Pak. j. life soc. Sci. (2025), 23(1): 2947-2955 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences

www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2025-23.1.00233

RESEARCH ARTICLE

Public Perceptions of Jordan's Cybercrime Law: Protecting Social Media Data and Aligning with International Standards

Khaled Mohammad Khwaileh

Khwaileh, Khaled Mohammad, Jadara University Faculty of Law, Jordan

ARTICLE INFO

Received: Aug 24, 2024

Accepted: Oct 6, 2024

Keywords

Cybercrime Law

Personal Information Protection

Public Perception and International Standards

***Corresponding Author:**

kh.khwaileh@jadara.edu.jo

ABSTRACT

This paper examines public perceptions of the Jordanian Cybercrime Law, focusing on its effectiveness in protecting personal information shared on social media and its alignment with international standards. As social media usage increases, concerns about data security and privacy have become more pronounced. This paper analyzes the Cybercrime Law's provisions related to social media, evaluating how well they protect users' data and deter violations. Via comparing the Jordanian legal framework with international norms. The findings expose that while the Jordanian Cybercrime Law has made strides in addressing data protection issues, there are significant gaps in its alignment with international standards such as the General Data Protection Regulation (GDPR). Public perception indicates a mixed level of confidence in the law's ability to safeguard personal information, with some concerns about its enforcement and effectiveness. The results suggest that improving legislative alignment with international data protection standards and enhancing public awareness could strengthen the law's effectiveness in protecting personal information in the digital age.

INTRODUCTION

In the digital era, the protection of personal information has emerged as a critical concern for individuals, governments, and organizations alike. The rapid expansion of social media platforms has brought with it an unprecedented level of connectivity, allowing users to share vast amounts of personal data online. While this has facilitated communication and social interaction, it has also exposed users to significant risks related to data privacy and security. As a result, governments worldwide have sought to enact legislation that addresses these challenges, aiming to protect citizens' personal information and prevent cybercrimes. In this context, the Jordanian Cybercrime Law potentially plays a crucial role in safeguarding personal data, particularly in the realm of social media, where the potential for data breaches and privacy violations is high.

Jordan's Cybercrime Law, first enacted in 2010 and subsequently amended, was introduced to combat the growing threat of cybercrime in the country. The law aims to provide a legal framework for addressing various forms of cybercrime, including unauthorized access to data, hacking, and online fraud. More specifically, it seeks to protect citizens' personal information from misuse or exploitation by establishing legal penalties for those who violate privacy rights in the digital sphere. Given the increasing reliance on social media platforms for communication, business, and social interaction, the law's effectiveness in safeguarding personal information shared on these platforms is of paramount importance.

However, despite the law's stated objectives, concerns have been raised about its effectiveness in providing comprehensive protection for personal information on social media. This paper argue that while the law includes provisions aimed at curbing cybercrimes, its enforcement may be inconsistent, and the legal framework may not fully address the complexities of data protection in the digital age. Additionally, there is an ongoing debate about whether the law aligns with international standards for data protection and privacy, which have evolved significantly in response to global challenges posed by cybercrime and data breaches.

International standards, such as the General Data Protection Regulation (GDPR) in the European Union, set a high bar for data protection by imposing strict requirements on how personal data is collected, stored, and processed (Namrata & Shallu, 2024). These standards emphasize the importance of user consent, data minimization, and the right to privacy, among other principles. As nations worldwide strive to enhance their cybersecurity frameworks, the question arises as to how well the Jordanian Cybercrime Law measures up to these international benchmarks. Does the law provide adequate safeguards for personal information on social media, or are there gaps that need to be addressed to ensure better alignment with global standards?

This paper seeks to explore these questions by evaluating the effectiveness of the Jordanian Cybercrime Law in protecting personal information on social media platforms. Also, examines the specific provisions of the law related to data protection, assess their implementation and enforcement, and compare them with international standards such as the GDPR. Through analyzing the strengths and weaknesses of the current legal framework, it aims to provide insights into how the law can be improved to better protect citizens' personal data in an increasingly interconnected digital environment.

Furthermore, this paper considers the broader implications of data protection laws on public perception and trust in digital platforms. As social media continues to play a central role in daily life, the ability of legal systems to effectively protect user data will be crucial in shaping how individuals engage with these platforms. A robust legal framework that aligns with international standards can enhance public confidence in the safety and security of their online activities, thereby fostering a more secure and trustworthy digital ecosystem.

This paper employs a comparative and analytical methodology, additionally, it reviews existing literature on the law's effectiveness and public perceptions, aiming to identify gaps and propose recommendations based on the comparison and analysis.

This paper is divided into four parts. Part one begins with an overview of the Jordanian Cybercrime Law No. 17 of 2023. Part two analyses the implementation of these provisions and their enforcement. Part three compares these provisions to the international standards as present in the GDPR. Part four develops recommendations for the changes in Jordan’s cybercrime law to make it more in sync with the international standards.

The following section begins with an overview of Jordan’s Cybercrime Law No. 17 of 2023, which establish the foundation for this paper by examining the legal framework of Jordan’s cybercrime laws.

1. Overview of the Jordanian Cybercrime Law No. 17 of 2023

Jordan's Cybercrime Law No. 17 of 2023 was ratified in July 2023 as a comprehensive legal framework addressing various forms of cybercrime, including character assassination, cyber extortion, and data protection (Alqudah, 2024). The law contains 41 sections, with several directly focused on safeguarding personal information on social media platforms (Turki &Elfawair, 2024). These provisions specifically address issues such as the unlawful collection, misuse, or disclosure of personal data, aiming to protect individual privacy in the digital space. However, the exact number of sections related to social media data protection may vary, as various provisions on privacy can apply broadly across online platforms, including social media.

1.1. Issues in the Earlier Versions of the Cybercrime Law

Prior to the 2023 amendments, Jordan's Cybercrime Law had several significant shortcomings, particularly in protecting personal data and social media privacy (Al-Amawi, 2023). The law lacked a clear and comprehensive definition of personal data, leading to ambiguity in applying protections (Maaytah & Kobarie, 2024). Additionally, there was limited guidance on the lawful collection, storage, and processing of personal information, which left users vulnerable to data misuse. Another major gap was the lack of regulations on obtaining user consent before data collection, putting individuals' privacy at risk (Maaytah & Kobarie, 2024). Data subject rights were also weak, as users had no legal authority to access, correct, or delete their personal data. Moreover, cross-border data transfers were not regulated, posing further risks given the global nature of social media platforms (Migdad, 2023). These gaps highlighted the need for reforms to better align the law with international data protection standards, such as the GDPR.

1.2. Improvements Made by the 2023 Amendments

The 2023 amendments to Jordan's Cybercrime Law addressed several of the earlier shortcomings. The amendments introduced a clearer and more specific definition of personal data, making it easier to apply legal protections consistently (Migdad, 2023). In terms of user consent, the amendments mandated that social media platforms must now obtain informed and explicit consent before collecting or processing any personal data, that bringing the law closer to international norms, such as the GDPR (Maaytah & Kobarie, 2024).

Furthermore, the amendments significantly strengthened the rights of data subjects, granting individuals the ability to access, correct, or delete their personal information from social media platforms, thus giving users more control over their online privacy. Another important reform was the introduction of regulations concerning cross-border data transfers, ensuring that personal data remains protected when transferred outside of Jordan (Nees, 2022). These amendments marked a considerable improvement in aligning Jordan's legal framework with global best practices in data protection.

1.3. Remaining Gaps in Data Protection on Social Media

Despite the progress made through the 2023 amendments, several gaps in social media data protection remain unresolved. The law still lacks a comprehensive definition of personal data specific to social media, leaving room for ambiguity regarding which types of data require protection. Additionally, while user consent requirements have been strengthened, the law does not fully align with international standards in providing robust protections for data subjects' rights, particularly in situations involving social media platforms' complex data processing practices.

Another major shortfall is the absence of specific provisions addressing the protection of minors on social media. Minors are particularly vulnerable to privacy violations, yet the law does not adequately account for the additional safeguards required to protect their data (Maaytah & Kobarie, 2024). These gaps demonstrate that while the 2023 amendments were an improvement, further reforms are still needed to address evolving challenges in data protection.

1.4. Enforcement Challenges and Jurisdictional Conflicts

Enforcement of the Cybercrime Law, even after the 2023 amendments, remains a significant challenge, particularly due to jurisdictional conflicts. Many social media platforms operate on a global scale, with servers and data processing facilities located outside of Jordan (Carr& Hayes, 2015). This makes it difficult for Jordanian authorities to monitor and enforce the law when personal data is stored or processed in foreign jurisdictions. Jurisdictional conflicts often arise when data breaches occur on servers in countries with different data protection laws, complicating efforts to hold foreign companies accountable (Fabbrini, Celeste & Quinn, 2021)

Moreover, Jordan lacks established mechanisms for cross-border cooperation, such as mutual legal assistance treaties, with countries where many of these platforms are headquartered. Cybercrime

has grown into a borderless and pervasive threat, affecting nations across all levels of development. The anonymity offered by the internet makes it a low-risk, high-reward (Peters & Jordan, 2019). Jordan, like many other countries, faces challenges in combating cybercrime due to a lack of established cross-border cooperation mechanisms, such as mutual legal assistance treaties (MLATs).

Without these agreements, Jordanian authorities face obstacles in investigating and prosecuting foreign entities for data protection violations affecting Jordanian citizens. These jurisdictional challenges weaken the law's ability to fully safeguard personal data on social media.

1.5. Limited Integration with International Data Protection Frameworks

While the 2023 amendments improved the alignment of Jordan's Cybercrime Law with international standards, such as the GDPR, the law remains inadequately integrated with global data protection frameworks. International frameworks rely on harmonized standards and reciprocal agreements between jurisdictions to ensure consistent enforcement of data protection laws. Jordan's legal framework lacks comprehensive agreements or harmonization with key international players, such as the European Union.

This disconnection from global efforts in data protection weakens Jordan's ability to enforce the law effectively, particularly in cases involving foreign social media companies or cross-border data transfers. The absence of a unified international framework for data protection complicates Jordan's legal landscape. Many countries have enacted their own privacy laws, leading to a fragmented approach that Jordan struggles to navigate (Rudraswamy & Vance, 2001). The European Union's stringent data protection regulations, such as the General Data Protection Regulation (GDPR), create barriers for non-compliant nations, limiting Jordan's ability to engage in trans-border data flows effectively (Kong, 2010).

Jurisdictional conflicts demonstrate that data often crosses borders without clear legal oversight, leaving Jordan vulnerable to external legal frameworks that may conflict with its own laws (Daskal, 2018). Also, extraterritorial application of laws from powerful states complicates enforcement, as multinational corporations, including social media platforms, may prioritize compliance with their home countries' regulations over Jordanian laws (Brkan, 2016). However, Jordan could leverage its strategic position to advocate for a more collaborative international approach to data protection, particularly on social media. This would strengthen its regulatory framework and enforcement mechanisms, ensuring better protection for its citizens' personal information.

The absence of an integrated legal approach to data protection limits the law's overall effectiveness in protecting personal information in a global digital environment.

1.6. Domestic Enforcement and Regulatory Challenges

The enforcement of Jordan's Cybercrime Law faces significant regulatory challenges, including a lack of coordination among legal bodies, insufficient resources, and the absence of a dedicated data protection authority. These structural weaknesses severely limit the law's ability to effectively address complex cybercrime cases, especially those involving breaches of personal data on social media platforms, where rapid response and cross-border collaboration are essential.

One of the main issues is the lack of effective collaboration between data protection authorities, cybercrime units, and the judiciary, resulting in fragmented enforcement efforts (Brenner, 2012). Existing cybercrime units often lack the necessary expertise and resources to handle sophisticated cases, especially those that involve intricate digital evidence or have international dimensions (Hunton, 2010). As social media data breaches typically span multiple jurisdictions, the absence of streamlined coordination further complicates investigations, leaving both citizens and businesses vulnerable to cyber threats.

Jordan currently does not have a dedicated data protection authority, a critical component for overseeing compliance with data protection standards and ensuring a cohesive approach to cybercrime investigations (Khan et al., 2010). In the absence of such an authority, enforcement

largely relies on cybercrime units that may not be fully equipped to manage the complexities of modern cyber threats, particularly those involving personal information on social media platforms (Grabosky, 2007). This gap in the regulatory structure weakens Jordan's overall capacity to safeguard its citizens' data.

This paper argue that Jordan could adapt its existing frameworks to improve coordination and resource allocation without the immediate need for a new authority. Through enhancing the collaboration between existing cybercrime units, legal bodies, and regulatory frameworks, the country might improve enforcement of its cyber laws (Brenner, 2012). However, this approach may still be insufficient given the rapidly evolving nature of cyber threats, especially in the context of data protection on global social media platforms. As cybercrime continues to grow in complexity and scale, Jordan will likely need to adopt more robust regulatory mechanisms to remain resilient in the face of such threats.

1.7. Technological Challenges in Enforcement

The enforcement of the Jordanian Cybercrime Law faces significant technological challenges due to the rapid evolution of digital technologies. While recent amendments have improved the legal framework, they lack provisions for equipping law enforcement with the necessary tools and expertise to address these advancements effectively.

The rise of encryption, AI, and blockchain complicates the identification and prosecution of cybercriminals, as these technologies often provide anonymity and sophisticated methods for evasion (Melnik, 2024). Inadequate Tools: Law enforcement agencies struggle with outdated technological capabilities, hindering their ability to monitor and investigate cybercrimes effectively (Cassidy et al., 2024).

The legal framework has not kept pace with technological advancements, resulting in a significant lag that impedes effective enforcement (AllahRakha, 2024). There is a pressing need for laws that can adapt to new technologies and cybercrime tactics, ensuring that enforcement remains relevant and effective (Suryanto & Mulyana, 2024).

In contrast, some argue that the existing legal frameworks can be effective if law enforcement agencies prioritize training and collaboration with tech experts. However, without addressing the technological gaps, the enforcement of cyber laws will remain limited.

In summary, while the 2023 amendments to Jordan's Cybercrime Law represent a significant step forward in addressing cybercrime and improving data protection on social media platforms, substantial challenges remain. Jurisdictional conflicts, limited integration with global frameworks, and inadequate domestic enforcement mechanisms continue to hinder the law's effectiveness. Additionally, the law struggles to keep pace with rapid technological developments, leaving gaps in the protection of personal information. Further reforms and a more integrated approach to data protection are necessary to address these issues and ensure that the law can fully safeguard personal data in a digital and globalized world.

2. Analysis of the Implementation and Enforcement of Jordan's Cybercrime Law

Jordan's Cybercrime Law No. 17 of 2023 aims to address a wide array of online offenses, but its implementation and enforcement face several challenges. Public skepticism arises from concerns over the law's clarity, particularly regarding its ability to protect personal information on social media platforms. While the law criminalizes offenses such as online impersonation, defamation, and privacy violations, there is a disconnect between the legislative intent and how the public perceives its effectiveness. The law's provisions are seen as vague, leading to doubts about its ability to tackle complex cyber threats, especially those involving personal data breaches (Siddik & Rahi, 2020).

A significant gap in the law is its limited coverage of emerging cyber threats. For instance, while the law addresses electronic defamation and slander, these provisions are insufficient to cover the complexities of offenses on social media, where personal data manipulation is common (Hunton,

2010). There is also a lack of clear mechanisms for victims to seek redress or demand data correction. Additionally, while the law includes provisions against cyber extortion and character assassination, it does not adequately account for the evolving nature of these crimes, particularly the use of advanced technologies by cybercriminals to evade detection. This leaves personal information vulnerable and points to the need for legislative updates (Grabosky, 2007).

The public's lack of awareness about the law further hampers its effectiveness. Many citizens are unfamiliar with their rights concerning data protection or the legal avenues available to them if their personal information is compromised (Khan et al., 2010). This lack of understanding weakens the deterrent effect of the law, as individuals and organizations may not fully grasp the legal risks of data misuse. To address this, increased public education and awareness campaigns are essential, helping citizens understand their rights and the protections available under the law (Brenner, 2012).

Enforcement mechanisms under the Cybercrime Law are also perceived as inadequate. While penalties for cybercrimes exist, the enforcement process is often slow and lacks transparency. Public frustration over inconsistent legal outcomes, as well as weak enforcement, diminishes trust in the law's capacity to serve as a deterrent (Hunton, 2010). The absence of clear data protection measures for organizations processing personal information further exacerbates the issue, leaving gaps in how violations are penalized and addressed (Siddik & Rahi, 2020). Improving enforcement through better-defined penalties and more rigorous legal processes would greatly enhance the law's effectiveness.

In summary, Jordan's Cybercrime Law No. 17 of 2023 represents a significant step toward combating online offenses, but several issues undermine its implementation. Public skepticism, gaps in addressing emerging cyber threats, and a lack of public awareness hinder its impact. Moreover, weak enforcement mechanisms and the absence of comprehensive data protection measures limit the law's capacity to safeguard personal information. Addressing these challenges through legislative reforms, enhanced enforcement, and public education would strengthen the law's effectiveness, helping Jordan protect its citizens in the rapidly evolving digital landscape.

3. Comparison with International Standard

A comparative analysis of the Jordanian Cybercrime Law No. 17 of 2023 and international data protection frameworks, such as the (GDPR), reveals significant differences in scope, individual rights protections, enforcement mechanisms, and cross-border data management. The GDPR stands as a comprehensive regulation designed to safeguard personal data across the European Union and beyond, offering an extensive framework that applies extraterritorially to non-EU entities processing EU citizens' data (Voigt & Von dem Bussche, 2017). In contrast, Jordan's Cybercrime Law primarily focuses on criminalizing online offenses without offering a full regulatory framework for personal data protection, leaving notable gaps in its approach to managing modern digital threats.

One of the most striking differences between the two frameworks is the range of rights granted to individuals. Under the GDPR, individuals have the right to access, rectify, and erase their personal data, as well as the right to object to data processing (Kuner, 2020). These rights empower users to maintain control over their personal information and hold data processors accountable. Jordan's Cybercrime Law, on the other hand, does not grant comparable rights to its citizens. While it criminalizes unauthorized access and disclosure of personal information, it lacks provisions allowing individuals to request data corrections or deletions, a crucial element of data protection in today's digital landscape.

Enforcement mechanisms under the GDPR are robust, with penalties for non-compliance reaching up to 4% of an organization's global annual revenue (Voigt & Von dem Bussche, 2017). This strong punitive structure ensures that organizations prioritize data protection. In contrast, Jordan's Cybercrime Law does not offer similarly stringent enforcement measures. The penalties for cybercrimes are less clearly defined and lack the same severity, reducing their deterrent effect. Furthermore, enforcement in Jordan is often seen as inconsistent, with public perception reflecting frustration over the slow and non-transparent legal processes (Al-Khasawneh, 2021). This lack of

rigorous enforcement undermines the law's effectiveness and weakens public confidence in its ability to address cyber threats.

The GDPR also excels in regulating cross-border data transfers, ensuring that personal data remains protected even when transferred outside the EU. It mandates that data transferred to third countries must meet equivalent levels of protection, using mechanisms such as Standard Contractual Clauses (SCCs) or binding corporate rules (BCRs) (Kuner, 2020). In comparison, Jordan's Cybercrime Law does not include provisions addressing cross-border data flows, leaving a significant gap in its legal framework. In an increasingly interconnected digital world, where data regularly crosses borders, this omission presents vulnerabilities, particularly when Jordanian citizens' data is handled by foreign entities (Siddik & Rahi, 2020).

Additionally, the GDPR offers explicit protections for social media users by requiring platforms to obtain informed consent before processing personal data and ensuring transparency in how user data is stored and shared (Albrecht, 2016). Jordan's Cybercrime Law, while targeting cyber offenses, does not offer similarly clear guidelines or protections for personal data shared on social media. This leaves social media users vulnerable to data breaches and other forms of cybercrime, further highlighting the need for Jordan to adopt stronger data protection measures.

In conclusion, when compared to international standards like the GDPR, Jordan's Cybercrime Law shows clear areas for improvement. While the law marks progress in addressing cybercrimes, particularly those related to social media, its focus remains limited. The law lacks the comprehensive scope, individual rights protections, cross-border data transfer provisions, and enforcement mechanisms seen in global frameworks like the GDPR. To enhance data protection and align with international norms, Jordan should adopt a more robust approach by incorporating individual rights, improving enforcement, and addressing cross-border data flows. By doing so, Jordan can strengthen its ability to protect personal data, deter cybercrime, and build public trust in its digital governance (Siddik & Rahi, 2020).

4. CONCLUSION

To align Jordan's Cybercrime Law with international standards like the GDPR, several key reforms are needed to strengthen its effectiveness in combating cyber threats and protecting personal information, particularly on social media platforms. First, the law should adopt comprehensive data protection principles similar to those found in the GDPR, including data minimization, purpose limitation, and stronger user consent regulations. This would ensure that personal data is collected and processed responsibly, with clear guidelines on its usage and storage. Incorporating data breach notification requirements would also enhance transparency, allowing individuals to be informed when their privacy is at risk.

In addition, Jordan's legal framework should empower individuals with stronger data protection rights, such as the ability to access, rectify, and erase personal data. These rights would give citizens greater control over their personal information and provide legal avenues for addressing misuse. Strengthening these individual protections would not only align Jordan with global standards but also bolster public confidence in the legal system.

Enhancing enforcement mechanisms is also crucial. The introduction of stricter penalties, along with more transparent and consistent enforcement processes, would deter cybercrimes and ensure better compliance with the law. Clear guidelines on penalties for violations, similar to the GDPR's approach, would improve accountability and legal uniformity.

Given the cross-border nature of cybercrime, Jordan should also pursue international cooperation by joining treaties that facilitate data protection and cybercrime prevention. This would enable smoother collaboration across jurisdictions, improving the investigation and prosecution of cybercrimes that transcend national borders.

To conclude, public awareness and education about the law must be prioritized. Ensuring that citizens understand their rights and how to protect their personal data would bridge the gap between

the law's intent and its practical application, fostering greater trust in Jordan's digital governance. By adopting these reforms, Jordan can create a more robust legal framework capable of addressing evolving cyber threats and ensuring stronger personal data protection in line with international standards.

BIBLIOGRAPHY

Adam, At, Thur, Jasson, Cassidy., Anis, Fuad., Muhammad, Ulil, Abshor, As, Shofy. (2024). 4. Emerging Trends and Challenges in Digital Crime: A Study of Cyber Criminal Tactics and Countermeasures. doi: 10.70063/techcompinnovations.v1i1.25

Ahmad, A., Enad, T., Nashat, B. H., Ali, A., Khaled, K., Khaled, A., … Tasnim, A. (2024). Sustainable Development Goals Against Unfair Business Competition Practices in Electronic Environment in Jordanian Legislation – Comparative Study. *Journal of Lifestyle and SDGs Review*, *4*(2), e02300. https://doi.org/10.47172/2965-730X.SDGsReview.v4.n02.pe02300

Ahmed, Ali, Al-Amawi. (2023). 4. The Crime of Character Assassination in The Jordanian Cybercrime Law. International journal of membrane science and technology, doi: 10.15379/ijmst.v10i2.2886

Al-zoubi, T. M. H., Alazzam, F. A. F., Shakhatreh, H. J. M., Khwaileh, K. M., Al-Maagbeh, M. M., & Alzubi, E. A. (2024). Arbitration in the Age of Globalization: Addressing Cultural and Legal Diversity in Commercial Disputes to Achieve Sustainable Development Goals in Society. *Journal of Lifestyle and SDGs Review*, *5*(1), e03168. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe03168

Brenner, S. W. (2012). Cybercrime: Criminal threats from cyberspace. Praeger.

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. Atlantic journal of communication, 23(1), 46-65.

Fabbrini, F., Celeste, E., & Quinn, J. (Eds.). (2021). *Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty*. Bloomsbury Publishing.

Grabosky, P. (2007). Electronic crime. Pearson Education.

Hammouri, J. A., Almahasneh, A. A. A., Khwaileh, K. M., & Al-Raggad, M. M. (2024). The Criminal Liability of Artificial Intelligence Entities. Available at SSRN 5004446.

Hunton, P. (2010). "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model." Computer Law & Security Review, 26(2), 128-136.

Jennifer, C., Daskal. (2018). 5. Borders and Bits. Vanderbilt Law Review,

Khan, S., Jan, M. A., & Haq, A. U. (2010). "Challenges to enforcing cybercrime laws." Journal of Information Technology & Software Engineering.

Linda, Nees. (2022). 5. Combating cyber-terrorism crime in the jordanian law. RIMAK International journal of humanities and social sciences, doi: 10.47832/2717-8293.20.9

Lingjie, Kong. (2010). 1. Data Protection and Transborder Data Flow in the European and Global Context. European Journal of International Law, doi: 10.1093/EJIL/CHQ025

Maja, Brkan. (2016). 3. Data protection and conflict-of-laws: a challenging relationship. European Data Protection Law Review, doi: 10.21552/EDPL/2016/3/8

Mohammad, Ali, Mohammad, Bani, Migdad. (2023). 1. Publishing Via Social Media Sites and The Civil Liability of the Publisher in The Jordanian Legislation. International journal of membrane science and technology, doi: 10.15379/ijmst.v10i1.2911

Muntaser, Alqudah., Ahmad, Al--Amawi., Tawfiq, Khashashneh., Hashem, Balas. (2024). 1. The Crime of Character Assassination in the Jordanian Cybercrime Law. International journal of religion, doi: 10.61707/gsfk2s22

Namrata, Singh., Shallu, Bishnoi, -. (2024). 1. Navigating GDPR Compliance: The Intersection of Data Governance, Accountability, and Organizational Culture. International journal of innovative research in engineering & multidisciplinary physical sciences, doi: 10.37082/ijirmps.v12.i4.230875

Odai, Turki., Abed, Alfattah, Elfawair. (2024). 2. Electronic Extortion is a Crime, According to Jordan's Electronic Crimes Law No. 17 of 2023. Deleted Journal, doi: 10.62271/pjc.16.3.979.990

Paul, Hunton. (2010). 3. Cyber Crime and Security: A New Model of Law Enforcement Investigation. Policing-an International Journal of Police Strategies & Management, doi: 10.1093/POLICE/PAQ038

Peter, Grabosky. (2007). 1. Requirements of Prosecution Services to Deal with Cyber Crime. Crime Law and Social Change, doi: 10.1007/S10611-007-9069-1

Peters, A., & Jordan, A. (2019). Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *J. Nat'l Sec. L. & Pol'y*, *10*, 487.

Sanaa, Maaytah., Hiba, Kobarie. (2024). 3. The Extent of the Impact of Cybersecurity Rules on Electronic Civil Transactions in Jordanian Law. International journal of religion, doi: 10.61707/ad442p10

Siddik, A., & Rahi, A. (2020). "Data protection and privacy laws: A comparison between Jordanian legislation and international standards." Jordanian Journal of Law and Public Policy, 7(2), 102-119.

Susan, W., Brenner. (2012). 2. Cybercrime and the Law: Challenges, Issues, and Outcomes.

Vanishree, Rudraswamy., David, A., Vance. (2001). 2. Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment. Logistics Information Management, doi: 10.1108/09576050110362717

Viktor, S., Melnik. (2024). 1. Technical and Legal Challenges in Seizure of Digital Assets: Between Innovations and Regulation. Rossijskij sledovatel', doi: 10.18572/1812-3783-2024-5-2-6