International Journal on Culture, History, and Religion
https://ijchr.net | eISSN: 3028-1318
Volume 7 Issue No. 1 | doi: https://doi.org/10.63931/ijchr.v7i1.492

Article

The Crime of Illegal Entry and Access to Official Information Systems and the Approach of Jordanian and Emirati Legislators to Confront it

Majed Al-Sarhan
Department of Law, Criminal Law, Zarqa University, Jordan-Alzarqa'a
Correspondence: majedfalah46@gmail.com

Abstract

The study outlines the elements of the crime of illegal entry and access to official information systems, whether they pertain to ministries, government agencies, public institutions, security, financial, or banking sectors, or companies owned or partially owned by any of these entities, or critical infrastructure.

It explained the approach of Jordanian and Emirati legislators in confronting this crime, whether the entry or access was solely for the purpose of viewing or for attacking the integrity of data and information on the information network, information technology, information system, or website belonging to those entities.

The study concluded that Jordanian and Emirati legislators did not limit themselves to criminalizing illegal entry or access but considered even authorized and legal entry or access to be criminal if the limits of authorization were exceeded or violated.

Keywords *crime, illegal entry, illegal access*

Suggested citation:
Al-Sarhan, M. (2025). The Crime of Illegal Entry and Access to Official Information Systems and the Approach of Jordanian and Emirati Legislators to Confront it. *International Journal on Culture, History, and Religion, 7*(1), 498-511. https://doi.org/10.63931/ijchr.v7i1.492

Introduction

All praise is due to Allah, and peace and blessings be upon the Messenger of Allah, his family, companions, and those who follow him.

Most legislations, including Jordanian law, have criminalized illegal access, considering it a crime that threatens the digital repository of secrets and violates individuals' electronic privacy. Illegal entry or access to confidential information or data, especially vital to national security, foreign relations, public safety, or the national economy, is considered more dangerous than other access or entry crimes. Therefore, both Jordanian and Emirati legislators have imposed stringent penalties, whether in fines or imprisonment, due to the potential threat this crime poses to national security. It involves a breach of state secrets and security, in addition to the considerable moral and financial losses that could result from the exposure of these secrets.

Significance of the Study

This study's significance lies in the subject matter's gravity and importance. The crime of illegal entry into official websites may target national security, foreign relations, public safety, or the national economy. Therefore, it is of utmost importance to clarify the dangers associated with this crime and explain the approaches of Jordanian and Emirati legislators in combating it.

Problem of the Study and Its Questions

Although both Jordanian and Emirati legislators have criminalized illegal entry in all its forms, they have imposed stricter penalties for illegal entry when the purpose is to access data or information not available to the public. Such data or information may concern national security, foreign relations, public safety, or the national economy. The crime of illegal entry may go beyond the mere intention of viewing to an assault on the integrity of data and information. The perpetrator may achieve the intended result of this assault or may fail to do so. In both cases, the act remains within the scope of criminalization. However, the penalty is harsher if the intended result is achieved than when the perpetrator fails to achieve their goal.

Therefore, the study addresses a central question: What is the crime of illegal entry and access to official websites, and what are the approaches of Jordanian and Emirati legislators in confronting it?

This central question branches into several sub-questions as follows:

1. What are the elements of the crime of illegal entry or access to an information network, information technology system, information system, or official website?
2. How have Jordanian and Emirati legislations addressed the crime of illegal entry or access to an information network, information technology system, information system, or official website?

Study Objectives

The study aimed to achieve several objectives, the most important of which are the following:

Clarifying the elements of the crime of illegal entry or access to an information network, information technology system, information system, or official website.

Demonstrating the legislative response to the crime of illegal entry or access to an information network, information technology system, information system, or official websites.

Contribution of this Study

None of the previous studies has addressed the crime of unauthorized access or entry to official information systems. Therefore, this study fills an important gap. Additionally, it is a comparative study of the latest Arab legislation regarding cybercrimes, namely, the Jordanian and Emirati legislations.

The Elements of the Crime of Unauthorized Access to Official Information Systems

The Material Element

The material element is considered the most important element in any crime, as legislation does not penalize a crime lacking it, for it is inconceivable for a crime to occur without it. The material element refers to the action or activity that leads to the criminal result, if there is a causal relationship between the act and the criminal result. It encompasses all physical assaults and violations of anything protected by law.

Technical activity is central to cybercrimes, as it is the key feature distinguishing the material element of cybercrimes from traditional crimes. Technical activity must involve cybercrimes, which require the user to possess specific skills to deal with technology. A conviction in these crimes necessitates knowledge of how to use electronic devices.

The Dubai Court of Cassation convicted an individual for hacking the information network of the Emirates Foundation, decrypting some devices, and

copying files. The Dubai Court of Cassation stated: "The defendant confessed to hacking the Emirates Foundation's internet network using programs to search for vulnerabilities that allowed him to obtain passwords for certain restricted websites that were off-limits to unauthorized employees. He decrypted some devices and copied some files, knowing the risks of doing so for unauthorized personnel. It constitutes an illegal use of the network, subjecting him to punishment.

In such cases, the result the perpetrator desired may or may not occur. The Jordanian and UAE legislators have imposed harsher penalties on the offender if the desired result is achieved, which will be discussed in Section Two of this study.

The Moral Element

The moral element of cybercrime consists of the offender's intent to cause the criminal result, which is punishable by law. The perpetrator of a cybercrime plans and prepares to commit the crime by acquiring electronic information by any means or hacking a computer network.

Intent can be either intentional (direct) or unintentional. Direct intent, such as an unlawful hack into a platform, includes the general criminal intent with both the knowledge and guilty will components. However, unintentional intent may apply when unauthorized access exceeds permissible access levels. Such cases could be considered as unintentional mistakes by the user.

Although the Jordanian legislator requires the presence of intent for unlawful access to non-governmental networks, systems, or information, this requirement is waived for government networks or information systems, likely to provide extra protection to them.

The Jordanian legislator also requires intent for unlawful access to government-owned websites. In contrast, the Emirati legislator does not require intent, whether the access is to non-governmental or government systems or websites, if the access is unlawful or violates licensing terms, or even if the stay is unauthorized.

Unlawful access to a government website is an intentional crime involving all forms of criminal conduct. The offender's intent is directed towards accessing information with the knowledge that such access is legally prohibited. The intent here involves the will to access confidential data or information, which is not available to the public and is significant, as it concerns national security, foreign relations, public safety, or the national economy.

However, one criticism of the Jordanian legislator is the failure to address the crime of unauthorized stay, which is considered a legislative gap despite its recentness.

In contrast, the Emirati legislator addressed the crime of unauthorized stay by defining hacking as unauthorized entry or entry in violation of licensing terms, or unauthorized stay within an information system, computer system, device operating system, machine, vehicle, or network.

Addressing the Crime of Unauthorized Access in Jordanian and Emirati Legislation

Addressing the Crime of Unauthorized Access in Jordanian Legislation

Penal Protection through Imposing Imprisonment and Fines

The Jordanian legislator has criminalized unauthorized access or entry, or exceeding or violating a permit for access to an information network, information technology system, or any part owned by a public authority, even if no impact is made on this network. The legislator has imposed a penalty of imprisonment for no less than six months for accessing an information network or technology system, or a minimum of four months if access is to a website. The maximum penalty can reach up to three years. In addition to imprisonment, the Jordanian legislator has imposed a fine ranging from a minimum of 2,500 Jordanian dinars to a maximum of 25,000 dinars. The judge has discretionary power to decide the minimum and maximum imprisonment limits or the fine.

The researcher observes a wide gap between the minimum and maximum limits of the penalty, whether related to imprisonment, with the difference between the two being six times, or the fine, where the difference is ten times. The researcher recommends that the Jordanian legislator reduce the gap between the minimum and maximum penalty limits.

Additionally, the Jordanian legislator has imposed a penalty of temporary labor for no less than three years, along with a fine ranging from 5,000 dinars to 25,000 dinars if the result intended by the perpetrator of unauthorized access is not achieved, such as modification or deletion. If the intended result is achieved, the penalty is temporary labor for no less than five years and a fine of 25,000 dinars.

Notably, the Jordanian legislator has imposed a fixed penalty for the fine if the perpetrator achieves the intended result by violating the integrity of data or information in any form. However, the judge has discretion to set the maximum penalty for temporary labor, which may reach up to 20 years, as stipulated in the Jordanian Penal Code.

Punishment for Attempting the Crime

The stage of attempting a crime is the one that follows the stages of thinking and preparation, and it is considered the first stage of execution. The Jordanian

legislator punishes the attempt to commit a crime when the crime is not completed for reasons beyond the offender's control. Attempting a crime is criminalized due to its inherent danger, even if no harm occurs.

The Jordanian legislator imposes the same punishment for attempting the crime of unauthorized access or entry if it pertains to ministries, government departments, public institutions, public or security institutions, financial or banking institutions, or companies owned or contributed to by these entities or critical infrastructure.

Similarly, the Jordanian legislator imposes the same punishment for attempting the crime of unauthorized access or entry if the intent is to harm the integrity of data or information in any form.

Punishment for the Original Offender and Other Participants in the Crime

Criminal liability in this crime does not extend only to the original offender but also includes any accomplices, instigators, and participants in the commission of the crime. It is outlined in Article (27) of the Jordanian Cybercrime Law, which states: *"Anyone who intentionally participates, intervenes, or instigates the commission of any of the crimes outlined in this law shall be punished with the same penalty as the original offender."* It is an explicit provision in Jordanian legislation, imposing responsibility on both the accomplices and instigators of the crime, with the same penalty as that of the original perpetrator".

Some argue that penalizing individuals other than the original offender, such as accomplices, participants, and instigators, is to deter unlawful access to information systems and provide additional protection for these systems.

Aggravating the Penalty When the Intended Result of the Offender Is Achieved

The intended result of the offender, such as alteration, deletion, or addition, may or may not be achieved. If the result is not achieved, the Jordanian legislator grants the judge discretionary power to impose a fine between 5,000 and 25,000 Jordanian Dinars and a penalty of temporary hard labor, with a minimum sentence of three years and a maximum of twenty years. The researcher believes that this discretionary power, with such a broad range for the penalty, may result in varying judicial outcomes. Therefore, the researcher recommends that the Jordanian legislator set an upper limit for this penalty, not exceeding five years, primarily when the intended result from the data integrity violation has not been achieved. The legislator has aggravated the penalty in cases where the intended result has been achieved by imposing a minimum sentence of five years for temporary hard labor. This means that the judge has discretionary power to impose a penalty exceeding the minimum

sentence, but is not authorized to reduce the minimum sentence to five years. As stipulated in the Jordanian Penal Code, the maximum penalty for temporary hard labor is capped at twenty years. As for the fine, the legislator has set a fixed penalty of 25,000 Jordanian Dinars, which is not subject to the judge's discretion.

Doubling the Penalty for Unlawful Access Under Certain Conditions

The Jordanian legislator has doubled the penalty for unlawful access, whether in terms of fines or custodial sentences, in cases where the offender is a public employee who exploits their position, job, or authority to commit this crime. In such cases, even if the employee was authorized to access the information system, but exceeded or violated the granted authorization, the penalty will be doubled. The penalty is also doubled in the case of repeat offenses. Furthermore, the penalty is also aggravated if the objective of committing the crime is to serve the interests of a foreign state or illegal organization, such as leaking information that affects the national security of Jordan.

Addressing the Crime of Unauthorized Access in UAE Legislation

Imposing Penalties of Imprisonment and Fines

The UAE legislator has set a penalty of temporary imprisonment in addition to a fine ranging from a minimum of two hundred thousand dirhams to a maximum of five hundred thousand dirhams for anyone who enters without authorization, violates licensing terms, or gains access illegally or remains unlawfully in an information system, computer, operating system of a device, machine, vehicle, network, or any equivalent belonging to state institutions, even if they do not harm the integrity of the data or information.

Furthermore, the UAE legislator has imposed a penalty of imprisonment for not less than five years and a fine of no less than a quarter of a million dirhams and no more than one and a half million dirhams if the integrity of the data and information is attacked. The result is achieved in any form, whether by causing damage, destruction, suspension, or disruption of an electronic website, information system, or information network, or the deletion, destruction, disclosure, alteration, copying, publishing, or re-publishing of any data or information, or the loss of confidentiality or any incident resulting from a cyber-attack.

Additionally, the legislator has set a penalty of imprisonment for not less than seven years and a fine not less than a quarter of a million dirhams and no more than one and a half million dirhams if the crime of unauthorized access is committed with the intent of obtaining data or information belonging to state institutions.

Enhancing Penalties Upon Achieving the Desired Outcome by the Offender

The UAE legislation follows a pattern of enhancing penalties if the intended result is achieved. It applies to both imprisonment and fines. If the result is achieved, the minimum penalty for imprisonment is set at five years, while the minimum sentence for temporary imprisonment is three years according to the UAE Penal Code. As for fines, the legislator increased the minimum fine by fifty thousand dirhams for the crime of unauthorized access without attacking the integrity of the data and information, and for the highest fine, it was increased by one million dirhams for the same crime.

Aggravating Circumstances for Unauthorized Access

The UAE legislator has deemed it an aggravating factor if an employee or someone authorized to perform a task requiring access to the information system commits a crime by violating or exceeding the authorization. In this case, the penalty is aggravated. The aggravating circumstance in UAE legislation is one that, if present in the crime, allows the judge to impose a penalty where, if the penalty is a fine, the court may double the maximum fine or impose imprisonment. If the penalty is imprisonment, the court may increase the maximum sentence, and in the case of temporary imprisonment, the penalty may extend to a maximum of fifteen years.

Similarities and Differences in Addressing the Crime of Unauthorized Access Between Jordanian and Emirati Legislation

Similarities in Addressing the Crime of Unauthorized Access Between Jordanian and Emirati Legislation

- *Agreement on Imposing Both Imprisonment and Fines for Unauthorized Access*

Both the Jordanian and Emirati legislations impose penalties of imprisonment and fines for the crime of unauthorized access. However, the penalty set by the Emirati legislation is harsher than that of the Jordanian legislation, both in terms of imprisonment and fines.

- *Increased Penalty in Case of Violation of Data and Information Integrity*

The Jordanian and Emirati legislations impose a stricter penalty in case of any data and information integrity violation. However, the Emirati legislation does not specify a situation where the offender intends to violate the data and information but fails to achieve the result.

- *Stricter Penalties in Certain Circumstances*

Both legislations impose stricter penalties for unauthorized access under certain circumstances. For example, suppose the offender is an employee or the crime was committed for the benefit of a foreign state or an illegal organization. In that case, both legislations provide for the aggravation of the penalty. However, the Jordanian legislators increased the penalty in case of repeated crimes, whereas the Emirati legislation does not have such a provision.

It is worth noting that the Jordanian legislator, in aggravating the penalty in these cases, does not grant the judge discretion, unlike the Emirati legislator, who allows the judge to impose the more severe penalty in cases of an aggravated circumstance.

Differences in Addressing the Crime of Unauthorized Access Between Jordanian and Emirati Legislation

Difference in Penalizing Attempts to Commit the Crime

Article (57) of the UAE Cybercrime and Anti-Rumors Law stipulates: *"An attempt to commit any of the crimes provided in this decree-law shall be punished by half the penalty prescribed for the completed crime."*

Upon reviewing the definition of a misdemeanor under the UAE Penal Code, as per Article 30) of the UAE Penal Code, it is a crime punishable by one or more of the following penalties:

Imprisonment.

A fine exceeding AED 10,000.

The penalty for temporary imprisonment falls under felonies as per the UAE Penal Code.

Therefore, the crime of unauthorized access, whether it involves violating the data and information belonging to state institutions or not, is classified as a felony under both scenarios in the Emirati legislation. However, the Emirati legislation does not specify the penalty for attempting a felony, only specifying the penalty for attempting a misdemeanor, which is half the penalty of the complete crime. It represents a legislative gap in the Emirati legislation, as it addresses the penalty for attempting a misdemeanor but does not specify the penalty for attempting a felony, even though the latter is more serious.

Thus, the researcher recommends that the Emirati legislator address this legislative gap and clarify the penalty for attempting the crime of unauthorized access related to state institutions.

Severity of Fines in the Emirati Legislation Compared to the Jordanian Legislation

Emirati legislation is stricter in imposing penalties than Jordanian legislation. The minimum fine for this crime in the Emirati legislation is AED 250,000, while the maximum fine in the Jordanian legislation is JOD 25,000. This means that the minimum fine in Emirati legislation is four times the maximum in Jordanian legislation.

Granting Discretionary Power to the Judge in the Emirati Legislation Compared to the Mandatory Penalty in the Jordanian Legislation for Certain Aggravating Circumstances

The Emirati legislator grants the judge discretionary power to impose an aggravated penalty when an aggravating circumstance is present. In contrast, the Jordanian legislator mandates the judge to impose an aggravated penalty in specific cases, such as when the offender is an employee, the crime was committed for the benefit of a foreign state or an illegal organization, or when the crime is repeated.

When increasing the penalty under these circumstances, it is noticeable that the Jordanian legislator does not grant the judge discretion, unlike the Emirati legislator, who leaves it to the judge to impose the more severe penalty when an aggravated circumstance applies.

Conclusions

Findings

- Unauthorized Access Crime refers to unauthorized entry or access to an information system, information technology, information network, or a website, whether this entry or access is complete or partial. It applies whether the purpose is to violate the integrity of data or information, or merely to access the system without permission.
- The Jordanian legislator has criminalized not only unauthorized access or entry but also considers access that exceeds the boundaries of authorized access a criminal act.
- The Emirati legislator has also criminalized staying unlawfully within a system.
- The Jordanian legislator has not criminalized unlawful stay, which is considered a shortcoming in Jordanian legislation despite its modernity.
- There is a significant gap in the minimum and maximum penalties regarding imprisonment or fines imposed for unauthorized access or entry without violating the integrity of data or information.
- The Emirati legislator is stricter compared to the Jordanian legislator in imposing penalties, whether related to deprivation of liberty (with the minimum penalty being three years, which is the maximum penalty for this crime in Jordanian law) or financial penalties (the minimum fine in

the UAE law exceeds the maximum fine in Jordanian law by 15,000 dinars).

- The Emirati legislation does not clarify the penalty for attempts to commit unauthorized access, which is considered a legislative flaw in Emirati law.
- The Jordanian legislator grants the judge discretionary power to impose a penalty of temporary hard labor when the offender intends to harm the integrity of data and information. The minimum term for this penalty is three years, while the maximum is twenty years. This discretionary power may lead to varying judicial rulings due to the wide range of possible penalties.
- Neither the Jordanian nor the Emirati legislations specify the means of entry or access, as the crime can be committed using any method. Any unauthorized access or entry method is sufficient to constitute the crime.
- The Emirati legislation lacks any provisions related to the criminal liability of accomplices, intermediaries, or instigators in the crime of unauthorized access.

Recommendations

- The researcher recommends that the Jordanian legislator reduce the gap between the minimum and maximum penalties, both concerning imprisonment and fines, imposed for the crime of unauthorized access or entry without violating the integrity of data or information.
- The researcher recommends that the Jordanian legislator set a maximum limit for the penalty of temporary hard labor in the case of unauthorized access or entry, if the offender intended to violate the integrity of data and information, so that it should not exceed five years, since the intended result of the offense against the integrity of data and information was not achieved.
- The researcher recommends that the Jordanian legislator criminalize unlawful stay to address the gap in Jordanian legislation on this issue, despite its modernity.
- The researcher recommends that the Emirati legislator address the legislative gap and clarify the penalty for attempts to commit the crime of unauthorized access to state institutions.
- The researcher recommends that the Jordanian and Emirati legislators maintain their position of not specifying methods of unauthorized access, as these methods may vary and evolve with the enormous technological advancements we witness in our contemporary world. Limiting these methods to specific ones could result in criminals using new methods not mentioned in the law escaping punishment.

- The researcher recommends that Emirati legislators include penalties for accomplices, intermediaries, and instigators in the crime of unauthorized access.

References

[1] Abdelqawi, A.-S. (2012). The digital court and cybercrime. Library of Law and Economics, Riyadh.

[2] Ahmed, R. A. (2025). Legal developments in the field of human rights in Jordan: An analytical study of national and analytical mechanisms. Al-Biruni Journal of Humanities and Social Sciences, 4, 11 June 2025. https://al-biruni-journal.jo/details_paper/24

[3] Al-Hudaifi, A. A. (2012). The crime of unauthorized access to websites in the Saudi system. International Law Research Journal, 10.

[4] Al-Jbour, M. (2012). The comprehensive guide to criminal law, general part. Dar Wail for Publishing, Amman.

[5] Al-Khais, A. J. (2011). Illegal use of computer systems from a penal law perspective—Damascus University Journal of Economic and Legal Sciences, 27(1).

[6] Al-Mansour, H. F. K. (2016). The crime of unlawful access to the information system and violation of its contents.

[7] Al-Marsafawi, H. S. (1972). Rules of criminal responsibility in Arab legislations. Institute of Research and Arab Studies, Cairo.

[8] Al-Meraghi, A. A. (2017). Cybercrime and the role of criminal law in limiting it. National Center for Legal Publications, Cairo.

[9] Al-Ojji, M. (2006). Criminal law. Al-Halabi Legal Publications, Beirut.

[10] Al-Qahouji, A. A. Q. (2004). Criminal protection mechanisms for automated reconciliation. Journal of Shari'a and Law, 2.

[11] Al-Rawashdeh, S., & Al-Hiyajneh, A. (2009). Combating cybercrime through criminalization and punishment: The English law model. Jordanian Journal of Law and Political Science, 1(3).

[12] Al-Sarraj, A. (n.d.). Explanation of the penal code.

[13] Al-Shawa, M. S. (1998). Information revolution and its impact on criminal law (2nd ed.). Dar Al-Nahda Al-Arabiya, Cairo.

[14] Al-Shennawi, M. (2008). Emerging fraud crimes. Dar Al-Kutub Al-Qanuniya, Cairo.

[15] Al-Shibli, M. (2019). The foundation of the theory of criminal participation in cybercrimes, according to the approach of the Jordanian legislator. Jordanian Journal of Applied Sciences, 21(1).

[16] Ananzeh, M. A. (2017). Criminal intent in cybercrimes (1st ed.). Dar Al-Ayyam is responsible for publishing and distribution in Amman.

[17] Azzam, Y. Q. (2025, June). The role of social media in shaping the social identity of Jordanian youth. Al-Biruni Journal of Humanities and Social Sciences, 4, 11 June 2025. https://al-biruni-journal.jo/details_paper/27

[18] Bakkar, H. H. M. (1988). The authority of the criminal judge in determining penalties and precautionary measures. Al-Dar Al-Jamahiriya (1st ed.).

[19] Batihi, N. (2019). The crime of unauthorized access or staying in an information system. Journal of Legal and Political Jurisprudence, 1(1).

[20] Bou Zeidi, E. (2022). The changing features of the legal element in business crimes. The Professor Researcher Journal for Legal and Political Studies, 7(2).

[21] Fikri, A. A. (2007). Information systems crimes. Dar Al-Jamiaa Al-Jadida, Alexandria.

[22] Hamoudi, N. (2015). Criminal protection of e-commerce [master's thesis, University of Algiers].

[23] Hassanein, S. A. (2023). The provisions of criminal responsibility for cybercrimes. Journal of Legal and Economic Studies, 9(3).

[24] Hossni, M. N. (1989). Explanation of criminal law, general part. Dar Al-Nahda Al-Arabiya, Cairo.

[25] Hussien, A. A. (2025, June). International commercial arbitration in Jordan: Legal framework and practical challenges. Al-Biruni Journal of Humanities and Social Sciences, 4, 11 June 2025. https://al-biruni-journal.jo/details_paper/25

[26] Ibitissem, M. (2011, September). Les infractions portant atteinte à la sécurité du système informatique d'une entreprise [master's thesis, University of Montreal].

[27] Jafar, R. M. M. (2017). Criminal intent in Internet and information-related crimes. Arab Studies Center for Publishing and Distribution, Egypt.

[28] Mohammad, L. J. (2016). Cybercrimes (1st ed.). Dar Khaled is responsible for publishing and distribution in Amman.

[29] Murtatha, A. (2025, June). Legislative transformations in the Jordanian penal code and their impact on criminal justice. Al-Biruni Journal of Humanities and Social Sciences, 4, 11 June 2025. https://al-biruni-journal.jo/details_paper/26

[30] Nawaiseh, A. I. (2016). The crime of unauthorized access is in the Arab cybercrime legislation. The Legal and Judicial Journal, 1. Ministry of Justice, Qatar.

[31] Pradel, J. (1990). Les infractions relatives à l'informatique. Revue Internationale de Droit Comparé, 42(42).

[32] Qatari, M. N. (2015). Legal issues in protecting information security. Sharjah Police Thought Journal, 24(93).

[33] Qoura, N. A. M. F. (2005). Cybercrimes in economics. Al-Halabi Legal Publications, Beirut.

[34] Ramadan, M. (2001). Criminal protection of e-commerce. Dar Al-Nahda Al-Arabiya, Cairo.

[35] Skicker, M. A. (n.d.). Cybercrime and how to combat it (1st ed.). Dar Al-Jumhuria, Egypt.

[36] Sufian, T. (2025, June). The role of the Great Arab Revolt in shaping Jordanian national identity. Al-Biruni Journal of Humanities and Social Sciences, 4, 11 June 2025. https://al-biruni-journal.jo/details_paper/31

[37] Yahia, J. M., & Al-Mana'a, O. A. (2010). Crimes of electronic information technology. Dar Al-Thaqafa, Amman.

[38] Za'tar, H. A. (2023). The legal issues of cross-border cybercrimes and ways to address them. Journal of Legal and Economic Research, 84.

Laws and Case References

[39] Appeal No. 230/2001, Dubai Court of Cassation, Dubai Public Prosecution, Scientific Seminar.

[40] Cass. Crim., 3 October 2007, Pourvoi No. 07-81045.

[41] Cour d'Appel de Paris, 5 April 1994.

[42] Egyptian Information Technology Crimes Law.

[43] Jordanian Cybercrime Law.

[44] Jordanian Penal Code, Law No. 16 of 1960 (and amendments).

[45] UAE Cybercrime and Anti-Rumors Law.

[46] UAE Penal Code, Law No. 31 of 2021.