Hume Studies,
ISSN / eISSN 0319-7336 / 1947-9921
Publisher HUME SOCIETY, OCCIDENTAL COLLEGE
Volume 26-Issue 1-(2026)
DOI: https://doi-0004.org/6812/17951569485190

Cyberbullying as a New Form of Cybercrime: What Protection Does Algerian Law Offer?

LAKLI Nadia[1], BRAHIMI Assia[2], HADJ BOUSSADA Fatiha[3]

[1]Lecturer "A", Faculty of Law, University of Ain Temouchent - Belhadj Bouchaib, Algeria, Laboratory: Philosophy, Science and Development in Algeria, university of Oran2, Algeria, https://orcid.org/0000-0002-2480-5351, E-mail: nadia.lakli@univ-temouchent.edu.dz

[2]Lecturer "A", Faculty of Law, University of Ain Temouchent - Belhadj Bouchaib, Algeria, E-mail: assia.brahimi@univ-temouchent.edu.dz

[3]Lecturer "A", Faculty of Law, University of Ain Temouchent - Belhadj Bouchaib, Algeria, E-mail: fatiha.hadjboussada@univ-temouchent.edu.dz

Received: 19/08/2026 ; Published: 20/11/2026

Abstract:

The technological development in our time has led to the emergence of a new type of crime that is completely different from traditional crimes, represented in "cybercrime", considering that they are carried out through computer networks.

Some of these crimes may affect the psychological safety of humans, such as cyberbullying, which has recently become common in various kinds, which affects the psychology of the victim, which may push her to end her life as a result of pressure on her.

Through this study, we will address the concept of cyberbullying and the extent of its impact on the psychology of its victims, and then address the deterrent aspect of this crime.

Keywords: cyberbullying, cybercrime, legal protection, psychological safety, penalties.

Introduction:

The spread of information technology and means of communication in our time has led to the emergence of a new type of crime that is completely different from traditional crimes in terms of their nature, characteristics, types and means of implementation, and they are called "cybercrimes" or "cybercrimes" or "cybercrimes». Regardless of the different names of this type of crime, the perpetrator uses the same means of computer, which is carried out through computer networks.

Cybercrime is distinguished from other traditional crimes by the ease of the victim's falling into its trap on the one hand and the difficulty of proving it on the other hand, and this crime has become common nowadays due to technological development, which

prompted various legislations to impose strict penalties on the perpetrators due to their seriousness due to their multiple types.

The Algerian legislature has tried to keep pace with technological development in the field of combating cybercrime by amending the Penal Code by Act No. 15-04, section VII bis of which is devoted to information crimes under the title "Prejudice to automated data processing systems".

The importance of this study is evident in the novelty and prevalence of this type of crime, and its difference from traditional crimes due to its characteristics and the difficulty of detecting it.

These crimes may affect the physical integrity of the human being, which is a constitutional right recognized in most legislation, and the most important of these crimes that have recently spread is "cyberbullying", which may reach the victim's suicide as a result of her inability to bear the psychological pressure exerted on her by the cyberbully.

The importance of this study lies in the widespread suicide cases among young people due to cases of cyberbullying they are exposed to.

This study aims to define the concept of cybercrime, identify its types, identify the concept of cyberbullying and highlight the role of Algerian legislation in deterring these crimes by imposing the necessary penalties on the perpetrators.

Based on the above, we pose the following problem: To what extent does cybercrime affect human physical integrity? Does Algerian legislation guarantee adequate protection for victims of cyberbullying?

To answer this problem, we will rely in our study on the descriptive and analytical approach, through which we will address in the first axis the legal nature of cybercrime by identifying its concept and characteristics, while in the second axis we will address cyberbullying as a type of cybercrime and deterrent penalties for these crimes.

I. The legal nature of cybercrime:

We will learn about the concept of cybercrime and the characteristics that distinguish it from other traditional crimes.

1- The concept of cybercrime:

Cybercrime is one of the crimes that have varied names, there are those who call it computer crime in relation to the tool used in it, and there are those who call it information crime as it affects confidential information, but the most likely name at the present time is cybercrime. The legal texts did not define the concept of this crime, but were based on its elements and means of commission.

Some define it as "*a criminal act that uses the computer as the main tool*" (G. CHAMPY, 1988), and others define it as (TIEDEMANN, 1993): "*It includes all forms of unlawful behavior committed using a computer*." Others define it as: "*Any intentional positive or negative act aimed at attacking information technology, whatever the purpose of the perpetrator*." (YOUSSEF, 2009).

Accordingly, cybercrime is the use of modern technical devices such as computers or mobile phones to carry out illegal purposes with the aim of harming society. (ZAIDAN, 2011).

As for the Algerian legislator, it did not address the concept of cybercrime, but used the term "*prejudice to automated data processing systems*" in articles 394 bis to 394 bis 7 of the Penal Code, and defined it in Law No. 09-04 containing the rules on prevention and combating of information and communication technologies in article II thereof as crimes against automated data-processing systems specified in the Penal Code and any other crime committed or facilitated through an information system or electronic communications system.

Thus, the Algerian legislator considers the information system and the data that enter the computer to be the essence of cybercrime, and the automated data processing system includes physical elements such as linking devices and moral elements such as software.

An automated data processing system is defined as "*a harmonious set consisting of one or several processing units, memory, programs, data, input and output units, and communication between these units that lead to the giving of a certain result, and this set is technically protected by any means of credit*". (LINANT, 2002).

The Algerian legislator defined the automated data processing system in Article II of Law No. 09-04 containing the rules on prevention and control related to information and communication technologies as: "*Any system or group of systems, whether separate, connected to each other or related, and one or more of them automatically processes data in implementation of a specific program*."

We point out that the automatic data processing system does not mean the computer only, but every system that would carry out this automatic processing, and therefore the Internet is an automated data processing system in addition to e-mail, websites and electronic cards such as bank electronic cards, as well as floppy disks, flash disks and CDs for storing information (DEVREZE, 2001).

2- Characteristics of Cybercrime:

The new nature of cybercrime distinguishes it from other traditional crimes, and perhaps one of the most important characteristics that distinguish cybercrime from other crimes is:

- The commission of the crime via the Internet, which makes it cross-border and not limited to a specific territory, the offender may be in one country and the victim in another, and this characteristic constitutes the greatest obstacle to the judicial authorities because of the difficulty of determining the competent judicial authority in adjudicating the dispute as well as the applicable law. (GHANIA, 2015).

- The difficulty or impossibility of proving the cybercrime because it does not leave any trace of the crime after its commission, as the offender can delete information and data related to him immediately after the commission of the crime, which is impossible to prove.

- The technical and technical expertise of the perpetrator of cybercrime, which leads to the ease of the victim's falling into his trap, and the difficulty of investigators carrying out their tasks in search and investigation, so it is preferable to seek the help of an expert investigator in information crimes, and this is currently in force in the United States of America. (SOUALMI, 2016).

- Lack of reporting of cybercrime by the victim due to the inability to prove it, in addition to the victim's keenness to preserve his reputation.

- The commission of crime through the computer and the Internet, each of which constitutes the main tool in the commission of crime.

- The personality of the offender in itself, as the perpetrators of cybercrimes are called "cybercriminals" to distinguish them from traditional criminals, and they are also called "hackers".

We will learn about cyberbullying as a type of cybercrime, and then we will address the penalties prescribed for these crimes.

3- Cyberbullying as a type of cybercrime:

It is difficult to enumerate all categories of cybercrime as they are based on modern technologies, but it can be divided into two types: cybercrimes committed by the information system, and those committed on the information system.

Cyberbullying is included in these types as it is carried out by one of the two means, so we will first learn about the types of these cybercrimes, and then learn about the concept of cyberbullying and the extent of its impact on the physical safety of humans.

II. The concept of cyberbullying and its impact on the victim's psyche:

Cyberbullying means the aggressive act carried out by the bully by using the Internet and modern means, with the aim of harming others, whether by mocking them or by blackmailing them with personal photos of them that may be embarrassing, or by threatening them, impersonating them or spreading rumors about them using their personal photos (Al-Sheikhi, 2019).

Although the Algerian legislature does not explicitly address the crime of cyberbullying due to its novelty, it applies the provisions of cybercrime to it as a criminal act that harms others.

Cyberbullying greatly affects the person, whether financially or morally, as this behavior generates a psychological feeling in the victim that may lead her to depression and live in constant fears, and may even end her life through suicide as a result of the psychological pressure exerted on her by the bully, especially when it comes to bullying children or adolescents whose personality is weak, as we actually notice the opening of accounts on various social networking sites (Facebook, Instagram, TikTok…). By children who have not reached the legal age allowed to open these accounts, and they publish videos and photos through these sites that the bully may exploit to blackmail them by modifying

them or publishing explicit pictures of them, which generates psychological pressure that pushes them to commit suicide.

1- Means of Committing Cyberbullying:

The means that the bully may resort to harm his victim vary, as the latter may commit the crime through or on the information system, and this is what we will address.

a- Cyberbullying committed by the information system:

The perpetrator aims to use a specific information system to identify people, also called personal Internet crimes as they affect individuals by accessing their personal identity by hacking their personal accounts and impersonating them or viewing their personal photos for illegal use, such as extorting them with the aim of earning money.

Therefore, the use of an information system to attack the sanctity of individuals is a crime punishable by law. Cybercrimes against individuals are the most common impersonation and defamation of artistic or political figures through websites by accessing the victims' information system, using their information and personal photos that have been stolen from their private accounts, and threatening them with them in exchange for money.

The criminal can also penetrate a person's information system to infringe on his intellectual, moral and artistic rights by stealing some scientific information, for example, and attributing it to him, or assaulting the patent, as all of them are considered legally protected personal moral rights. (YOUNES, 2004) Cybercrimes against individuals are often carried out by accessing their email to obtain their personal identity.

b- Cyberbullying committed on the information system:

In addition to cyberbullying committed by the information system, there are cybercrimes in which the information system itself is the subject of the crime, and these crimes target either the physical or logical components (programs) of the information system or the information included in the information system. (AL-MALT, 2006).

The perpetrator of this crime is characterized by high technical knowledge in the field of information, and these crimes are represented in entering the person's information system and staying in it to modify or delete his data or seize personal data for illegal purposes, such as stealing money and often in the field of financial institutions, and this crime is also manifested through manipulating programs by planting a subprogram in the original program that allows access in any information system. The crime of remaining in the information system is a continuous crime because it is associated with a period of time in which the crime continues.

The program can also be equipped with an additional set of instructions that are easily accessible by a code that allows obtaining all the data contained in the information system. (AL-MALT, 2006). The automatically processed information is the basis of the work of the information system, so it may be the subject of cybercrime by modifying the information inside the system or destroying it through the use of some viral programs, and ***the Trojan horse program*** is one of the most famous of these programs, which is a type of harmful

virus that appears in the form of a useful program to deceive the victim, but it contains a virus that allows a person to spy on others and steal their data with ease.

We point out that the mere use of the computer virus indicates the existence of a legally criminalized act, so it is always recommended to download anti-virus programs in order to protect the information system from them.

Accordingly, the crime of attacking the information system can manifest itself through illegal access and stay, i.e. the continued presence inside the processing system without the permission of its owner (Brahimi, 2012), and access to the information system does not constitute a prohibited act in itself, but failure to authorize such access constitutes a crime. (KARA, 2007). Entering the information system is considered a formal crime that does not require the material element to achieve its criminal result, as it constitutes a prohibited act merely entering all or part of the information system without the knowledge or permission of its owner, and this is understood from the text of Article 394 bis of the Penal Code. Anyone who fraudulently enters or remains in all or part of an automated data processing system or attempts to do so..." The wording of the article came in general, as it did not require that the information system be technically protected to prohibit entry, but rather criminalizes access to the information system even if it is not protected, provided that a license is not obtained.

Thus, the crime of fraudulent access to the information system is considered as the wrong entry does not constitute an act punishable by law due to good faith, but it is difficult to prove the intention of the offender in this type of crime. (ALAIN, 1996).

Fraudulent survival in the information system is considered the next stage of entering into it, and this survival may be the result of entering a project, i.e. by mistake or chance, and it may also be the result of fraudulent entry with the aim of harming the information system. Some define fraudulent survival in the information system as an unusual connection to the information system through the information network and looking at the data contained in this system without the knowledge of its owner (LINANT, 2002).

2- Deterrent Penalties for cyberbullying:

The Algerian legislator did not provide an explicit penalty for cyberbullying, but by referring to articles 394 bis to 394 bis 7 of the Penal Code, we find that the Algerian legislator punishes cybercrimes in general, as it imposes penalties on people who attack the information systems of others by illegally entering and staying in them with the aim of disabling them, modifying or erasing their data, or disclosing the secrets of others. The crime may manifest itself through fraudulent deletion of information data, regardless of the nature of or the value of this data, as the crime may manifest itself through the modification of information data and change it from the state in which it was originally, regardless of the way in which the data was modified.

The prohibited behavior may also be manifested through the introduction of information data on the system without the knowledge of its owner, such as the introduction of viruses (Shawa, 1993), additional data or programs, and the law also punishes the crime

of designing pirated information data, such as preparing piracy programs with the aim of hacking information systems without the knowledge of their owners and then disseminating them.

In this context, we distinguish between the original and complementary sanctions.

a- Original Penalties:

Article 394 bis of the Penal Code stipulates a penalty of imprisonment from three months to one year and a fine of 50,000 to 200,000 dinars for anyone who fraudulently enters or remains in all or part of an automated data processing system or attempts to do so. We point out that this penalty is doubled in the event of deletion or change of the system's data or in the case of sabotage of the system's operating system, and this is what is explicitly stipulated in the same article in its two paragraphs. The second and last.

Article 394 bis 2 of the Penal Code stipulates that: "Whoever deliberately and fraudulently commits the following:

1. Designing, researching, collecting, providing, publishing or trading data stored, processed or transmitted through an information system in which the crimes stipulated in this section can or are committed.

2. Possessing, disclosure, publishing or using for any purpose whatsoever data obtained from one of the crimes stipulated in this section."

We note that the text of the article is broad and includes various types of cybercrime, and therefore cyberbullying can be classified within it due to the means committed by the bully, which is represented in the data.

b- Supplementary Penalties:

In addition to the original penalties prescribed for perpetrators of cybercrime, the legislator provides complementary penalties to further deter these crimes. These penalties are represented in the confiscation of the devices, programs and means used, with the closure of the sites where the crime is located, as well as the closure of the place or place of exploitation in the event that the crime is committed with the knowledge of the owner, and this is explicitly recognized by Article 394 bis 6 of the Penal Code, such as the closure of an electronic café in which the information crime was committed with the knowledge of its owner.

We note that the Algerian legislator has introduced some preventive measures taken in advance by the concerned services to avoid or detect cybercrimes under the aforementioned Law No. 09-04, which contains the rules for the prevention and combating of crimes related to information and communication technology, as article III of which stipulates that: "Subject to the legal provisions guaranteeing the confidentiality of correspondence and communications, the requirements of the protection of public order or the requirements of ongoing investigations or judicial investigations may, in accordance with the rules set forth in Code of Criminal Procedure In this law, technical arrangements are established for the monitoring of electronic communications, the timely collection and

recording of their content, and the conduct of search and seizure procedures within an information system."

The monitoring of electronic communications is an important measure, and article IV of Act No. 09-04 specifies the cases in which the use of electronic surveillance is permitted:

"- Prevention of acts characterized as crimes of terrorism, sabotage or crimes against the security of the State;

- In the event of information about a possible attack on an information system that threatens public order, national defense, state institutions or the national economy,

- for the requirements of investigations and judicial investigations, when it is difficult to reach the conclusion of the interests of ongoing research without resorting to electronic surveillance,

- In the context of the implementation of requests for international mutual judicial assistance...".

However, electronic surveillance may be carried out only with the written permission of the competent judicial authority.

Article V of the same Act authorizes the competent judicial authorities and judicial police officers to access the information system in the aforementioned cases for the purpose of searching, while article VI authorizes the seizure of data deemed useful by the authority conducting the search to be useful for detecting the crime or its perpetrator.

Electronic communication service providers have also been involved in the prevention of cybercrime by imposing on them some obligations such as the obligation to cooperate with the security services, the obligation to preserve data, the obligation to immediately withdraw content that can be accessed by others, and the commitment to develop technical arrangements to limit access to distributors that contain information that is contrary to public order and morals.

The Algerian legislature did well when it obligated electronic service providers to contribute to the prevention of information crimes as they are a link between the offender and the crime, as the offender may deliberately resort to using a computer in the information services center instead of his personal computer to commit the crime to shade the judicial bodies, so this procedure allows facilitating the process of accessing the identity of the offender.

Conclusion:

Through this study, we learned about a modern cybercrime phenomenon rampant in various countries of the world, represented by cyberbullying, the latter of which is classified as cybercrime because of the harm it carries to people as it may lead to harm to their physical safety. Although the Algerian legislature does not explicitly provide for this crime, it has imposed penalties against the perpetrators of cybercrimes, but they remain penalties that do not amount to deterrence compared to the seriousness of these crimes.

We therefore propose the following recommendations:

- It is advisable to explicitly include cyberbullying in the legal texts related to cybercrime, given the danger of this behavior to the lives of people, especially children.

- States must take strict measures to confront these crimes by imposing deterrent penalties against the perpetrators, as the penalties imposed on cybercriminals are not commensurate with the seriousness of this crime, which relates to the secrets of the person.

- Multiple international agreements must also be established on how to combat cybercrime as a cross-border crime, as international cooperation plays an effective role in combating these crimes.

- In addition to the need to rely on modern technical means in investigation and investigation procedures by training judicial officers on how to deal with this type of crime, and the formation of specialized teams in electronic investigation.

- It is also advisable to educate individuals about the seriousness of cybercrime, and urge them to avoid storing their personal photos through social networking sites, computers or smart devices and tablets, and not to download any program from an unknown source. - In addition to the need to educate parents to monitor their children and not to allow them to open accounts through social networking sites before reaching the legal age.

References:

1. ALAIN, B. (1996). *Internet: legal aspects.* France: Hermes.
2. AL-MALT, A. K. (2006). *Information Crimes.* Egypt: Dar Al-Fikr Al-Jamia.
3. Al-Sheikhi, M. M. (2019, March 28). *Cyberbullying*. Retrieved from https://www.new-educ.com/%D8%A7%D9%84%D8%AA%D9%86%D9%85%D8%B1-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A.
4. Brahimi, J. (2012). Combating Cybercrime in Algerian Legislation. *Critical Journal of Law and Political Science,Mouloud Mammeri Tizi Ouzou University, Algeria,*, 113-129.
5. DEVREZE, A. L. (2001). *IT & Internet Law.* France: Dalloz.
6. G. CHAMPY. (1988). *Computer Fraud Definition.* France: Dalloz.
7. GHANIA, B. (2015). *Cybercrime "A Comparative Study".* Algeria: Algerian House for Publishing and Distribution.
8. KARA, A. (2007). *Penal Protection of Informatics in Algerian Legislation.* Algeria: Dar Houma for Printing, Publishing and Distribution.
9. LINANT, A. H. (2002). *Practice of computer law.* France: Delmas.
10. Shawa, M. S. (1993). *The Information Revolution and its Implications for the Penal Code.* Egypt: Dar Al-Nahda Al-Arabiya.
11. SOUALMI, M. (2016, 05 02). the Supposed Element of Information Crime. *the Supposed Element of Information Crime*. ALGERIA, Faculty of Law and

Political Science, University of Biskra, Algeria: Faculty of Law and Political Science, University of Biskra.
12. TIEDEMANN, K. (1993). *Fraud and other business crimes commited usig electronic computers.* France: Dalloz.
13. YOUNES, P. B. (2004). *Crimes Arising from the Use of the Internet.* Egypt: Dar Al-Nahda Al-Arabiya.
14. YOUSSEF, A. (2009). *Information crimes on the internet.* Egypt: University Press.
15. ZAIDAN, Z. (2011). *Information Crime in Algerian and International Legislation.* Algeria: Dar El Houda.