ISSN: 3068-9503

Research Article | AI and Intelligent Systems: Engineering, Medicine & Society

Aggravating and Mitigating Circumstances and Their Role in Combating Cybercrimes: A Comparative Study Between the United Arab Emirates and Jordanian Legal Systems

Shamma Mohammed Al Shehhi*

Ph.D. candidate, Public law, College of Law, United Arab Emirates University Al Ain, United Arab Emirates

***Corresponding Author**
Shamma Mohammed Al Shehhi, Ph.D. candidate, Public law, College of Law, United Arab Emirates University Al Ain, United Arab Emirates.

Submitted: 2026, Sep 04; **Accepted:** 2026, Oct 07; **Published:** 2026, Oct 16

Citation: Al Shehhi, S. M. (2026). Aggravating and Mitigating Circumstances and Their Role in Combating Cybercrimes: A Comparative Study Between the United Arab Emirates and Jordanian Legal Systems. *AI Intell Sys Eng Med Society, 2*(3), 01-06.

1. Introduction

The primary aim of criminal punishment is to combat crime and preserve social stability. Criminal policy, therefore, is not static; it evolves in response to changing societal conditions, technological progress, and the varying nature of offenses. This evolution reflects the need to align penal systems with the broader goals of justice, deterrence, and rehabilitation. In this regard, legal frameworks have developed various mechanisms to ensure flexibility in sentencing, including aggravating and mitigating circumstances, exemption clauses, and the suspension or substitution of sentences.

Cybercrimes, in particular, represent a distinctive category of modern offenses that pose unique challenges to traditional legal systems. Their transnational nature, rapid spread, and reliance on sophisticated technologies make them especially difficult to predict, detect, and prevent. Consequently, many jurisdictions have tended toward intensifying penalties to deter such crimes and protect digital security. However, at the same time, some legal systems have recognized the need for mitigation or exemption in certain cases—specially to encourage the reporting of offenses or cooperation with investigative authorities.

Balancing between severity and leniency in cybercrime punishment has thus become a central issue in contemporary criminal policy. This research examines the approaches adopted by both the United Arab Emirates (UAE) and Jordanian legislators concerning the aggravation and mitigation of penalties in cybercrime offenses. The study aims to determine the extent to which each legal system has achieved an appropriate balance that fulfills the objectives of deterrence, justice, and the effective prevention of cyber offenses.

1.1. Research Problem

To what extent have the UAE and Jordanian legislators succeeded in achieving the required balance between aggravation and mitigation in addressing cybercrimes?

1.2. Significance of the Study

The significance of this study lies in the seriousness of cybercrimes, which require a specialized approach to address and confront their unique dangers. This, in turn, calls for a partial departure from the general rules of aggravation and mitigation to ensure the realization of punishment objectives and the effective confrontation of this type of crime.

2. Research Methodology

This study adopts both the analytical and comparative approaches. The provisions of UAE and Jordanian laws related to the aggravation and mitigation of penalties are analyzed and comparatively examined.

3. Structure of the Study

Based on the research problem and objectives, this study is divided into two main parts: the first part discusses aggravating circumstances and harsher punishment, while the second part examines mitigating circumstances and exemption from punishment.

3.1. Part One: Manifestations of Aggravated Punishment in Cybercrimes

Before examining the manifestations of aggravated penalties in cybercrimes, it is important to clarify the concept and purpose

of such penalties, as they reflect the legislator's intent to impose stricter punishment in response to greater danger or harm. After that, the study will review the circumstances recognized in UAE and Jordanian laws that justify aggravation, analyzing them in light of legislative objectives and criminal justice principles.

3.1.1 First: The Nature of Aggravated Penalties and Their Purpose

3.1.1.1. Definition of Aggravating Circumstances

The aggravating circumstance is defined as any condition or fact that, when accompanying a crime, increases its penalty, whether this aggravation changes the legal classification of the offense or keeps it unchanged. It is clear from this definition that aggravating circumstances merely increase the severity of the penalty without altering the legal classification of the crime.

3.1.1.2. The Purpose of Aggravated Penalties

Is linked to the surrounding circumstances of the crime, which may indicate greater harm or danger. Punishment aims to achieve deterrence proportionate to the crime's gravity; thus, it is reasonable to increase it when the offense occurs under more serious conditions than usual.

For example, in the case of theft, the penalty is aggravated when the crime is committed in a place of worship, a residence, or during the night. The reason for aggravating the punishment for theft from a residence lies in the victim's sense of security and privacy, as well as the sanctity of the home, which no one may enter without consent or legal authorization. When someone violates this sense of safety and stability, they rightfully deserve stricter punishment.

As for theft committed at night, the aggravation is due to the offender's deliberate choice to commit the crime when detection and prevention are more difficult. The darkness conceals the offender, facilitates escape, and limits the victim's ability to protect themselves or their property [1].

By analogy, the rationale for aggravating penalties in cybercrimes becomes evident. These crimes are often committed through innovative methods that victims cannot easily foresee. As technology advances, new techniques of fraud, hacking, and exploitation emerge. In practice, many offenders impersonate government institutions to obtain victims' personal data or money, and because most official and private transactions are now conducted electronically, it becomes difficult for individuals to distinguish between legitimate and fraudulent communications.

Moreover, offenders can commit cybercrimes effortlessly, sometimes from their homes, using fake accounts or specialized software that enables them to convincingly impersonate legitimate entities and threaten victims without revealing their identity. This makes their arrest extremely difficult. The ease of committing such offenses has led to a significant increase in cybercrime cases, which justifies the need for harsher penalties to deter offenders and reduce their spread.

In criminal doctrine, aggravating circumstances are used to distinguish more dangerous offenses from ordinary ones. These include cases involving vulnerable victims, the presence of specific criminal intent, or the abuse of authority or position in committing the crime [2].

3.1.2. Second: Aggravated Penalties in the UAE and Jordanian Laws

After outlining the concept and purpose of aggravation, this section reviews the general and specific reasons for stricter penalties in both UAE and Jordanian laws, assessing their approach to cybercrimes. Before that, some basic legal principles guiding punishment aggravation should be briefly noted.

3.1.2.1. Principles to Consider When Aggravating Penalties

Criminal punishment aims to achieve justice and deterrence, and its aggravation must be based on clear and justified purposes to avoid arbitrariness. Scholars have identified key principles to guide this process:

- Proportionality Between Punishment and the Offense: The penalty should match the gravity of the crime and the offender's degree of guilt. Any unjustified aggravation becomes arbitrary and inconsistent with justice [3].
- The Purpose of Punishment: Aggravation seeks to reinforce deterrence and justice. General deterrence warns society of the consequences of crime, while specific deterrence discourages the offender from reoffending. These goals can be achieved by increasing the severity of punishment or ensuring swift enforcement [4].

In the context of cybercrimes—often serious, widespread, and hard to detect—stricter penalties act as an effective preventive measure. Specific deterrence also aims to curb the offender's criminal inclination by making them realize the seriousness of their actions [5].

Finally, justice requires harsher penalties for those who commit crimes under aggravating circumstances, such as abusing authority or exploiting a victim's weakness, as these acts make the offense more severe and deserving of greater punishment.

3.1.2.2. Analysis of the UAE and Jordanian Legal Provisions on Aggravated Penalties in Cybercrimes

As the Penal Code serves as the main reference when no specific provisions exist, this analysis includes both the Cybercrime Laws and the relevant Penal Code provisions in the UAE and Jordan. Reviewing the UAE and Jordanian cybercrime and penal laws reveals the following points:

a) The Jordanian Penal Code does not provide general grounds for aggravation, limiting such circumstances to specific crimes. This restricts its scope as a comprehensive reference for determining aggravating conditions. In contrast, the UAE Penal Code incorporates both general and specific aggravating circumstances applicable to cybercrimes, alongside those explicitly provided in the Cybercrime Law. This dual framework ensures that, in the absence of a specific provision,

the Penal Code functions as a complementary source for determining the appropriate penalty.

b) Both the UAE (Article 60/1) and Jordanian (Article 28/1) Cybercrime Laws increase penalties when the offender exploits their employment, authority, or official capacity to commit a cybercrime. This legislative choice seeks to reinforce deterrence against those entrusted with public authority who misuse their position and access to confidential systems [6]. Moreover, the UAE legislator explicitly categorizes abuse of office as a general aggravating factor, reflecting a strong commitment to upholding public integrity and preventing the misuse of entrusted power.

c) Both laws further aggravate penalties (UAE Art. 60/3; Jordan Art. 28/4) when the offense is committed for the benefit of a foreign state, a terrorist organization, or an unlawful group. This demonstrates the legislator's intent to protect national security and state sovereignty, as such offenses—when facilitated through digital means—pose a grave threat to internal stability and public safety.

d) The Jordanian Cybercrime Law (Art. 28/2, 3) introduces two aggravating circumstances not found in the UAE legislation: cases involving multiple victims and cases of recidivism. Multiple victims signify broader harm and justify harsher punishment, particularly given the speed and magnitude with which cybercrimes can spread. Recidivism, or repeated criminal behavior, indicates a persistent criminal inclination that warrants increased severity of penalty. Although the UAE Cybercrime Law does not explicitly identify recidivism as an aggravating factor, the general provisions of its criminal procedure law implicitly treat it as such by excluding repeat offenders from leniency measures like electronic monitoring or reconciliation. This implicit exclusion operates as an indirect form of aggravation [7].

e) The UAE Cybercrime Law introduced an aggravating circumstance absent in Jordanian legislation—when a crime is committed using electronic means, even if not explicitly mentioned in the law [8]. This reflects the UAE legislator's awareness of emerging digital crimes and their potential risks, a proactive approach the Jordanian legislator could beneficially adopt.

f) The UAE Penal Code establishes two general aggravating factors applicable to cybercrimes [6]:

1. **Malicious Motive:** Which reveals a heightened degree of criminal intent and moral depravity. In cybercrime contexts, this includes manipulating victims through artificial intelligence, fabricated images or videos, and voice-altering technologies—conduct that demonstrates premeditation and thus warrants harsher penalties.
2. **Exploitation of Victim Vulnerability:** Encompassing the targeting of children, the elderly, or persons with disabilities. The broad and open-ended wording of the provision allows judicial discretion in interpreting "vulnerability," ensuring comprehensive protection for all victims and stricter penalties for offenders who exploit weakness or dependency in others.

3.1.3. Specific Aggravating Cases

By reviewing the UAE and Jordanian Cybercrime Laws, both impose stricter penalties in certain cases.

- **Similarities:**

a) Both aggravate penalties for crimes targeting the state, institutions, or critical infrastructure.

b) Both protect vulnerable groups such as children and People of Determination; the Jordanian law enhances penalties for exploiting them in pornography or incitement, while the UAE law focuses on child exploitation and abuse of victim weakness.

c) Both hold managers or legal entities liable for negligence in preventing cybercrimes.

d) Both impose strict penalties on crimes targeting financial and banking systems due to their major social and economic risks [9].

- **Differences:**

a) Scope of Aggravation in Political and National Security Crimes: The UAE law is broader in criminalizing acts that harm national unity, social peace, or offend state leaders.

b) Financial Penalties: The UAE law imposes significantly higher fines, reaching up to five million dirhams.

c) Handling Rumors and False News: The UAE law specifically criminalizes spreading rumors or false information during crises, with strict penalties for acts harming national unity, social peace, or state leaders [8].

- **Evaluation of Deterrence Effectiveness:**

a) In Terms of Proportionality

- Jordanian law clearly links aggravation to the criminal outcome, ensuring balance between crime and punishment.
- The UAE law is stricter in offenses affecting national security, enhancing general deterrence.

b) In Terms of Penalty Gradation

- Jordanian law shows a clear progression in penalties based on the seriousness and consequences of the act.
- The UAE law also applies a structured gradation, emphasizing the gravity and impact of the crime.

In conclusion, both legislations represent significant progress in combating cybercrimes, achieving strong deterrence while maintaining proportionality and gradation. Their effectiveness depends on each country's legal and social context, with potential to benefit from each other's strengths in future legislative development.

3.2. Part Two: Forms of Mitigation, Exemption, Substitution, or Suspension of Punishment in Cybercrimes

mitigating excuses, lenient circumstances, alternative sanctions, exemption, and suspension of sentence execution. It also evaluates how effective these measures are in combating cybercrimes and compares the approaches adopted by the UAE and Jordanian legislations.

3.2.1. First: Forms of Mitigation or Exemption from Punishment

Before discussing their impact on cybercrime control, it is important to understand what mitigating and exempting circumstances mean and why they exist.

1. Definition and Purpose of Mitigating and Exempting Circumstances

Mitigating circumstances are conditions that call for leniency and reduce punishment when linked to a crime. Mitigating excuses are similar but are clearly stated in the law and reduce the offender's responsibility and penalty. The main difference is that excuses are defined by legislation, while mitigating circumstances are determined by the judge based on the case details [1].

Both serve the same purpose—to make punishment fair and proportionate to the seriousness of the act and the offender's intent. They also consider the offender's personal situation or the surrounding conditions of the crime, allowing the court to apply justice with fairness and leniency [10].

We believe that, besides considering the offender's situation, mitigation can also help uncover crimes. Cybercrimes are often hard to detect because of advanced technology that hides the offender's identity. Therefore, reducing or waiving punishment in return for cooperation or reporting can encourage disclosure and help authorities expose other offenders. This balance between leniency and enforcement strengthens efforts to fight cybercrime effectively.

2. Mitigating and Exempting Excuses in UAE and Jordanian Legislation

A review of the UAE and Jordanian Penal Codes and Cybercrime Laws shows several forms of mitigation, summarized as follows:

In the UAE Penal Code, Article 97 lists general reasons for mitigation, such as the offender's young age, acting under non-malicious motives, or committing the crime as a result of serious provocation by the victim without justification. In contrast, the Jordanian Penal Code mentions only one excuse—serious provocation by the victim without legal justification.

All these excuses relate to the offender personally, reflecting circumstances like youth or emotional provocation that justify leniency. Although these reasons do not directly support combating cybercrimes, they do not contradict that goal either. By allowing courts to consider the offender's personal circumstances, such provisions uphold one of the main purposes of punishment—achieving justice and fairness within society.

As for the specific provisions under the Cybercrime Laws, the mitigating aspects can be summarized as follows:

a) Under the Jordanian Cybercrime Law No. (17) of 2023:

- **Article (29):** The penalty may be reduced by half if the offender provides information that helps uncover the crime or arrest other offenders. However, this benefit is limited to those who cooperate during the early investigation stages, before referral to the Public Prosecutor, which restricts its scope.

- **Article (38):** Grants the court discretion to determine jurisdiction if the crime has effects inside or outside the Kingdom. Mitigating aspect: This procedural flexibility ensures fair prosecution and trial by allowing application of the most appropriate procedural rules for the offender.

b) Under the UAE Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes:

- **Article (61):** Provides full exemption from punishment if the offender voluntarily reports the crime before the authorities become aware of it, or partial exemption if the report, after detection, leads to the arrest of other offenders or the recovery of tools, funds, or evidence. This tiered approach incentivizes cooperation, recognizing the difficulty of detecting cybercrimes and balancing deterrence with effective investigation.

- **Article (56):** States that confiscation shall not affect the rights of third parties acting in good faith. This exception protects innocent individuals from the consequences of cybercrimes, reinforces the principle of personal criminal responsibility, and reduces the indirect harm caused by such crimes.

3.2.2. Second: Suspension or Substitution of Penalties

This section examines two mechanisms aimed at reducing or delaying the enforcement of criminal penalties—suspension and substitution of punishment. The discussion first addresses suspension, followed by substitution.

1. Suspension of Penalties

Suspension of punishment refers to temporarily halting the enforcement of a sentence during a probationary period prescribed by law [2]. If the offender demonstrates good conduct during this period, the sentence is nullified; otherwise, it is enforced.

This measure applies to cases where the nature of the offense or the offender's circumstances justify leniency, such as minor offenses (e.g., insult or simple assault), good behavior, advanced age, deteriorating health, reconciliation, or waiver by the victim. The penalty must not exceed one year or be limited to a fine [6]. Such leniency reflects the legislator's intent to encourage rehabilitation while maintaining deterrence.

- **Main Question:** Have the UAE and Jordanian legislators adopted the suspension of punishment in cybercrime cases? Neither Cybercrime Law expressly grants courts the authority to suspend sentences in such cases. However, under the general provisions of criminal law in both jurisdictions, suspension may apply when its conditions are satisfied—including good conduct, reconciliation, or short imprisonment.

a) Under the UAE Cybercrime Law:

- **Article (2):** Unauthorized access or hacking—punishable by imprisonment from six months to one year.
- Article (19): Publishing or sharing online content contrary to media standards—punishable by imprisonment up to one year and a fine.

b) Under the Jordanian Cybercrime Law:

- **Article (3):** Unauthorized access to a network or information system—punishable by imprisonment from one week to three months.
- **Article (4):** Intentional unauthorized access or exceeding authorization—punishable by imprisonment from six months to three years.

Accordingly, suspension may be applied to certain cybercrimes under both laws. However, limiting its application to general provisions diminishes its effectiveness in combating cybercrime. It is therefore recommended that both the UAE and Jordanian legislators introduce a specific provision within their Cybercrime Laws granting courts explicit authority to suspend punishment when doing so serves the objectives of prevention and offender rehabilitation.

2. Substitution of Penalties

Due to the growing number of cases in courts and the legislators' aim to overcome the justice crisis—along with the influence of globalization and comparative systems such as the American plea-bargaining model—many legal frameworks have adopted reconciliatory approaches like penal orders, criminal settlements, and restorative mechanisms [11]. In addition, several jurisdictions have adopted alternative sanctions such as community service and electronic monitoring to reduce the negative effects of imprisonment while maintaining the goals of justice and deterrence.

- Main Question: To what extent are these alternatives effective in combating cybercrimes, and have the UAE and Jordanian legislators incorporated them within their legal frameworks?

From our perspective, such alternatives should not be viewed merely as lenient measures but as complementary tools that enhance judicial flexibility. Judges, through their discretionary authority, can choose to suspend, mitigate, exempt, or substitute punishment based on the circumstances of the case and the offender. Granting this flexibility ensures fairness, promotes rehabilitation and reintegration, and helps uncover cybercrimes by encouraging offenders to cooperate with authorities.

Regarding the question of whether alternative sanctions can be applied to cybercrimes, a review of both the UAE and Jordanian Cybercrime Laws shows no explicit provision addressing this issue. Therefore, it is necessary to refer to the general rules governing the scope and conditions for applying such measures.

Community Service and Electronic Monitoring are among the key alternatives. Community Service refers to obliging the convicted person to perform community work in an institution designated by the competent authority under specific conditions [6]. Electronic Monitoring refers to requiring the convicted person to undergo a rehabilitation program determined by the court to correct and improve their behavior [12].

a) Under the UAE Law: Community Service may be imposed in misdemeanor cases as an alternative to imprisonment not exceeding six months or to a fine [13]. The UAE Cybercrime Law punishes the offense of electronic begging with imprisonment not exceeding three months [8]. This indicates that community service may be applied to this offense. Given that this crime is not of a serious nature, community service appears appropriate, as it can help rehabilitate the offender, enhance responsibility, and prevent reoffending, thereby supporting the prevention of cybercrimes.

As for Electronic Monitoring, Article 391 of the Federal Criminal Procedure Law No. 38 of 2022 excludes its application to crimes punishable by death or life imprisonment, crimes against the internal or external security of the state, and crimes requiring deportation. Accordingly, there is no legal barrier to applying electronic monitoring to cybercrime offenders unless one of these exclusions applies. However, applying this measure to cybercrimes is not advisable, as serving a sentence at home may enable offenders to reoffend without detection. Moreover, monitoring devices only track movement, making it difficult to ensure compliance with instructions issued by the Public Prosecution.

b) In Jordanian Law: The application of either alternative requires that the sentence concern a misdemeanor and that the court assess, based on a social report, whether Community Service or Electronic Monitoring is appropriate, except in cases of recidivism [12]. Most crimes under the Jordanian Cybercrime Law are classified as misdemeanors, which makes it possible to apply either alternative where the court finds it suitable.

In conclusion, community service is supported as an effective alternative in some cases, as it fulfills the rehabilitative and reformative purposes of punishment and contributes to addressing crimes in general and cybercrimes in particular. However, electronic monitoring is not recommended for offenses committed through electronic means.

4. Conclusion

This study examined the impact of aggravating and mitigating punishment on combating cybercrimes. The analysis leads to the following conclusions:

1. The UAE legislator adopts a stricter approach, especially in crimes that affect national security, state leaders, or social peace, and often imposes severe financial penalties. The Jordanian legislator, however, takes a more flexible approach that focuses on proportionality and gradual punishment.
2. Electronic Monitoring is of limited effectiveness in cybercrimes. Offenders may continue committing crimes from home while under surveillance, which reduces the measure's deterrent value and may even increase the likelihood of reoffending.

3. Both the UAE and Jordanian legislators have aggravated penalties when the victim is in a vulnerable position, though they differ in approach. The UAE allows judicial discretion in interpreting "vulnerability" under the Federal Crimes and Penalties Law, which is a positive development that broadens legal protection.
4. Combating cybercrimes requires more than imposing harsher punishments. Authorities need mechanisms that help detect crimes early, along with measures that support offender rehabilitation and reintegration. These goals are achieved through mitigation, substitution of penalties, and suspension of sentence execution.

Based on these findings, the following recommendations are proposed for both the UAE and Jordanian legislators:

1. Amend UAE legislation to increase penalties in cases involving multiple victims or repeat offenses, ensuring proportionality between punishment and the seriousness of the act.
2. Encourage the Jordanian legislator to adopt the UAE's approach by imposing stricter penalties for crimes committed through electronic means, even if not explicitly mentioned in the law.
3. Include clear provisions allowing sentence suspension in cybercrime laws, conditional upon the offender providing information that helps uncover crimes or perpetrators, to grant judges broader discretion.
4. Expand the use of community service for minor cybercrimes as a reformative alternative to imprisonment, promoting rehabilitation and reintegration.
5. Exclude the application of electronic monitoring to cybercrimes, as offenders may exploit technology at home to recommit offenses, reducing the effectiveness of this measure.

References

1. Al-Bughal, Al-Sayyid Hassan. (1957). Aggravating and mitigating circumstances in criminal law: Doctrine and jurisprudence. Dar Al-Fikr Al-Hadeeth.
2. Hosni, Mahmoud Naguib. (2018). Explanation of the penal code – General part: The general theory of crime, punishment and preventive measures. Dar Al-Nahda Al-Arabiya.
3. Hamleeli, Sidi Mohamed, & Dali, Bashir. (2023). The principle of proportionality between guilt and punishment. African Journal of Legal and Political Studies, Ahmed Draya University.
4. Al Dhaheri, F. S. (2025). CRIMINAL SETTLEMENT IN THE UAE CRIMINAL PROCEDURE LAW.
5. Hosni, Mahmoud Naguib. (1967). Penal science. Dar Al-Nahda Al-Arabiya.
6. Federal Decree-Law No. 31 of 2021 Issuing the Crimes and Penalties Law.
7. Federal Decree-Law No. 38 of 2022 Promulgating the Criminal Procedures Law.
8. Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes.
9. Jordanian Cybercrime Law No. 17 of 2023.
10. Obaid, Hassanain Ibrahim Saleh. (1970). The general theory of mitigating circumstances: A comparative study. Dar Al-Nahda Al-Arabiya.
11. Abu Al-Wafa, Mohammed Abu Al-Wafa. (2022). Security and Law Journal. Dubai Police Academy.
12. Alshrouf, H., Issa, H. M. A., Siam, Y. A., & Kundakova, M. (2026). FROM SIGNATURE TO SENTENCE: CRIMINAL LIABILITY OF CORPORATE AUTHORIZED SIGNATORIES IN JORDANIAN LAW. Corporate Law & Governance Review, 8(3), 22.
13. UAE Ministry of Justice. (2021). Community service provisions.https://www.moj.gov.ae/ar/media-center/news/23/11/2021/--قباينانا-قماعلا-لدلو-ةلو-توضح-ةيعمتجملا-قمدخلامكاحأ.aspx

Copyright: *©2026 Shamma Mohammed Al Shehhi. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*