Journal of Posthumanism
2025
Volume: 5, No: 4, pp. 1459–1472
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i4.1271

Criminal Protection Against Cybercrime: A Comparative Legal Analysis of Jordanian, Arab, and International Legislations

Mohammad Airout[1]

Abstract

Cybercrime presents a growing threat to legal frameworks across the globe, especially in digital-transitioning regions. This report critically examines Jordan's legislative framework for addressing cybercrime, referring specifically to Cybercrime Laws No. 27 of 2015 and No. 17 of 2023. It compares Jordan's framework with that of selected Arabian states—the United Arab Emirates, Saudi Arabia, and Egypt—highlighting the major similarities and deviations between legislative scope, enforcement measures, and regulatory approach. The research also positions Jordanian law within the international framework of instruments such as the Budapest Convention and United Nations-driven initiatives. Notwithstanding legislative advances, the report identifies major gaps in cross-border enforcement, evidence procedures, legal flexibility, and digital rights protection. Building on these findings, the paper suggests a series of reform measures such as clearer legalterminology, the creation of a central cybersecurity agency, improved training for the judiciary, and expanded international cooperation. The findings emphasize the necessity of legislatures in the Arabian region striking a balance between security needs and core freedoms and assuring that their legal frameworks remain agile and attuned to change. This comparative approach contributes towards more systematic and rights-focused Arabian regional cybercrime policy development.

Keywords: *Cybercrime, Jordanian Law, Arab Legal Systems, Digital Regulation, Budapest Convention, Cybersecurity, Cybercrime Enforcement, Legal Reform, Information Technology Law, Human Rights Online.*

Introduction

In today's more digitalized age, one of the most serious threats facing national security, economic stability, and individual privacy has come from cybercrime. Cybercrime, by broad definition, includes any criminal activity that occurs through, or is aimed at, a computer or network device. Cybercrime has grown in both sophistication and scope with such offenses as identity theft, financial fraud, cyberterrorism, ransomware extortion, and unauthorized access to data systems. The global nature of the crimes represents tremendous legal and practical challenges requiring an effective criminal justice response based on both domestic legislation and international cooperation (Morshed & Khrais, 2025).

There has been an increasing usage of information and communication technology (ICT) in Jordan, prompting legal reform in countering cyberrime threats. The key cyberrime laws in Jordan cover Cybercrime Law No. 27 of 2015, which criminalizes online offenses and offers penalties thereto. Cybercrime Law No. 27 of 2015 was amended in 2023 with the objective of enhancing the legislative framework and broadening the scope of offenses punishable under the law as a measure of adapting to global cyberrime trends (Al-Billeh, 2022; Chang, 2020). Legislative responses have varied from the complete cybersecurity law with advanced rules of

[1] Faculty of Law, Department of Law, Middle East University, Amman, Jordan.

procedure and specialized institutions of the United Arab Emirates and Saudi Arabia to others' reliance on comprehensive criminal codes with sparse provisions on ICTs. Regional cooperation under the umbrella of the Arab League and instruments such as the Arab Convention on Combating Information Technology Offences of 2010 also continue to be critical but underexploited mechanisms for harmonization.

Internationally, texts such as the Council of Europe's 2001 Budapest Convention on Cybercrime and the cybercrime and international security resolutions of the UN serve as pointers for drafting legislation. Not only do these texts give legal definitions, but also cross-border cooperation standards, evidence handling guidelines, and human rights safeguards in cyberspace (Keyser, 2017).

This article will compare and analyze Jordanian law criminal protection mechanisms for cybercrime with selected Arab legislations and major international instruments. Through legal strength identification, inconsistencies, and overlaps, the analysis will measure the effectiveness of existing laws in deterring and prosecuting cybercrime. It will also seek to identify gaps in enforcement, jurisdiction, and regional cooperation and make practical suggestions for legislative change and policy formulation.

The Concept and Typology of Cybercrime

Legal Definition of Cybercrime

Cybercrime legal understanding has developed in concert with the intensified incorporation of digital technology into daily life. More broadly, cybercrime includes illegal actions that either depend on information and communication technology (ICT) for their implementation or target explicitly computer systems, data, or networks (Payne, 2020). This dual focus—separating ICT-dependent and ICT-enabled offenses—presents challenging complexities for legislators, particularly in maintaining legal definition as both specific and technologically dynamic (Strikwerda, 2014).

Jordan derives its core legal framework from Cybercrime Law No. 27 of 2015 that outlines a range of offenses carried out through the means of information systems and digital platforms. Article 3 of the law criminalizes unauthorized access into information systems for the specific aim of altering, deleting, or hindering information or services. Articles 4 and 5 also criminalize interference with data and systems. Jordan broadened the legal framework with the issuance of Cybercrime Law No. 17 of 2023 that oversees socio-digital harms such as hate speech, online slander, extortion, and spreading false information. This signifies an increasing realization of the psychological and social aspects of cybercrime and not just its narrow technical aspects (Al-Sarayreh, 2024).

At the regional level, the Arab Convention on Combating Information Technology Offences of 2010 offers a harmonized legal response among members of the Arab states. Article 2 gives a definition of cybercrime as a criminal offence through the application of ICTs that jeopardizes the confidentiality, integrity, or accessibility of information schemes or data. It focuses on intergovernmental cooperation, uniform legal frameworks, and coordinated enforcement between members of states (Saqf Al Hait, 2023).

Internationally, the most effective legal tool remains the Budapest Convention on Cybercrime of 2001. Article 1 of the convention identifies central cyber crimes of illegal access, interference with data and systems, and fraud and forgery involving computers. These articles have been used

in many jurisdictions as templates for legislative drafting of their respective domestic cybercrime laws, thus coordinating cross-border cooperation and extradition (Wicki-Birchler, 2020)

Together, these global, regional, and national instruments depict an evolving framework of understanding and combating cybercrime with varying scopes, legal definitions, and mechanisms for enforcement. As technology becomes more advanced, legal frameworks have the task of providing both specificity in prosecuting offenses and flexibility in adapting to new technology.

Typology of Cybercrime

It is necessary to comprehend the typology of cybercrime in order to design effective legal and enforcement measures. Cybercrime is not one specific offence but a wide range of illegal digital offences. Researchers and practitioners typically categorize these offences by the type of target, the techniques used, and their impact on society (Phillips et al., 2022). The majority of legal and theoretical frameworks divide cybercrimes into three broad categories: (1) crimes against the confidentiality, integrity, and availability of data and systems, (2) traditional crimes enabled through cyberspace, and (3) offences related to content (Sabillon et al., 2016).

Offenses Against the CIA Triad

It is necessary to comprehend the typology of cybercrime in order to design effective legal and enforcement measures. Cybercrime is not one specific offence but a wide range of illegal digital offences. Researchers and practitioners typically categorize these offences by the type of target, the techniques used, and their impact on society (Mabunda, 2025). The majority of legal and theoretical frameworks divide cybercrimes into three broad categories: (1) crimes against the confidentiality, integrity, and availability of data and systems, (2) traditional crimes enabled through cyberspace, and (3) offences related to content (Chitadze, 2023).

Cyber-Enabled Traditional Crimes

This category comprises offenses that existed before the digital era but have either been amplified by, or have taken on revised forms through, digital technology. Examples are online extortion, identity theft, impersonation, cyberstalking, and digital fraud. Articles 10 and 11 of the Jordan 2015 Law and provisions inserted by the 2023 amendment criminalize these offenses. Offenses such as online hate speech and online defamation are also given more prominence as public discourse and civil peace are influenced by digital conduct (Leukfeldt et al., 2020)

At the regional level, Articles 8 and 9 of the Arab Convention cover impersonation and internet fraud, and these are placed within categories of computer fraud and forgery under the Budapest Convention. It has been noted by scholars that the internet's cross-border characteristics make legal enforcement of these crimes and prosecution more difficult (Musotto & Nussbaum, 2022)

Content-Related Offenses

Content-based cybercrimes aim at the transmission of illegal or dangerous content. It embraces child sexual abuse content, terrorist material, hate speech, and incitement of violence. The offenses present difficult questions of legal control, digital ethics, and freedom of speech (Singh, 2023).

Jordan’s 2023 Cybercrime Law amendment imposed tighter provisions on content that provokes sectarianism, disunites the country, or offends religious values. Article 8 of the Arab Convention criminalizes content that is morally offensive and socially destabilizing. Although the Budapest

Convention avoids explicit content regulation, it mandates the criminalization of child pornography by name (Article 9) and leaves room for states to enact other forms of harmful content under national norms (Oddis, 2017).

Upcoming Cybercrime Trends

With the rapid development of digital technology, so too do the methods and resources of cybercriminals. While legislation continues to deal with traditional types of cybercrime, new modes of offending increasingly blur conventional legal boundaries, enforcement powers, and investigative methods (Batrachenko et al., 2024). The constantly evolving environment demands not only ongoing refinement of legislation but also an improved understanding among lawmakers, magistrates, and enforcement authorities.

Ransomware and System-Dependent Attacks

Among the most damaging modern threats is ransomware, a malware that encrypts the data of a victim and asks for payment in exchange for decryption keys, usually in cryptocurrency. Ransomware attacks have regularly hit key infrastructure like financial institutions, healthcare institutions, and government institutions, leading to extensive operational and economic disruptions (Berardi et al., 2023).

Jordanian law does not have a specific mention of ransomware, but Articles 4 and 11 of the Cybercrime Law deal with unauthorized interference and digital extortion, which encapsulate the essence of such attacks. The Budapest Convention (Articles 2–5) and the Arab Convention (Articles 3 and 7) also have legal bases for charging ransomware under more generic provisions of unauthorized access and extortion (Metaxakis, 2023).

Cryptocurrency and Blockchain-Related Crimes

Blockchain technology, in the form of cryptocurrencies like Bitcoin and Ethereum, provides privacy features that have been used for illegal payments, money laundering, and anonymous ransom payments (Maurushat & Halpin, 2022). Although they have legitimate uses in financial services and data protection, these technologies present multifaceted legal and regulatory dilemmas.

In Jordan, there is limited legislation regarding cryptocurrency. There have been warnings and partial restrictions made by financial authorities, but there are no full regulatory schemes in place. The Gulf states have started incorporating cryptocurrency regulation into anti-money laundering tools (Maurushat & Halpin, 2022). Globally, the Budapest Convention urges the harmonization of cybercrime law with financial innovation, while not specifically referring to blockchain technology.

Deepfakes and Synthetic Media

Deepfakes—hyper-realistic but artificial audio and video content created with the application of artificial intelligence (AI)—have become more pervasive in online disinformation campaigns, extortion schemes, and political influence operations (de Rancourt-Raymond & Smaili, 2023). They blur the boundaries between fact and fiction and thus threaten public trust and complicate evidentiary expectations in legal proceedings.

Jordan's Cybercrime Law Amendment of 2023 specifically criminalizes the dissemination of fake or doctored material, such as AI-produced media, as part of its campaign on countering misinformation as well as online impersonation. Neither the Arab Convention nor the Budapest

Convention explicitly references deepfakes, but they both deal with fraud content and privacy infringement in phrases that could be applied expansively towards such technology.

Social Engineering and Human-Focused Attacks

Social engineering attacks like phishing, spear-phishing, and business email compromise (BEC) are still among the most effective vectors of cyber intrusion because they are based on human psychology and not on technical weaknesses (Nifakos et al., 2025). All these attacks are hard to identify and prosecute, particularly in jurisdictions lacking digital forensics capacity.

While not explicitly indicated under Jordanian legislation, these crimes fall under the umbrella of provisions on fraud and unauthorized access. Globally, they are usually prosecuted under broad cyber-fraud laws, but specific legal definitions are uncommon throughout the Arab region (Ghazi-Tehrani & Pontell, 2022).

Legal Framework in Jordan

Primary Legal Instruments

Jordan's legal approach to fighting cybercrime has evolved as a response to increasing digital connectivity, advances in technology, and rising cases of online misconduct. The legal framework hinges on two main instruments: Cybercrime Law No. 27 of 2015 and Law No. 17 of 2023, its amending law. The two aim at harmonizing local cybercrime policy with global norms and local legal, political, and social interests.

Cybercrime Law No. 27 of 2015

Jordan's first systematic effort to legalize offenses pertaining to information and communication technology (ICT) was made through the 2015 law. It was enacted in response to growing fears of online threats, such as unauthorized access, digital frauds, and privacy violations (Al-Sarayreh, 2024). The law comprises substantive and procedural provisions and tackles a broad spectrum of criminal offenses:

- Article 3 Criminalizes unauthorized access into computerized information systems.
- Articles 4 and 5: Sanction interference with systems or with data, such as deletion, modification, and service interruption.
- Article 6: Forbids illegal interception of communications, evidencing concern for digital privacy.
- Article 11: Discusses fraud and impersonation by means of ICT tools.

It also provides criminal liability for accomplices and instigators, recognizing the usually collaborative aspects of cybercrime (Maghaireh, 2024).

Cybercrime Law No. 17 of 2023

By the 2020s, the limitations of the law of 2015 became clear. Sudden acceleration in the use of social media, online defamation, disinformation, and hate speech created mounting pressure on legislative bodies to update the legislation. The 2023 reform extensively expanded the scope of criminal conduct covered by the law to encompass content offenses and digital behavioural harms.

New provisions under the 2023 amendment criminalize

The dissemination of false information that may lead to panic or disturbance in public order.

Online insult, slander, and defamation, particularly on social media like Facebook, Twitter (X), and TikTok.Hate speech, incitement of sects, and material that lowers the country.

Digital extortion, especially blackmail through threatening the disclosure of private content.

These adjustments not only track technological advancements but also state interests in maintaining public morality and state cohesion. Although in line with regional standards of the Arab Convention on Combating Information Technology Offences of 2010, provisions have been criticized. Academics and civil society leaders contend that terms like "undermining national unity" or "influencing public morals" are too vague and are susceptible to interpretation and abuse by journalists, activists, and political opposition (Chinchaladze, 2023; Femi-Adeyinka et al., 2024).

Alignment with International Norms

Jordan's legal framework, while not harmonized fully with international instruments such as the Budapest Convention, has considerable similarity in the categorization of offenses and standards of enforcement. Components of hacking, interference with data, and computer fraud replicate core offenses in the Budapest Convention. Similarly, criminalization of hate speech and defamation replicates trends in various Arab states in the context of the Arab Convention.

However, reconciling legal regulation with constitutional rights, especially the right of privacy and freedom of expression, continues to be challenging. The success and equity of Jordan's cybercrime laws will continue to be contingent on upcoming judicial interpretation and the development of stronger procedural protections (Amoo et al., 2024).

Institutional Framework and Enforcement Mechanisms

The success of any law on cybercrime relies not just on the legislation but on the institutional ability to apply them. In Jordan, there has been increased acknowledgment of the technical nature and transnational scope of cybercrime, resulting in the creation of a multi-faceted enforcement regime. This comprises specialized law enforcement units, forensic facilities, and trained judiciary officials in conjunction with international partners. Yet the challenges extend into strategic coordination, resourcing, and technical-legal harmonization (Zhang & Gong, 2024).

Law Enforcement Infrastructure

Leading the charge on enforcing cybercrime is Jordan’s Public Security Directorate’s (PSD) Cybercrime Unit, founded in 2008. The unit’s responsibilities include investigating computer crimes, processing and acting on public complaints, collecting electronic evidence, and building cases for prosecution. Its members undergo training in digital forensics, malware analysis, and tracing on the network, which equips them with the skills necessary to tackle cases from internet fraud to ransomware and digital extortion (Zhang & Gong, 2024).

Backing up the Cybercrime Unit is the Information and Communications Technology Crime Laboratory, which conducts technical examination of digital devices that have been seized. The laboratory extracts encrypted material, scrutinizes metadata, and helps with the identification of geolocation and digital signatures—vital tools for attribution in cases of cybercrime (Al-Kasassbeh & Ghazleh, 2023).

These institutions function according to procedure standards that serve the function of securing the legality and admissibility of electronic evidence before the courts. Nonetheless, according to regional cybersecurity experts, procedural definitiveness and limited resources continue to limit investigating capacity within complicated or transnational cases.

Judicial Capacity and Legal Training

Understanding the specialized character of cybercrime, Jordan has initiated training for members of the judiciary, especially public prosecutors and trial judges, in fields like ICT law, digital evidence, and protective measures. Training programs are done jointly with international partners like the Council of Europe, UNODC, and the Arab League, frequently under the auspices of the Budapest Convention capacity-building programs.

Jordan's Judicial Council has held workshops, seminars, and certification sessions that discuss such topics as blockchain crime, hate speech on the internet, and harassment on the web. The activities are meant to prepare the judges not only to enforce existing legislation but also interpret that legislation according to new digital realities (Alramamneh & Abuanzeh, 2023).

Regional and International Cooperation

In light of its transnational character, Jordan has deepened its engagement in regional and international enforcement cooperation. Jordan, as a party to the Arab Convention on Combating Information Technology Offences of 2010, benefits from a mutual legal assistance, extradition, and collaborative investigation framework. Despite not being a party to the Budapest Convention, Jordan’s legislation and institutional operations increasingly converge with its principles—especially on the preservation of data, the requests for cross-border access, and standards of evidence (Alramamneh & Abuanzeh, 2023).

Jordan also works together with Europol and INTERPOL to assist global operations on cybercrime and facilitate mechanisms for sharing information (Calcara, 2013). All these collaborations are crucial for monitoring advanced cybercriminal networks that span several jurisdictions and online platforms.

Challenges and Strategic Gaps

In spite of the advances, a number of institutional challenges hamper the effective implementation of Jordan’s cybercrime framework. Among them is the fact that there isn’t a single, coordinated national cybersecurity approach that interlinks legal, enforcement, and policy goals. The absence of such strategic coordination results in policy incoherence between enforcement institutions and weak capacity for responding to emergencies. Additionally, the Cybercrime Unit and affiliate bodies have limitations in terms of funds, manpower, and access to technologically advanced investigative tools—most importantly, AI tools used for deepfake detection, tracking of crypto-transactions, or processing of encrypted content. Sustained capacity building, investment in digital infrastructure, and inclusion of private sector experience are necessary for countering the dynamically-changing threat environment of cyberspace.

Comparative Analysis with Other Arab Countries

United Arab Emirates (UAE)

The United Arab Emirates has created one of the region’s most robust sets of cybercrime laws under Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes. It covers both technical offenses (for example, hacking and data breaches) and content offences, for

example, for defamation, hate speech, and promoting fake news—reflecting but building on Jordan's Cybercrime Legislation No. 27 of 2015 and No. 17 of 2023.

Some key differences are the UAE's stricter punishments, with some cybercrimes punishable by life imprisonment (e.g., Article 24), and broader regulation of expression online, such as criticism of the state and religously offensive material. Jordan's 2023 amendments introduced comparable content restrictions, but the UAE enforces them more extensively and punitively.

Institutionally, the UAE has a centralized cybersecurity model, wherein institutions like the Cybersecurity Council and the Electronic Crime Department are endowed with sophisticated monitoring tools. Jordan, on the other hand, places greater reliance on its Cybercrime Unit under the Public Security Directorate with lesser central monitoring (Tubaishat & AlAleeli, 2024; Younies & Al-Tawil, 2020).

Together, they have a similar regional legal alignment and intensified cybercrime agendas, but the UAE has a security-dominant and punitive approach, while Jordan takes a moderate and developmental legislative approach.

Saudi Arabia

Saudi Arabia's legal framework for computer crime is underpinned chiefly by the Anti-Cybercrime Law (Royal Decree No. M/17 of 2007), which is still the basis for online offenses. The law deals with unauthorized access, interference with data, financial fraud, and defaming. Like Jordan's computer crimes, it codifies content- and systems-based offenses into law but with Saudi Arabia placing particular emphasis on upholding public morals and order.

Particularly, Saudi law is more explicitly worded, with provisions criminalizing behavior that 'offends public morals' or that 'has an impact on public security'—albeit in a similar spirit of Jordan's 2023 reform, but under tighter interpretation. For example, Internet insult or clerical criticism could be punished with serious penalties, such as up to 5 years' imprisonment or up to 3 million SAR fines.
Saudi Arabian institutions have a centralized enforcement model headed by the Saudi Authority for Cybersecurity and backed by specialized units of the Ministry of Interior. The model maximizes the efficacy of investigations and synthesizes enforcement of cybercrime with country security objectives. Jordan, on the other hand, has no central agency such as the SAC but uses inter-agency coordination. Jordan and Saudi Arabia share both legal objectives of countering cyber threats and maintaining social cohesion, but the Saudi approach remains more punitive, more centralized, and more religio-politically conservative due to its legal and cultural environment (Al Amro, 2017; Alzubaidi, 2021).

Egypt

Egypt's cybersecurity law has its foundation on Law No. 175 of 2018 for Combating Information Technology Crimes and provides the criminalization of such cyber crimes, such as hacking, data breaching, unauthorized access of content, and online dissemination of false news. It further provides procedural mechanisms for blocking websites and storing data.

Similar to Jordan's 2023 amendment, Egypt's law focuses particularly on content control, criminalizing online slander, spreading 'false news,' and online conduct that 'endangers public morality or national security.' Egypt builds on that by granting wide-ranging surveillance powers to officials, blocking, or shutdown of sites deemed to be breaking the law (Articles 7–9), something criticized for likely stifling digital freedoms. Institutionally, enforcement rests with

Egypt's Supreme Council for Media Regulation and Cybercrime Unit under the Ministry of Interior. The judiciary has also played an active part in prescribing internet cases, usually involving activists, bloggers, and online media workers—demonstrating the political dynamics of enforcement. Jordan, on the other hand, uses its laws with more focused aim and limited scope of the judiciary, although both have comparable challenges of harmonizing regulation with rights. Egypt's total cybercrime law has structural parallels with Jordan's in that they have a mixture of technical and content offenses, but Egypt has more state-driven and surveillance-focused model, reflecting local security priorities (Hassib & Alnemr, 2021; Abdelmeguid, 2024).

International Legal Framework

The Budapest Convention on Cybercrime

Budapest Convention of 2001 is the first international treaty of combating cybercrime via harmonized law and mutual legal assistance. It sets out key crimes such as unauthorized access, interference with systems/data, fraud using computers, and child pornography, and also provides for procedural tools for cross-border investigations and evidentiary preservation.

While Jordan remains a nonsignatory state, its Cybercrime Law of 2015 and Cybercrime Law of 2023 share many provisions with the Convention, most notably on technical offenses and fraud. The same may be said of Egypt and the UAE, where elements of the Convention have become part of local law.

While the Convention calls for effective cooperation and legal transparency, many of the states of the region have not ratified the Convention on account of their concern for their sovereignty. It remains nonetheless an influential model of regional reform (Apsimet & Muratova, 2025).

Other International Frameworks and the United Nations

The United Nations played a key role in shaping global norms on cybercrime through General Assembly actions and activities of mechanisms like the UN Office on Drugs and Crime (UNODC). Activities of the UN focus on consolidating legal cooperation, capacity-building, and protecting human rights in undertaking digital investigations.

It may not have submitted a binding convention on cybercrime, but the UN has begun negotiating an international convention on cybercrime with the participation of Arab states, one of which includes Jordan.

Other key frameworks include regional efforts by INTERPOL on cybercrime and initiatives by the GCC and Arab League, for example, the Arab Convention on Combating IT Offences of 2010. Both have coordination platforms but are less procedurally mature than the Budapest Convention. Together, UN efforts supplement available conventions by encouraging global cooperation although harmonization of the law remains work in progress (Hakmeh, 2024; Tennant & Paula Oliveira, 2024).

Criminal Protection: Loopholes and Obstacles

While Jordan, together with some other Arab states, has made major legislative progress towards criminalizing online offenses, a host of legal, institutional, and procedural shortcomings persist that hamper effective enforcement. All these drawbacks define the practical application of online crime laws and restrict their deterrent effect, particularly with regard to rapidly evolving technology challenges.

Jurisdiction and Cross-Border Enforcement

Cybercrime routinely involves offenders and infrastructure that cross jurisdictions. Limited bilateral cooperation and absence of accession into international instruments such as the Budapest Convention, however, underlies poor cross-border legal cooperation. For example, Jordan lacks a binding legal framework for mutual legal cooperation with several states due to which it becomes difficult to obtain digital evidence or extradite foreign-based suspects. It is also constrained by weak harmonized legal protocols for foreign data request processing.

Limitations of Procedures and Evidence

Evidence collection, preservation, and production pose great technical and legal challenges. Although Jordan's Cybercrime Division has digital forensics training, digital protocols expertise among judges remains scarce. Encryption of data, ephemeral messaging (e.g., self-destructing messages), and cloud storage complicate antiquated evidence protocols. For the majority of cases, the judiciary will likely be lacking the procedure tools necessary for authenticating digital records, IP tracing, or metadata, thereby weakening prosecution findings.

Ambiguity and overregulation of

A frequent point of concern among Arab legal codes is the over-criminalization of content available online, for instance, libel, hate speech, and dissemination of false news. Unclear phrases like "damaging national unity" or "spreading rumors" in Jordan's 2023 revision have the potential of being applied on a personal interpretation basis. The same provisions are found in UAE and Egypt. This has the likelihood of overreaching by the law, downgrading public confidence and potential breaches of international norms about freedom of expression and right of access to information.

Institutional Oversight Bifur

While the UAE and Saudi Arabia have unified central institutions such as the Cybersecurity Council or Saudi Authority for Cybersecurity, Jordan lacks a unified national cybersecurity agency. It has shared responsibilities among the Cybercrime Unit, the ICT Crime Lab, the Judiciary, and ministries, oftentimes in an unstructured way. This fragmentation creates overlapping mandates, response delays, and gaps in strategic direction.

Lagging Legal Adapt

Jordanian and most Arab law in force does not include provisions for addressing new challenges such as deepfakes, disinformation generated by artificial intelligence, blockchain crime, and ransomware attacks on crucial infrastructure. Even though such offenses may be prosecuted indirectly under broad provisions, the lack of explicit sanctions and specific language undermines legal specificity and may complicate enforcement by the judiciary. Continued legal development and technical discussion are required for bridging such adaptability gaps.

Jordan and other Arab governments' criminal protection infrastructure for cybercrime remains underdeveloped. Key weaknesses of cross-border cooperation, evidence procedures, institutional integration, and technology foresight threaten the efficacy of the laws in place. Without specific reform and stronger protections, these gaps will further impede the legal systems' capacity for protecting digital society.

Recommendations for Legal Reform

- Revise vague legal terms (e.g., "public morals," "national unity") to ensure clarity and avoid misuse.
- Introduce specific provisions for new forms of cyberviolations (e.g., ransomware, deepf
- Install a unified central national cybersecurity agency that will manage policy and enforcement.
- Enhance procedural tools: access to real-time data, encryption of handled data, cross-border collaboration.
- Supply specialized training on digital forensics and cyber law for judges, prosecutors, and investigators.
- Join the Budapest Convention and enhance regional and bilateral cooperation.
- Human rights protections: judicial review, transparency, and freedom of expression safeguards.

Conclusion

Cybercrime is an escalating threat to Jordan's, and the region's, national security, social stability, and individual privacy. Although there have been considerable efforts made by Jordan through Cybercrime Laws No. 27 of 2015 and No. 17 of 2023, these efforts remain marred by considerable limitations of enforcement, procedural definition, and legal flexibility.

A comparison with the UAE, Saudi Arabia, and Egypt identifies common patterns of broadening the criminalization of online material but with key differences regarding penalties, institutional setups, and regulatory approaches. Internationally, although Jordan isn't a party to the Budapest Convention, its legislation increasingly becomes aligned with international norms. Cooperation with United Nations mechanisms and regional agreements provides other avenues of legal harmonization and collaboration.

In an effort to fill existing gaps, Jordan needs to work on defining legal concepts, institutional coordination, building capacity for digital evidence, and applying a balance of enforcement and rights protection. All these changes are not only necessary for preventing cybercrime but also for creating a just and robust digital legal framework.

References

Abdelmeguid, H. (2024). Digital Repression in the Middle East: The Strategic Weaponization of Cybercrime Laws in MENA. McGill Undergraduate Law Review, 9. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4909215

Al Amro, S. (2017). Cybercrime in Saudi Arabia: Fact or fiction? International Journal of Computer Science Issues (IJCSI), 14(2), 36.

Al-Billeh, T. (2022). Legal Controls of the Crime of Publishing a Program on the Internet in Jordanian Legislation. Pakistan Journal of Criminology, 14(1). http://www.pjcriminology.com/wp-content/uploads/2022/08/1.-Legal-Controls-of-the-Crime-of-Publishing-a-Program-on-the-Internet-in-Jordanian-Legislation.pdf

Al-Kasassbeh, F. Y., & Ghazleh, A. M. A. (2023). International and National Efforts to Protect Cyber Security: Jordan Case Study. International Journal of Cyber Criminology, 17(2), 350–363.

Alramamneh, I. M., & Abuanzeh, A. (2023). International and National Procedural Framework for

Combating Cybercrime. International Journal of Cyber Criminology, 17(2), 330–349.
Al-Sarayreh, D. R. (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.
Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1). https://www.cell.com/heliyon/fulltext/S2405-8440(21)00121-3
Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205–217.
Apsimet, N. M., & Muratova, A. Z. (2025). On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud. Bulletin of the Karaganda University "Law Series," 11730(1), 87–97.
Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: Analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal, 6. https://www.malque.pub/ojs/index.php/msj/article/view/1860
Berardi, D., Giallorenzo, S., Melis, A., Melloni, S., Onori, L., & Prandini, M. (2023). Data flooding against ransomware: Concepts and implementations. Computers & Security, 131, 103295.
Calcara, G. (2013). The role of INTERPOL and Europol in the fight against cybercrime, with reference to the sexual exploitation of children online and child pornography. Masaryk University Journal of Law and Technology, 7(1), 19–33.
Chang, L. Y. C. (2020). Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. In T. J. Holt & A. M. Bossler (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 327–343). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_6
Chinchaladze, T. (2023). Social Networks and Security Challenges. In Analyzing New Forms of Social Disorders in Modern Virtual Environments (pp. 21–41). IGI Global. https://www.igi-global.com/chapter/social-networks-and-security-challenges/328103
Chitadze, N. (2023). Basic principles of information and cyber security. In Analyzing New Forms of Social Disorders in Modern Virtual Environments (pp. 193–223). IGI Global. https://www.igi-global.com/chapter/basic-principles-of-information-and-cyber-security/328110
de Rancourt-Raymond, A., & Smaili, N. (2023). The unethical use of deepfakes. Journal of Financial Crime, 30(4), 1066–1077.
Femi-Adeyinka, C., Kose, N. A., Akinsowon, T., & Varol, C. (2024). Digital forensics analysis of youtube, instagram, and tiktok on android devices: A comparative study. 2024 12th International Symposium on Digital Forensics and Security (ISDFS), 1–6. https://ieeexplore.ieee.org/abstract/document/10527244/
Ghazi-Tehrani, A. K., & Pontell, H. N. (2022). Phishing evolves: Analyzing the enduring cybercrime. In The New Technology of Financial Crime (pp. 35–61). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003258100-3/phishing-evolves-analyzing-enduring-cybercrime-adam-kavon-ghazi-tehrani-henry-pontell
Hakmeh, J. (2024). The UN convention on cybercrime: A milestone in cybercrime cooperation? Journal of Cyber Policy, 9(2), 125–130. https://doi.org/10.1080/23738871.2024.2441549
Hassib, B., & Alnemr, N. (2021). Securitizing cyberspace in Egypt: The dilemma of cybersecurity and democracy. In Routledge Companion to Global Cyber-Security Strategy (pp. 521–533). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-50/securitizing-cyberspace-egypt-bassant-hassib-nardine-alnemr
Keyser, M. (2017). The council of Europe convention on cybercrime. In Computer Crime (pp. 131–170).

Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315095493-7/council-europe-convention-cybercrime-mike-keyser

Leukfeldt, E. R., Notté, R. J. (Raoul), & Malsch, M. (Marijke). (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. Victims & Offenders, 15(1), 60–77. https://doi.org/10.1080/15564886.2019.1672229

Mabunda, S. (2025). The South African and Senegalese Legislative Response to Malware-Facilitated Cybercrime. In D. Gritzalis, K.-K. R. Choo, & C. Patsakis (Eds.), Malware (Vol. 91, pp. 233–249). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-66245-4_10

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.

Maurushat, A., & Halpin, D. (2022). Investigation of Cryptocurrency Enabled and Dependent Crimes. In D. Goldbarsht & L. De Koker (Eds.), Financial Technology and the Law (Vol. 47, pp. 235–267). Springer International Publishing. https://doi.org/10.1007/978-3-030-88036-1_10

Metaxakis, E. (2023). Ratifying an international treaty: Is it enough? (Shortcomings of the ratification of the Budapest Convention by Greece). International Cybersecurity Law Review, 4(4), 451–470. https://doi.org/10.1365/s43439-023-00099-6

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. Journal of Risk and Financial Management, 18(1), 41.

Musotto, R., & Nussbaum, B. H. (2022). Cyber-Enabled Crime as an Enabler in Market Manipulation Schemes. In Next-Generation Enterprise Security and Governance (pp. 121–134). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003121541-5/cyber-enabled-crime-enabler-market-manipulation-schemes-roberto-musotto-brian-nussbaum

Nifakos, S., Chandramouli, K., & Stathakarou, N. (2025). Social Engineering: The Human Behavior Impact in Cyber Security Within Critical Information Infrastructures. In N. Pitropakis & S. Katsikas (Eds.), Security and Privacy in Smart Environments (Vol. 14800, pp. 173–184). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-66708-4_8

Oddis, D. I. (2017). Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime. In Computer Crime (pp. 285–326). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315095493-11/combating-child-pornography-internet-council-europe-convention-cybercrime-dina-oddis

Payne, B. K. (2020). Defining Cybercrime. In T. J. Holt & A. M. Bossler (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 3–25). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_1

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. Forensic Sciences, 2(2), 379–398.

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. International Journal of Computer Networks and Communications Security, 2016, 4 (6). https://openaccess.uoc.edu/handle/10609/78507

Saqf Al Hait, A. (2023). Cyber hacking: Building a harmonised criminal legal framework for addressing cyber hacking in the Arab convention on combating information technology offences: a comparative study between Jordanian & Saudi cyber laws [PhD Thesis, Anglia Ruskin Research Online (ARRO)]. https://aru.figshare.com/articles/thesis/Cyber_hacking_building_a_harmonised_criminal_legal_framework_for_addressing_cyber_hacking_in_the_Arab_convention_on_combating_information_technology_offences_a_comparative_study_between_Jordanian_Saudi_cyber_laws/24147432

Singh, D. (2023). Cyber Crime against Children: Is POCSO Sufficient? Issue 2 Indian JL & Legal Rsch., 5,

1.
Strikwerda, L. (2014). Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic and constitutional dimension. Information & Communications Technology Law, 23(1), 31–60. https://doi.org/10.1080/13600834.2014.891870

Tennant, I., & Paula Oliveira, A. (2024). Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN 'cybercrime' treaty. Journal of Cyber Policy, 9(2), 221–238. https://doi.org/10.1080/23738871.2024.2428655

Tubaishat, A., & AlAleeli, H. (2024). A framework to prevent cybercrime in the UAE. Procedia Computer Science, 238, 558–565.

Wicki-Birchler, D. (2020). The Budapest Convention and the General Data Protection Regulation: Acting in concert to curb cybercrime? International Cybersecurity Law Review, 1(1–2), 63–72. https://doi.org/10.1365/s43439-020-00012-5

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). Journal of Financial Crime, 27(4), 1089–1105.

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. https://doi.org/10.1177/13657127231187059.