

Reasons for permissibility and prohibitions of punishment in cybercrime

Mamene besma^{1,*}

¹Laboratory of State and Social Security, Health and Food Security, Faculty of Law, Abbas Leghrouh University, Khenchela, Algeria.)

mamen.besma@univ-khenchela.dz

Received: 27 /03 / 2025 Accepted: 04 /10 / 2025

Published: 04 /11 / 2025

Abstract:

The development that Algerian society has experienced in using information technology, like other societies, has led it to encounter new types of crimes, primarily cybercrime. Whether these crimes involve hacking personal accounts, international institutional accounts, intelligence accounts, or other related crimes, it became necessary for the Algerian legislator to intervene through numerous legal texts to confront these crimes. However, sometimes there are circumstances that justify the act and nullify its criminal effect, called grounds of justification, as well as circumstances called punishment barriers such as insanity, minority, and coercion. The presence of one of the punishment barriers or grounds of justification results in exemption from punishment, as well as exemption from criminal responsibility depending on the case. The objective of this study is to shed light on the extent to which grounds of justification and punishment barriers can be available in cybercrimes.

Keywords: Cybercrime, reasons, permissibility, contraindications, punishment, Incrimination

المخلص :

ان التطور الذي عرفه المجتمع الجزائري في استخدام تكنولوجيا المعلومات على غرار باقي المجتمعات جعله يعرف انواع من الجرائم المستحدثة وعلى رأسها الجريمة الالكترونية سواء اكانت هاته الجريمة لها علاقة بتهكير الحسابات الشخصية او حسابات المؤسسات العالمية او حتى الاستخباراتية وغيرها من الجرائم ذات الصلة ، فكان لزاما على المشرع الجزائري التدخل عبر العديد من النصوص القانونية لمواجهة هذه الجريمة الا انه في بعض الاحيان تقوم حالات تبرر الفعل وتبطل عنه مفعول التجريم تسمى اسباب الاباحة، وأيضا حالات تسمى موانع العقاب كالجنون وصغر السن والإكراه. وتوافر احد موانع العقاب او اسباب الاباحة ينتج عنه الاعفاء من العقوبة ، وكذا الاعفاء من المسؤولية الجزائية حسب الحالة ، فالهدف من هذه الدراسة هو تسليط الضوء على مدى امكانية توفر اسباب الاباحة وموانع العقاب في الجرائم الالكترونية

الكلمات المفتاحية : الجريمة الالكترونية ، اسباب ، الاباحة ، موانع ، العقاب، التجريم

* mamene besma

I. INTRODUCTION:

Recent years have witnessed scientific and technical development in all aspects of life. Among the technological innovations the world is experiencing is what is known as the information network, which has dominated most areas of life. There is hardly an institution, bank, government agency, or home without a computer that plays a fundamental and effective role in managing workflow within these entities. Despite the positive aspects of technology, negative matters have emerged alongside it, including cybercrime.

Out of the Algerian legislator's desire to address the phenomenon of cybercrime and its accompanying considerable harm to individuals and state institutions on one hand, and his attempt to remedy the existing legislative vacuum in this field on the other hand, he has worked since the second millennium to amend many national laws, including penal legislation, foremost among them the Penal Code, to make them responsive to criminal developments in the field of information and communication technology. He also created other laws to ensure criminal protection for electronic transactions. However, in return, cybercrime may occur but be accompanied by one of the grounds of justification, which are:

Circumstances that justify the act and nullify its criminal effect, termed justification situations. These are crimes committed under circumstances that exempt their perpetrator from criminal responsibility, where these circumstances are called grounds of justification or barriers to establishing criminal responsibility. The principle in Islamic Sharia is that criminalized acts are prohibited for everyone in general, but the legislator, as an exception to the original rule, may permit some criminalized acts for those who possess special qualities. Individual circumstances require this permission, such as legitimate defense and performance of duty, and also in cases of punishment barriers such as insanity, minority, and coercion.

Responsibility barriers are personal, unlike justified acts which are considered objective reasons that do not remove the criminal character from the criminalized act, as it remains unlawful, unlike justified acts which remove that character so that the act becomes lawful.

The presence of one of the criminal responsibility barriers results only in exemption from punishment, making it possible with their presence to impose a precautionary measure in addition to civil compensation. This is unlike justified acts which remove both criminal and civil responsibility. However, the matter becomes more complex when it concerns cybercrimes, which leads us to raise the following problematic: **To what extent is it possible for grounds of justification to be available in cybercrimes? And can a punishment barrier be available given the specificity of this crime?**

1. Definition of cybercrime

Negative behaviors take multiple forms, evolve, and assume countless shapes according to the means available to humans for committing acts and achieving their results in practical reality and achieving their results in scientific reality.

Cybercrime is among the crimes that emerged from the misuse of the information technology revolution, which differs greatly from traditional crime in its nature, types, and tools. Therefore, it was necessary to clarify its essence and the Algerian legislator's position on it.

1.1. The Juridical Definition of Cybercrime

Cybercrime possesses a criminal danger the world has never witnessed in traditional crimes. It is a phenomenon that has affected various countries through the use of different services available on the internet. For this reason, (Saghir, 2013/2014, p. 7). there appeared differences in definitions, and among these definitions are the following:

The jurist "Marwi" defines cybercrime as: "The unlawful act in which a computer is involved in its commission."

Dr. "Huda Qashqoush" sees in this regard that cybercrime is: "Any unlawful or unauthorized behavior concerning automatic data processing systems."

Professor and jurist "Abdullah Abdul Hakim" defined it as: "Cybercrime is those crimes resulting from the use of modern technology represented by computers and the internet in criminal works and activities.." (Rahman, 2004, p. 106)

Through these definitions, it becomes clear that cybercrime has both a narrow and a broad definition.

1.1.1- The Narrow Definition of Cybercrime:

The narrow definition of cybercrime refers to criminal acts that are directly committed through the use of electronic devices or networks. This definition includes crimes related to systems and devices, such as hacking, data theft, and the distribution of malware that targets systems, as well as financial crimes like online fraud, identity theft, and the use of stolen credit cards.

Finally, it also includes sexual harassment crimes and crimes related to children, such as exploiting children online or distributing pornographic materials. (Momeni, 2008, p. 48)

1.1.2 -Broad definition of cybercrime:

The broad definition of cybercrime includes all criminal activities that occur over the internet, or those that benefit from modern technology to achieve unlawful gain, and includes:

Any illegal act executed using technology, regardless of the means, whether through the internet, smart devices, or the dark web. It is also defined as any intentional criminal act, whatever its connection to informatics, that results in a loss to the victim or a gain achieved by the perpetrator.

Among its negative effects on individuals and communities are spreading hatred, rumors, false information, and electronic threats. It may appear in the form of invisible activities such as crimes related to digital data and information, including information piracy and violations of intellectual property rights.

It may also appear in the form of crimes that have national and international effects, such as cyberattacks that affect governments or companies across borders.

***The difference between the two definitions:**

a- Focus:

- The narrow definition focuses on criminal acts that directly use technology
- The broad definition includes the effects of technology on crime in a broader concept that goes beyond just the criminal act to its impact on individuals and communities

b- Scope:

- The narrow definition tends to define a more specific scope in studying crimes
- The broad definition provides a more comprehensive perspective on the phenomenon, reflecting the complexities of cybercrime in the modern era

We conclude that choosing the appropriate definition of cybercrime depends on the context in which the crime is being discussed. The narrow definition is suitable for basic crime investigations, while the broad definition provides a framework for understanding the impact of technology on criminal activities comprehensively (Momeni, 2008, p. 49)

1.2. Legal Definition

Unlike the French legislator, who did not provide a definition for cybercrime, the Algerian legislator has termed it "crimes related to information and communication technology." While they did not define cybercrimes, they adopted the term "infringement of automated data processing systems" to denote the crime (communication, 2009)

Based on the Algerian Penal Code, cybercrimes were not defined, and it sufficed with punishing certain acts under the title "Crimes Affecting Automatic Data Processing Systems." The Algerian legislator defined cybercrime in Article 02 of Law 09/04 as: "Crimes affecting automatic information processing systems specified in the Penal Code or any crime committed or facilitated through an information system or electronic communications system."

It is observed through this definition that:

The Algerian legislator adopted the criterion of combining several criteria to define cybercrime: first, the criterion of the crime's means, which is the electronic communications system; second, the criterion of the crime's subject matter - violation of automatic data processing systems; and third, the criterion of applicable law or the legal element of the crime stipulated in the Penal Code.

The Algerian legislator also adopted a fourth criterion in determining the scope of cybercrime as he acknowledged that cybercrime is committed in an information system or facilitated by it. This expands the scope of cybercrimes in Algerian law. Most legislators in comparative systems have avoided establishing a legislative definition of automatic data processing systems and left this task to jurisprudence and judiciary.

1.3. The legal nature of cybercrime

Cybercrime is distinguished by its special nature, which it derived from the means by which it is committed, represented by the global internet network.

The discussion about the legal nature of cybercrime centers on the legal status of programs and information. Jurisprudence has been divided into two directions:

a. The special nature of information

This direction believes that according to general rules, only material things accept possession and appropriation, and that the object of theft must be material, i.e., have a tangible material entity so that it can be transferred and possessed through embezzlement that constitutes the material element in the crime of theft. Since information has a moral nature and cannot be considered among values capable of possession and appropriation except in light of intellectual property rights, ideas and information are excluded from the field of theft, unless they are recorded on a disk or tape.

b. Information is an emerging set of values

This direction sees that information is nothing but a set of values capable of appropriation independent of their material support. Information has economic value capable of being unlawfully possessed, and it is connected through an adoption relationship between them like the legal relationship represented by the relationship of the owner to the thing he owns. This means that information is property capable of ownership and exploitation based on its economic value and not based on its material entity. Therefore, it deserves legal protection and treatment as property. (Amal, 2007, p. 71)

2. The Basis for Considering Justifications as Barriers to Liability in Cybercrime

2.1. Justification as a Barrier to Establishing Responsibility for Cybercrimes

The basis of crime is its stipulation through a legal text that criminalizes these acts. An act does not constitute a crime unless there is a text that determines it. Similarly, the same acts may be permitted by the legislator in certain cases to favor a particular interest.

Justification in cybercrimes is defined as a principle that makes an act that is criminalized and punishable by legal text permissible and not punishable for its perpetrator.

As for the definition of grounds of justification, they are a set of circumstances attached to the material element of the crime that strip the incident of its criminal character and make the act permissible. The Algerian legislator confirmed these cases through explicit texts regulated by the Algerian Penal Code in the first part related to crime within the second book related to acts and persons subject to crime. (Marzouq, 2011)p124

The grounds for justification are divided into two aspects:

- **The objective aspect** is divided into: general and special causes. General causes are those that permit any crime without exception, such as legitimate defense, exercise of right, and performance of duty, because each can be envisioned in every crime if its conditions are met. Special causes are those that apply to specific crimes and not others, such as the right of defense before courts, as this right only permits defamation and insult.

- **The personal aspect** is divided into absolute and relative causes. Absolute causes benefit all people, such as legitimate defense. Relative causes do not benefit all people but only specific persons, such as an official who executes an order issued by a superior whose obedience is mandatory.

2.2. Punishment Barriers in Cybercrime

Impediments to punishment do not relate to the legal or moral elements of a crime; rather, they concern the punishment itself. These are cases of exemption from punishment. The perpetrator is considered a criminal because their act is not permissible but is a criminal act (Marzouq Cybercrime does not differ from other crimes in terms of impediments to 126) .2011 responsibility. All cases of impediments to responsibility can apply in the following ways:

a- Minority

Islamic Sharia is considered the first law in the world that distinguished between minors and adults in terms of criminal responsibility and the first law that established rules for minor responsibility that have not developed since they were established. Despite 13 centuries passing, they are considered the most recent rules upon which minor responsibility is based in our present era.

Information technology has contributed to expanding and developing the fields of using automated media devices, smartphones, and related technical means, which enabled minors to deal professionally and creatively with their applications. However, practical reality recorded both positives and negatives, the latter represented in increasing the number of crimes committed through electronic means such as insult, defamation, and publishing indecent images, in addition to curiosity-driven attempts or commission of legally criminalized acts represented by unauthorized entry, access, and piracy.

b.Insanity

Islamic legislation considers humans criminally responsible if they are aware and have choice. If one of the two elements is absent, human obligation is lifted. The meaning of awareness in obligation is to be enjoying mental faculties. If he loses his mind due to disability, accident, or insanity, he has lost awareness. (Faraj, p. 79)

Despite considering insanity synonymous with the absence of mind permanently or temporarily, totally or partially, it does not prevent the use of electronic devices, which may cause losses to others even by chance. Sometimes the cause of insanity is sharp, misdirected intelligence.. (Khalafa, p. 121)

c.Coercion

Some jurists define coercion as an act performed by one human against another that eliminates consent or corrupts choice and as an act that obliges the coerced person. Coercion occurs in all its physical and moral forms against persons to compel them to commit cybercrimes, where, like other crimes, coercion represents a barrier to establishing responsibility. (al-Hasani)

2.2.3. The Principle of Good Faith and Its Relationship to Cybercrimes

The principle of good faith in the scope of criminal law is linked to the moral element of crime, specifically in the field of criminal intent consisting of two elements: knowledge and will, as it is one of the influential factors in the principle of good faith in legal transactions due to the close connection of the principle. (Faraj, p. 384)

a- The Principle of Good Faith in Unintentional Crimes Generally

Islamic Sharia is based on the principle that matters are by their intentions. The intentions and purposes of worshippers are the subject of the lawgiver's consideration regarding what he commands his worshippers. Good faith is a means to obtain reward and avoid punishment, or at least mitigate it.

The principle of good faith in the field of punishment is clearer in the field of criminalization. It is accepted that justice does not mean mere material equality between harm and punishment but looks at the intent of the perpetrator who caused that harm and his intention. As the principle of good faith has a role in justice, it also has a role in reform, which does not bear fruit unless the motives that drove the offender to commit the crime are examined, because they are important influences indicating the offender's personality.

Unintentional crime occurs in the absence of the offender's will, whether due to negligence and shortcoming or recklessness and lack of insight. It does not require bad intent aimed at inflicting harm and evil on others. It is based on will without the criminal and familiar consequences of the act. This bad result, even if not intended by the offender, can be expected by an ordinary person, and thus the crime is considered natural to his fault and negligence.

b- The Principle of Good Faith in Unintentional Cybercrimes

In the cybercrime system, Saudi law established special protection for good faith. The system stated that good faith has a role in punishment, represented in confiscation related to devices and programs. Article 13: Without prejudice to the rights of persons in good faith, devices, programs, or means used in committing any of the crimes stipulated in this system or money obtained therefrom may be confiscated. The website or service provision place may also be ordered to be closed permanently or temporarily.

Article 394 bis 06 of the Algerian Penal Code addressed the following: "While preserving the rights of third parties in good faith, devices, programs, and means used shall be confiscated with the closure of sites that are the subject of a crime among those punished according to this section, in addition to closing the shop or place of operation if the crime was committed with the knowledge of its owner."

On this basis, it can be said that good faith focuses on the general intent of the crime, as it negates the knowledge characteristic that represents one of the two elements of general criminal intent. With the absence of the latter, the crime is negated from its foundation.

However, if the crime requires special criminal intent, the defense of good faith cannot be envisioned here, as that intent in itself negates good faith. The lesson is in considering the special criminal intent whose existence is inferred from the criminal behavior of the offender. For example, a website may provide hosting on the electronic site, and some people exploit this feature to facilitate communication between terrorist groups or members of organized criminal

organizations, without the host's knowledge. (al-Hasani, Commentary on the Penal Code, p. 581)

Conclusion:

The Algerian legislator attempted to address the phenomenon of information crime through adopting a dual policy, guided on one hand by modifying the substantive and procedural aspects of general penal legislation and making them keep pace with new challenges resulting from the tremendous development of modern technology, and on the other hand by creating other special laws more responsive to the special nature of cybercrimes.

By examining these legal texts, we find that the Algerian legislator defined the prohibited acts whose commission under certain conditions constitutes a crime. These texts multiply with the multiplicity of acts prohibited by law and are called criminalization texts. An act cannot be considered a cybercrime unless it falls under one of these texts.

However, there are acts criminalized according to general rules, yet the law permits them to achieve public interest. Grounds of justification are objective, erasing the criminal character of the act and are limited to the material circumstances of the act. Punishment barriers relate to personal circumstances. Neither was specifically addressed by the Algerian legislator, leaving them subject to general rules.

Therefore, we suggest the following:

- Dedicating a special chapter on grounds of justification in cybercrimes specifically and precisely according to each case while adhering to the principle of restriction to avoid confusion
- Allocating special legal texts to address punishment barriers in cybercrimes

Referrals and references:

- **Books :**

- Amal, Kara. (2007). *Criminal Protection of Information Technology in Algerian Legislation*. Algeria: Dar Homa for Printing, Publishing and Distribution.

-Khalafa, Ahmed. *Fundamentals of Criminal and Judicial Psychology*. Cairo: Dar Al-Fikr Al-Arabi.

- Faraj, Reda . *Commentary on the Algerian Penal Code, general section*. algiria: National Publishing and Distribution Company.

- **University theses:**

-Momeni, Nahla. Adel.Qader AL (2008). *Cybercrime. Magister's Degree in Criminal Information Law* . algiria: Culture House for Publishing and Distribution, first edition.

-Marzouq, AL Ruke. Marwan Bin. (2011, 06 12). *Mens rea in cybercrime. a comparative study, Magister's thesis in Criminal Justice*, Faculty of Graduate Studies, Department of Criminal Justic: Naif University for Security Sciences, Faculty of Graduate Studies

-Rahman, Ghazi. Abdul. (2004). *Legal protection against cybercrime. thesis for the degree of Doctor of La)*Rahman(2004 ‘w . Lebanon, Faculty of Law, Islamic University, Lebanon: Islamic University.

- Saghir, Youssef. (2013/2014). Crime committed via the Internet. *Magister thesis in Law, Specialization in International Business Law, Faculty of Law and Political Science* . Tizi-Ouzou, Faculty of Law and Political Science, Algeria.