

The Information Criminal and Its Criminal Motives

المجرم المعلوماتي ودوافعه الإجرامية



BENAHMED Mohamed ^{1*},

¹ University of Ibn Khaldoun Tiaret, Algeria

Mohamed.benahmed@univ-tiaret.dz

Date of transmission: 21/10/2025 date of acceptance: 23/11/2025 date of publication: 01/12/2025

Abstract:

It is said that cybercrime is the crime of the intelligent, unlike traditional crime, in which the offender often relies on physical strength and violence to carry out their criminal plans. From this perspective, studying the cybercriminal requires examining them from multiple angles, the most important of which are defining the jurisprudential and legal concepts of this type of criminal, analyzing the circumstances and reasons that led them to commit their crime, and addressing the main traits and characteristics that distinguish them from other criminals.

Keywords: Cybercriminal – Characteristics of criminals – Causes and motives of crime.

الملخص:

يُقال إن الجريمة المعلوماتية تُعد جريمة الأذكاء، بخلاف الجريمة التقليدية التي يعتمد فيها المجرم غالباً على القوة البدنية والعنف لتنفيذ مخططاته الإجرامية. ومن هذا المنطلق، فإن دراسة المجرم المعلوماتي تستوجب النظر إليه من زوايا متعددة، أهمها تحديد المفهومين الفقهي والقانوني لهذا النوع من المجرمين، مع تحليل الظروف والأسباب التي دفعته إلى ارتكاب جريمته، بالإضافة إلى التطرق إلى أبرز سماته وخصائصه التي تميزه عن غيره من المجرمين. الكلمات المفتاحية: المجرم المعلوماتي – سمات المجرمين – أسباب ودوافع الإجرام.

*** Corresponding Author**

Introduction

Cybercrimes are among the greatest challenges we face today. These emerging offenses raise numerous legal and practical issues, which some scholars refer to as the **substantive problems of criminal law** when confronting this type of criminality. This is because they are a new type of crimes that challenge the

traditional rules of criminalization and punishment which require the essential elements of a crime to be met for its existence.

Given that cybercrime is a modern phenomenon, easily finding its precise nature and specific characteristics is difficult, whether in the interpretations of **criminal jurisprudence**, the rulings of specialized courts, or even in relevant legal texts. This is due to its nature as a new criminal trend with a distinct legal character that sets it apart from other crimes. The concept of a crime, in general, requires a full understanding, and grasping the essence of any crime necessitates identifying its features, particularly within a globalized system.

Cybercrimes have produced **new classifications of offenders** who can be grouped into several distinct categories and patterns. Various studies and research in this field have revealed the existence of many types of cybercriminals. Naturally, this doesn't mean every offender falls under only one specific category; a single cybercriminal may exhibit a blend of multiple types making this classification more complex than some may believe.

Furthermore, it is legally established that the offender who commits cybercrimes is often referred to in much of the legal doctrine by the term "**cybercriminal**," which is distinct from the perpetrator of traditional crimes, known as the "**traditional criminal**." The cybercriminal is not like other traditional offenders; they possess features that distinguish them from others. Therefore, when dealing with cybercrime, we must examine the perpetrator from several angles, including the circumstances and reasons that drove them to commit their crime as well as identifying the specific types and characteristics of these offenders.

Due to the spread of the **digital information revolution** and the resulting increase in cybercrimes, both globally and nationally, criminological research in this area has received significant attention through numerous legal studies. These studies attempt to unveil the concept of the cybercriminal, focusing on the groups they belong to, their specific patterns, and, crucially, the factors that motivate them to commit these types of crimes.

On the light of the introductory context, the following questions are raised:

To what extent has **legal jurisprudence** been able to define the concept of the **information criminal**? What are their most important characteristics and classifications that distinguish them from other **traditional criminals**? And what are the most prominent motives and reasons for committing this type of crime?

To answer the above questions, we need to structure and study this research as follow:

First: The Nature of the Information Criminal and their Main Classifications

The nature of the information criminal and their main classifications are among the most essential components through which a deeper understanding of what is called the information criminal can be achieved, even if researchers and scholars in this field have adopted several classifications for them. This is what we will proceed to study in terms of both the concept of the information criminal and their most important classifications.

A. The Concept of the Information Criminal and their Most Important Characteristics

It means that we address the clarification of both the definition of the information criminal, and then we move on to studying the most important characteristics that distinguish this criminal, as follows.

1) Definition of the Information Criminal: Among the most important definitions addressed by specialists in determining the meaning of the information criminal, we mention, for example, the following:

- The information criminal is: **A person who commits illegal criminal activities** using electronic devices and digital communication means, including crimes of manipulating digital information to steal or damage data or cause material and moral harm to the victim¹.
- They were also defined as: **Every person who has the ability to transform their criminal thoughts into a digital language** using computers and the internet, by performing an act or refraining from performing one, which causes material or moral losses as a result of violating the applicable regulations and laws².
- They were also mentioned by some jurisprudence as: **The person who commits their crimes using Information and Communications Technology (ICT)** to target information systems and the data they contain³.

¹ Mohamed Ali El-Eryan: Information Crimes, New University House, Alexandria, Egypt, 2004, p. 70

² Khalili Siham: "The Specificity of the Electronic Criminal," Al-Fikr Journal, Biskra University, Issue 15, 2016, p. 405

³ Youssef Abu Al-Hajjaj: The Most Famous Computer and Internet Crimes, Arab Book House, Cairo, Egypt, 2010, p. 18.

- They were also mentioned as: **Every person who commits positive or negative criminal acts** using information technology to cause an assault on a right or interest protected by law¹.
- It was also defined as: **That person who commits an unlawful act and assaults another's right** in the broad sense by using **modern technical methods and techniques** involving **computing and informatics**².
- It was also defined as: **That person who combines professionalism in computer science with knowledge of the secrets of the Internet**, as they possess a high degree of **intelligence and extensive expertise** in specializations related to **information systems** in their technical and electronic fields all for the purpose of committing their crimes³.

2) Characteristics of the Information Criminal

To better understand information technology crimes, it is necessary to describe the characteristics and traits of their perpetrators. After outlining the most important definitions of the information criminal, particularly in terms of their control over the modern technology they utilize, we attempt now to clarify the main distinct characteristics and traits that differentiate the information criminal from the ordinary criminal.

2.1) The Information Criminal is Social by Nature

The information criminal being **social by nature** means they are **integrated with their society** and do not live in isolation from it. They often have a **respectable social standing** within their community and may even be respected.

Therefore, the perpetrator of information crimes differs from the traditional criminal in that they **live within society quite normally**. They pursue their usual work in the IT field or even in other fields; they are inherently a **social person**⁴. As a matter of practice, many information crimes are committed out of **fun**, or for **revenge**, or to **demonstrate superior capability** against the security of social systems⁵.

Consequently, the **information criminal's personality** is often content with **boasting** among their peers or simply seeking **personal gain** from their

¹ Mohamed Abdullah Abu Bakr: Computer and Internet Crimes, Modern Arab Office, Alexandria, Egypt, 2007, p. 53.

² Mohamed Mohamed Sheta: The Idea of Criminal Protection for Computer Programs, New University House, Alexandria, Egypt, 2001, p. 66.

³ Mostafa Mohamed Moussa: Criminal Methods with Digital Technology, A Comparative Study, Legal Books House, Cairo, Egypt, 2005, p. 18.

⁴ Ahmed Abdullah Al-Maraghi: Electronic Crime and the Role of Criminal Law in Limiting It, A Comparative Study, National Center for Legal Publications, Cairo, Egypt, 2017, p. 40.

⁵ Mohamed Ali El-Eryan: Previous Reference, p. 77.

crimes. The **hacker**, for example, doesn't place themselves in a state of hostility toward the society they live in; rather, they are **integrated** with it.

Furthermore, some studies conducted on these individuals indicate that the results confirm that **information system hackers are educated individuals** who are **more willing to help** than they are enemies who enjoy causing harm. This is what helps them in the process of **social adaptation**. Additionally, perpetrators of this type of **automated data processing crime** are often **individuals with status in society**. They are frequently people in **vital positions** at their workplaces whether in the **private sector** environment such as companies, institutions, economic establishments, and private financial banks, or in the **public sector** and its government agencies and bodies. The typical example for that is the **employee who is terminated from their job** and resorts to **revenge** against those who caused it¹.

2.2) The Information Criminal is Characterized by Intelligence, Knowledge, and Skill

The information criminal is not ordinary person; they are first and foremost characterized by **intelligence**. This means they possess a high level of **quick comprehension, rich knowledge, strong observation skills, and advanced mental activity**². For this reason, information crime is often called "**Crimes of the Intelligent**" (Criminels intelligents) or "**Intelligence Crimes**" (Crimes intelligence), especially when compared to **traditional crime**, which often lacks the use of such intelligence³.

The information criminal also stands out for their ability to **handle all systems and networks** as well as their capacity to deal with **all developments in computing and its software**. They are a person who possesses the **skills** necessary to **modify and develop information security systems** so that their criminal acts cannot be traced or followed. This intelligence is the key to information crime, enabling them to **discover the secrets of vulnerabilities for breaching protected programs and websites**. Numerous studies and statistics have proven that those involved in such crimes have a **high degree of intelligence and superiority** that allows them to carry out their crimes with **extreme precision**, out of fear of being exposed or caught during their risk-

¹ Khaled Hassan Ahmed Lotfy: Internet Crimes Between Electronic Piracy and Electronic Extortion Crimes, A Comparative Study, University Thought House, Alexandria, Egypt, 2019, p. 23.

² Yazid Bouhalit: Electronic Crimes in Algerian Law, New University House, Alexandria, Egypt, 2019, p. 87.

³ Mohamed Ali El-Eryan: Previous Reference, p. 63.

taking and adventuring. This is often accompanied by an **overconfidence** and a feeling that they can commit their crimes **without being discovered**¹.

2.3) The Information Criminal is a Professional and a Specialist

The characteristic of **professionalism and specialization** in the inner workings of computers and related systems is also one of the most important traits distinguishing information criminals. They can have a **complete visualization of their crimes** even before carrying them out and executing them. This is also due to the nature of the **scene** where the information crime occurs—the **computer system and its electronic environment**. The offender can easily and professionally apply their crime to **similar systems** during execution.

The common thread among professional information criminals is their **high degree of familiarity with modern technology**, their acquisition of **practical knowledge**, and their belonging to **specializations related to computers**, particularly from a functional perspective. These traits are quite similar to the characteristics of **white-collar criminals**². Criminals of this category belong to the class of the **educated and cultured** and those who have a **specialized ability to deal with computer devices**³.

The information criminal has a **superior ability in technical skills** which they exploit to breach the defensive fortifications set up by programming companies. They may acquire these skills through specialized study in the field or through **experience gained** in modern technologies. However, it's not a fixed rule that the information criminal must possess a high degree of professional and specialized knowledge. Judicial practical reality has proven that a considerable number of information criminals have not received the necessary academic study but rather use their **intuition and skills** to commit this type of crime⁴.

2.4) The Information Criminal is a Natural Person

The criminal in an information crime may be a **natural person** working on their own account, usually aiming to achieve **personal gain**. However, a natural person can also commit this act on behalf of a **legal entity** such as companies or institutions that work in the field of informatics or rely on information

¹ Ghania Batli: Electronic Crime, A Comparative Study, Algerian Publishing and Distribution House, Algeria, 2016, p. 35.

² Khaled Hassan Ahmed Lotfy: Previous Reference, p. 22.

³ Khaled Mamdouh Ibrahim: Information Crimes, University Thought House, Alexandria, Egypt, 1st ed., 2009, p. 98.

⁴ Mohamed Ali Swailem: Explanation of the Egyptian Information Technology Crimes Law, University Publications House, Alexandria, Egypt, 2019, p. 116.

technology for their work. This is done with the aim of **breaking into an information system** or **causing damage to others**. Statistics show that the legal entities that commit these crimes do not always try to harm individuals but rather to **affect institutions and companies** because they can absorb the damages and burdens due to their financial reserves¹.

2.5) The Information Criminal is a Person Who Does Not Use Violence

The information criminal is among those who **do not resort to using violence** at all in committing their crimes. This is because they belong to the category of "**Crime of Subterfuge, Deception, or Fraud**" (Délit de fraude). They do not use violence to execute their crimes because this type of offense **does not require any effort or strain** to carry out. Information crimes are "**soft crimes**" by nature and do not require violence or resistance².

Another reason is that the information criminal enjoys a certain degree of **authority**. Authority here refers to the **rights and privileges** that qualify and enable the criminal to complete their crime in the best possible way. Many information criminals have either **direct or indirect authority** over the information subject to the crime, in addition to their **complete familiarity with the crime scene and its tools**, which spares them sudden situations that could lead to the failure of their plan and their exposure.

This is also due to the **simplicity of the means used**. This refers to the capabilities the information criminal may need to complete their crime. These means are often **simple and easy to obtain**, especially if the computer system they are working with is a well-known and common one in the market. However, if the system is an unfamiliar one, these means become complex and highly difficult, requiring some **intellectual effort**.

2.6) The Information Criminal is a Recidivist

The information criminal is also characterized as a person who **always returns to crime** whenever the opportunity arises, either with the aim of **pleasure in harming others** or as a result of their feeling of **capability and skill in penetration**³. This is done by **unauthorized access to network systems** repeatedly. They may not achieve their goal in the first crime, so they strive to achieve it in subsequent crimes.

The recidivism of information criminals is also due to a **desire to close previous loopholes and errors** that led to their identification and prosecution.

¹ Mohamed Mohamed Sheta: Previous Reference, p. 99.

² Nahla Abdel Qader Al-Momani: Information Crimes, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st ed., 2008, p. 58.

³ Mohamed Ali Swailem: Previous Reference, p. 118.

This is a strong reason that leads many of them to **return (recidivate) to crime**, and they may end up being brought to trial again on the second offense¹.

B. Classifications of the Information Criminal

Numerous academic and scientific studies and research have confirmed that the classification of information criminals or offenders falls into **different categories and groups** which can be divided into two main sections: **Amateur and Novice Criminals**, and another section called **Specialized and Professional Criminals**.

1) Amateur and Novice Criminals

The pattern of amateur and novice criminals is considered **less dangerous** compared to other criminals who commit technical crimes professionally. This is due to their **lack of experience** in the field of informatics, as well as the **frequent absence of criminal intent** when they commit some forms of these crimes. This is because this type of "**Informatics Enthusiasts**" (Passionnés d'informatique) **lack sufficient experience** in using computer technologies, which sometimes leads them to make many **errors** that may result in them committing information crimes.

This class of **Amateur and Novice Criminals** includes a significant number of sub-groups mentioned in many legal research papers and studies. Among the most important are:

1.1) The Pranksters / Fraudsters (Pranksters_ Fraudeurs)

These are individuals who possess a **reasonable degree of technical capability** in the world of computers and are usually people with **cognitive competence**. They proceed to commit certain criminal acts by **fraudulently or deceitfully accessing information systems** for the purpose of **amusement and jest**. This often stems from a feeling of **boredom** with their families and peers, and they **do not intend to cause any harm** to the victims². They commit their criminal acts against others through **deception** without the specific intent to cause harm.

This category includes the **Petits cyber criminels (Small Cybercriminals)**, who are a group of gifted minors, or "**Génie de l'informatique (Informatics Geniuses)**," who are passionate about the information revolution and computer technology, own them at an early age, and have a **tendency and curiosity** to

¹ Mohamed Ali Swailem: Same Reference, p. 117. [6] Mahmoud Ragab Fathallah: Previous Reference, p. 244.

² Mahmoud Ragab Fathallah: Previous Reference, p. 248.

understand the uses and programs of this technology, often staying in front of their computers late into the night¹.

They may also be part of the **adult youth category** who have been fascinated by the information revolution and possess a reasonable amount of **computer expertise**. They are referred to as "**Informatique jeunesse (Informatics Youth)**." Consequently, they practice their talents using technology from their mobile phones, such as YouTube, tablets, mobiles, and other devices, for the purpose of **amusement or as a hobby of playing** to gain access to information systems without knowing which entity the system belongs to. These young people may commit certain criminal acts through the **reckless use** of their personal computers. For this group of young people, the matter may develop into learning **automated programming operations** and discovering entry points. Nevertheless, their goal is usually just **amusement and observation**, and they lack the underlying criminal intent to commit acts classified as information crimes. Furthermore, their actions have **no geographical boundaries** and may reach systems and centers far from their locations².

1.2) The Intruders or Malicious Hackers (Malicious Harckers)

They are also called "**Etrangers (Strangers)**," meaning "**Des inconnus en informatique (Unknowns in Informatics)**." These are **intruders or foreigners** to those information systems with **no connection** to them. This category includes users of a system or website who **do not have prior authorization** to access and work on that system, which may belong to an institution, a company, or an individual. Many **virus creators and users** fall under this designation³.

Intruders are **intelligent and creative individuals** whose work is the **unauthorized entry into information systems** for the purpose of **pleasure, mischief, or crime**⁴. In most cases, **vandalism/sabotage** is the goal of these intruders and hackers, meaning they access a foreign system to commit **unlawful acts**⁵. Undoubtedly, this process of entry by these strangers has a **severely damaging impact** that may cost the system owner huge sums to repair the security systems that were corrupted by the sabotage operations. The motive

¹ Ghania Batli: Previous Reference, p. 37.

² Mohamed Sami Al-Shawa: The Information Revolution and its Repercussions on Penal Law, The Egyptian General Book Organization, Cairo, Egypt, 2003, p. 53.

³ Mostafa Mohamed Moussa: Previous Reference, p. 26.

⁴ Mohamed Sami Al-Shawa: The Information Revolution, Previous Reference, p. 45.

⁵ Bilal Amin Zein El-Din: Crimes of Automated Data Processing Systems in Comparative Legislation and Islamic Law, University Thought House, Alexandria, Egypt, 2008, p. 41.

behind the entry of these strangers into information systems may also be for **amusement and jest** with others or for **reconnaissance as merely a hobby**, to defeat and overcome the system to demonstrate intelligence, and without the intent to cause losses or harm to the victims¹.

1.3) The Hackers (Hackers)

The class of **Hackers** is quite similar to the category of **Informatics Geniuses** but surpasses it in terms of **knowledge, expertise, and extensive familiarity** with programming operations, penetration, observation, and intrusion into systems².

Hackers are **intruders** whose goal is to **assault the security protection measures** of information systems and networks. They usually do **not** have sharp criminal or destructive motives; rather, they are driven by a motive of **challenge and self-affirmation**. Their aim in illegally accessing systems is to **break the security barriers** placed for that purpose, seeking to **learn and gain experience**, or out of **curiosity**, or simply to **confirm their ability to penetrate and overcome** these barriers. Occasionally, the motive is **illegal financial gain** or to cause **disruption and losses to others**. These hackers often **return to penetrate the same information systems** after they have been repaired or had their technical protection systems developed by the owners, which **renews their spirit of challenge** to penetrate again³.

2) Professional Criminals (Criminels professionnels)

Professional Criminals are individuals who hold **high degrees** in computer and informatics specializations and work as **system analysts and programmers**⁴. They possess **extensive knowledge** of operating systems and **deep familiarity** with the secrets and security vulnerabilities within information systems. Among the professional criminals in the field of information crime, we find, for example:

2.1) The Crackers (Crackers)

The term "**Crackers**"⁵ is usually applied to **professional information criminals**. A cracker is any **specialized or expert person** in the field of computers and informatics who carries out **illegal activities** consisting of attacks

¹ Deyab Al-Badayneh: Security and Information Warfare, Dar Al-Shurooq, Amman, Jordan, 2002, p. 133.

² Khalifa Ahmed Al-Malt: Information Crimes, University Thought House, Alexandria, Egypt, 2nd ed., 2006, p. 117.

³ Mostafa Mohamed Moussa: Previous Reference, p. 26.

⁴ Bilal Amin Zein El-Din: Previous Reference, p. 43.

⁵ Mahmoud Abdullah Hussein Ali: Theft of Information Stored in the Computer, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2002, p. 54.

that reflect the **extent of their danger and criminal tendencies**. These tendencies are based on their desire to **cause harm to others and destroy information systems**¹, not to mention other objectives that primarily aim for **financial gain** for themselves or to satisfy the desires of the party that commissioned them to commit modern technology crimes. Some of their attacks also aim to achieve **political goals** or express an **intellectual or religious stance**².

Individuals in this category are often classified into multiple **sub-patterns and groups**, either according to their **specialization** in a specific type of crime or according to the **means** they use to commit the crimes. For example, we find the pattern of professionals in **espionage** of all kinds: economic, political, security, military, and industrial. We also find the pattern of **information fraud and forgery criminals**, whose aims are directed towards achieving **profitable financial gain** by **seizing the money of others** through the theft of funds from electronic bank accounts.

A cracker is a person who has a **strong passion for learning programming and operating systems**. They use existing software but **develop it with their own knowledge** as necessity dictates, and they may be able to **break its programming code** to copy and distribute it for free. This class has emerged strongly in recent years. Its spread has been contributed to by two main factors: the **proliferation of computers and software**, their abundance, and the ease of dealing with them, and the **high prices of original software and applications** for computers sold by companies. This has motivated these individuals to find other ways to copy these original programs and resell them at **prices much lower** than their set values. The most dangerous cracker is the **novice** because they like to **try out attack programs without understanding their applications**, using them randomly, which sometimes leads to **extensive destruction without realizing what they are doing**.

2.2) The Personal Problem Solvers

This is the **most common and widespread** class among the rest of the information criminals. They commit their crimes, which in most cases result in **great losses** inflicted upon the victims. The **motive** behind these crimes is to **find solutions to their material problems** that the offender cannot solve through ordinary and traditional means³. They aim to achieve **illegal material**

¹ Khaled Ayad Al-Halabi: Investigation Procedures in Computer and Internet Crimes, Dar Al-Thaqafa, Amman, Jordan, 2011, p. 33.

² Mostafa Mohamed Moussa: Previous Reference, p. 31.

³ Mahmoud Ragab Fathallah: Previous Reference, p. 248.

profit through their criminal activity, although there is a **similarity in this trait** between the traditional criminal and the information criminal of this class.

On the other hand, some academic studies and research have confirmed that the **Personal Problem Solvers** class does not always seek financial or other profitable gains. Instead, they commit their criminal activities driven by a desire for **revenge, retaliation, and resentment**. They are the **Spiteful-malveillant** individuals. For this reason, they are divided into **employees of the system** who have some relationship with the system under attack, or **strangers to the system** who have the same reasons for revenge against the targeted person in their activities. The closest example of this is when a young man, motivated by revenge against his girlfriend who left him, went to her personal website on the Internet—which was open to a large number of her friends—and, without her knowledge, posted some of her **pornographic images** accompanied by **vicious verbal comments** about her morals and behavior.

2.3) The Vandalizers (Vandales)

This category includes the **Information System Thieves** (Les voleurs de système d'information), who use all methods and means to **illegally access information systems**. They are also referred to as "**Fanatics of Informatics**" (Fanatiques de l'informatique). They are not extremists to the point of international terrorism, but their goal is the **sabotage of the information system**, which is their way of satisfying their desires¹. This is in contrast to **Hackers and Crackers**, who typically perform their actions for less serious purposes.

The purpose behind this sabotage may be to wage **war** via modern information technology media, carried out by an individual, a state, or a terrorist group against a hostile state. Through this, they seek to **destroy informational service websites** that provide electronic services to citizens under what is known as the "**Failure of E-governments**" (E-gouvernement)². This group is characterized by its **danger** as it tends towards acts of **piracy and information terrorism** using means of great **ingenuity** in their creation and design, such as **planting viral programs, resorting to electronic force, and information burglary**, all to achieve their criminal aims.

This is not to mention the **extremists** who advocate for a specific cause or goal unrelated to their direct personal interests. The reason may be **political, ideological, or religious**. Thus, they do not have specific criminal intentions but

¹ Ghania Batli: Previous Reference, p. 41.

² Mostafa Mohamed Moussa: Previous Reference, p. 36.

rather **employ the knowledge** they acquired in the field of informatics to **promote agendas** that serve their orientation. This is what leads them to **penetrate individual or collective websites** to **change the information** they contain and thereby draw attention to their ideas and beliefs¹.

Second: Reasons and Motives for Information Crime

The reasons leading to the commission of this type of crime differ from those known in traditional crime, even though they share some commonalities. The **incentives and motives** that push the information criminal to commit this type of crime may differ from the incentives and motives for committing crimes by the traditional criminal. The reason for this is that the difference between criminal behaviors in the **physical and real world** differs in turn from those that occur in the **virtual world**, which is fundamentally based on the **specificity of the computer and digital network environment**.

It is established that there are a considerable number of **reasons and motives** that may be behind the commission of information crimes, whether they occur at the **personal level of the individual** or at the **societal level**.

A. Personal (Individual) Reasons and Motives

There are multiple **individual and personal motives and reasons** that drive an individual to practice this criminal behavior, whether motivated by **malice or revenge**. However, the common feature among these criminals when committing an information crime lies in one common trait: the mere **hobby and amusement** at the beginning, a result of their fascination with the technological and information revolution and the accompanying development in computer systems².

1) Seeking Learning, Excitement, Pleasure, and Challenge

Many studies have proven that **information system hackers** have a keen interest in computers and a **passion for learning how they work**. It has even been said that entering computer systems and networks can teach you **how the world works**. Based on this, computers and the information systems they contain are nothing more than a **space for learning and research**, and the act of a person **discovering new methods** to enhance their self-information and utilize it to gain knowledge is highly **exciting**.

In addition, some information crimes are committed by **reckless youth and minors** out of **pleasure, challenge, or perhaps a desire for media attention**. This group often ceases such behaviors at a later age, especially after their

¹ Mostafa Mohamed Moussa: Same Reference, p. 29.

² Mohamed Ali El-Eryan: Information Crimes, Previous Reference, p. 81.

twenties when they gain a **sense of responsibility**¹. Despite the inclination of the perpetrators of these acts to demonstrate their superiority, high level, and creativity, some jurists have called for **not holding the perpetrators of these crimes accountable**, especially if the motive is the **search for learning, excitement, pleasure, and challenge**. This is because their actions are intended to show their superiority without malicious intent, driven instead by their fascination with modern technology. Therefore, these individuals are **not highly dangerous** in a criminal sense; rather, they generally prefer to achieve **technical victories** without having any malicious intentions, and their actions are not considered to involve **sinful intent**.

2) Psychological Motives and Personal Influences

Psychological motives and personal influences are numerous. Among these motives, we find those associated with people who suffer from **computer addiction** (La dépendance à l'ordinateur). A specialized psychiatrist mentioned that a patient came to him complaining that his family was in danger. It was later revealed that the root of his problem lay in the nature of his work as a computer programmer in an institution, where it became clear that he was spending most of his time with the computer, neglecting his family². Dr. **Perky Black**, a professor of psychology at New York University, states that all information system hackers are possessed by a **feeling and sense of power** toward modern technology, which often leads them to commit crimes³.

Furthermore, individuals are sometimes affected by some **external influences** surrounding them. Due to their passion and addiction to the automated data processing environment and its systems, and with the availability of these external influences, the matter inevitably culminates in their **commission of information crime**. This is a result of a **psychological affliction** that affects some of these individuals, leading them to resort to **unlawful acts** against information systems, such as destroying software with **viruses or logic bombs** by planting them, which causes severe harm to the victims⁴.

3) Motive of Malice and Revenge

The reasons that may drive the criminal to commit such behavior can also be **malice or revenge**. This malice may be directed at a **person, several people, an institution, or a specific professional position**, or it may be **financial malice**

¹ Mahmoud Ragab Fathallah: Previous Reference, p. 252.

² Ahmed Abdullah Al-Maraghi: Electronic Crime, Previous Reference, p. 41.

³ Hossam Shawky: Information Protection and Security on the Internet, Dar Al-Kutub Al-Ilmiyya, Cairo, Egypt, 2003, p. 58.

⁴ Mohamed Ali El-Eryan: Information Crimes, Previous Reference, p. 83.

due to their inability to fully meet their financial obligations, leading them to resort to unlawful acts against information systems. The motive behind committing the information crime may also be **revenge against the institution** to which the criminal belongs, especially when they are **fired from their job**, which can create the appropriate environment and a strong motive for committing their crime¹.

Malice, hatred, and revenge drove a young **electronic accountant** to **manipulate the information system programs** of the company he worked for before he was fired. He designed a program that would penetrate the company's system devices to **erase all data** related to its clients six months after his departure. What he intended happened after this period ended².

Another example is when a person working at a large shipping company, upon learning that he had been **removed from his managerial position**, sent a **virus** before leaving that was designed to **erase the contents of all management and service files**. The company consequently incurred devastating and unexpected losses.

4) Motive of Earning Money and Achieving Profits

Sometimes, the motive behind **penetrating and hacking websites and information systems** is to **obtain financial profit** by **extorting** for the programs or information obtained by **embezzlement** from the computer, or by using a **forged or expired ATM card**. In this regard, an association concerned with **Information Security** (Sécurité informatique) indicated that the perpetrators of most information crimes have a desire to **achieve wealth and earn financial profits**, and this is one of the basic factors for committing this type of crime, such as **embezzling funds, stealing information and extorting its owners**, and other information crimes directed against money³.

Need may also drive some individuals to seek **rapid enrichment** by providing access to **specific, highly important information** for those who request it⁴. Some **commercial and industrial companies** may seek to obtain software and information by **stealing them** through the people responsible for the computer systems, often by **bribing, tempting with money, or exploiting** this employee⁵. An example of this is an employee who worked as a computer

¹ Mohamed Ali El-Eryan: Information Crimes, Same Reference, p. 84.

² Mohamed Amin Al-Roumi: Computer and Internet Crimes, University Publications House, Alexandria, Egypt, 2004, p. 25.

³ Mohamed Amin Al-Roumi: Same Reference, p. 29.

⁴ Mohamed Ali El-Eryan: Information Crimes, Previous Reference, p. 82.

⁵ Ghania Batli: Electronic Crime, Previous Reference, p. 31.

programmer for a German commercial company. He stole **twenty-two magnetic tapes** containing vital information related to **clients and the company's production secrets**. The thief threatened to sell them to competing companies unless they paid him a ransom of **\$200,000 USD**. The company analyzed the situation and assessed that the losses resulting from the sale of this information would far exceed the demanded amount, so the company chose to **pay the amount to recover the stolen magnetic tapes**¹.

B. Social (Societal) Reasons and Motives

There are also incentives and motives behind the commission of information crimes that appear at the **societal level**—those whose main cause is **society**, potentially triggered by certain **social conditions**. Among these, we find:

1) Urbanization and Globalization

Urbanization (Urbanisation) is considered one of the main causes of information crime in general, due to the inherent difference between the inhabitants of **urban areas and large cities** and the residents of **rural and village areas**. Despite the many positives of this urban aspect for these residents, it also comes with some negatives. A major negative is the **inability to meet the demands of urban life**. As a result, some people find themselves in competition and **unable to keep up**, which leads them to delve into the secrets of **modern technologies and techniques** and invest in them, as these may not require a large capital outlay for them².

The relationship between urbanization and information crime can also be explained through **changes in people's routine daily activities** and their exposure to certain **Western cultures**. With the advent of the **Internet** and its numerous and diverse **social media tools**, people's ways of communicating and interacting with others have changed, especially in their personal, family, recreational, and commercial relationships, among others. All of this has created **opportunities for offenders to pirate valuable and easy targets** in cyberspace and the information sphere, often with a **lack of surveillance and security protection**.

2) Deprivation, Poverty, and Unemployment

The general pressures faced by society from **deprivation and poverty** (Privation et pauvreté) and **difficult economic circumstances** are among the most significant factors pressing on society in general, and especially on the **youth category**. This can generate **negative and resentful feelings** toward

¹ Mohamed Sami Al-Shawa: The Information Revolution, Previous Reference, p. 50.

² Mahmoud Ragab Fathallah: Previous Reference, p. 257.

certain segments of the population, pushing them to resort to **unlawful acts** to cope with these circumstances, including **electronic human trafficking, sex trade, pornography, and other information crimes**¹.

Information crimes, like all traditional crimes, may also be linked to the **specter of unemployment** (Le chômage), which is spreading widely among different age groups of youth. Thus, many young people who possess **computer knowledge** invest it in certain **information crime activities**².

3) Weakness of Law and its Application in Information Crime

Many countries have **not developed their criminal legislation** to keep pace with the technical progress in the field of **information crime** and the electronic methods used to commit it. This is not limited to legislative texts but also includes the **justice apparatus**, such as the judicial police and judicial bodies, and **how they deal with information crime and digital evidence**, although this varies from one law and country to another³.

Consequently, the **weakness in law enforcement and its applications** in information crimes can negatively affect judicial and police practices in **monitoring, tracking, and prosecuting** such crimes and their perpetrators, whether domestically or those that **cross national borders**⁴.

Conclusion

All the aforementioned reasons, and many others, that drive the commission of such unlawful acts—whether motivated by **money, revenge, a love of adventure, amusement, or curiosity**—mean that this modern criminal phenomenon is now genuinely **threatening the integrity of the electronic environment**. Therefore, strong action must be taken to confront it, curb its spread, and eliminate it.

It is worth noting that the causes of information crimes vary according to their types, the nature of the right being targeted, the offender's profile, the level of execution, and the nature of the motive behind them, whether individual or societal. The causes for crimes committed by **amateur youth** differ from those of **professional criminals**. They also vary based on their goal, whether it is merely the **theft of information** or the desire to **illegally profit from trading it**.

¹ Mahmoud Ragab Fathallah: Previous Reference, p. 258.

² Ali Adnan Al-Fail: Criminal Responsibility for Misuse of Electronic Credit Card, 1st ed., Modern Establishment for Books, Lebanon, 2011, p. 22.

³ Mahmoud Ragab Fathallah: Same Reference, p. 260.

⁴ Ibrahim Bin Awad Al-Otaibi: "Use of Technology in Security Investigations," Technology and Security Journal, King Khalid College, Saudi Arabia, Issue 80, 2005, p. 10.

Nevertheless, **financial gain** remains the primary incentive behind the commission of most information crimes.

References:

1. Ahmed Abdullah Al-Maraghi. *Electronic Crime and the Role of Criminal Law in Limiting It: A Comparative Study*. National Center for Legal Publications, Cairo, Egypt, 2017.
2. Ali Adnan Al-Fail. *Criminal Responsibility for Misuse of Electronic Credit Card*. 1st ed., Modern Establishment for Books, Lebanon, 2011.
3. Bilal Amin Zein El-Din. *Crimes of Automated Data Processing Systems in Comparative Legislation and Islamic Law*. University Thought House, Alexandria, Egypt, 2008.
4. Deyab Al-Badayneh. *Security and Information Warfare*. Dar Al-Shurooq, Amman, Jordan, 2002.
5. Ghania Batli. *Electronic Crime: A Comparative Study*. Algerian Publishing and Distribution House, Algeria, 2016.
6. Hossam Shawky. *Information Protection and Security on the Internet*. Dar Al-Kutub Al-Ilmiyya, Cairo, Egypt, 2003.
7. Ibrahim Bin Awad Al-Otaibi. "Use of Technology in Security Investigations." *Technology and Security Journal*, King Khalid College, Saudi Arabia, Issue 80, 2005.
8. Khaled Ayad Al-Halabi. *Investigation Procedures in Computer and Internet Crimes*. Dar Al-Thaqafa, Amman, Jordan, 2011.
9. Khaled Hassan Ahmed Lotfy. *Internet Crimes Between Electronic Piracy and Electronic Extortion Crimes: A Comparative Study*. University Thought House, Alexandria, Egypt, 2019.
10. Khaled Mamdouh Ibrahim. *Information Crimes*. University Thought House, Alexandria, Egypt, 1st ed., 2009.
11. Khalifa Ahmed Al-Malt. *Information Crimes*. University Thought House, Alexandria, Egypt, 2nd ed., 2006.
12. Khalili Siham. "The Specificity of the Electronic Criminal." *Al-Fikr Journal*, Biskra University, Issue 15, 2016.
13. Mahmoud Abdullah Hussein Ali. *Theft of Information Stored in the Computer*. Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2002.
14. Mohamed Abdullah Abu Bakr. *Computer and Internet Crimes*. Modern Arab Office, Alexandria, Egypt, 2007.

15. Mohamed Ali El-Eryan. *Information Crimes*. New University House, Alexandria, Egypt, 2004.
16. Mohamed Ali Swailem. *Explanation of the Egyptian Information Technology Crimes Law*. University Publications House, Alexandria, Egypt, 2019.
17. Mohamed Amin Al-Roumi. *Computer and Internet Crimes*. University Publications House, Alexandria, Egypt, 2004.
18. Mohamed Mohamed Sheta. *The Idea of Criminal Protection for Computer Programs*. New University House, Alexandria, Egypt, 2001.
19. Mohamed Sami Al-Shawa. *The Information Revolution and its Repercussions on Penal Law*. The Egyptian General Book Organization, Cairo, Egypt, 2003.
20. Mostafa Mohamed Moussa. *Criminal Methods with Digital Technology: A Comparative Study*. Legal Books House, Cairo, Egypt, 2005.
21. Nahla Abdel Qader Al-Momani. *Information Crimes*. Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st ed., 2008.
22. Youssef Abu Al-Hajjaj. *The Most Famous Computer and Internet Crimes*. Arab Book House, Cairo, Egypt, 2010.
23. Yazid Bouhalit. *Electronic Crimes in Algerian Law*. New University House, Alexandria, Egypt, 2019.