
Cybercrime in Algerian law and Islamic Shari'ah

Dr. HALLABI Abdelkader

University of Ghardaia, Algeria

Email: aekhallabi@gmail.com

How to Cite:

HALLABI, A. (2026). Cybercrime in Algerian law and Islamic Shari'ah. *Art Law and Accounting Reporter*, 45(1), 18-29. <https://journalalar.org/index.php/online/article/view/30>

Art Law and Accounting Reporter © 2026

ALAR is open access and licensed under  CC BY-NC-ND 4.0

Submitted: 07 Jun 2025 | Revised: 02 Dec 2025 | Accepted: 07 Jan 2026

Abstract---In modern times, crimes have emerged that have sounded alarm bells, as they did not exist in earlier eras. This has led the West to underestimate the Islamic religion and accuse it of inadequacy on the grounds that no explicit rulings were articulated regarding such crimes, among them cybercrime. The latter has not been explicitly addressed by classical jurists, as it falls within the category of *nawāzil* (unprecedented contemporary issues). Accordingly, this study aims to clarify the reality of cybercrime, to examine the perspective of Islamic Sharī'ah toward it, to identify its constituent elements, and to elucidate the motives that drive the perpetrator to commit it, despite the fact that such perpetrators are often considered educated individuals possessing high intellectual capacities.

Keywords---cybercrime, cyberspace, Islamic Sharī'ah.

INTRODUCTION

Allah the Exalted has bestowed upon humanity the blessing of Islam, which is the complete and comprehensive religion, as stated in His saying: ﴿الْيَوْمَ أَكْمَلْتُ لَكُمْ دِينَكُمْ وَأَتَمَمْتُ عَلَيْكُمْ نِعْمَتِي وَرَضِيتُ لَكُمُ الْإِسْلَامَ دِينًا﴾¹

This represents the greatest of Allah's blessings upon this Ummah, insofar as Allah the Exalted has perfected their religion for them². However, the state of progress and prosperity in which humanity finds itself has led people to assume that they themselves are attaining perfection.

The modern electronic revolution has transformed society into a small village, rendering communication among individuals exceedingly easy. This form of communication has, in turn, generated a new type of crime, namely those referred to as electronic crimes or cybercrimes. Societies and states have consequently become entangled in confronting these modern crimes due to the difficulty of proving them and the challenge of identifying perpetrators, given that this type of crime is committed remotely and from disparate locations. The scene of the crime is the virtual or cyber space, and multiple perpetrators may be involved in a single offense, with each offender possibly residing in a different country. Espionage against states, interference in their privacy, access to their secrets, violations of their sovereignty, and the instigation of discord within them have thus become relatively easy, as this type of crime is not constrained by geographical boundaries. Accordingly, the following central problem may be posed: what is cybercrime and what are its characteristics? Moreover, does Islamic Sharī'ah have a position regarding it, given that this crime is considered among modern crimes and falls within the category of *nawāzil*?

¹ Surat al-Ma'idah, verse 3.

² *Mukhtaṣar Tafsir Ibn Kathir*, taḥqīq wa-ikhtīṣār Muḥammad 'Alī al-Ṣabūnī, Dar al-Qur'an al-Karīm, Beirut, Lebanon, 7th ed., vol. 3, p. 482, 1981, 1402 AH.

SECTION ONE: CYBERCRIME IN POSITIVE (STATUTORY) LEGISLATION

Crime, in its general form, is an ancient phenomenon; however, with the development of societies and the advancement of technology, new types of crimes have emerged in the modern era. These crimes are extremely serious and difficult to detect, as they leave no tangible physical traces at the level of the victim, and the perpetrator is often far removed from the crime scene. This is what is known as cybercrime.

First Requirement: The Concept Of Cybercrime

Following the emergence of the computer and the Internet, the notion of geography began to recede. By the end of the nineteenth century, communication networks expanded, and with them appeared a new form of crime associated with computers. Jurists initially differed in determining its designation, as it was variously termed *computer fraud*, crimes facilitated by the computer, crimes involving the misuse of the computer, then white-collar crimes³, and finally cybercrimes.

Among the comprehensive definitions of information crimes is the Belgian definition contained in the Belgian response to the questionnaire conducted by the Organisation for Economic Co-operation and Development (OCDE) in 1982 concerning information fraud, wherein the following definition was stated: "Any act or omission that constitutes an infringement upon tangible or intangible property, resulting, directly or indirectly, from the unlawful use of information technology." It is noteworthy that this definition reflects the distinctive technical character under which the most prominent forms of cybercrime fall. It also encompasses the specification of its moral element, namely criminal intent, and through this definition it is possible to address future technological developments⁴.

As for the Saudi system for combating information crimes, it defined such crimes in Article One as: "Any act committed involving the use of a computer or an information network in violation of the provisions of this system."⁵

Second Requirement: Cybercrime in Algerian Legislation

The criminalization of electronic crime was introduced in Chapter Three of the Algerian Penal Code, within Section Seven bis, under the title "Infringement of Automated Data Processing Systems," pursuant to Law No. 04-15 dated 10 November 2004, and Law No. 06-23 dated 20 December 2006.

Through an examination of these provisions, it can be concluded that the Algerian legislator did not provide a precisely formulated definition of cybercrime. Rather, it

³ Ma'ashi Samirah, *al-Jarimah al-Ma'lumatiyyah - Dirasah Taḥlīliyyah li-Mafhum al-Jarimah al-Ma'lumatiyyah*, *Majallat al-Mufakkir*, Jami'at Muḥammad Khayḍir Biskrah, no. 17, 2006, p. 400.

⁴ *SD Arabia*, <https://sdarabia.com>

⁵ Rawan bint 'Atiyyat Allah al-Ṣaḥafi, *al-Majallah al-Ilktruniyyah al-Muta'addidat al-Takhaṣṣusāt*, no. 24, May 2020, p. 9.

considered all crimes infringing information systems as electronic crimes. According to the legislator's conception, the offenses stipulated in the aforementioned laws are regarded as cybercrimes.

1. The Crime of Unauthorized Access or Entry

Article 394 bis stipulates: "Any person who, by fraudulent means, enters or remains in all or part of an automated data processing system, or attempts to do so, shall be punished by imprisonment and a fine. The penalty shall be doubled if such acts result in the deletion or alteration of the system's data, or if the aforementioned acts cause the disruption of the functioning of the system." The legislator criminalized the attempt to commit this offense through the phrase "or attempts to do so."⁶

2. The Crime of Information Forgery

Article 394 bis 1 provides: "Any person who, by fraudulent means, inputs data into an automated data processing system, or deletes or modifies, by fraudulent means, the data contained therein, shall be punished by imprisonment and a fine."

3. The Crime of Damaging and Destroying Data

Article 394 bis 1 states: "Any person who, by fraudulent means, inputs data into an automated data processing system, or deletes, by fraudulent means, the data contained therein, shall be punished by imprisonment or a fine."

4. The Crime of Appropriation of Data

Article 394 bis 2 stipulates: "Any person who intentionally and by fraudulent means designs, searches for, collects, provides, publishes, or trades in stored or processed data, or correspondence transmitted through an information system, or who possesses, discloses, publishes, or uses for any purpose whatsoever data obtained from one of the crimes stipulated in this section."

5. The Crime of Information Fraud

This crime is stipulated in Article 394 bis 2, which provides: "Any person who, by fraudulent means, designs, searches for, collects, provides, publishes, or trades in stored or processed data, or correspondence transmitted through an information system, shall be punished by imprisonment and a fine."

6. Internet Activities Constituting Content-Related Crimes and Acts Affecting Others

Article 394 bis 2 criminalizes acts of possession, disclosure, publication, and use, regardless of the purpose of such acts, when they concern data obtained from one of the crimes set forth in Section Seven bis of the Penal Code, for purposes such as

⁶ Amal Qarah, *al-Ḥimayah al-Jaza'iyyah lil-Ma'lumatīyah fi al-Tashri' al-Jaza'iri*, 1st ed., Dar Huma, p. 99.

unfair competition, espionage, terrorism, incitement to immorality, and all other unlawful acts. The provisions prescribe penalties of imprisonment and fines, in addition to supplementary penalties, including the closure of premises associated with the commission of the crime.

Third Requirement: The Elements of Cybercrime

The Material Element

Crime in general constitutes a manifestation of criminal conduct that reflects the criminal intent of the offender. As for the material element, it represents the tangible aspect of the crime and possesses a material nature perceptible by the senses. It consists of the external activity emanating from the offender that causes harm to others and is punishable by law⁷. It is a voluntary conduct that results in a criminal outcome. In the case of cybercrime, the material element is realized through the perpetrator's commission of one of the following acts:

- ✓ Entering or remaining, by fraudulent means, in all or part of an automated data processing system, or attempting to do so, or deleting or altering the system's data, or disrupting the functioning of the system.
- ✓ Fraudulently inputting data into an automated data processing system, or deleting, modifying, damaging, or destroying data.
- ✓ Fraudulently designing, searching for, collecting, providing, publishing, or trading in stored data or correspondence, or possessing, disclosing, or using such data for any purpose whatsoever.

The Legal (Statutory) Element

The legal element of a crime is established by the existence of a legal text that prohibits the committed act and prescribes a penalty for it, in accordance with the juristic principle: "There is no crime and no punishment except by virtue of a legal text."⁸ Accordingly, if no text criminalizes a given conduct, it is deemed permissible so long as it does not result in harm. If harm does result, the act becomes criminalized pursuant to the relevant prohibitive provisions⁹. This element consists of the set of legal texts that define and criminalize such acts, which the Algerian legislator has enumerated and codified in Law No. 04-15 dated 10 November 2004 and Law No. 06-23 dated 20 December 2006.

⁷ Sa'īd Ṣalīḥ Shuqayṭ Najm al-Juburi, *al-Jara'im al-Irhabiyyah fi al-Qanun al-Jina'i*, Dar al-Jami'ah al-Jadidah, 2013, p. 156.

⁸ 'Abd al-Qadir 'Awda, *al-Tashri' al-Jina'i*, p. 16.

⁹ Rizq Muḥammad Ghazi Rashdi al-Gharayli, *al-Aḥkam al-Fiqhiyyah lil-Jara'im al-Iliktruniyyah al-Muta'alliqat bi-Isti'mal Shabakat al-Tawāṣul al-Ijtima'i: Dirasah Fiqhiyyah Maqāṣidiyyah*, MA thesis, Jami'at al-Azhar, Ghazza, 2017, p. 40.

The Moral (Mental) Element

The realization of a crime is not complete by the mere existence of its material and legal elements; rather, a third element is required, namely the moral element. The moral element is established through the internal intent concealed within the offender, and it is manifested in every material act carried out by the offender through¹⁰ the exercise of his or her will.

SECTION TWO : THE SHARI'AH FOUNDATIONS OF CYBERCRIMES

Intrusion into cyberspace is a modern phenomenon; therefore, the jurists of Islamic Shari'ah in earlier eras did not address this type of crime. However, what distinguishes our noble Shari'ah is that it has not neglected any matter without providing guidance or addressing it, as our true religion is complete and comprehensive, keeping pace with all times and eras, and resolving problems that have proven intractable for Western thinkers. Accordingly, the question arises: how has Islamic Shari'ah addressed this crime?

First Requirement: In the Qur'an

The Lawgiver has prohibited crimes of all types, as crimes constitute transgressions against the rights of others. Allah the Exalted says: ﴿وَقَتُلُوا فِي سَبِيلِ اللَّهِ الَّذِينَ يُقْتُلُونَكُمْ وَلَا تَعْتَدُوا إِنَّ﴾¹¹ Crime is also considered an act of injustice, and injustice is prohibited. Allah the Exalted says: ﴿وَلَا تَحْسَبَنَّ اللَّهَ غَافِلًا عَمَّا يَعْمَلُ الظَّالِمُونَ إِنَّمَا يُؤَخِّرُهُمْ لِيَوْمٍ تَشْخَصُ فِيهِ﴾¹² (الْأَبْصَارُ)

Dr. Ahmad al-Sha'ir states that Islam is a religion of peace that combats injustice¹³. Crimes are regarded as one of the manifestations of corruption on earth, as Allah the Exalted says: ﴿مَنْ قَتَلَ نَفْسًا بِغَيْرِ نَفْسٍ أَوْ فَسَادٍ فِي الْأَرْضِ فَكَأَنَّمَا قَتَلَ النَّاسَ جَمِيعًا﴾¹⁴ He also says: ﴿إِنَّمَا جَزَاءُ الَّذِينَ يُحَارِبُونَ اللَّهَ وَرَسُولَهُ وَيَسْعَوْنَ فِي الْأَرْضِ فَسَادًا﴾¹⁵

Cybercrime constitutes an infringement upon the rights of others through the hacking of their computers and the theft of information, research, and results attained by researchers, which amounts to an infringement of authors' rights. Among cybercrimes are also acts that constitute espionage against the state, through unauthorized access to its private accounts, the disclosure of its secrets, economy, and strategic weapons, the stirring of unrest among citizens, the spread of fear, the undermining of security, and the removal of tranquility from society. All of this is considered a form of corruption on earth, as stipulated in the Noble Qur'an.

¹⁰ Ahmad Busqī'ah, *al-Wajiz fi al-Qanun al-Jaza'i al-'Amm*, Dar Huma, 5th ed., 2007, p. 105.

¹¹ Surat al-Baqarah, verse 190.

¹² Surat Ibrahim, verse 42.

¹³ Al-Ittihad, <https://www.alittihad.ae/article/27410/2016/>

¹⁴ Surat al-Ma'idah, verse 32.

¹⁵ Surat al-Ma'idah, verse 33.

Noble Qur'ān and the honored Sunnah, we find indications of the appropriate punishment that serves to deter criminals.

This crime may be subsumed under the category of *hirābah*, insofar as it constitutes an infringement upon the rights of others and the infliction of harm upon them. Allah the Exalted says: ﴿إِنَّمَا جَرَأُوا الَّذِينَ يُحَارِبُونَ اللَّهَ وَرَسُولَهُ وَيَسْعَوْنَ فِي الْأَرْضِ فَسَادًا أَنْ يُقَتَّلُوا أَوْ يُصَلَّبُوا أَوْ تُقَطَّعَ أَيْدِيهِمْ وَأَرْجُلُهُمْ مِّنْ خَلْفٍ أَوْ يُنْفَوْا مِنَ الْأَرْضِ ذَلِكَ لَهُمْ خِزْيٌ فِي الدُّنْيَا وَلَهُمْ فِي الْآخِرَةِ عَذَابٌ عَظِيمٌ﴾²⁰

It was narrated by 'Alī ibn 'Abd Allāh, who said: Sufyān narrated to us; Abū al-Zinād narrated to us, from al-A'raj, from Abū Hurayrah, who said: Abū al-Qāsim (PHPD) said: «لَوْ أَنَّ امْرَأً أَطْلَعَ عَلَيْكَ بِغَيْرِ إِذْنٍ فَخَذَفْتَهُ بِحَصَاةٍ فَفَقَأَتْ عَيْنَهُ، لَمْ يَكُنْ عَلَيْكَ جُنَاحٌ»²¹.

From this, it follows that spying on others and pursuing their secrets are considered criminal acts from the perspective of Islamic Shari'ah.

Muḥammad used to say: The Messenger of Allah (PHPD) spoke the truth; that was the case, saying: "Have I conveyed (the message)?" twice.

It is narrated on the authority of Abū Hurayrah, from the Prophet (PHPD), that he said: «لَعَنَ اللَّهُ السَّارِقَ، يَسْرِقُ الْبَيْضَةَ فَتُقَطَّعُ يَدُهُ، وَيَسْرِقُ الْحَبْلَ فَتُقَطَّعُ يَدُهُ».

Theft may pertain to tangible matters, such as the theft of wealth; however, in the contemporary era there exists another form of theft, namely the theft of intellectual and practical effort of individuals—especially scholars and intellectuals—which is referred to in positive law as intellectual property.

Third Requirement: The Characteristics of Cybercrime, Its Motives, and Its Prevention

Empirical reality confirms that the Italian mafia succeeded in using intelligent software through which it was able to transform its private documents into meaningless characters that could not be deciphered except by the organization itself. Likewise²², the Russian mafia employed university professors and certain men of science, offering them attractive remuneration, and utilized them to penetrate the systems of a number of major companies and banks²³.

²⁰ Surat al-Ma'idah, verse 32.

²¹ *Ṣaḥīḥ al-Bukhari*, Kitab al-Diyat, Bab man ittala'a fi bayt qawm fa-faqa'u 'aynahu fa-la diyata lahu, hadith no. 6902, p. 9.

²² Ilham Sa'ad, *al-Ta'sil al-Qanuni li-Zahirat al-Ijram al-Munazzam fi al-Tashri' al-Duwali wa-al-Waṭani*, Dar Balqis, Algeria, p. 29.

²³ Ibid., p. 30.

First: Characteristics of Cybercrime

Crimes vary according to their objectives. There are crimes that target human life, such as murder; crimes that aim at the acquisition of wealth, such as theft; and crimes that target honor and reputation. Each crime possesses characteristics and features that distinguish it from others. Accordingly, it is necessary to identify the specific characteristics of cybercrime under consideration.

1. A Specialized and "Soft" Crime

Cybercrime is considered a specialized crime, as its perpetrator is not an ordinary criminal; rather, he is characterized by exceptional intelligence, extensive experience, and a high level of technical and technological skill, particularly in the use of computers and continuous interaction with the Internet. As for its "soft" nature, this crime is carried out without physical exertion; a single click of a computer button may suffice to accomplish it.

2. A Transnational Crime

The Internet has transcended all geographical borders between states and has rendered the world akin to a single village in which communication among individuals and groups is easy. Consequently, cybercrime has become one of the crimes that transcend geographical boundaries and has thereby acquired an international character.

3. Difficulty of Proof

One of the most salient features of the perpetrator in this type of crime is that he possesses sharp intelligence not typically found among conventional criminals, as such offenders often leave no traces that may lead to their identification²⁴. Cybercrime is thus considered among the most difficult crimes to prove, as it is a "clean" crime that leaves no tangible physical traces, unlike murder and other traditional crimes. Moreover, due to the spatial distance between the offender and the victim, evidentiary difficulties are further compounded. This crime is often committed within a very short time frame, sometimes measured in seconds, and proving it requires the availability of highly advanced devices and systems, as well as investigating judges who possess scientific competence in the fields of informatics and digital technologies.

Second: Motives of Cybercrime

Crimes are committed with the aim of achieving objectives that arise in the mind of the perpetrator. Thus, in the crime of murder, the offender's objective may be to conceal another crime, such as the violation of honor, or to exact revenge; in theft,

²⁴ Yusuf Khalil al-'Afifi, *al-Jara'im al-Iliktruniyyah fi al-Tashri' al-Filastini: Dirasah Tahliyyah Muqaranah*, MA thesis, al-Jami'ah al-Islamiyyah, Gaza, 2012, p. 19.

the objective is the acquisition of wealth. As for cybercrime—where the perpetrator is often far removed from the victim—the question arises as to the objective behind committing such a crime.

1. Material Motives

The perpetrator's objective in committing cybercrime may be the acquisition of money. The pursuit of financial gain is among the most prevalent and prominent motives, as the offender typically obtains material returns from this crime. Often, the perpetrator is experiencing financial hardship, which drives him to steal funds from the accounts of companies, banks, or individuals via the Internet and transfer them to his own account.

2. Inflicting Harm upon the Employer

In committing this crime, the offender may aim to sabotage information at the level of the company by using Internet networks and stealing data through unauthorized access to databases²⁵. This may be motivated by retaliation against the employer due to a dispute between them, or as a result of the employer's exploitation of the offender's intellectual capacity in exchange for meager financial compensation. This motive is considered among the most dangerous motives associated with this type of crime²⁶.

3. The Desire to Demonstrate Intellectual Superiority over Others

The age of perpetrators of cybercrime typically ranges between 18 and 45 years²⁷. The offender employs his skills in the use of computers or mobile phones and seeks to distinguish himself among his peers, demonstrating the superiority of his intellectual and cognitive abilities over others, including those responsible for designing programs intended to protect electronic websites and bank accounts. Accordingly, he attempts to penetrate these systems repeatedly, persisting without boredom or fatigue until his efforts ultimately succeed.

Third: Combating Cybercrime

Providing Anti-Spyware and Anti-Hacking Software

There exist numerous programs designed to combat spyware, whether at the level of individuals or wired and wireless networks, including the following:

- ✓ *Promiscan*, which is effective in detecting spyware programs.
- ✓ *GFI Sniffer Detector for LanGuard*, which protects network devices from malicious programs. In addition, it is essential to possess adequate knowledge

²⁵ Nurah al-Zu'bi, <http://akhbar-alkhaleej.com/news/article/1130006>

²⁶ Lina Mahdi, <https://e3arabi.com/?p=208249>

²⁷ Isra' Jibril Rashad Mar'i, *al-Jarimah al-Iliktruniyyah: al-Ahdaf, al-Asbab, Turuq al-Jarimah wa-Mu'alaqatuha*, *Majallat al-Dirasat wa-al-I'lam*, al-Markaz al-Dimuqrati al-'Arabi, no. 1, January 2018, p. 430.

regarding methods for removing spyware and hacking files from computer systems²⁸.

Encryption refers to the process of converting information into incomprehensible symbols, thereby rendering access to the information difficult for unauthorized individuals.

CONCLUSION

Traditional crimes have become relatively easy to detect and control their perpetrators. However, with the development of modern technology and contemporary means of communication, crimes have emerged that are difficult to control, among them cybercrimes. The origin of the term "cyber" is English (*cyber*), and it is closely associated with Internet networks, smartphones, and computers.

The cybercriminal is the individual who commits this type of crime. One of its defining characteristics is that the crime scene is remote, and it is often referred to as a crime of "white-collar offenders," as it involves neither bloodshed nor physical violence. The perpetrator's objective is typically the theft or sabotage of information in exchange for material gain, or the demonstration of his skill and intelligence in controlling computer systems and modern technologies before his peers. Cybercrime is also characterized as a transnational crime that is difficult to detect and investigate. It may result in the disruption of military systems and the control of modern weapons, given that these systems have become heavily dependent on technology. Cybercrime is often committed with the mere press of a button. Within Islamic Shari'ah, this crime falls under the category of *hirābah*, as it constitutes an infringement upon the rights of others and a form of corruption on earth.

States are therefore urged to develop programs that prevent the penetration of their information systems, to establish specialized research institutions in this field, and to motivate academics to exert greater efforts through conferences and scientific seminars in order to identify precise and effective means of combating such crimes.

Bibliographies

Primary Sources

- *Al-Qur'an Al-Karim*.
- *Ṣaḥīḥ al-Bukhari*.

²⁸ Muḥammad ibn 'Abd Allāh Al Fay' al-'Asiri, Ḥusayn ibn Aḥmad al-Shahri, *al-Irḥab al-Ilktruni wa-Ba'd al-Ṭuruq al-Ḥadithah li-Mukafa'atihi*, Markaz al-Buḥuth wa-al-Dirasat, Jami'at Nayif, 2012, p. 226.

Books

- 1- Mukhtaṣar Tafsir Ibn Kathir. Taḥqīq wa-ikhtīṣar Muḥammad ‘Alī al-Ṣabūnī. Dar al-Qur‘an al-Karīm, Beirut, Lebanon, 7th ed., 1981, 1402 AH.
- 2- Busqī‘ah, Aḥmad. *al-Wajiz fi al-Qanun al-Jaza‘i al-‘Amm*. Dar Huma, 5th ed., 2007.
- 3- Qarah, Amal. *al-Ḥimayah al-Jaza‘iyyah lil-Ma‘lumatīyah fi al-Tashri‘ al-Jaza‘iri*. Dar Huma, 1st ed.
- 4- Sa‘ad, Ilham. *al-Ta‘ṣil al-Qanuni li-Ḍahirat al-Ijram al-Munazzam fi al-Tashri‘ al-Duwali wa-al-Waṭani*. Dar Balqis, Algeria.
- 5- Shuqayṭ, Sa‘īd Ṣalīḥ; al-Jubūrī, Najm. *al-Jara‘im al-Irḥabiyyah fi al-Qanun al-Jina‘i*. Dar al-Jamī‘ah al-Jadidah, 2013.
- 6- ‘Awda, ‘Abd al-Qadīr. *al-Tashri‘ al-Jina‘i*.
- 7- al-‘Asīrī, Muḥammad ibn ‘Abd Allāh Al Fay‘; al-Shahri, Ḥusayn ibn Aḥmad. *al-Irḥab al-Iliktruni wa-Ba‘ḍ al-Ṭuruq al-Ḥadithah li-Mukafa‘atihi*. Markaz al-Buḥuth wa-al-Dirasat, Jamī‘at Nayif, 2012.

Academic Theses

- 1- Rizq, Muḥammad Ghazī Rashdī al-Gharaylī. *al-Aḥkam al-Fiqhiyyah lil-Jara‘im al-Iliktruniyyah al-Muta‘alliqat bi-Isti‘mal Shabakat al-Tawāṣul al-Ijtima‘i: Dirasah Fiqhiyyah Maqaṣidiyyah*. MA thesis, Jamī‘at al-Azhar, Gaza, 2017.
- 2- al-‘Afīfī, Yūsuf Khalīl. *al-Jara‘im al-Iliktruniyyah fi al-Tashri‘ al-Filastini: Dirasah Taḥlīliyyah Muqaranah*. MA thesis, al-Jamī‘ah al-Islamiyyah, Gaza, 2012.

Journal Articles

- 1- Ma‘ashi, Samīrah. *al-Jarimah al-Ma‘lumiyyah - Dirasah Taḥlīliyyah li-Mafhum al-Jarimah al-Ma‘lumiyyah*. *Majallat al-Mufakkir*, Jamī‘at Muḥammad Khayḍir Biskrah, no. 17, 2006.
- 2- Mar‘ī, Isrā‘ Jibrīl Rashad. *al-Jarimah al-Iliktruniyyah: al-Aḥdaf, al-Asbab, Ṭuruq al-Jarimah wa-Mu‘alajatuhā*. *Majallat al-Dirasat wa-al-I‘lam*, al-Markaz al-Dimuqrati al-‘Arabi, no. 1, January 2018.
- 3- Dawūd, ‘Abd al-‘Azīz ibn Fahd ibn Muḥammad. *al-Jarimah al-Saybaraniyyah: Dirasah Taṣiliyyah*. *Majallat al-Ijtihadat lil-Dirasat al-Qanuniyyah wa-al-Iqtisadiyyah*, vol. 9, no. 3, 2020.

Websites

- 1- Al-Ittihad. <https://www.alittihad.ae/article/27410/2016/>.
- 2- SD Arabia. <https://sdarabia.com>.
- 3- al-Zu‘bi, Nurah. <http://akhbar-alkhaleej.com/news/article/1130006>.
- 4- Mahdi, Lina. <https://e3arabi.com/?p=208249>