ITJ | The International Tax Journal

Proving Cybercrime in Light of the General Rules of Criminal Evidence

Abdelkader Amimer [1]

[1] Faculty of Law, University of Algiers 1, Algeria
Email: aek.amimer@hotmail.com

Abstract---This study highlights the issues surrounding the proof of cybercrime and the debate among criminal law scholars regarding whether general rules of evidence are sufficient to accommodate this type of crime despite its unique characteristics. It also discusses the need to establish specific rules that align with the peculiarities and nature of cybercrime.

Keywords---general principles of evidence, elements of crime, common provisions.

Introduction

Most scholars of classical criminal law believe that general procedural rules, including those relating to criminal evidence, are applicable to all crimes, regardless of their nature. Therefore, these rules can be applied to any crime, eliminating the need to develop special procedures whenever a new type of crime arises due to technological advancement. Conversely, another group of scholars argues that the unique characteristics of certain emerging crimes, including cybercrime, necessitate reconsidering and modifying these principles. Amidst this divergence of opinion, as researchers in criminal law and emerging crimes, we must question whether the general rules of evidence are sufficient to encompass this type of crime despite its unique characteristics.

To research this issue, we must first understand the general rules of criminal evidence and how they are applied to cybercrime. We will then examine the general elements of crime and how they are applied to cybercrime, before discussing the common provisions of crime and how they are applied to cybercrime.

Section One: Application of General Principles of Criminal Evidence to Cybercrime

Criminal evidence is based on general rules which some scholars view as boundaries that must be respected in order to protect individual rights and ensure justice. These rules control the subject of the

How to Cite:
Amimer, A. (2025). Proving cybercrime in light of the general rules of criminal evidence. *The International Tax Journal*, *52*(5), 2249–2256. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/235

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370
Submitted: 13 February 2025| Revised: 16 June 2025| Accepted: 25 August 2025

dispute and organise the judge's work during the investigation or adjudication phase. These principles manifest in three fundamental rules: the principle of 'freedom of evidence', the principle of 'presumption of innocence', and the principle of placing the burden of proof on the prosecution, which is referred to in criminal law literature as the 'burden of proof'.

Subsection One: Application of the Presumption of Innocence in Cybercrime

A person is presumed innocent until proven guilty, and this presumption can only be overturned by contrary evidence. This presumption remains in favour of the accused until definitive and conclusive proof of guilt is established by a final judgement. This means that their legal status prior to conviction must be that of an innocent person.

However, the emergence of the social defence school and its demands to mitigate this principle in favour of the higher interests of society have led some contemporary scholars to advocate this adjustment concerning emerging crimes, especially those linked to technological advancements. The aim is to facilitate the gathering of evidence, as the technological era has provided criminals with numerous opportunities to evade punishment, placing an additional burden on criminal justice systems that lack the resources and capabilities to keep pace with the evolving nature of crime. This hinders their ability to fulfil their commitment to serve and protect society. Therefore, this perspective argues that, in light of existing legal safeguards and the serious consequences stemming from such crimes, including cybercrime, mitigating the presumption of innocence does not violate the principle of procedural legality.

Subsection Two: Application of the Principle of Freedom of Evidence to Cybercrime.

The principle of freedom of criminal evidence enables all parties in a criminal case to present evidence that proves or disproves the occurrence of the crime, without restriction or limitation. In line with this principle, comparative legislation, including that of Algeria, does not restrict reliance on any specific type of evidence in its rulings.

However, given the growing role of modern scientific methods in criminal investigations, it has become essential to utilise these methods to prove certain emerging crimes, including cybercrime. In many cases, judges rely on digital evidence to prove these crimes, reflecting the nature of how cybercrime is committed.

This makes it difficult for ordinary individuals to obtain digital evidence without resorting to entities that monopolise information services, as they face technical and material barriers that are limited to official bodies authorised to conduct investigations. Some believe that evidence in this type of crime is becoming increasingly restricted, resulting in a contraction of the scope of the principle of freedom of evidence. Digital evidence is not accessible to everyone, and even law enforcement agencies must comply with conditions and formalities regarding access to such data in order to protect personal privacy.

Subsection Three: Application of the Principle of Burden of Proof to the Prosecution in Cybercrime

A general principle of evidence is that the public prosecution bears the burden of proof, in accordance with the civil rule that states that the burden of proof lies with the claimant and that a person is presumed innocent until proven guilty. Based on this principle, the prosecution must prove all elements of the crime, both material and moral. This was affirmed by the Algerian Supreme Court in one of its decisions, which stated: 'The principle is that the accused is presumed innocent until proven guilty, and the burden of proof lies with the public prosecution, which initiates and conducts the public action.' As the authority representing the accusation, the prosecution must provide evidence that the accused committed the criminal act. Sometimes, the victim, who can claim civil rights, assists the prosecution in this regard. The accused has the right to deny the alleged crime and is not legally required to provide evidence to support their denial or justify the crime; it is the prosecution's responsibility to present this evidence.

However, regarding cybercrime, this type of crime has created a new situation, leading some scholars to argue that the burden of proof should shift from the prosecution to the accused. This is due to the unique characteristics of cybercrime, especially its transnational nature, which enables perpetrators to scatter evidence across multiple countries and complicate efforts to apprehend and prosecute them.

Section Two: Application of the General Elements of Crime to Cybercrime

Like other traditional crimes, cybercrime consists of three essential elements: the legal, material and moral elements, as well as a specific element known as the presumed element. However, cybercrime has certain peculiarities that distinguish its elements from those of traditional crimes, which we will discuss below.

Subsection One: The Legal Element of Cybercrime

The legal element of any crime refers to the existence of a legal text that criminalises the act and specifies the ensuing punishment. It also refers to the unlawful nature resulting from the application of the criminalisation provision in the law to the behaviour or act committed by the perpetrator. This unlawful nature can be negated if a justification exists that removes this characteristic.

In the context of cybercrime, most criminal law scholars agree on the necessity of enacting legal texts that criminalise acts and violations that occur within or against information systems. Against this backdrop, the European Council issued a recommendation in 1989 to encourage member states to adopt specific penal provisions for cybercrime. Countries have differed in how they have organised this matter: some have included these provisions in their penal codes, as with Algerian legislation, while others have established specific cybercrime laws.

Subsection Two: The Material Element of Cybercrime

The components of the material element vary depending on the type of crime. In formal crimes, the material element consists solely of the act. In result-based crimes, however, the material element comprises three components: the act, the result and the causal relationship. In order to determine the elements of the material component in cybercrime, we must first establish whether it is a formal or result-based crime.

To answer this question, we can examine the legal texts that regulate this crime in the Algerian Penal Code and compare them with other legal systems. It is evident from these that Algerian legislation does not require a specific result to occur; the mere presence of the material act is sufficient for cybercrime to be established, regardless of any harm caused to the victim. For example, the law punishes mere entry into the information system without requiring any resulting damage. It considers achieving the result through deceit in the information system to be an aggravating circumstance rather than a condition for punishment.

Furthermore, the law imposes the same penalty for attempting to commit these acts as it does for committing them, and any resulting harm merely serves as an aggravating circumstance for the punishment or grounds for a civil claim for compensation. This means that cybercrime is classified as a formal offence, where the material element is satisfied by the mere presence of the act, regardless of whether a result or causal relationship is present. In this type of crime, the act takes the form of positive behaviour, such as entering or remaining within the system.

The physical activity or behaviour involved in cybercrime requires certain conditions and circumstances that align with the specific characteristics of this type of crime. It is committed in a digital environment by someone who is assumed to have a certain level of knowledge about computer systems and how to use them. The unlawful activity performed by the cybercriminal, which is essential for establishing cybercrime, occurs within this environment and derives its specificities from it. This is because cybercrime utilises information technology through the information system as a means to commit the act or attack this system. Thus, the unlawful activity or behaviour in cybercrime varies according to the type of crime committed, as cybercrime encompasses both crimes committed using information systems and crimes committed against such systems.

Subsection Three: The Moral Element of Cybercrime

From a legal standpoint, the moral element is essential for establishing a crime. The presence of the material element of the crime is not sufficient; the law also requires a psychological link between the perpetrator and the material act they have committed. This psychological link is known as the moral element of the crime. There can be no crime without a moral element.

Criminal intent consists of two elements: knowledge and will. These are the necessary conditions for establishing criminal responsibility. If either of these conditions is absent, criminal intent is also absent and, without it, criminal liability cannot be established. Criminal intent can take various forms, including general or specific intent, and direct or indirect intent. General intent exists in all intentional crimes and represents the perpetrator's intention to commit the criminal act, knowing that it is prohibited by law. For example, in the crime of intentional murder, it violates the right to life.

By contrast, specific intent refers to the objective that the perpetrator intends to achieve by committing the crime. This type of intent is required by law for certain crimes, in addition to general intent. In the case of murder, for example, the law requires more than general intent (the will to commit the act and knowledge of its illegality): it also requires the intention to cause death. If a person strikes another person without intending to kill them, but the victim dies as a result, this is not intentional murder; rather, it would be a case of assault causing death without intent, lacking the specific criminal intent to cause death.

Regarding cybercrime, it is categorised as an intentional crime, meaning that the presence of general criminal intent is sufficient for its establishment. This general intent includes the perpetrator's knowledge of the elements of the crime and their intention to cause harm to a person, property or data stored in a computer. Based on this, under Algerian legislation, criminal responsibility for cybercrime applies to anyone who commits any of the acts specified in Articles 394 bis to 394 bis 7 of the Penal Code. However, it is also important to note that some forms of cybercrime require specific criminal intent, such as defamation crimes committed online.

Subsection Four: The Presumed Element in Cybercrime

The material and moral elements are fundamental and general components shared by all crimes. However, certain types of crime, including cybercrime, require more than just these two elements to be established. The legal model of these crimes necessitates the presence of specific characteristics that distinguish them from other crimes. These characteristics may pertain to the perpetrator or the victim, or to other elements, such as the means of committing the crime or its subject matter. These characteristics are intrinsically linked to this type of crime, whether they exist or not. They have been referred to by various names, including 'special crimes' or 'crimes with a specific characteristic'. In other words, these are crimes for which the presumed element must exist when the perpetrator carries out their actions; without it, the actions cannot be classified as a crime. The law requires this presumed element to exist for a crime to be recognised or categorised as a specific type (felony or misdemeanour).

In cybercrime, it is the automated data processing system that distinguishes this crime from others. Without it, an act cannot be classified as cybercrime. This system may be the subject of the crime or the means by which it is committed. The Algerian Penal Code protects this system from all forms of assault by criminalising certain acts that infringe upon it or any of its components. These acts aim to gain unauthorised access to the system or part of it to view its contents, benefit illegally from its services or access its components with the intention of damaging or disabling them.

Article 394 bis of the Algerian Penal Code criminalises entering an information system, or attempting to do so. The penalty is more severe if this results in the deletion or alteration of the system's data. If the entry leads to the destruction of the operating system, the legislator has set a penalty ranging from three months to three years and a fine between 500,000 and 2,000,000 DZD. Attacks targeting individual devices and support systems do not fall within the scope of these crimes, as the interconnection of devices, support systems, and programmes is essential to defining an information system. All assaults on any part of this system fall under traditional crimes such as destruction, damage and theft. Even integrated systems that are out of service are not subject to cybercrime provisions, as are assaults on unactivated, stored devices.

Furthermore, the information system plays a crucial role in the commission of this type of crime and is therefore considered an essential element of cybercrime. This means that the perpetrator of cybercrime must be familiar with the techniques for using this system, accessing the internet and visiting websites. They must operate the information system to commit the crime, which may involve downloading or creating hacking programs. They may also need to prepare and upload pages containing immoral or indecent materials to the host device. Alternatively, they may commit crimes by creating viruses in preparation for their dissemination.

Section Three: Common Provisions of Cybercrime

Cybercrime is characterized by specific features concerning the common provisions of crime, whether related to the issue of attempted crime, criminal participation, or conspiracy. We will discuss these below.

Subsection One: Provisions of Attempt in Cybercrime

The definition and criminalization of attempts are subject to two opposing schools of thought: the material school, which requires that the perpetrator begin to commit one of the acts constituting the material element of the crime, disregarding any prior actions, which proponents of this school classify as preparatory stages of the crime

The second school is the personal school, which considers criminal intent and classifies an act as an attempt if the perpetrator performs a specific act with the intention of subsequently committing an act that leads to the achievement of the criminal result. The Algerian legislator addressed the issue of attempts in Article 30 of the Penal Code, which states: 'All attempts to commit a felony that begin with an attempt at execution or with unequivocal acts that lead directly to its commission are considered the felony itself, unless they are stopped or lose their effect as a result of circumstances beyond the perpetrator's control, even if the intended goal is not reached due to circumstances unknown to the perpetrator.' Article 31 of the Penal Code states: 'Attempts in misdemeanours shall not be punished except by a clear provision in the law.'

According to Algerian legislation, if the perpetrator exceeds the preparatory stage of the crime, they are considered to have started executing it, thus entering a new phase called an attempt. An attempt is realised in two cases: the first is when the intended result does not occur, as in the case of unsuccessful or interrupted crimes; the second is when the intended result is achieved, but the causal relationship between the perpetrator's actions and the result is interrupted by an unforeseen factor. Therefore, the attempt phase occurs when the perpetrator surpasses the stages of contemplation and preparation to commit the crime, but does not reach full execution. Therefore, intent to commit a crime, preparatory acts, or attempts to commit it do not constitute an attempt.

In the context of cybercrime, Article 11 of the Budapest Convention addresses attempted cybercrime, stating: 'Each Party shall adopt legislative measures and any other measures it deems necessary to criminalise under its domestic law any intentional attempt to commit one of the crimes referred to in Articles 3, 5, 7, 8 and 9, paragraph 1(a).'

The Algerian legislator has punished such attempts under Article 394 bis 7 of the Penal Code, which states: 'Attempting to commit the misdemeanours provided for in this section is punishable by the penalty prescribed for the misdemeanour itself.'

Some argue that the material theory of attempts is more appropriate because most forms of cybercrime require a single physical action, primarily involving interaction with the information system. The personal school cannot be applied here as this would lead to the criminalisation of preparatory acts in these crimes. However, the French Parliament debated how to prove attempts at cybercrime. One member mentioned that attempts to unlawfully breach systems can be detected through logs within these systems that retain records of unauthorised breach attempts. From a technical perspective, therefore, it is possible to detect attempts at execution; however, it is difficult to distinguish between beginning execution and preparatory acts, particularly in cases of remote access. This prompted the French legislator to adopt the principle of punishing conspiracies to commit cybercrimes conducted within an agreement or group, as these constitute an attempt or preparatory act in themselves. This

suggests that they adopted the concept of conspiracy in relation to attempts, similar to that adopted by the Algerian legislator. Examining Article 394 bis 5 reveals that it is included under Article 394 bis 7, meaning that the Algerian legislator also punishes attempts to commit cybercrimes in conspiracy.

Subsection Two: Provisions of Criminal Participation in Cybercrime

Criminal participation occurs when multiple perpetrators contribute to the commission of a crime. Therefore, the crime is the result of the activity of several individuals, meaning it was not committed by one person, but by multiple individuals each playing a role. We can therefore deduce that criminal participation is based on two elements: the plurality of perpetrators and the unity of the crime. If either of these elements is absent, the concept of criminal participation is negated. Several terms have been used to refer to this, including 'criminal participation' and 'complicity in the crime'.

Due to the varying roles played by participants in a crime, legal issues arise in determining the effect of this variation. The principle is that one person or several individuals should undertake all the elements that constitute the criminal activity and take on a primary role. In this case, they are referred to as the perpetrators of the crime. Here, criminal participation is considered to be original participation. Others may contribute to this activity through a secondary or ancillary role that does not involve the direct execution of the crime, such as providing assistance. In this case, criminal participation takes the form of ancillary participation. There is usually no debate in cases of original participation in the crime due to the clarity of its provisions. However, disputes arise regarding ancillary participation, which affects original participation due to the strong relationship between the two. The disagreement primarily concerns two views: one that recognises multiple crimes with multiple participants, and another that maintains the unity of the crime despite the plurality of offenders.

The Algerian legislator has organised the provisions relating to criminal participation in Articles 41 to 46 of the first chapter of the second section of the first part of the Penal Code, which are grouped together under the heading 'Participants in the Crime'. Article 41 states that anyone who contributes directly to the execution of the crime or incites its commission is considered a perpetrator. Meanwhile, Article 42 classifies anyone who does not participate directly as a partner in the crime.

Regarding participation in cybercrime, Article 394 bis 5 of the same law states: 'Anyone who participates in a group or agreement formed for the purpose of preparing one or more of the crimes mentioned in this section, the preparation of which is embodied in one or more physical acts, is punishable by the same penalty prescribed.'

A scenario for criminal participation in cybercrime could be two or more individuals agreeing to commit a cybercrime. Examples could include defamation via an information system, defaming a person through a website, or attacking someone's email account by one party obtaining files and another party publishing them online or threatening to publish them unless a sum of money is paid. In this case, we are dealing with criminal participation in a cybercrime.

Subsection Three: Provisions of Conspiracy to Commit Cybercrime

Conspiracy is defined as an agreement between two or more individuals to commit a crime. The material element of this crime is the agreement between two or more individuals to commit a felony or misdemeanour. This is realised when one of the participants expresses their intention, whether verbally, in writing, through gestures or by implication, in a manner that reaches and is accepted by all participants. All participants must accept the agreement in a manner that establishes its existence.

Conspiracy is an intentional crime that requires criminal intent among the perpetrators. This consists of two elements: the first is knowledge of the subject of the agreement, including the nature of the act or acts agreed upon, and the characteristics that the legislator relies on to attribute criminality to the act.

The second element is intention, meaning that a person must intend to enter into the agreement and become a party to it, performing the role assigned to them. If this intention is not present, the individual may merely be exploring the intentions of the other members of the conspiracy, or they may be joking and intending to deceive them, thus lacking criminal intent. There is no specific form required for criminal conspiracy; a simple agreement suffices, and it does not have to be organised or in the form of an association.

This crime has specific characteristics that distinguish it, making it impossible to attempt conspiracy. This is because conspiracy is a psychological state that occurs through the convergence of wills and has no beginning or end. This crime either occurs or it does not, and most scholars agree that it cannot be initiated. Thus, it is classified as a formal crime. Additionally, criminal conspiracy is established as soon as an agreement to commit a felony or misdemeanour is reached, and withdrawal afterwards does not exempt one from punishment, since the material element of this crime has been completed.

Furthermore, there is no conflict between the crime of conspiracy and conspiracy as a form of participation, since they apply in different contexts. Participants in a conspiracy are not considered accomplices unless the crime that is the subject of the conspiracy is actually committed, or an attempt is made to commit it. In contrast, conspiracy is established upon agreement alone, regardless of whether the underlying crime has occurred.

Based on the above, it is conceivable that a material difference could exist between the crime of conspiracy and the crime to which the conspiracy relates if the latter is completed or attempted. In this case, the harsher penalty would apply, naturally being that for the completed crime or an attempted crime. According to Article 394 bis 5, the Algerian legislator has punished conspiracy for the purpose of preparing crimes affecting information systems with the same penalty prescribed for the prepared crime. If multiple crimes are involved, the penalty would be that for the most serious crime.

Conclusion:

This research shows that this topic is complex and intricate, and it is impossible to cover all its aspects in a single study. Instead, theoretical and field studies are required, as well as an analysis of rulings and judicial decisions that reflect the efforts of those working in the judiciary. From a general perspective, however, and based on a preliminary personal impression, it can be cautiously stated that technological advancement has led to the evolution of crime in general, including cybercrime. This requires the adoption of a judicial criminal policy that alleviates strict adherence to traditional principles and rules of procedural law, in favour of achieving justice and considering the peculiarities of certain crimes and the difficulties in proving them. This approach should be applied to cybercrime to achieve the desired objectives of this policy.

I. References in Arabic:

A. Fattah Bayoumi Hijazi, Computer and Internet Crimes in Arab Countries, Dar Al-Nahda Al-Arabiya, 2009, p. 39.

Idris Belmehjoob, 'The Impact of Cybercrime on Financial Credit', Series of Seminars of the Court of Appeal in Rabat, Morocco, No. 7, 2014, pp. 33–34.

Lina Mohammed Al-Asadi, The Effectiveness of Criminal Law Provisions in Combating Cybercrime, Dar Al-Hamid for Publishing and Distribution, Amman, Jordan, 2015, p. 156.

Ali Abdul Qader Qahouji, Explanation of the Penal Code, General Section, Volume One: General Theory of Crime, Dar Al-Matbu'at Al-Jami'iya, Alexandria, 1997, p. 357.

II. References in Foreign Languages:

André Vitu: Treatise on Criminal Procedure, 1st edition, Maison de la Presse Universitaire Française, 1957.

David Thompson, 'Current Trends in Computer Crime', Computer Control Quarterly, Vol. 9, No. 1, 1991.

Nicolas Arpagian, Cybersecurity, Press Universitaire de France (PUF), Paris, France, 2010.

Philippe Merel: Legal Presumptions in Criminal Law, with a preface by André Vitu, Paris: L.G.D.J., General Library of Law and Jurisprudence.

M. Vivant, 'On Informational Links', J.C.P., 1984.

H. Donnedieu de Vabres, The System of Universal Repression: Its Historical Origins and Contemporary Forms.

Liang Jiansheng, 'Computer Crime', Internship Report, Professional Higher Diploma in Information Science and Libraries.

R. Garraud, Theoretical and Practical Treatise on Criminal Investigation and Procedure, Paris: Sirey, 1929.

M. Raoul Comblidiaeu, The Judge and the Truth, Aspects of Criminal Law in the Annals of the University of Social Sciences of Toulouse, T. XXVI, 1978.

Global Action on Cybercrime Extended (GLACY+), a joint project of the European Union and the Council of Europe, Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence, October 2020, www.coe.int/cybercrime.

Rihab Yousfi and Wahiba Louarem, 'Digital Evidence and Proving Cybercrime: Between High Technology and Legal Constraints', AFAK for Science Journal, Algerian Scientific Journal Platform, Vol. 9, No. 4 (2024), pp. 97–113.

Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations', Computer Law & Security Review, Volume 49, July 2023, 105801.