



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

Cheifa Badiaa *

Amar Telidji University of Laghouat
Laboratory of Law and the Development of
Community
b.cheifa@lagh-univ.dz

KHATOUI MESSAOUD

Amar Telidji University of Laghouat
Laboratory of Law and the Development of
Community
me.khatoui@lagh-univ.dz

Received: 03/01 /2026

Accepted: 22/03 /2026

Published: 31/03 /2026

Abstract:

This study addresses the necessity of activating the principle of the universality of criminal law to combat cybercrimes under Algerian law. The research highlights the challenges Algeria faces in applying laws against cybercrimes amidst the rapid technological advancements and transnational electronic crimes. It explores how Algerian law can activate the principle of the universality of criminal law to address crimes that threaten digital security, such as hacking, espionage, and online fraud. The study also focuses on the importance of enhancing international cooperation and updating local legislation to align with global standards for combating cybercrimes. Ultimately, the study aims to provide recommendations on how to improve the effectiveness of the Algerian legal system in fighting digital crimes and ensuring justice in this area.

Keywords : Universality of criminal law , Cybercrimes , Combating electronic crimes , International cooperation, Combating online fraud, Digital securit

Introduction

In light of the massive developments accompanying globalization, several phenomena have emerged as an inevitable consequence, reflecting the darker aspects of globalization. One of the most prominent of these is the rise of transnational and global crimes, which demonstrate a close link between globalization and crime. Crime globalization has made significant strides through its reliance on technological advancements, making traditional crime control methods ineffective. Consequently, crimes have increased while the number of offenders apprehended has declined, leading to new opportunities for criminals to

* Corresponding author



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

evade justice. Among these crimes, cybercrime has become a major international challenge, prompting the global community to seek ways to combat its spread. This effort has led to the formulation of various international agreements and treaties emphasizing the need to adopt the universality principle as an additional judicial jurisdiction alongside traditional ones such as territorial, objective, and personal jurisdiction. Algeria, like other nations, has taken steps to address this global crime by enacting legal provisions aligned with international conventions. However, adapting national laws to international agreements is merely an initial step toward universalizing criminal law. Here is how you can write the objectives, importance, and problem of the study in English:

The importance of this study lies in:

1. **Filling the gap in Algerian law:**

1. The study addresses the challenges Algeria faces in combating cybercrimes due to outdated laws that do not fully account for modern technological threats.

1. **Global relevance:**

1. It highlights the need for international collaboration in addressing cybercrimes that transcend national borders and cannot be dealt with by any single country alone.

1. **Improving legal frameworks:**

1. The study aims to propose practical solutions for modernizing Algerian laws to effectively combat cybercrimes and ensure the protection of digital spaces.

1. **Contributing to global legal standards:**

1. By aligning Algeria's legal framework with international standards, the study contributes to global efforts to combat cybercrimes and promote justice.

Objectives of the Study

The objectives of this study are:

1. To examine the current state of Algerian law concerning cybercrimes and the challenges it faces.



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

1. To analyze how activating the principle of universality of criminal law can help Algeria address cybercrimes more effectively.

1. To assess the role of international cooperation in enhancing the effectiveness of the Algerian legal system in tackling digital crimes.

1. To propose recommendations for updating Algerian legal provisions and strengthening cooperation with international legal bodies.

Problem of the Study

The problem addressed by this study is:

- The difficulty of effectively addressing cybercrimes within the current Algerian legal framework, which is not fully equipped to deal with modern technological challenges.

- The challenge of prosecuting individuals involved in cybercrimes that span across borders, where national laws and jurisdictional issues complicate enforcement and cooperation.

- The need for Algeria to adopt a more proactive stance in combating digital crimes by aligning its laws with international standards and fostering greater global cooperation.

Chapter One: The Substantive Aspects of Global Crime and Cybercrime

The landscape of crime has undergone significant transformations with the advent of globalization and rapid technological advancements. Traditional forms of crime have expanded beyond national borders, giving rise to global crime, which encompasses a wide range of illicit activities that impact multiple countries. Among the most concerning and complex manifestations of global crime are cybercrimes, which are increasingly becoming a major threat to both individuals and nations.¹

Cybercrimes, which include hacking, data breaches, online fraud, and cyber terrorism, are unique in their ability to transcend geographical and jurisdictional boundaries. Unlike traditional crimes that are often confined to a specific location or country, cybercrimes exploit the interconnected nature of the digital world,

¹ Hanane Ouachene, *The Globalization of Criminal Law as a Protection Mechanism against Cybercrime* National Conference on Cybercrime, University of Biskra, 2015; Rahman Khalfi, *General Criminal Law*, Belqis Publishing House, Algeria, 2017.



allowing perpetrators to operate from anywhere and affecting victims worldwide. This chapter aims to explore the substantive aspects of global crime and cybercrime, focusing on their legal, social, and technological dimensions.²

Understanding the nature of these crimes is crucial for addressing them effectively. In this chapter, we will examine the various types of global crime, with a particular emphasis on cybercrime, and analyze the legal frameworks that have been developed to combat these threats. Additionally, we will explore the challenges countries face in dealing with cybercrimes and discuss the need for an integrated, global approach to law enforcement and legal cooperation. Through this examination, we aim to provide a deeper understanding of the evolving nature of global crime and the pressing need for international collaboration in addressing cyber threats.³

Section One: Definition and Characteristics of Global Crime and Cybercrime

In the interconnected world of the 21st century, crime has evolved beyond national and regional borders.

Global crime, as a broad concept, encompasses a range of illicit activities that affect multiple countries and often involve transnational criminal organizations. One of the most prominent and rapidly growing forms of global crime is cybercrime, which leverages digital technologies to commit criminal acts.⁴

As technology continues to advance, so too do the methods and sophistication of criminals who exploit the internet and digital infrastructure to perpetrate their crimes.⁵

This section will focus on defining global crime and cybercrime, while also examining the key characteristics that differentiate them from traditional forms of crime.

² Mahmoud Ahmed Abana, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa Publishing, Amman, 2009; Nahla Abdelkader Al-Moumni, *Cybercrimes*, Dar Al-Thaqafa Publishing, Amman, 2010.

³ Shawqi Yash Tamam & Aziza Shabri, "Activating the Universality Principle in Cybercrime Prosecution," *Judicial Jurisprudence Journal*, Issue No. 15, 2017; Shaikha Hussein Al-Zahrani, "International Cooperation in Combating Cyber Attacks," *Journal of Sharjah University*, 2020.

⁴ Younis Arab, *Computer and Internet Crimes*, Arab Publishers Union, Beirut, 2002; Brahimi Jamal, "Combating Cybercrime in Algerian Legislation," *Algerian Journal of Law and Political Science*, University of Mouloud Mammeri, 2016.

⁵ Adel Yusuf Abdul Nabi Al-Shakri, "Cybercrime and the Crisis of Criminal Legitimacy," *Kufa University Journal*, Iraq, 2008; Fareda Aidaoui, "Cybercrime in Algerian Legislation," *Algerian Journal of Economic and Legal Sciences*, n.d



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

By understanding the scope and nature of these crimes, it becomes easier to assess the challenges they pose to legal systems and law enforcement agencies worldwide.

Global crime, in general, can involve activities such as human trafficking, drug smuggling, and terrorism, while cybercrime includes offenses like hacking, identity theft, and online fraud.

We will explore how the digital age has given rise to new methods of committing crime and how these crimes often defy traditional legal frameworks.

The section will also highlight the impact of globalization on the rise of cybercrime, including the challenges of jurisdiction, enforcement, and the need for international cooperation.

Through a comprehensive understanding of these definitions and characteristics, we can better address the complexities of global crime and cybercrime in the modern world.

Definition of Global Crime

The term "global crime" is rarely found in legal studies. Instead, it is often referred to as transnational crime, cross-border crime, or international crime.⁶

Essentially, global crime predates modern history but has evolved significantly due to technological advancements in trade, transportation, and communication.⁷

These developments have greatly contributed to the rise of transnational crimes, which disregard national borders.⁸

Global crime is fundamentally a conventional crime that has been internationalized due to its impact on the international community.

⁶ Rahman Khalfi, *General Criminal Law*, Belqis Publishing House, Algeria, 2017; Sohaib Gazi Zamil, "Universal Jurisdiction as a Mechanism for Combating International Crime," *The Researcher's Journal for Legal and Political Studies*, n.d.

⁷ Hanane Ouachene, *The Globalization of Criminal Law as a Protection Mechanism against Cybercrime*, National Conference on Cybercrime, University of Biskra, 2015.

⁸ Ramadan Ibrahim Sayed Ahmed, "The Principle of Universal Jurisdiction in International Law," *Egypt Contemporary Journal*, 2017.



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

Because of its severity, nations collaborate to combat it by extending legal jurisdiction and penalizing such offenses beyond their own borders.⁹

Definition of Cybercrime

Cybercrime, like global crime, is surrounded by ambiguity.

The lack of a unified definition has led to various terminologies, such as information crime, computer crime, or internet crime¹⁰.

Some scholars define it broadly as any criminal act committed with the assistance of a computer or within a digital environment, while others define it narrowly as any unlawful act requiring significant knowledge of computer systems.¹¹

The Algerian legislator refers to it as "crimes affecting automated data processing systems" and has adopted the definition provided by international agreements on cybercrime. Law No. 09-04, which addresses crimes associated with information and communication technology, classifies cybercrime into two categories:

Crimes targeting automated data processing systems.

Crimes facilitated or committed using an information system or electronic communications network.¹²

Section Two: The Challenges of Prosecuting Cybercrime

Despite legislative efforts to address cybercrime, significant challenges remain in prosecuting these offenses:¹³

Jurisdictional Issues: Cybercrimes often transcend national borders, making it difficult to determine which country has the legal authority to prosecute offenders.¹⁴

⁹Shawqi Yash Tamam & Aziza Shabri, "Activating the Universality Principle in Cybercrime Prosecution," *Judicial Jurisprudence Journal*, Issue No. 15, 2017.

¹⁰Younis Arab, *Computer and Internet Crimes*, Arab Publishers Union, Beirut, 2002; Naila Adel Mohammed Farid, *Economic Computer Crimes*, Jabal Publications, 2002.

¹¹ Mahmoud Ahmed Abana, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa Publishing, Amman, 2009; Nahla Abdelkader Al-Moumni, *Cybercrimes*, Dar Al-Thaqafa Publishing, Amman, 2010.

¹² Algerian Penal Code, as amended by Law No. 09-04 of 25 February 2009, relating to offences connected with information and communication technologies; Arab Model Law on Cybercrime, 2003.

¹³ Brahimi Jamal, "Combating Cybercrime in Algerian Legislation," *Algerian Journal of Law and Political Science*, University of Mouloud Mammeri, Tizi Ouzou, 2016.



Evidence Collection: Digital evidence is volatile and can be easily altered or erased, complicating forensic investigations.

International Legal Disparities: Differences in cybercrime laws across countries hinder effective international cooperation.¹⁵

Weak Judicial Cooperation: Although agreements like the Budapest Convention exist, their implementation is often hindered by bureaucratic and legal complexities.¹⁶

Chapter Two: Procedural Aspects of Cybercrime Prosecution

As cybercrime continues to proliferate across the globe, the legal systems of various countries are confronted with unprecedented challenges in prosecuting these crimes. Unlike traditional crimes that are often localized and easier to investigate, cybercrimes involve sophisticated techniques that can span multiple jurisdictions, creating significant hurdles for law enforcement agencies and judicial systems. The prosecution of cybercrime requires a specialized approach that integrates both legal frameworks and technological expertise to effectively address the complexities of these offenses.

This chapter will explore the procedural aspects involved in the prosecution of cybercrimes, focusing on the unique challenges faced by authorities and the legal mechanisms available to prosecute these offenses. It will cover key aspects such as evidence collection, international cooperation, jurisdictional issues, and the role of digital forensics in building a case. Additionally, the chapter will examine how traditional procedural rules must be adapted or expanded to accommodate the digital nature of cybercrimes.

By understanding the procedural requirements and challenges involved in cybercrime prosecution, this chapter aims to highlight the need for specialized training for law enforcement, the importance of cross-border collaboration, and the integration of advanced technologies into the legal process. Through this analysis, we seek to provide insights into the evolving nature of criminal prosecution in the

¹⁴ Mahmoud Ahmed Abana, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa Publishing, Amman, 2009; Nahla Abdelkader Al-Moumni, *Cybercrimes*, Dar Al-Thaqafa Publishing, Amman, 2010.

¹⁵ Younis Arab, *Computer and Internet Crimes*, Arab Publishers Union, Beirut, 2002; Adel Yusuf Abdul Nabi Al-Shakri, "Cybercrime and the Crisis of Criminal Legitimacy," *Kufa University Journal*, Iraq, 2008.

¹⁶ Council of Europe, *Convention on Cybercrime (Budapest Convention)*, opened for signature on 23 November 2001; Shaikha Hussein Al-Zahrani, "International Cooperation in Combating Cyber Attacks," *Journal of Sharjah University*, 2020.



digital age and the need for innovative approaches to ensure justice in the fight against cybercrime.

Section One: International Agreements on Cybercrime

Budapest Convention (2001)

The Council of Europe adopted the Budapest Convention as the first international treaty specifically addressing cybercrime. The convention aims to:

Improve and reform measures to prevent and suppress cybercrime.¹⁷

Emphasize regional and international cooperation.

Balance fundamental human rights, freedom of expression, and privacy with the need for cybersecurity.

Standardize legislative measures to combat cybercrime.¹⁸

Arab Model Law on Cybercrime

Endorsed by the Arab Council of Interior Ministers in 2003, this law defines various cyber offenses and mandates jurisdiction over crimes committed wholly or partially outside a nation's territory if they affect its interests.¹⁹

However, it relies primarily on the principle of objective territoriality rather than universality, limiting its effectiveness in transnational cybercrime prosecution.²⁰

United Nations Efforts

The United Nations has played a significant role in combating cybercrime through various conferences, including the 1985 Milan Conference and the 1994 Rio de Janeiro Conference, which emphasized the need for a legal framework to address international cyber offenses.

¹⁷ Council of Europe, Convention on Cybercrime (Budapest Convention), opened for signature on 23 November 2001, Budapest.

¹⁸ Shaikha Hussein Al-Zahrani, "International Cooperation in Combating Cyber Attacks," Journal of Sharjah University, United Arab Emirates, 2020.

¹⁹ Arab Council of Interior Ministers, Arab Model Law on Cybercrime, adopted in 2003.

²⁰ Shawqi Yash Tamam & Aziza Shabri, "Activating the Universality Principle in Cybercrime Prosecution," Judicial Jurisprudence Journal, Issue No. 15, 2017.



Section Two: Jurisdictional Principles in Cybercrime Cases

Traditional Jurisdictional Principles

Territorial Principle: Applies to crimes committed within a country's borders

Personal Principle: Based on the nationality of the offender or victim.

Objective Principle: Applies when national interests ²¹are harmed regardless of the crime's location.

The Universality Principle in Cybercrime

Since cybercrime does not conform to traditional jurisdictional boundaries, the universality principle emerges as a crucial tool for prosecution. This principle allows states to prosecute cybercriminals regardless of where the crime was committed or the nationality of the offender.²²

The universality principle is grounded in:

The Geneva Conventions (1949):

These treaties established the obligation of states to prosecute war criminals regardless of where the crimes occurred.²³

The UN Convention Against Torture (1984):

Mandates states to prosecute individuals accused of torture, reinforcing the universality principle.²⁴

The Rome Statute of the International Criminal Court: Introduced permanent international jurisdiction over serious crimes, further strengthening universal jurisdiction.²⁵

²¹ Hanane Ouachene, "The Globalization of Criminal Law as a Protection Mechanism against Cybercrime," National Conference on Cybercrime, University of Biskra, 2015.

²² Rahman Khalfi, General Criminal Law, Belqis Publishing House, Algeria, 2017; Ramadan Ibrahim Sayed Ahmed, "The Principle of Universal Jurisdiction in International Law," Egypt Contemporary Journal, 2017.

²³ Sohaib Gazi Zamil, "Universal Jurisdiction as a Mechanism for Combating International Crime," The Researcher's Journal for Legal and Political Studies, n.d.

²⁴ Geneva Conventions, adopted on 12 August 1949.

²⁵ United Nations, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, adopted on 10 December 1984.



Section Three: Challenges to Implementing the Universality Principle

The Council of Europe adopted the Budapest Convention as the first international treaty specifically addressing cybercrime. The Convention aims to improve and reform measures to prevent and suppress cybercrime, emphasize regional and international cooperation, balance fundamental human rights—such as freedom of expression and privacy—with the need for cybersecurity, and standardize legislative measures to combat cybercrime.²⁶

Arab Model Law on Cybercrime (with Footnotes)

Endorsed by the Arab Council of Interior Ministers in 2003, the Arab Model Law on Cybercrime defines various cyber offenses and establishes jurisdiction over crimes committed wholly or partially outside a state's territory if they affect its interests. However, the law relies primarily on the principle of objective territoriality rather than the universality principle, which limits its effectiveness in prosecuting transnational cybercrimes.²⁷

United Nations Efforts (with Footnotes)

The United Nations has played a significant role in combating cybercrime through several international conferences, including the Milan Conference of 1985 and the Rio de Janeiro Conference of 1994. These conferences emphasized the need to establish an international legal framework capable of addressing cyber offenses with transnational dimensions.²⁸

Section Two: Jurisdictional Principles in Cybercrime Cases

Traditional Jurisdictional Principles

The territorial principle applies to crimes committed within a state's borders, while the personal principle is based on the nationality of either the offender or the

²⁶ Council of Europe, Convention on Cybercrime (Budapest Convention), opened for signature on 23 November 2001, Budapest.

²⁷ Arab Council of Interior Ministers, Arab Model Law on Cybercrime, 2003; Brahimi Jamal, "Combating Cybercrime in Algerian Legislation," Algerian Journal of Law and Political Science, University of Mouloud Mammeri, 2016.

³ Shaikha Hussein Al-Zahrani, "International Cooperation in Combating Cyber Attacks," Journal of Sharjah University, United Arab Emirates, 2020.

⁴ Rahman Khalfi, General Criminal Law, Belqis Publishing House, Algeria, 2017; Sohaib Gazi Zamil, "Universal Jurisdiction as a Mechanism for Combating International Crime," The Researcher's Journal for Legal and Political Studies, n.d.

²⁸ Geneva Conventions, 1949; United Nations Convention Against Torture, 1984; United Nations, Rome Statute of the International Criminal Court, 1998.



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

victim. The objective principle applies when national interests are harmed, regardless of the location where the crime was committed.²⁹

The Universality Principle in Cybercrime (with Footnotes)

Since cybercrime does not conform to traditional jurisdictional boundaries, the universality principle emerges as a crucial legal mechanism for prosecution. This principle allows states to prosecute cybercriminals regardless of the place of commission of the crime or the nationality of the offender. The universality principle is grounded in several international legal instruments, including the Geneva Conventions of 1949, which established the obligation of states to prosecute war criminals irrespective of where crimes occurred, the United Nations Convention Against Torture of 1984, and the Rome Statute of the International Criminal Court, which introduced permanent international jurisdiction over serious crimes.³⁰

Challenges to Implementing Universal Jurisdiction in Cybercrime (with Footnotes)

Despite its importance, implementing universal jurisdiction in cybercrime cases faces several significant obstacles.

Conflicts of Laws: Different legal systems may simultaneously claim jurisdiction over the same cyber offense, leading to jurisdictional conflicts and procedural complications.⁶

Political Considerations: States may be reluctant to prosecute foreign nationals involved in cybercrimes due to political, diplomatic, or strategic concerns.

Legal Gaps: Many countries still lack specific domestic legislation that explicitly incorporates the universality principle into cybercrime prosecution, weakening its practical application.³¹

²⁹ Ramadan Ibrahim Sayed Ahmed, "The Principle of Universal Jurisdiction in International Law," *Egypt Contemporary Journal*, 2017.

³⁰ Shawqi Yash Tamam & Aziza Shabri, "Activating the Universality Principle in Cybercrime Prosecution," *Judicial Jurisprudence Journal*, Issue No. 15, 2017.

³¹ Adel Yusuf Abdul Nabi Al-Shakri, "Cybercrime and the Crisis of Criminal Legitimacy," *Kufa University Journal*, Iraq, 2008; Fareda Aidaoui, "Cybercrime in Algerian Legislation," *Algerian Journal of Economic and Legal Sciences*, n.d.



Conclusion

Cybercrime has emerged as one of the most serious global threats confronting contemporary legal systems, due to its transnational nature and its reliance on rapidly evolving digital technologies. Traditional principles of criminal law have proven—territorial, personal, and objective jurisdiction—namely territorial jurisdiction increasingly inadequate in addressing cyber offenses that transcend national borders and challenge conventional notions of sovereignty and legal authority.

In this context, the principle of the universality of criminal law appears as a fundamental and indispensable legal mechanism for combating cybercrime effectively. By allowing states to exercise jurisdiction over cyber offenses regardless of the place of commission or the nationality of the offender, universal jurisdiction contributes to closing jurisdictional gaps, preventing safe havens for cybercriminals, and reinforcing the global fight against impunity.

For Algeria, as for other states, adopting the universality principle in the cybercrime response represents not only a legal necessity but also a strategic response to the growing threats posed to digital security, economic stability, and individual rights. The effective application of this principle requires legislative coordination, and enhanced international cooperation in order to build a coherent and efficient legal framework capable of responding to the challenges of cyberspace.

Recommendations

Activating the principle of the universality of criminal law constitutes a crucial step toward strengthening global criminal justice, particularly in the face of transnational and technologically sophisticated crimes such as cybercrime. In light of the analysis conducted in this study, the following recommendations are proposed:

1. Legislative Reform and Harmonization

States, particularly Algeria, should amend their national criminal legislation to explicitly incorporate the principle of universal jurisdiction in relation to cybercrimes, expanding jurisdictional offenses. This includes clearly defining provisions, and aligning domestic laws with relevant international conventions and standards.

2. Strengthening International Judicial Cooperation



3. Effective prosecution of cybercrime requires robust international cooperation mechanisms, including mutual legal assistance, extradition time information sharing between judicial and law -agreements, and real mechanisms will enhance the ability enforcement authorities. Strengthening these .of states to investigate and prosecute cybercriminals across borders

3. Developing a Unified International Legal Framework

4. The international community should work toward establishing a legal framework for cybercrime prosecution, comprehensive and unified global under the auspices of international organizations such as the United Nations. Such a framework would reduce legal disparities between states and promote consistent .application of universal jurisdiction principles

Capacity Building and Specialized Training

Judicial authorities, prosecutors, and law enforcement personnel should receive specialized training in cybercrime investigation, digital evidence handling, o ensure the effective application and international criminal cooperation, in order t .of universal jurisdiction in practice

5 Balancing Security and Fundamental Rights

While expanding jurisdictional powers, states must ensure that the application of universal jurisdiction respects fundamental human rights, including due process, privacy, and freedom of expression, in accordance with international .shuman rights standard

References and Citations

International Agreements:

1. Budapest Convention (2001): Adopted by the Council of Europe as the first international treaty addressing cybercrime. Opened for signature in Budapest on November 23, 2001.

2. Geneva Conventions (1949): Established the obligation of states to prosecute war criminals regardless of where the crimes were committed.

3. United Nations Convention Against Torture (1984): Mandates states to prosecute individuals accused of torture, reinforcing the universality principle.



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

4. Rome Statute of the International Criminal Court (1998): Introduced permanent international jurisdiction over serious crimes, strengthening universal jurisdiction.

Legislative Texts:

1. Algerian Penal Code (as amended by Law No. 09-04 of 2009): Provides a legal framework for prosecuting cybercrimes and adapting national laws to international standards.

2. Arab Model Law on Cybercrime (2003): Endorsed by the Arab Council of Interior Ministers, defining various cyber offenses and outlining jurisdictional principles.

3. Algerian Law No. 15-04 (2015): Amendments to the penal code to further strengthen cybercrime legislation.

Books and Academic Studies:

1. Rahman Khalfi (2017), General Criminal Law, Belqis Publishing House, Algeria.

2. Mahmoud Ahmed Abana (2009), Computer Crimes and Their International Dimensions, Dar Al-Thaqafa Publishing, Jordan.

3. Naila Adel Mohammed Farid (2002), Economic Computer Crimes, Jabal Publications.

4. Nabil Saqr (Year Unknown), The Mediator in Explaining Financial Crimes, Al-Huda Publishing, Algeria.

5. Nahla Abdelkader Al-Moumni (2010), Cybercrimes, Dar Al-Thaqafa Publishing, Jordan.

6. Younis Arab (2002), Computer and Internet Crimes, Arab Publishers Union, Beirut.

Research Papers and Journal Articles:

1. Brahimi Jamal (2016), Combating Cybercrime in Algerian Legislation, Algerian Journal of Law and Political Science, University of Mouloud Mammeri, Tizi Ouzou.



The Necessity of Activating the Principle of Universality of Criminal Law to Address Cybercrimes in Algerian Law

2. Shawqi Yash Tamam & Aziza Shabri (2017), Activating the Universality Principle in Cybercrime Prosecution, Judicial Jurisprudence Journal, Issue 15.
3. Shaikha Hussein Al-Zahrani (2020), International Cooperation in Combating Cyber Attacks, Journal of Sharjah University, UAE.
4. Adel Yusuf Abdul Nabi Al-Shakri (2008), Cybercrime and the Crisis of Criminal Legitimacy, Kufa University Journal, Iraq.
5. Fareda Aidaoui (Year Unknown), Cybercrime in Algerian Legislation, Algerian Journal of Economic and Legal Sciences.

Conference Papers:

1. Hanane Ouachene (2015), Globalization of Criminal Law as a Protection Mechanism against Cybercrime, National Conference on Cybercrime, Biskra University.
2. Sohaib Gazi Zamil (Year Unknown), Universal Jurisdiction as a Mechanism for Combating International Crime, The Researcher's Journal for Legal and Political Studies.
3. Ramadan Ibrahim Sayed Ahmed (2017), The Principle of Universal Jurisdiction in International Law, Egypt Contemporary Journal.