specific laws that prohibit any infringement on these rights. Additionally, it is prohibited to seize any publication, recording, or other means of communication except by judicial order. **(Maadawi, 2020, p. 130)**

9.2.2. According to Algerian Penal Code:

In order to address legal gaps, the Algerian legislator introduced a series of provisions criminalizing acts related to automated data processing. The penalties for such actions include imprisonment for a period ranging from 3 months to 1 year, and a fine ranging from 50,000 to 100,000 DZD, for anyone who gains access or remains through cheating in all or part of the automated data processing system or attempts to do so. The penalty is increased if this leads to the deletion or alteration of data in the system. If these actions result in the sabotage of the system's operation, the penalty includes imprisonment for a period of 6 months to 2 years and a fine ranging from 50,000 to 150,000 DZD. **(Maadawi, 2020, p. 134)**

9.2.3. Combating Information crime through criminal procedural law:

The pursuit of Information crime follows the same procedures as traditional crimes, such as inspection, examination, questioning of the suspect, apprehension, testimony, and expertise. The Algerian legislator has extended the local jurisdiction of the public prosecutor in cybercrimes and emphasized inspection. However, the legislator considered that the inspection imposed on information systems differs from the conventional inspection in general procedural rules, both in formal and substantive conditions. While inspection is part of the investigative procedures, the legislator has surrounded it with strict rules.

The legislator also addressed the consideration of the crime of tampering with processing systems, interception of communications, capturing images, and under these provisions, the Algerian legislator allows investigative authorities, when necessary to investigate a caught crime or cybercrime, to resort to intercepting wired and wireless communications, recording conversations, capturing images, and using all necessary technical arrangements to uncover and prove the details of a crime without being bound by the usual rules of inspection and control. **(Mahdaoui, 2022, p. 1068)**

10. The impact of Information crime on social security:

10.1. Regarding individuals:

Information crimes impact the lives, well-being, and even the culture of civilians, targeting them through their media messages and the public specific to the societies they terrorize and intimidate. This is manifested through: **(Kaziz, Qat, 2018, p. 129)**

- Crimes where unauthorized access is gained to individuals' electronic identities, such as email accounts and passwords, reaching the point of identity theft and seizing important files and images from their devices, with the aim of threatening them to comply with the perpetrators' demands.

- Sabotage of the social relationship system and the moral fabric by interfering with family relationships due to the various consequences caused by certain types of cybercrimes, such as defamation of individuals, spreading false news, and rumors.

- Emergence of cases of kidnapping and assassinations even after ransom payments, in addition to the phenomenon of young people becoming addicted to electronic games, especially teenagers aged between 12 and 16.

10.2. For the economy:

It has become known that many companies have lost their reputation and declared bankruptcy due to crimes such as hacking their accounts, leaking information, and data of their clients and customers, as well as electronic embezzlement crimes that annually cause deficits in their budgets, especially for financial institutions such as banks, for example.

10.3. For the state:

Countries can be affected by cybercrime through the leakage of secret information related to their national security or economy, or the dissemination of data and secrets of state personalities and symbols, which may pose a threat to their security and stability. **(Jemawi, 2021, p. 138)**

10.4. For the economy:

It has become known that many companies have lost their reputation and declared bankruptcy due to crimes such as hacking their accounts, leaking information, and data of their clients and customers, as well as electronic embezzlement crimes that annually cause deficits in their budgets, especially for financial institutions such as banks, for example.

10.5. For the state:

Countries can be affected by cybercrime through the leakage of secret information related to their national security or economy, or the dissemination of data and secrets of state personalities and symbols, which may pose a threat to their security and stability**. (Jemawi, 2021, p. 138)**

II. Conclusion:

In conclusion, this study reveals that Information crime in the digital environment poses a new challenge confronting society in the era of digital technology. It demonstrates a close connection with social structures and interactions, influenced by technological culture and the social distribution of digital skills. Moreover, this study emphasizes the need to focus on multiple sociological aspects for a profound understanding of cybercrime in the digital environment. The social analysis should be balanced with technological advancements to comprehend the social factors influencing the nature and prevalence of these crimes.

To confront Information crime cybercrime in the digital environment, the need for comprehensive and effective solutions is crucial. Here are some proposed solutions:

1- Enhancing Digital Awareness and Education:

- Raise awareness about various types of cybercrimes and prevention methods.

- Provide training and education to individuals and institutions on best practices in digital security and protecting personal information.

2- Developing Effective Laws and Policies:

- Establish strong and appropriate laws and policies to combat cybercrime in the digital environment.

- Update legislation to encompass all categories of cybercrimes and define suitable penalties for perpetrators.

3- Promoting International Cooperation:

- Strengthen collaboration between countries and international organizations to combat cross-border cybercrime.

- Exchange information, experiences, and expertise to develop effective strategies for addressing cybercrime.

4- Improving Digital Security:

- Enhance digital security by developing and improving technology and security tools.

- Provide solutions for data and media encryption and enhance protection and threat detection systems.

5- Innovative Technologies:

-Utilize innovative technologies in the fight against cybercrime, such as artificial intelligence, data analysis, and advanced cyber security.

Referrals and references:

Books :

- Bin Saud Abdullah, The Effectiveness of the Methods Used in Proving the Crime of Electronic Forgery, Naif Arab University for Security Sciences, (Riyadh, 2011).

- Samia Hassan Al-Saati, Criminal Sociology, Dar Al-Fikr Al-Arabi, (Cairo, 2005).

- Philippe, rose, la criminalité informatique, collection que sais – je,(1988).

Theses :

- Barhoum El-Taher, Electronic Forgery Crimes, a memorandum submitted to obtain a master's degree in criminal law and criminal sciences, El-Arabi El-Tebsi University - Tebessa, 2018/2019.

- Brahmi Hanan, The crime of forging an official administrative document of an informative nature, a thesis submitted to obtain a doctorate degree in criminal law, Mohamed Kheidar Biskra University, 2014/2015.

- Fayez Mohamed, Information Crimes in Algerian and Yemeni Law, a dissertation for obtaining a PhD in Law, University of Algiers-1, Faculty of Law, 2009/2010.

- Sagheer Youssef, Crime Committed Through the Internet, a memo for obtaining a master's degree in law, Mouloud Mamari University, Tizi Ouzou, 2013/2014.

- Suri Yasmina, Information Crime and its Economic Effects - A Case Study of the Information Virus, Center for Research in Scientific and Technical Media (CERIST), Training Report for a Certificate of Applied University Studies D.E.U.A, University of Continuing Education, Algeria Center, 2004/2005.

Articles:

-Aliwa Salim, Information Crime, The Researcher Journal for Legal and Political Studies, Volume 6, Issue 1, 2021.

- Ben Ammar Yasmina and Bakhush Najib, Manifestations of Symbolic Violence in the Virtual Environment: A Semiological Approach to Images of Symbolic Violence on Algerian Facebook Pages, Journal of Humanization for Research and Studies, Volume 12, Issue 01, 2021.

- Khalili Siham, Privacy of the Cybercriminal, Al-Mufaker Magazine, University of Mohamed Kheidar Biskra, Issue 15, 2017.

- Khalaf Badr Al-Din, Legal Regulation of Information Crime in Algeria, Journal of Legal and Social Sciences, Volume Six, Number Two, 2021.

- Mahdawi Hanan, Legal Regulation of Cybercrime in Algerian Legislation, Journal of Legal and Political Thought, Volume 6, Issue 2, 2022.

- Maadawy Najia, The Electronic Contract in Confronting Information Crime, Al-Sada Journal for Legal and Political Studies, Issue 4, 2020.

- Maashi Samira, Information Crime (An Analytical Study of the Concept of Information Crime), The Thinker Magazine, Issue 17, 2018.

-Mohamed Al-Saeed Zanati, Information Crime in Light of Algerian Legislation and International Conventions, Elysee Journal for Research and Studies, Issue 2, 2017.

-Natija Gemawi, Cybercrime and its Impact on Social Security, Dafater Al Mokhbar Journal, Volume 16, Issue 2, 2021.

-Ramzi Houhou and Mounira Balourgi, Confronting Information Crime in Algeria, Journal of Rights and Freedoms, Issue 2, 2014.

-Sabah Kziz, Samir Qat, the impact of cybercrime on the security and stability of countries: hacking the website of the Qatar News Agency as a model, Al-Naqid Journal for Political Studies, Issue 3, 2018.

- Salami Saidani, The Development of International Legislation and Conventions in the Field of Information Crimes (Facts and Approaches), The Researcher Journal for Legal and Political Studies, Issue 10, Volume 1, 2018.

- Tala Lamia, From the Information Society to the Knowledge Society: Towards a Conceptual Approach, Journal of Social Sciences and Humanities, Volume 11, Issue 01, 2021.

-Tayyar Mona and Hamlawi Mohamed Nadir, Confronting Information Crime in Algerian Legislation, Research Journal, Volume 6, Issue 1, 2021.