

Criminal Liability for Cyber Blackmail through Social Media under Jordanian Law: An Analytical Study in Light of the Applicable Legislation and Recent Judicial Trends

Zaid Ibrahim Yousef Gharaibeh, Faculty of Law, Jadara University. Irbid, Jordan, gharaibehzaid8@gmail.com, z.garaibeh@jadara.edu.jo, <https://orcid.org/0000-0002-3143-7753>.

Abstract

The ability to blackmail over social media creates a major problem for one's privacy and dignity as well as for their reputation and mental stability. This paper analyzes the criminal liability related to cyberblackmail in Jordan. Specifically, it analyzes the new Cybercrime Law No. 17 of 2023 as it relates to the Jordanian Penal Code and recent developments in case law. This research analyzes the framework of the law, the judicial decisions, legal writings, pertinent international legal documents, and the crime of cyber blackmail. This research also analyzes the crime of cyberblackmail and the importance of electronic evidence in ascribing liability to a crime. The study shows that the 2023 Cybercrime law adds to Jordan's ability to legislate against cybercrimes. The real impact will come from the ability and will of the courts to interpret the law, the availability of electronic evidence, the development of digital forensics, the creation of legal norms and an international context for collaboration. This study identifies the challenges resulting from the digital anonymity of cybercriminals, artificial intelligence, and other rapidly changing technologies. This paper establishes the importance of balancing protecting the criminal victims of cyber blackmail and protecting the civil rights of law-abiding citizens.

Keywords: Cyber Blackmail; Criminal Liability; Social Media; Jordanian Cybercrime Law No. 17 of 2023; Jordanian Law; Electronic Evidence; Digital Forensics.

Introduction

The proliferation and acceleration of digital communication technologies have made social interaction easier and provided new avenues for crime. Cyber blackmail, in particular, has become a greater threat to privacy, dignity, reputation, and personal security. Unlike traditional blackmail, cyber blackmail uses social media and electronic communication technologies to extort victims by the threat of revealing or distributing private messages, photographs, videos, or other electronic materials to the public (Lahiani & Alkhazalah, 2023; Hussein & Abdul Manap, 2024). The growing use of social media has made blackmail easier and has provided offenders with additional means to use private and public data, victim contacts, and social media to carry out blackmail, threats, and coercive messaging (Alshehadeh et al., 2026). The legal and social problems posed by blackmail and the commercial and financial exploitation of social media have led various platforms of social media to become safer environments for the practice of blackmail and sextortion. The psychological, financial, and sexual exploitation of blackmail has originated from the social media environments of blackmail and extortion (Edwards & Hollely, 2023; AlGhanboosi et al., 2023). Cyberblackmail is further complicated by the anonymous identities of users, the reach and perpetual global nature of the Internet, and the jurisdictional fragmentation of victims, offenders, service providers, and the digital evidence. At the international level, the Budapest Convention on Cybercrime seeks to provide a significant mechanism to combat cybercrime and enhance international cooperation with access to electronic evidence.

In Jordan, the growth of digital services and social media has made it easier to commit crimes that involve information systems and electronic networks. One significant digital crime, especially in the case where the perpetrator uses digital content to threaten and/or blackmail the victim, is cyber blackmail. There are prevalent studies that describe the phenomenon of cyber blackmail and its negative repercussions in Jordan, especially one written by Jordanian prosecutors (Lahiani & Al-Khaza'leh, 2023). Consequently, Jordan passed the Cybercrime Law No. 17 of 2023, which broadens the scope of legal protection of crimes that are committed and caused by the use of information systems, electronic networks, and digital platforms (Al-Sarayreh, 2024). However, some important questions are still unresolved, such as the scope of criminal liability, the relationship between the Cybercrime Law and the Jordanian Penal Code, the evaluation of electronic communication as evidence, the attribution of offenders, and jurisdiction in cases of cross-border crime (Al-Billeh et al., 2024; Sachoulidou, 2024; Saleh & Ghnaimat, 2025). For the Jordanian cybercrime framework to work effectively, there is a need for judicial interpretation for determining the intent of a crime, assessing electronic evidence, and enforcing judicial norms. Cyber criminality has captured a sizable amount of literature. In contrast, the criminal liability of cyber blackmail that occurs on social media has been almost completely neglected in Jordanian legal scholarship after the enactment of Cybercrime Law No. 17 of 2023, especially in the context of the Jordanian Penal Code and recent developments in case law. To fill this research gap, this study examines the criminal liability for cyber blackmail. The study analyses applicable legislation and judicial developments. The study identifies several major legal and practical barriers. The study also recommends ways to strengthen the effectiveness of legislation and the judiciary to provide better legal protection to persons vulnerable to cyber blackmail.

Research Method

This study uses a doctrinal legal research method to investigate the legal issues concerning Jordanian law on the criminal liability of cyber blackmail via social media. It adopts an analytical approach to the Jordanian Cybercrime Law No. 17 of 2023, the Jordanian Penal Code, and other related laws on cyber evidence and criminal procedures. This study considers the elements of cyberblackmail, the framework for criminal liability, and the intersection of the Cybercrime Law and the general concepts of Jordanian criminal law. Moreover, the study evaluates available Jordanian court decisions and legal assessments on criminal liability, cyber evidence, criminal intent, and the legal and judicial practice of cyber blackmail. This study aims to determine the interpretive approach of Jordanian law on cybercrime and its application to social media cyberblackmail. Furthermore, the study analyzes international legal frameworks, especially the Convention on Cybercrime-Budapest and other modern doctrines related to cybercrime, cyber evidence, digital forensics, and cyber blackmail. In the context of Jordanian law, these sources create a more comprehensive framework of the relevant international legal theories and doctrines. This study is qualitative and does not engage in the collection and analysis of empirical data. Legal texts, court decisions, international legal frameworks, and scholarly work are the main sources. The study analyses existing Jordanian legislation on cyberblackmail using doctrinal and descriptive-analytical techniques to gauge its adequacy in establishing criminal liability on the matter. It also proposes reforms to improve legislative responsiveness, judicial consistency, procedural safeguards, and legal protection to match the pace of ongoing technological advancements.

Literature Review

The Concept of Cyber Blackmail through Social Media

The evolution of ICT (Information and Communication Technologies) has built a new framework of methodologies which criminals use to execute a different type of crime. Cyber blackmail is one of these new methodologies which violate a person's right to privacy and dignity (Lusthaus, 2024). Blackmail is an offence that systematically violates a person's right to privacy. It is the act of electronically coercing a victim to fulfil illegal demands or requests in order to avoid the threatened release or publication of their private or sensitive digital resources (e.g., videos, images, and other content). Compared to traditional blackmail, cyber blackmail is more sophisticated because it allows criminals to communicate at any distance, use digital resources, and conceal their identities across borders (AlGhanboosi et al., 2023; Hussein & Manap, 2024; Manap & Aljuboori, 2024; Shakhathreh et al., 2023). The increasing use of various social media platforms means that blackmailers now have more methods and means to create contact with users in order to gather sensitive data which they can later use to create digital blackmail. Research on online sextortion gives a good example of socially enabled cyber blackmail to illustrate how offenders of a crime perpetrated on a victim using a social media network can use that same network to create contact and apply psychological or sexual pressure on that victim (Edwards & Hollely, 2023). In conclusion, cyber blackmail is much more than blackmailing a victim to extract financial resources. It is blackmailing a victim to extort sexual favors, to pressure a victim psychologically, to damage a victim's reputation, and to trade off a victim's personal privacy and digital security.

Table 1. Key Legal and Technological Characteristics of Cyber Blackmail through Social Media

Characteristic	Description	Legal Significance
Digital communication	Offence committed through social media, messaging apps, or digital systems.	Distinguishes cyber blackmail from conventional blackmail.
Unlawful threat	Threat to disclose or publish private information or intimate content.	Constitutes the main <i>actus reus</i> of coercion.
Coercive demand	Threat intended to obtain money, action, or compliance.	Demonstrates the coercive and criminal purpose.
Intentional conduct	Deliberate use of digital means to threaten or coerce.	Establishes the required <i>mens rea</i> .
Electronic evidence	Messages, screenshots, metadata, account records, and forensic reports.	Requires authenticity, integrity, reliability, and admissibility.
Anonymity and cross-border reach	Use of anonymous accounts, encryption, or foreign digital services.	Creates challenges for attribution, jurisdiction, and cooperation.
Victim harm	Financial, psychological, reputational, and privacy-related harm.	Supports effective criminal protection and victim safeguards.

Source: Prepared by the author based on Lusthaus (2024), AlGhanboosi et al. (2023), Hussein and Manap (2024), Manap and Aljuboori (2024), and Edwards and Hollely (2023).

The legal intricacies of cyber blackmail stem from how activities in cyberspace are unique. Offenders can leverage unidentifiable accounts, use encrypted messages, and take advantage of digital systems that span many different jurisdictions (Al-Salamat et al., 2023). Victims can be in different jurisdictions from the offender, and the evidence can span multiple jurisdictions from the service providers. These aspects of cyber blackmail create difficulties in the attribution of the offender during the investigation as well as in the collection and verification of electronic evidence (Lusthaus, 2024; Zhang & Gong, 2024). Cyber blackmail can merge with other offending behaviors such as unauthorized access, identity-related crimes, interference with privacy, and the unlawful dissemination of personal information. This calls for the legal classification and enforcement of the principles of criminal liability. Effective enforcement of such crimes also relies on electronic evidence and digital-based criminal investigations and judicial cooperation. The verification of electronic evidence and digital communications obtained through foreign service providers is critical where communications are rendered anonymous (Manap & Aljuboori, 2024). Despite the growing concern of cyber blackmail internationally, the criminal liability of cyber blackmail through social media in the context of the Jordanian Cybercrime Law No. 17 of 2023 has been the focus of little legal research. Other studies have dealt with the broad context of cyber blackmail and related crimes and have focused on the interplay between the Cybercrime Law and the Jordanian Penal Code, judicial developments and social-media-based electronic evidence. There is a research gap in this area. This study aims to investigate the Jordanian legal system dealing with cyber blackmail and assess if the system is flexible enough to deal with modern technological practices while offering adequate criminal and legal protection.

Criminal Liability for Cyber Blackmail under Jordanian Law

Jordanian law allows for criminal liability where the components of a crime are established. With respect to liability for cyber blackmail, it is insufficient to prove the presence of an unlawful threat (Gharaibeh & Ibrahim, 2024). It must also be shown that the perpetrator purposefully utilized technology or social media to make a threat or to attempt to compel the victim to perform, refrain from performing, or endure a demanded action against his or her will. Therefore, criminal liability is evaluated according to the general principles of Jordanian criminal law and the provisions of the law on cybercrime (Saleh & Ghnaimat, 2025). According to Jordanian law, the liability for cyber blackmail is dependent upon the satisfaction of three main components: the legal component, the factual component (*actus reus*), and the psychological component (*mens rea*). The legal component involves the presence of a law; the factual component involves the illegal act performed via the electronic medium; and the psychological component involves wilfulness and knowledge of the act and its unlawful nature. Therefore, the presence of electronic communication alone is insufficient to ground criminal liability; the relevant components of a crime and the intent must be present (Khwaileh & Makhadmeh, 2026).

Table 2. Essential Legal Elements and Evidentiary Requirements for Cyber Blackmail under Jordanian Law

Element / Requirement	Description	Relevant Legal Framework
Legality	Conduct must be criminalised by existing law and subject to a prescribed penalty.	Jordanian Cybercrime Law No. 17 of 2023 and Penal Code.
Material element (<i>Actus Reus</i>)	Use of digital means to make unlawful threats or coercive conduct.	Cybercrime Law No. 17 of 2023 and relevant criminal provisions.
Mental element (<i>Mens Rea</i>)	Intentional conduct aimed at intimidation, coercion, or unlawful benefit.	General principles of Jordanian criminal responsibility.
Electronic evidence	Digital communications, screenshots, metadata, account records, and forensic reports may establish the offence.	Rules governing electronic evidence, criminal procedure, and judicial practice.

Source: Prepared by the author based on Khwaileh and Makhadmeh (2026), the Jordanian Cybercrime Law No. 17 of 2023, the Jordanian Penal Code, and relevant legal scholarship.

Legal Elements of the Crime of Cyber Blackmail

To establish cyber blackmail, it is necessary to meet the specific criteria of the offence. Harm is not enough to prove liability. It is necessary to prove legal, material (*actus reus*), and mental (*mens rea*) elements. Cyber blackmail is executed with the use of modern technologies. However, the basic principles of criminal law assess the act with a combination of additional aspects relevant to the assessment of electronic communications and digital evidence (Zhang & Dong, 2023). The legal element corresponds to the principle of legality, expressed by the maxim of no crime and no punishment without law. The Cybercrime Law No. 17 of 2023, and the applicable provisions of the Jordanian Penal Code, provide the main legislative framework for cyber blackmail in Jordan. As a result, criminal liability is incurred if the act of the accused is in accordance with the provisions of the law (Hafizhah et al., 2024; Al-Sarayreh, 2024; Al-Zaqeba et al., 2023). The *actus reus* is the offence of external conduct. In a case of cyber blackmail, this type of conduct can be the sending of threats to the victim, using any social media or instant messaging application, to offer a demand, which the victim can fulfill only to prevent the disclosure of private information, photos, videos or communications. In many cases, this element can be proven by the assessment of digital communications and accounts of the accused (Hussein & Abdul Manap, 2024). The possession of private information or the existence of threats, in the form of electronic communications, is not sufficient to constitute a criminal act unless the unlawful threats or coercive actions meet the elements of the crime.

The mental element (*mens rea*) focuses on whether actions were conscious and deliberate. It should be shown that the accused purposefully transgressed the law by using electronic means to threaten or intimidate a victim (Naggi, 2024). The intent may also be inferred from the demand and its reasonable relationship to the means and methods of communication, the relationship of the parties, and other factors. The intersection of Jordanian Cybercrime Law No. 17 of 2023 and the Jordanian Criminal Code is also important for determining intent. The Cybercrime Law delineates specific crimes, whereas the Criminal Code and Jordanian law articulate the concepts of participation, attempt, and intent. The two systems thus complement one another (Saleh &

Ghnaimat, 2025). To establish applicable crime and prosecution, various forms of electronic evidence, such as messages, screenshots, metadata, account logs, and forensic analysis, may be required (Alkhseilat et al., 2024; Romaniuk & Ablamskyi, 2024). Criminal liability may also be incurred by those who aid the commission of the crime or facilitate it (Airout, 2025). The effective attribution of criminal liability thus requires appropriate substantive law, reliable electronic evidence, and procedural safeguards (Maghaireh, 2024).

Table 3. Legal Elements of Cyber Blackmail under Jordanian Law

Legal Element	Description	Application to Cyber Blackmail
Legality	Prohibited conduct and punishment must be established by law.	Cyber blackmail must fall under Jordanian Cybercrime Law No. 17 of 2023 and applicable Penal Code provisions.
Material element (<i>Actus Reus</i>)	The external conduct constituting the offence.	Use of electronic means to make unlawful threats or coercive communications.
Mental element (<i>Mens Rea</i>)	Knowing and intentional commission of the prohibited conduct.	Deliberate use of digital means to threaten, intimidate, coerce, or obtain an unlawful benefit.

Source: Prepared by the author based on the Jordanian Cybercrime Law No. 17 of 2023, the Jordanian Penal Code, Hafizhah et al. (2024), Al-Sarayreh (2024), Hussein and Abdul Manap (2024), and Naggi (2024).

The Role of Electronic Evidence in Establishing the Legal Elements

Independent of the cyberblackmail law's elements, electronic evidence is critical in constructing the offence's elements (material and mental). Messages, social media messages and conversations, screenshots, metadata, records, files stored on account and cloud storage, and digital forensic reports are all examples of important related evidence. Each type of evidence has value when it is authentic, intact, credible, and has been collected and stored in a lawful manner (Alhawtmeh et al., 2026; Alkhseilat et al., 2024; Romaniuk & Ablamskyi, 2024). Evidence of electronic communication is not sufficient to prove the offender's identity, the unlawful nature of the conduct, or the intent to commit a crime. Because of this, the courts evaluate digital evidence in the light of the circumstances of each case.

Judicial Interpretation of Cyber Blackmail

The onus of determining the scope of criminal liability for cyber blackmail relies on the judicial interpretation of the Jordanian Cybercrime Law No. 17 of 2023 and the generalized principles of criminal law. Courts will need to examine the nature of electronic conduct, threats, and demands made to the victim and will consider the purpose of the accused. The existence of electronic conduct is inadequate for judicial determination of cyber blackmail, unless such conduct is demonstrably unlawful and the requisite criminal intent is established (Al-Sarayreh, 2024; Saleh & Ghnaimat, 2025). Of paramount importance to such cases is the conduct of electronic

communication. Courts are called to assess the authenticity, integrity, and reliability of electronic evidence, as well as the legality of its acquisition and the manner in which it has been preserved. Digital forensic expertise may provide assistance to courts in addressing verification and analysis of communication pertaining to electronic evidence (Alkhseilat et al., 2024; Romaniuk & Ablamskyi, 2024). Furthermore, the use of pseudonym identities, foreign service providers, and evidence that resides outside the territorial jurisdiction of the Hashemite Kingdom of Jordan may hinder the identification of the offender and may require the issuing of a letter rogatory (Sachoulidou, 2024). The interpretation of the courts is required to ascertain the application of the Cybercrime Law to the specific circumstances surrounding cases of cyberblackmail and to attend to the need for legal certainty with the application of flexible principles of criminal law in order to keep pace with the advancement of digital technologies (Saleh & Ghnaimat, 2025).

Table 4. Key Judicial, Evidentiary, and Investigative Issues in Cyber Blackmail Cases under Jordanian Law

Judicial / Evidentiary Issue	Key Consideration	Legal Significance
Qualification of cyber blackmail	Determine whether electronic conduct meets statutory requirements.	Ensures liability is based on applicable law.
Criminal intent	Establish intentional threats, intimidation, or coercion.	Confirms <i>mens rea</i> and distinguishes intentional conduct.
Electronic evidence	Assess messages, screenshots, metadata, recordings, and forensic reports.	Requires authenticity, integrity, reliability, and admissibility.
Digital forensic expertise	Authenticate, analyze, and preserve electronic evidence.	Supports courts in evaluating complex digital evidence.
Offender identification	Link anonymous or concealed accounts to the accused.	Establishes reliable attribution and prevents unsupported liability.
Cross-border nature	Offenders, victims, or evidence may be located abroad.	Requires jurisdictional mechanisms and international cooperation.
Method of commission	Cyber blackmail may occur through social media, messaging apps, or email.	Requires cybercrime-specific investigative mechanisms.
Evidence preservation	Digital evidence can be altered, deleted, or manipulated.	Protects evidence integrity and admissibility.

Source: Prepared by the author based on Al-Sarayreh (2024), Saleh and Ghnaimat (2025), Alkhseilat et al. (2024), Romaniuk and Ablamskyi (2024), Sachoulidou (2024), and Rakha (2024).

Challenges in Establishing Criminal Liability for Cyber Blackmail through Social Media

The rapid growth of technology posed law, procedure and enforcement challenges for proving cyber blackmail. Although Jordan's Cybercrime Law No. 17 of 2023 improved the law, enforcement depends on the ability to identify offenders, retain electronic evidence, ensure the correct jurisdiction and balance the control of emerging technology with the protection of fundamental rights. With an increased reliance on digital evidence, a forensic specialist and the right techniques will be essential (Almatarneh et al., 2026; Allah Rakha, 2024; Matijašević et al., 2024).

Identification of Offenders and Anonymous Digital Identities

There is a growing reliance on either anonymous accounts or fraudulent digital identities, making it impossible to associate an online account with a specific individual. This problem is magnified when offenders and/or victims, as well as relevant service providers, are in different jurisdictions. In such cases, effective identification requires digital forensics and the ability to obtain electronic evidence across jurisdictions (Sachoulidou, 2024; Allah Rakha, 2024).

Collection, Preservation, and Authentication of Electronic Evidence

When compared to physical evidence, digital evidence is more easily manipulated, altered, deleted or reproduced. In the cyber blackmail context, evidence may consist of text communications, screenshots, metadata, records, cloud storage, and forensic information. In order for these forms of evidence to be valuable, they must be authentic and legally obtained and preserved. It is critical to have means to collect, preserve, and authenticate digital evidence (Allah Rakha, 2024; Matijašević et al., 2024).

Jurisdiction and Cross-Border Cybercrime

The phenomenon of cyber blackmail can include a mix of victims, offenders, service providers, and platforms, as well as electronic evidence, spread out across multiple jurisdictions. This poses problems for applicable law, investigative power, and the jurisdiction of the courts. Hence, access to evidence located in other jurisdictions may necessitate mutual legal assistance and international cooperation in the field of justice (Billow, 2024; Sachoulidou, 2024).

Artificial Intelligence and Deepfake Technologies

The integration of AI, and especially the use of deepfakes and AI-generated images and speech, poses additional problems. Given the potential to create highly realistic, altered, and artificial content, these pose challenges for reputation and coercion. As a result, these pose challenges for the sufficiency of laws and standards of evidence for the attribution of criminal liability (Čučilović, 2024; Maghaireh, 2024).

Protection of Fundamental Rights and Procedural Safeguards

The response to cyber blackmail may include the infringement of private communications, digital devices, and online accounts, which may infringe on the right to privacy, the confidentiality of communications, and the right to freedom of expression. Thus, investigative measures should be

within a clearly defined legal framework and be proportional and subject to legal scrutiny. In Jordan, this is critical after the introduction of the Cybercrime Law No. 17 of 2023 (Maghaireh, 2024; Al-Sarayreh, 2024).

Legislative and Institutional Challenges

These challenges illustrate that the reform of laws is insufficient for effective enforcement. Consequently, Jordan requires the development of the judiciary, specialized cybercrime and forensics, international cooperation, and the periodic reassessment of laws to keep pace with emerging technologies and shifting trends in cyber blackmail (Saleh & Ghnaimat, 2025; Al-Sarayreh, 2024).

Table 5. Major Challenges in Establishing Criminal Liability for Cyber Blackmail

Challenge	Legal and Practical Impact	Appropriate Response
Anonymous digital identities	Difficulty attributing online conduct to offenders.	Specialized digital forensics and attribution mechanisms.
Electronic evidence	Alteration or loss may affect authenticity and admissibility.	Standardized collection, preservation, and authentication procedures.
Cross-border offences	Different jurisdictions complicate law enforcement and evidence access.	Mutual legal assistance and international cooperation.
AI and deep fakes	Difficulty verifying authenticity and evidentiary reliability.	Updated evidentiary standards and legislative review.
Privacy and procedural rights	Digital investigations may affect privacy and fundamental rights.	Legal authorization, proportionality, and judicial oversight.
Institutional and technical capacity	Limited expertise may hinder digital investigations.	Specialized cybercrime units and enhanced forensic capabilities.

Source: Prepared by the author based on Allah Rakha (2024), Matijašević et al. (2024), Sachoulidou (2024), Billow (2024), Maghaireh (2024), Al-Sarayreh (2024), and Saleh and Ghnaimat (2025).

Discussion

The current study confirms that the enactment of the Jordanian Cybercrime Law No. 17 of 2023 constitutes a significant advancement in the legal handling of cyber-enabled crime in Jordan, including social media cyber blackmail. The law creates a more precise legal framework for dealing with unlawful activities that occur through the use of information systems, electronic networks, and digital platforms. Nevertheless, the study shows that the rapid development of cybercrime and the means of communication will hinder the enforcement of the law, even with the legislative reform (Al-Sarayreh, 2024; Saleh & Ghnaimat, 2025). The results of the study indicate that the prosecution of social media cyber blackmail will depend, like any other crime, on the fulfilment of the three primary constituents of a crime: the legal, the material (actus reus), and the

mental (*mens rea*). Cyber evidence is, therefore, not an independent fourth constituent. Electronic communication is, however, a significant means of proof for the accomplishment of the aforementioned constituents. The fact that electronic communication is present is not sufficient for criminal liability. Electronic communication is, however, a significant means of proof for the fulfilment of the aforementioned constituents.

The study also examines the Cybercrime Law No. 17 of 2023 and the Jordanian Penal Code and their complementarity within the legal system. Jordan’s Cybercrime Law focuses more on technology-related crimes, while the Jordanian Penal Code more generally deals with legal principles and doctrines on the liability of offenders. The comprehensive implementation of these provisions will again require a harmonious interpretation by the judiciary in line with the general principles of Jordanian criminal law (Al-Sarayreh, 2024; Saleh & Ghnaimat, 2025). Another finding was related to the role of electronic evidence in cases of cyber blackmail. It was found that digital communication, screenshots, metadata, accounts, and even forensic reports may all play a role in proving that a crime had taken place and that the accused had committed that crime. However, these findings are evidence of the crime and may still lack value if evidence was not properly collected, maintained, and preserved. This also emphasizes the need for established and adequate procedures and evidence in collecting and presenting electronic evidence (Alkhseilat et al., 2024; Romaniuk & Ablamskyi, 2024).

The findings suggest that anonymous criminal digital identities, cross-border digital evidence, and the challenges of fast-evolving technologies impact the efficacy of criminal enforcement. This may cause more difficulties in identifying offenders and/or accessing electronic evidence. Therefore, more reliance on international collaboration and skilled digital forensics may be required (Sachoulidou, 2024; Allah Rakha, 2024). Emerging technologies like artificial intelligence and deep fakes will create even more difficult problems. These technologies can create altered digital content that is more sophisticated and difficult to prove the authenticity of evidence and apply the provisions of criminal law (Čučilović, 2024; Maghaireh, 2024). For a Jordanian response to cyber blackmail to be effective, it will need to adequately combine the elements of legislation, the interpretation of legislation, electronic evidence, specialized investigation, and adequate methodologies. The Cybercrime Law No. 17 of 2023 will provide an important legislative base. For it to be effective, the law will require the support of the courts and proactive adjustments to keep pace with trends in cyberblackmail, while balancing the rule of law, the protection of rights, and legal certainty (Saleh & Ghnaimat, 2025; Al-Sarayreh, 2024).

Table 6. Analytical Summary of the Main Findings

Research Dimension	Principal Finding	Legal Implication
Legislative framework	Cybercrime Law No. 17 of 2023 provides the main framework for cyber-enabled offences.	Establishes the basis for prosecution alongside the Penal Code.
Legal elements of liability	Liability requires <i>actus reus</i> and <i>mens rea</i> and other statutory requirements.	Ensures liability is imposed only when legal requirements are met.

Research Dimension	Principal Finding	Legal Implication
Electronic evidence	Digital communications, screenshots, metadata, and forensic evidence are central to proving offences.	Requires authenticity, integrity, lawful acquisition, and admissibility safeguards.
Judicial interpretation	Courts must assess digital conduct, intent, and electronic evidence.	Promotes consistency and legal certainty.
Offender identification and jurisdiction	Anonymous identities and cross-border evidence complicate investigations.	Requires specialized investigation and international cooperation.
Digital forensic capacity	Electronic evidence requires specialized forensic examination.	Strengthens authentication and evaluation of digital evidence.
AI and deep fakes	AI-generated content creates new classification and evidentiary challenges.	Requires continuous legislative and judicial adaptation.
Fundamental rights and safeguards	Cybercrime investigations may involve private communications and devices.	Requires lawful, proportionate, and procedurally safeguarded investigations.

Source: Prepared by the author based on the findings of the present study and the relevant literature, including Al-Sarayreh (2024), Saleh and Ghnaimat (2025), Alkhseilat et al. (2024), Romaniuk and Ablamskyi (2024), Sachoulidou (2024), Allah Rakha (2024), Čučilović (2024), and Maghaireh (2024).

Conclusion

This research focused on the criminal liability surrounding cyberblackmail via social media within Jordanian law, focusing on the Cybercrime Law No. 17 of 2023, particular articles of the Jordanian Penal Code, and the advancements concerning the judicial and evidential treatment of cyber-enabled criminal activities. This study shows that cyber blackmail, partially, has the potential to attack privacy, dignity, mental health and reputation, as well as the digital security of victims. The use of social media provides greater opportunities to commit these kinds of crimes, as well as significant challenges to the identification of offenders and the provision of electronic evidence and criminal procedural safeguards. This study argues that the Jordanian legal system has a sufficient legal basis for the legal regulation of cyberblackmail in the combined use of the Cybercrime Law No. 17 of 2023 and the general provisions of the Jordanian Penal Code. Cyber blackmail, like any other crime, is the result of the fulfilment of the legal, material (actus reus), and mental (mens rea) components. Electronic evidence, in relation to cyber blackmail, does not represent the legal component of the crime and is an important means of proving the elements of the crime. This study argues that the application of criminal law provisions to the rapidly changing digital environment relies, to a large degree, on the interpretation of the law by courts. Anonymous digital identities, cross-border digital evidence, encrypted communication, and new technologies

carry problems relating to recognizing perpetrators and determining guilt. The introduction of AI and deep fakes increases this problem and creates further ambiguity regarding digital content and the law. Deep fakes and AI will require constant legislative, judicial, and forensic structural alterations to cope.

Recommendations

This study proposes a review of Cybercrime Law No. 17/2023, an enhancement of digital forensics and judiciary capacity, and an increase in the collaboration of states on cross-border cybercrime issues. The study proposes the development of law in regard to AI and deep fakes and strengthened judicial and legal safeguards to privacy, due process, and digital rights. The study places emphasis on cyber blackmail and digital safety education, on legal cooperation with social media platforms to uphold the law and protect citizens, and on social media to keep and safeguard digital evidence.

Table 7. Recommendations for Strengthening Criminal Liability for Cyber Blackmail

Recommendation	Objective	Expected Impact
Periodic review of the Cybercrime Law	Address technological developments and emerging cyber blackmail.	Greater legal adaptability and clarity.
Strengthening digital forensics	Improve handling and analysis of electronic evidence.	More reliable evidence and stronger investigations.
Judicial and prosecutorial training	Improve understanding of cybercrime law and digital evidence.	Greater consistency in proceedings.
Expanding international cooperation	Facilitate cross-border investigations and evidence collection.	More effective prosecution of offenders.
Addressing AI-generated content	Develop responses to deep fakes and synthetic content.	Better handling of emerging cyber blackmail.
Strengthening procedural safeguards	Protect privacy, due process, and proportionality.	Greater protection of rights and public trust.
Increasing public awareness	Improve digital literacy and reporting awareness.	Better prevention and victim protection.
Cooperation with digital platforms	Facilitate lawful preservation and disclosure of evidence.	More efficient investigations and prosecutions.

Source: Prepared by the author based on the findings of the present study.

Contribution of the Study

The study engages with emerging trends in law and provides a comprehensive doctrinal evaluation of social media-based cyber blackmail and criminal responsibility in Jordan after the Cybercrime Law No. 17 of 2023. This study differs from others that analyze cybercrime in a broad sense or examine particular aspects of digital evidence or offences. This study integrates the elements of

cyberblackmail, the Cybercrime Law-Jordanian Penal Code nexus, the law and its judicial interpretation, evidence and emerging technology problems. The study thus offers an analysis tool to cyber blackmail for legislators, judges, prosecutors, lawyers and researchers in Jordan.

Conflict of Interest

The author declares that there is no financial, professional or personal conflict of interest that influenced the research, the interpretation of the evidence or the conclusions made in this article. This study was conducted independently and objectively, adhering to the principles of academic research and ethics.

Funding Source

This paper is supported by Jadara University.

References

- Airout, M. (2025). Criminal Protection Against Cybercrime: A Comparative Legal Analysis of Jordanian, Arab, and International Legislations. *Journal of Posthumanism*, 5(4), 1459-1472.
- Al-Badayneh, D., Khelifa, M., & Brik, A. B. (2024). Cyberbullying and cyberbullicide ideation among Jordanian College Students. *International Journal of Cyber Criminology*, 18(1), 58-82.
- Al-Billeh, T., Al-Hammouri, A., Khashashneh, T., Makhmari, M. A., & Al Kalbani, H. (2024). Digital evidence in human rights violations and international criminal justice. *Journal of Human Rights, Culture and Legal System*, 4(3), 842-871.
- AlGhanboosi, B., Ali, S., & Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. *Computers in human behavior*, 144, 107702.
- Alhawatmeh, O., Alrababah, R., Al-Shoura, L., Alazzam, F & Jarah, B. (2026). Legal compliance as a mediating variable between project management practices and supply chain performance in Jordanian companies. *Journal of Project Management*, 11(2), 591-598.
- Alkhseilat, A., Al-Billeh, T., Albazi, M., & Ali, N. A. (2024). The authenticity of digital evidence in criminal courts: a comparative study. *International Journal of Electronic Security and Digital Forensics*, 16(6), 720-738.
- Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican law review*, 16(2), 23-54.
- Almatarneh, Z., Alawneh, N. F., Al-Jarrah, M. M., Alzubi, E. A., & Jarah, B. A. F. (2026). Legal Challenges and Digital Accounting Adoption in Jordanian Commercial Companies: The Moderating Role of Legislative Solutions. *Journal of Organizational Behavior Research*, 11(1), 178-189.

Al-Salamat, M., Garaibeh, Z., & Alshible, M. (2023). The Effect of the Victim's Consent in the Crime of Human Trafficking Under the Jordanian Human Trafficking Prevention Law. *Pakistan Journal of Criminology*, 15(4), 363.

Al-Sarayreh, R. M. (2024). Jordanian cybercrime law No.(17) of 2023 between regulating social media sites and restricting freedom of opinion. *Scholars International Journal of Law, Crime and Justice*, 7(09), 339-351.

Alshehadeh, A., Assaf, N., Al-Shoura, L., Altaamneh, Y., Jarah, B & Alazzam, F. (2026). The legal role of supply chain governance in reducing contractual risks in Jordanian Islamic banks. *Journal of Project Management*, 11(2), 362-370.

Al-Zaqeba MAA, Shubailat OM, Abdul Hamid S, Jarah BAF, Ababneh FAT, and Almatarneh Z (2023). The influence of board of directors' characteristics on corporate social responsibility disclosures in Jordanian Islamic banks. *International Journal of Advanced and Applied Sciences*, 10(11): 1-13.

Billow, J. (2024). No country is an island: embracing international law enforcement cooperation to reduce the impact of cybercrime. *Journal of Cyber Policy*, 9(2), 149-158.

Billow, J. (2024). No country is an island: embracing international law enforcement cooperation to reduce the impact of cybercrime. *Journal of Cyber Policy*, 9(2), 149-158.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, 2, 100038.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, 2, 100038.

Gharaibeh, Y., & Ibrahim, Z. (2024). Legal Support for Sustainable Development in Middle East. *International Journal of Sustainable Development & Planning*, 19(4), 1439.

Hafizhah, A., Leviza, J., & Mulhadi, M. (2024). An Overview of the Principle of Legality: Common Law VS Civil Law. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 4(1), 38-47.

Hussein, O. A., & Manap, N. A. (2024). The crime of cyber blackmail in the era of artificial intelligence. *Journal of Infrastructure Policy and Development*, 8.

Khwaileh, K. M., & Makhadmeh, N. M. (2026). Criminal liability for spreading fake news: a study of Jordanian law in light of international standards. *Frontiers in Sociology*, 11, 1815400.

Lahiani, H., & Al-Khaza'leh, M. S. (2023). Cybercrime and harassment: The impact of blackmailing on Jordanian Society as a case study. *Journal of Intercultural Communication*, 23(3), 117-123.

- Lusthaus, J. (2024). Reconsidering crime and technology: What is this thing we call cybercrime?. *Annual Review of Law and Social Science*, 20(1), 369-385.
- Maghaireh, A. M. (2024). Cybercrime laws in Jordan and freedom of expression: a critical examination of the electronic crimes act 2023. *International Journal of Cyber Criminology*, 18(1), 15-36.
- Manap, N. A., & Aljuboori, O. (2024). Legal Protections for Victims of Cyber Blackmail in the Republic of Iraq, the United States, and Malaysia. *Malaysian J. Syariah & L.*, 12, 334.
- Matijašević, J., Bingulac, N., & Darko, M. (2024). DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS—CHALLENGES AND SOLUTIONS. *Pravo—teorija i praksa*, 41(4), 18-33..
- Naggi, IMA (2024). Legislative regulation of both crimes of threat and informational blackmail-analytical fundamental study of saudi informational crimes law. *Journal of Law and Sustainable Development* , 12 (3), 5.
- Romaniuk, V. V., & Ablamskyi, S. Y. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law & Safety*, 140.
- Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of ‘judicial’ cooperation. *New Journal of European Criminal Law*, 15(3), 256-274.
- Saleh, I. M., & Ghnaimat, A. R. A. (2025). Electronic Impersonation Crimes in the Jordanian Criminal Legislation: A Critical Analysis. *International Annals of Criminology*, 63(2), 280-296.
- Shakhatreh, H. J. M., Salman, A., Aldrou, K. K. A. R., Comite, U., & Alazzam, F. A. F. (2023). Analyzing the relationship between inventory policies and CSR practices: Case of Jordanian companies. *Economics*, 11(s1), 141-163.
- Wang, X. (2025). Global (re-) framing of cybercrime: An emerging common interest in flux of competing normative powers?. *Leiden Journal of International Law*, 38(2), 235-261.
- Zhang, H., & Gong, X. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. *The International Journal of Evidence & Proof*, 28(1), 21-44.
- Zhang, Y., & Dong, H. (2023). Criminal law regulation of cyber fraud crimes—from the perspective of citizens’ personal information protection in the era of edge computing. *Journal of Cloud Computing*, 12(1), 64.
- Zlati, G. (2024, September). Romanian jurisprudence on cybercrime: focus on illegal access to an information system. In *ERA Forum* (Vol. 25, No. 3, pp. 425-440). Berlin/Heidelberg: Springer Berlin Heidelberg.