*Pakistan Journal of Criminology*
Vol. 16, No. 03, July—September 2024 (979-990)

# Electronic Extortion is a Crime, According to Jordan's Electronic Crimes Law No. 17 of 2023

Odai Turki Abed Alfattah Elfawair[1]

**Abstract**

In recent years, cyber extortion has emerged as one of Jordan's most concerning and prevalent cybercrimes. This has necessitated a multi-pronged approach to tackle the issue, including legal measures. The previous cybercrime law of 2015 lacked provisions to address cyber extortion and establish appropriate penalties for perpetrators. Article 415 of the Jordanian Penal Code served as its sole source of traditional legislation. Recognising this gap, the new 2022 cybercrime law introduced a specific provision, Article 18, to explicitly address cyber extortion. This study reveals that the Jordanian legislature has adopted a punitive approach towards cyber extortion. Article 18 prescribes a combination of imprisonment and a fine, aiming to eliminate ambiguity during legal proceedings. This ensures judges do not have the discretion to choose just one penalty based on personal judgement. Furthermore, the study offers recommendations for combating cyberextortion and curtailing its spread within Jordanian society. However, the provided excerpt does not include these recommendations.

**Keywords:** Cyber blackmail crime, cybercrime law, Jordan

## Introduction

The surge in illegal activities has coincided with significant advancements in communication technologies, the internet, and social media platforms (Curtis & Oxburgh, 2023). The emergence of cybercrime, which has seen a continuous rise in prevalence and a constant evolution in its methods, is particularly concerning. Cyber extortion crimes, specifically, stand out as a major threat due to their widespread nature and rapid proliferation (Salim & Dhafri, 2024).

In Jordan, statistics paint a concerning picture. During 2023, cyber extortion cases, encompassing both sexual and financial forms, reached a staggering 4688. This equates to an alarming 25.5% of the total number of cybercrimes registered in the same year (Jordanian Cybercrime Law, 2022). The detrimental effects of cyber extortion extend far beyond individual victims, posing a significant danger to families, society as a whole, and national security (Al Rousan et al., 2023).

Recognising the gravity of these novel crimes, many countries have taken action to adapt their legal frameworks to address and deter them (Alrousan &

[1]Doctor of Public Law, independent researcher, Jordan. Odai.alfaouri12@gmail.com

Faqir, 2023). Jordan is a pioneer in the Arab world when it comes to combating cybercrime through legislation (Abuanzeh & Søndergaard, 2023). The nation took its first step in 2010 with the passage of Interim Information Systems Crimes Law No. 30. Electronic Crimes Law No. 27 of 2015 followed this but was later repealed and replaced by Electronic Crimes Law No. 17 of 2023. This most recent legislation is considered the most stringent in Jordan, imposing harsher penalties on perpetrators of cybercrimes (Tubishat, 2024).

This research seeks to delve into the legal framework surrounding cyber extortion crimes in Jordan (Abuanzeh & Alshurideh, 2022). The objective is to assess the adequacy of Jordanian law for effectively confronting these crimes and curbing their spread. Furthermore, the research aims to propose recommendations that could contribute to reducing the prevalence of cyber extortion and mitigating its detrimental impact on Jordanian society and the nation as a whole.

**Problem Statement**

The rapid rise of electronic extortion crimes in various forms has become a pressing issue, raising serious concerns at both government and societal levels (Curtis & Oxburgh, 2023). A significant factor contributing to this problem appears to be the relative novelty of the legal text, specifically criminalising cyber extortion. While Electronic Crimes Law No. 17 of 2023 introduced Article 18 to address this issue, the previous legislation, Electronic Crimes Law No. 27 of 2015, lacked a dedicated framework for cyber extortion. Instead, it relied on the more general provisions of Article 415/2 of the Jordanian Penal Code (Abuanzeh & Alshurideh, 2022). The recent significant increase in cyber extortion crimes in Jordan is believed to be a result of a lack of specific and stringent penalties (Salim & Dhafri, 2024). Statistics for 2023, in particular, show a potentially worrying doubling or even quadrupling of these crimes compared to 2022 (Jordanian Cybercrime Law, 2022). This sharp rise serves as a stark alarm, underscoring the urgent need for effective measures to confront and prevent cyber extortion. Therefore, this study aims to examine the effectiveness of the legal framework established by Electronic Crimes Law No. 17 of 2023 (Abuanzeh & Søndergaard, 2023). The core question is whether these legal texts adequately address cyber extortion crimes, deter perpetrators, and contribute to a reduction in their prevalence and harmful impact on Jordanian society.

**Research objectives**

The goal was to fulfill the following research objectives: How does Article 18 of the Electronic Crimes Law No. 17 of 2023, a new legal provision, help Jordan combat cyber extortion crimes?

What were the shortcomings of the previous legislation, Electronic Crimes Law No. 27 of 2015, in dealing with cyber extortion, and how did it impact the prevalence of such crimes?

To what extent has Jordan's cyber extortion laws been effective in deterring perpetrators and reducing the prevalence of these crimes?

**Methodology**

We adopted a descriptive analytical approach to examine cyber extortion crimes and their legal countermeasures within the framework of Electronic Crimes Law No. 17 of 2023. This analysis extended to relevant legislation, including the Penal Code and the Code of Criminal Procedure. The research involved a thorough examination of these legal texts, followed by an analysis and critical evaluation.

**Literature Review**

The Legal Framework for The Crime of Electronic Extortion in Jordanian Law

Electronic extortion is a serious cybercrime that preys on an individual's privacy, causing immense harm to both the victim and society. Recognising this threat, Jordan established a legal framework within Electronic Crimes Law No. 17 of 2023 to address these crimes. This framework defines electronic extortion and outlines penalties for perpetrators.

**Definition of the Crime of Electronic Extortion**

Electronic extortion in Jordan involves threatening to expose private information, like photos or videos, to coerce a victim into specific actions. This analysis explores the definition within Jordan's legal framework. Article 18(a) of the Electronic Crimes Law No. 17 of 2023 criminalizes "blackmail or threats" using information technology to gain benefits. Notably, the law focuses on threats against the direct victim, unlike the broader protection offered by the Penal Code which extends to a victim's family.

However, the current legal framework presents areas for improvement. The interchangeable use of "threat" and "extortion" could benefit from clarification with "threat" being the sole term. Additionally, ambiguity exists regarding initiating prosecution. Electronic extortion's severity might warrant automatic action, or it could be treated as a Penal Code misdemeanour requiring a victim's complaint. Finally, the Electronic Crimes Law definition lacks details on methods of extortion compared to the Penal Code. A more comprehensive definition encompassing various means of committing this crime would be preferable. By highlighting these areas, the analysis emphasizes the need for clear

and unambiguous language in future Jordanian cybercrime laws.

**Photos of Cyber Extortion Crimes**

Electronic extortion, or cyberextortion, encompasses a diverse range of crimes with distinct motivations (Al Rousan et al., 2023). It can target victims for financial gain, sexual gratification, or political influence. In financial extortion, blackmailers threaten to expose sensitive information or damage data unless the victim pays a ransom (Curtis & Oxburgh, 2023). Hackers may also steal data and demand payment for its return (Abuanzeh & Alshurideh, 2022). Sexual extortion involves perpetrators collecting compromising photos or videos and threatening to expose them in exchange for sexual acts, often targeting vulnerable individuals on social media platforms (Salim & Dhafri, 2024; Al Rousan et al., 2023). Finally, political extortion targets influential figures to gain non-financial benefits like favors or sway over political outcomes. This is particularly prevalent during elections, where hackers may threaten to leak damaging information about candidates to influence the results (Alrousan & Faqir, 2023). These diverse forms of cyberextortion highlight the crime's complexity and far-reaching impact.

**Components of the Electronic Extortion Crime**

Cybercrime, and electronic extortion in particular, share a fundamental similarity with traditional crimes: the need for specific elements to be present for the act to be considered a complete offence. This allows law enforcement to effectively investigate and prosecute these crimes. These general elements, common across most crimes, are essential building blocks for any criminal case.

**The Legal Weaponry:**

Jordan's legal system has taken a significant leap forward in combating cyber extortion with the introduction of Electronic Crimes Law No. 17 of 2023. This law specifically addresses the previously neglected issue by introducing Article 18, which defines cyber extortion and prescribes penalties for offenders. This legislative advancement demonstrates Jordan's commitment to a constantly evolving legal system that protects its citizens from the ever-changing threats of the cyber world.

**The digital battlefield:**

In cyber extortion cases, the perpetrator's digital actions form the core of the criminal activity. These actions, facilitated by computers and the internet, typically involve threats or coercion designed to frighten victims into compliance with the extortionist's demands. Regardless of whether the extortion is successful or unsuccessful, the law concentrates on initiating criminal activity with criminal intent. Even attempted cyber extortion, though not explicitly addressed in the

legislation, may be punishable depending on the severity and duration of the threats. However, clear definitions around what constitutes "initiation" are crucial for legal proceedings, and connections to other crimes might influence sentencing decisions.

**The Mental Landscape:**

The moral element, also known as mens rea, delves into the mental state of the perpetrator in cyberextortion cases. The perpetrator must have knowingly used coercive tactics and intended to use threats to force victims into submission for conviction. While motivation is not a necessary element, it may hold some weight in certain situations. However, a lack of awareness regarding the act's illegality can potentially prevent cyber extortion charges, even if the perpetrator believes they have a legitimate claim against the victim. Ultimately, the crime of cyber extortion hinges on the act of threatening and coercing the victim, regardless of the perpetrator's motives.

Punitive policy and preventive measures to counter cyber extortion crimes

The Jordanian legislator has established specific penalties for cyber extortion within Electronic Crimes Law No. 17 of 2023 (Abuanzeh & Alshurideh, 2022). Article 18 outlines the punishments for those who commit this crime (Abuanzeh & Søndergaard, 2023). Article (18/A) combines imprisonment and fines as punishment for cyber extortion (Al Rousan et al., 2023). This avoids confusion in practical application and removes the judge's discretion to choose one or the other based on personal views (Alabdallat, 2020). It clarifies the legislator's intent and ensures consistent enforcement (Al-Billeh et al., 2023). If the threat involves committing a crime or attributing dishonourable or defamatory information to the victim, the penalty increases (Al-Hammouri et al., 2023). This is especially true when accompanied by a request (explicit or implicit) to perform or refrain from an action (Ali, 2023). This reflects the understanding that such extortion material can severely damage the victim's reputation and social standing (Alrousan & Faqir, 2023).

The article defines two types of requests: explicit (direct and clear) and implicit (indirect suggestions or hints) (Alshible, 2023). If the blackmailer's threat includes a request for an illegal act, it qualifies as cyberextortion, which is legally punishable (Amer & Al-Omar, 2023).

The researcher notes that while the penalty can be severe, the burden of proof lies with the prosecution (Bourtal, 2024). This means that clear and explicit evidence, not implicit suggestions, is required to convict the perpetrator of an explicit request (Curtis & Oxburgh, 2023). Article 18/A sets a minimum imprisonment period but leaves the upper limit open. This suggests that it be

classified as a misdemeanour with a penalty range of one to three years (Issa & Khater, 2023). However, Article 18/B allows for an increase to temporary hard labour, with a penalty range of three to twenty years based on the severity of the case (Khater, 2024). This inconsistency raises the question of whether cyber extortion should be classified as a felony or a misdemeanour (Mahafzah et al., 2023). Given the potential severity of the crime and the punishment range in Paragraph (B), it's conceivable that the initiation (attempt) of cyber extortion could be punishable here. Misdemeanours typically do not punish attempted crimes. The Jordanian legislator appears to differentiate between attempted and completed cyber extortion based on the seriousness of the offence (Salim & Dhafri, 2024).

The concept of initiation (attempt) might not be readily applicable to all electronic crimes, particularly those involving intangible elements like defamation or pornography (Tubishat, 2024). However, Al Rousan et al. (2023) consider cyber extortion a formal crime, completing it once the perpetrator initiates criminal activity (threats or extortion). The act itself is punishable, even if it fails to achieve the desired outcome.

This section delves into additional aspects of cyber extortion in Jordan beyond the main perpetrator's core penalties. The Jordanian law treats those who intentionally assist with, incite, or participate in cyber extortion as harshly as the main perpetrator (Article 27). This guarantees the accountability of all those involved, irrespective of their specific role in the crime. Similar to the Jordanian Penal Code, exemptions from punishment for cyber extortion apply in specific situations. For instance, Article 425/1 exempts crimes committed between spouses or close relatives as long as they rectify the damage caused. Additionally, Article 29 of the Cybercrime Law offers reduced penalties if the perpetrator reveals information about the crime or its perpetrators before prosecution, potentially leading to their arrest. This incentivizes cooperation from those involved in cyberextortion. For first-time offenders who demonstrate good conduct and a low risk of re-offending, the Jordanian Penal Code allows for suspended sentences in misdemeanour cases, which can include electronic extortion (Article 427 BIS). These suspensions typically last three years but can be revoked if the offender commits another crime during that period.

Repeat offenders face harsher punishments under Article 28 of the Cybercrime Law. If the crime involves electronic extortion, the penalties double. While the Cybercrime Law establishes its own penalties, Article 30 clarifies that these don't preclude even harsher punishments from other Jordanian laws. However, as of now, no such laws exist with stricter penalties for cyber extortion.

* Using a position of authority or employment. * Against multiple victims. *

Repeatedly. * For the benefit of a foreign state or illegal organisation.

Punishment policy for cyber extortion crimes in accordance with Jordanian law

Jordan's fight against cyber extortion requires a multi-faceted approach beyond just laws. Users must be cautious online; families must guide children towards safe internet habits; and government institutions must collaborate with NGOs. Public awareness campaigns, educational initiatives, and coordinated efforts to tackle cybercrime activities can create a safer online environment, minimising the threat of cyberextortion for Jordanians.

**Preventive measures for users**

Internet and social media users are the primary targets of cyberextortion crimes. Blackmailers threaten these victims, forcing them to act or refrain from acting in a certain way. Therefore, users have a significant role to play in protecting themselves. This includes fortifying their online accounts, being mindful of their online activity, and exercising caution when dealing with anonymous emails, suspicious friend requests, or recent interactions with strangers. These seemingly innocuous exchanges can be the first steps in a blackmailer's plan to lure a victim and commit cyberextortion.

Family-related preventive measures

The family plays a crucial role in combating cyber extortion crimes, with their efforts divided into two key areas:

- Instilling moral values: A healthy family environment is essential. By raising them with strong morals and a clear understanding of right and wrong, families can help prevent them from engaging in cybercrime, including extortion. This includes fostering social responsibility and a rejection of deviant behaviour in all its forms, especially online criminal activity.
- Cybersecurity Awareness: Families also play a vital role in educating their children about the dangers of the internet and social media. This includes raising awareness of cyberextortion and its tactics. Due to their lack of experience, young people, particularly girls, can be especially vulnerable. Open communication and guidance can help children recognise and avoid suspicious activity online, such as accessing inappropriate sites or engaging with strangers.

Preventive measures in relation to official and media institutions

Beyond individual vigilance, a collective effort is crucial to curbing cyberextortion. Here's how official institutions can contribute:

- Educational Institutions: Schools and universities can play a significant role in organising awareness campaigns on cyberextortion. School broadcasts, dedicated courses, or curriculum integration can all help students learn about

online safety and how to protect themselves from cybercrime.

- Religious Institutions: Religious leaders have a powerful voice in guiding their communities. By promoting moral values and highlighting the dangers of cyber extortion, they can help deter potential perpetrators and encourage ethical behaviour online.
- Media Institutions: The media plays a vital role in raising public awareness. By dedicating programmes to discussing cyber extortion, its methods, and its legal consequences, media outlets can educate the public and empower them to identify and avoid extortion attempts. These programmes can also feature legal and social experts offering guidance on how to address and prevent such crimes.

The participatory role of the Cybercrime Unit and civil society institutions

To effectively combat cyberextortion in Jordan, a multifaceted approach is required (Abuanzeh & Alshurideh, 2022). Beyond individual vigilance, institutions like the Electronic Crimes Unit play a crucial role (Abuanzeh & Søndergaard, 2023). This unit employs various strategies to raise public awareness: maintaining an informative Facebook page, conducting educational workshops at universities and schools, and collaborating with NGOs like the Jordan Women's Solidarity Institute Association and the Justice Centre for Legal Assistance (Al Rousan et al., 2023; Alabdallat, 2020). These combined efforts empower communities with the knowledge and resources to identify and avoid cyber extortion attempts, fostering a safer online environment for all (Al-Billeh et al., 2023).

**Findings**

The current cyber extortion law's narrow focus is a key limitation. While it protects victims from direct threats, it doesn't encompass situations where threats are directed toward relatives for honour-based blackmail or used to obtain illegal benefits for third parties. Jordan's Penal Code (Article 415) offers broader protection than this limited scope. This discrepancy reveals a gap in the legal framework's ability to address diverse cyberextortion scenarios. The wording of Article 18/A raises concerns about potential redundancy and ambiguity. It uses both "threat" and "extortion," which might lead to confusion during interpretation. Ideally, the law should solely focus on the concept of "threat," as extortion inherently involves using threats to coerce victims.

The law's silence on automatic prosecution of cyber extortion complaints is another noteworthy issue. This reliance on general Penal Code provisions regarding complaints might not be well-suited for cybercrime cases, potentially creating procedural hurdles. The combination of imprisonment and fines as the

sole punishment for cyber extortion deserves discussion. While intended as a deterrent, this approach might limit judicial discretion during sentencing. The rigidity of the punishment structure raises questions about its effectiveness in addressing the varying degrees of cyber extortion crimes. The significant rise in reported cyber extortion cases in Jordan, with a fourfold increase from 2022 to 2023, highlights the seriousness of this issue. The prevalence of this crime underscores its severe social, psychological, and security consequences for victims. This dramatic increase emphasises the urgent need for effective legal measures and robust enforcement strategies.

**Discussion**

The analysis of Jordan's legal framework for tackling cyber extortion reveals several key areas requiring attention and potential reform. Firstly, the law's limited scope presents a significant challenge. While it protects victims from direct threats, it doesn't encompass threats against relatives for honor-based blackmail or for acquiring illegal benefits for others (as cited in Abuanzeh & Alshurideh, 2022). This gap necessitates a more comprehensive framework that can effectively address the diverse forms and nuances of cyber extortion within Jordanian society. Secondly, the potentially redundant wording in Article 18/A, using both "threat" and "extortion," raises concerns about ambiguity (Abuanzeh & Søndergaard, 2023). Clear legal language is essential for effective implementation and enforcement. Streamlining terminology within the law should be considered to enhance its efficacy.

Another critical aspect is the absence of explicit provisions guaranteeing automatic prosecution of cyber extortion complaints. This reliance on general Penal Code provisions (Al Rousan et al., 2023) might not be well-suited for cybercrime cases, potentially leading to procedural challenges and hindering law enforcement. Furthermore, the combination of imprisonment and fines as the sole punishment, while aiming to deter crime, may inadvertently limit judicial discretion during sentencing (Khater, 2024). Balancing the severity of punishments with the flexibility needed for judges to consider individual circumstances is crucial for achieving justice and fairness in sentencing cyber extortion cases. Finally, the alarming rise in reported cyber extortion cases, with a fourfold increase from 2022 to 2023 (Salim & Dhafri, 2024), underscores the urgent need for effective measures. The prevalence and impact of cyber extortion extend beyond individual victims, posing significant social, psychological, and security consequences for Jordanian society as a whole (Tubishat, 2024). The analysis, in conclusion, identifies several areas for strengthening Jordan's legal framework to combat cyber extortion. These include expanding the law's scope,

clarifying legal terminology, streamlining complaint procedures, and ensuring appropriate sentencing measures. Addressing these shortcomings is essential for effectively combating cyber extortion and safeguarding the rights and security of Jordanian citizens in the digital age.

**Conclusion**

Cyberextortion has become a pervasive and dangerous threat, impacting personal freedom, finances, and the social fabric. While the international community and national authorities, such as Jordan's Cybercrimes Law No. 17 of 2023, have made significant efforts to combat this crime, reality shows a rise in cyber extortion alongside the growing use of the internet and digital services. This study aimed to explore the effectiveness of Jordan's national legislation in addressing cyber extortion. The researcher concludes that while Jordanian law provides a framework for punishment, a multifaceted approach is necessary for true progress.

This study investigated the effectiveness of Jordan's Cybercrime Law No. 17 of 2023 in addressing cyber extortion. Here's a summary of the key findings and recommendations:

**Recommendations**

- Refine Legal Wording: Revise Article 18/A to remove "extortion" and expand coverage to include threats against the victim's relatives, aligning with the Penal Code's broader protection.
- Invest in Investigation Teams: Enhance training and qualifications for personnel handling cybercrime investigations, particularly cyber extortion. This includes knowledge sharing and technical expert exchange with other countries, as well as the potential involvement of IT professionals during evidence collection and investigation.
- Strengthen International Cooperation: Foster stronger collaboration with Arab and regional authorities in combating cyber extortion through international and regional agreements.
- Encourage Reporting: Promote awareness campaigns urging all community members, including girls, to report threats and extortion attempts. This will help to deter perpetrators and reduce the spread of cyber extortion.
- Parental guidance: Families play a crucial role. Promote a proper upbringing with strong values, discourage deviant behaviours, and educate children, especially girls who may be more vulnerable, about online safety and dealing with potential extortionists on social media.

**References**

Abuanzeh, A. A., & Alshurideh, M. (2022, November). Cyberspace and Criminal Protection of Privacy in the Jordanian Legislation Under the Corona Pandemic: A Comparative Study. In *International Conference on Advanced Intelligent Systems and Informatics* (pp. 540-557). Cham: Springer International Publishing.

Abuanzeh, A., & Søndergaard, E. (2023). International Perspectives on Jordan's Legislation on Deprivation of Liberty Prior to Trial. *Arab Law Quarterly*, *1(aop)*, 1-18.

Al Rousan, S. M., Al Rousan, M. A., Al Rousan, R., & Al-Massarweh, S. S. (2023). Electronic Violence Against Women After Bridge Via Whatsapp Messages: An Analytical Study Based on the Reality of Jordanian Society. *Kurdish Studies*, *11*(3).

Alabdallat, W. I. M. (2020). Toward a mandatory public e-services in Jordan. *Cogent Business & Management*, *7*(1), 1727620.

Al-Billeh, T., Al-Khawaldah, M. H. A., Rabbo, K. K. A., AlQudah, Y. A., Al Ali, N., Al-Freihat, M., & Al-Khsielat, A. A. (2023). Guarantees for Questioning the Accused in the Jordanian Criminal Procedures. *Journal of Namibian Studies: History Politics Culture*, *34*, 2205-2225.

Al-Hammouri, A., Al-Billeh, T., Khashashneh, T., AL-Khalaileh, L., & Belghit, R. (2023). Penal Protection Contained in the Framework Law on Waste Management and Instructions for the Management of Electrical and Electronic Waste. *Pakistan Journal of Criminology*, *15*(4).

Al-Husban, M. M., & Al-Amaren, E. M. (2023). Jordan's Ability to Complete the Third Trade Policy Review at the WTO. *Global Trade and Customs Journal*, *18*(5).

Ali, A. (2023). Disaggregating Jordan's Syrian refugee response: the 'many hands' of the Jordanian state. *Mediterranean Politics*, *28*(2), 178-201.

Ali, A. M., & Mohammed, R. I. (2023). Money Laundering in the Digital Age: A Comparative Analysis of Electronic Means in Egypt, Jordan, the UAE and Iraq. *Pakistan Journal of Criminology*, *15*(4). 193-212

Al-Rai, A. F. K., & Alansari, M. A. A. A. (2024). The Legal Organization of Digital Drugs in Jordanian Criminal Legislation: Comparative Study. *Kurdish Studies*, *12*(2), 2243-2253.

Alrousan, E. M., & Faqir, R. S. (2023). Security forecasting for detecting organized crimes: new strategies and trends. *Journal of Namibian Studies: History Politics Culture*, *33*, 2820-2841.

Alshible, M. (2023). Legislative Confrontation of Cyberbullying in Jordanian Law. *Pakistan Journal of Criminology*, *15*(1). 17-30

Amer, T. B., & Al-Omar, M. I. A. (2023). The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

Bourtal, A. (2024). Proving Electronic Crime With Digital Evidence According to Algerian Legislation. *Revue Algérienne des Sciences Juridiques et Politiques, 61*(1), 46-60.

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal, 96*(4), 573-592.

Issa, H. A., & Khater, M. (2023). Distance Indecent Assault Crime in Jordanian Law Perspective. *Pakistan Journal of Criminology, 15*(1). 125-138

Khater, M. N. (2024). Criminalization of Forgery of Electronic Payment Cards in Jordanian Legislation. *Pakistan Journal of Criminology, 16*(01), 441-455.

Mahafzah, E., Alshible, M., & Garaibeh, Z. (2023). Legal protection of personal data in Jordan considering international standards. *Journal of Southwest Jiaotong University, 58*(1).

Salim, I. F., & Dhafri, M. R. (2024). The Criminal Agreement in Cybercrimes in Iraqi, Emirati, and Qatari Law. *Kurdish Studies, 12*(2), 4060-4087.

Tubishat, B. M. A. R. (2024). Electronic Commerce and Consumer Protection in Jordan: The Emerging Trend. *International Journal of Religion, 5*(2), 328-345.